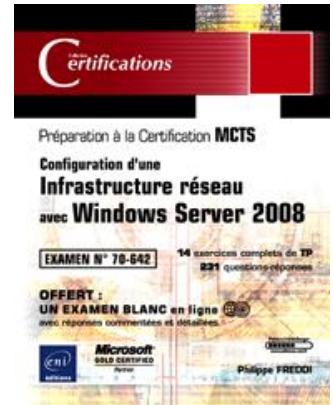


# Windows Server 2008

MCTS 70-642 - Configuration d'une infrastructure réseau

Philippe FREDDI



## Résumé

L'examen **MCTS 70-642** "Configuration d'une infrastructure réseau avec Windows Server 2008" est l'un des examens obligatoires pour l'obtention de la certification MCITP Administrateur de serveurs ou MCITP Administrateur informatique en entreprise.

Pour vous aider à préparer efficacement l'examen, **ce livre couvre tous les objectifs officiels**, tant d'un point de vue théorique que d'un point de vue pratique. Il a été rédigé en français (il ne s'agit pas d'une traduction) par un formateur professionnel reconnu, également consultant, certifié techniquement et pédagogiquement par Microsoft. Ainsi, les savoir-faire pédagogique et technique de l'auteur conduisent à une approche claire et visuelle, d'un très haut niveau technique.

Chapitre après chapitre, vous pourrez **valider vos acquis théoriques**, à l'aide d'un grand nombre de **questions-réponses** (231 au total) mettant en exergue aussi bien les éléments fondamentaux que les caractéristiques spécifiques aux concepts abordés.

Chaque chapitre donnant lieu à des **travaux pratiques** vous aurez les moyens de mesurer votre autonomie en réalisant 14 exercices complets de TP. Ces manipulations concrètes, au-delà même des objectifs fixés par l'examen, vous permettront de vous forger une première expérience significative et d'acquérir de véritables compétences techniques sur des mises en situations réelles.

A cette maîtrise du produit et des concepts, s'ajoute la préparation spécifique à la certification : vous pourrez accéder gratuitement à 1 examen blanc en ligne, destiné à vous entraîner dans des conditions proches de celles de l'épreuve. Sur ce site, chaque question posée s'inscrit dans l'esprit de la certification MCTS et, pour chacune, les réponses sont suffisamment commentées pour combler ou identifier vos ultimes lacunes. A vous de juger quand vous serez prêt pour l'examen final !

## L'auteur

**Philippe Freddi** a créé en 1988 sa société d'informatique, il en est le consultant principal et opère régulièrement auprès de grands comptes en tant qu'architecte pour les bases de données et la Business Intelligence et en tant qu'auditeur pour améliorer les processus de gestion. Il est entre autres certifié MCITP Enterprise Administrator sur Windows Server 2008. Il intervient depuis plusieurs années en entreprise et pour Microsoft en tant que formateur MCT, MCLC (bases de données, technologies systèmes, réseau, développement...) et présente régulièrement des séminaires autour des technologies Microsoft.

*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*

# Préparation à l'examen 70-642 - Configuration d'une infrastructure réseau

L'examen **MCTS 70-642** "Configuration d'une infrastructure réseau avec Windows Server 2008" est l'un des examens obligatoires pour l'obtention de la certification MCITP Administrateur de serveurs ou MCITP Administrateur informatique en entreprise.

Pour vous aider à préparer efficacement l'examen, **ce livre couvre tous les objectifs officiels** dont la liste est donnée en annexe. Il se divise en 12 chapitres comportant chacun l'organisation ci-après :

- Une définition des objectifs à atteindre : permet d'exposer précisément les compétences données par le chapitre une fois celui-ci validé.
- Une partie **cours théoriques** : permet de définir les termes et concepts abordés et de schématiser sous forme d'un fil conducteur les différents points à assimiler.
- Une partie **application du cours** : permet de suivre le déroulement précis d'une manipulation (copies d'écran et schémas).
- Une partie **validation des acquis** proposée sous forme de questions/réponses (231 au total). Ces questions mettent en exergue aussi bien les éléments fondamentaux que les caractéristiques spécifiques aux concepts abordés. La partie réponses reprend les questions posées avec des réponses rédigées pour chacune d'elles.
- Les **travaux pratiques**, regroupés en fin d'ouvrage (14 au total) : ils permettent d'illustrer précisément certaines parties du cours et vous donnent aussi les moyens de mesurer votre autonomie. Ces manipulations concrètes, au-delà même des objectifs fixés par l'examen, vous permettront de vous forger une première expérience significative et d'acquérir de véritables compétences techniques sur des mises en situations réelles.

Pour la préparation spécifique à l'examen 70-642, vous pouvez accéder **gratuitement à 1 examen blanc en ligne à l'adresse <http://www.edieni.com/francais/certifications>**, afin de vous entraîner dans conditions proches de celles de l'épreuve. Sur ce site, chaque question posée s'inscrit dans l'esprit de la certification MCTS et, pour chacune, les réponses sont suffisamment commentées pour contrôler et identifier vos ultimes lacunes.

## **Objectifs du chapitre**

Passer un examen et le réussir n'est pas une chose facile. Généralement il couronne les efforts et les sacrifices effectués pendant une longue période pour apprendre, comprendre et maîtriser un sujet.

Le chapitre commence par vous expliquer l'organisation du livre puis vous donne des conseils pour vous préparer au mieux avant l'examen ainsi que pour le jour et durant le long moment de solitude.

Ensuite, les nouveautés, l'évolution de la philosophie et les points importants du produit, les versions et les éditions disponibles ainsi que leurs principales caractéristiques sont décrites.

Enfin la vision de Microsoft de la virtualisation est présentée succinctement afin de se familiariser avec ces technologies et le vocabulaire.

# Comment ce livre est organisé

L'un des objectifs lors de l'écriture de ce livre est qu'il vous serve de référence autant à la préparation à l'examen **70-642 - Configuration d'une infrastructure réseau avec Windows Server 2008** en dépassant les objectifs décrits, que de livre de référence pour connaître ou approfondir un des sujets traités.

En effet, durant la phase d'apprentissage on apprend beaucoup de technologies, on cite des outils sans vraiment les utiliser, on effectue des tests que l'on oublie car pour notre travail on est cantonné à utiliser toujours les mêmes outils et la même procédure.

Dans ce livre, nous allons briser cette monotonie en vous présentant également des outils de type ligne de commandes qui sont parfois requis pour l'examen car ils sont souvent plus puissants que leurs équivalents graphiques. Bien qu'étant hors sujet, j'ai voulu vous sensibiliser aux avantages qu'offrent les scripts en automatisant au maximum les tâches répétitives pour obtenir un gain de temps et en permettant également de diminuer les erreurs de saisie, etc. Automatiser signifie créer des scripts ou des batch, gardez à l'esprit que le batch le plus simple se compose d'une action, soit une commande sans paramètre.

Le livre a été découpé en chapitres dont la logique permet de ne pas le lire uniquement chapitre par chapitre mais également de sélectionner le ou les chapitres ou les sujets qui vous intéressent. Pour chaque sujet, vous trouverez des éléments théoriques, des procédures pas à pas vous expliquant comment effectuer des tâches pouvant aller de la configuration au dépannage en passant par la gestion. Des informations supplémentaires sur comment utiliser la technologie présentée en entreprise, son intérêt, ses avantages et ses inconvénients sont également présentes. Le dernier chapitre est un grand travail pratique récapitulatif vous permettant de voir comment les technologies présentées peuvent être enchaînées les unes aux autres.

Dans chaque chapitre vous trouverez la correspondance avec les objectifs de l'examen, et en fin de chapitre des questions théoriques vous permettant de valider vos acquis. Pour effectuer les procédures présentées le nom de l'ordinateur (virtuel) à utiliser est indiqué. Enfin, les exercices correspondants se trouvant dans le chapitre **Travaux pratiques** sont indiqués.

Le premier chapitre consacré à l'**introduction** présente succinctement les objectifs de l'examen et comment bien se préparer à l'examen. Puis Windows Server 2008, ses éditions et ses caractéristiques et la virtualisation sont introduits.

Le second chapitre, consacré à la **création du bac à sable**, vous présente comment préparer les environnements nécessaires pour effectuer tous les exercices ainsi que les travaux pratiques à l'aide de procédures pas à pas. Vous y verrez notamment l'installation manuelle et automatique de Windows Server 2008 que ce soit pour une installation complète ou une installation minimale (**Server Core**).

Le chapitre consacré aux **rôles et fonctionnalités** décrit chaque rôle et chaque fonctionnalité en fonction des différentes éditions et installations puis les procédures pas à pas sont décrites pour les installer et les supprimer.

Le chapitre consacré aux **outils de configuration et de gestion** présente les principaux outils graphiques ou en ligne de commandes utilisés dans Windows Server 2008 comme le gestionnaire de serveur, la console MMC, l'administration à distance, les commandes ServerManagerCmd, ocsetup, pkgmgr, PowerShell et Windows RemoteShell.

Le chapitre consacré à la **configuration des services réseaux de base** commence par une partie théorique consacrée aux nouveautés de la version 2008, une présentation de l'adressage IPv4 et une introduction à l'adresse IPv6 suivie par la configuration de la carte réseau. Ensuite ce sont des présentations consacrées au routage pour terminer par une présentation du dépannage.

Le chapitre consacré à la **configuration de la résolution de noms** commence par présenter la théorie relative au service DNS avant de montrer les procédures pas à pas pour sa mise en œuvre. La deuxième partie présente les différentes méthodes utilisées par Windows pour résoudre un nom en adresse IP.

Le chapitre consacré aux **configurations autour du protocole DHCP** commence par présenter la théorie relative au serveur DHCP avant de décliner les procédures pas à pas pour sa mise en œuvre.

Le chapitre consacré à la **mise en œuvre du serveur de fichiers** reprend les notions de partitions et de volumes FAT à NTFS pour présenter ensuite les permissions NTFS et de partage puis quelques fonctionnalités pour terminer par la sauvegarde. La fin du chapitre est consacrée au rôle Services de fichiers et surtout à l'utilitaire Gestionnaire de ressources du serveur de fichiers.

Le chapitre consacré à la **mise en œuvre du serveur d'impression** présente l'impression sous Windows, le rôle de serveur d'impression, l'impression IP et l'impression LPD.

Le chapitre **Configuration des services réseaux avancés** présente le pare-feu intégré y compris le protocole IPSEC, le NAT et le NAP.

Le chapitre **Gestion et surveillance d'une infrastructure réseau** présente ce que l'on entend par optimisation puis présente les outils de performance et WSRM et les outils importants mais inclassables dans un des précédents chapitres comme l'assistance à distance, le gestionnaire des tâches, l'observateur d'événements ainsi que le moniteur réseau et le protocole SNMP. Enfin le service WSUS est également présenté.

Enfin le chapitre **Travaux pratiques** est un exercice récapitulatif proche de ce que vous pourrez rencontrer dans la réalité. Il vous faudra implémenter les technologies apprises en commençant par définir le système d'adressage IP jusqu'à l'implémentation de NAP.

## Cet examen compte pour les certifications suivantes

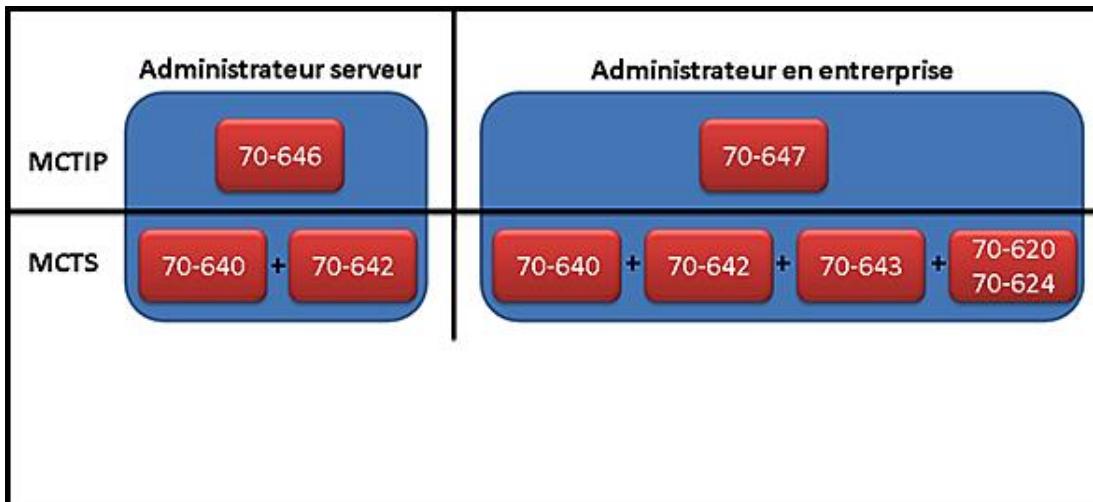
L'examen 70-642 compte pour les certifications MCTS et MCTIP.

Pour devenir **MCTS : Configuration d'une infrastructure réseau avec Windows Server 2008** il vous suffit de passer l'examen 70-642.

Concernant le **MCTIP**, l'examen 70-642 vous donne des crédits pour les deux certifications suivantes :

- **MCTIP : Administrateur serveur**
- **MCTIP : Administrateur en entreprise**

La figure suivante montre les examens à passer pour devenir MCTIP :



Bien entendu, si vous êtes MCTIP Administrateur serveur, il vous faut passer uniquement les examens manquants à savoir 70-643 et 70-647 et soit le 70-620 ou le 70-624.

Si vous êtes certifié MCSA sur Windows Server 2003, vous pouvez ne passer qu'un examen, soit le 70-648 pour devenir MCTS Windows Server 2008. En fait vous deviendrez deux fois MCTS car cet examen regroupe les exigences des examens 70-640 et 70-642.

Si vous êtes certifié MCSE sur Windows Server 2003, vous pouvez ne passer qu'un examen soit le 70-649 pour devenir MCTS Windows Server 2008. En fait vous deviendrez trois fois MCTS car cet examen regroupe les exigences des examens 70-640, 70-642 et 70-643.

Dans ces deux derniers scénarios, pour devenir MCTIP, il vous faut encore passer l'examen 70-646 pour devenir MCTIP Administrateur serveur et les examens 70-647 plus soit l'examen 70-620 soit l'examen 70-624 pour devenir MCTIP Administrateur en entreprise.

Résumé des examens :

Numéro	Titre de l'examen
70-640	Configuration d'une infrastructure Active Directory® avec Windows Server 2008
70-642	Configuration d'une infrastructure réseau avec Windows Server 2008
70-643	Configuration d'une infrastructure d'applications pour Windows Server 2008
70-646	Administrateur Windows Server 2008
70-647	Administrateur d'entreprise sur Windows Server 2008
70-620	Configuration de Microsoft Windows Vista
70-624	Déploiement et maintenance de clients Windows Vista et de postes de travail Microsoft Office system 2007

70-648	Mise à niveau de MCSA Windows Server 2003 à MCTS Windows Server 2008
70-649	Mise à niveau de MCSE Windows Server 2003 à MCTS Windows Server 2008

## Compétences testées à l'examen 70-642

Le tableau suivant montre la correspondance entre les chapitres et les compétences testées à l'examen :

Compétences	Chapitre
Configurer l'adressage IPv4 et IPv6	5
Configurer DHCP ( <i>Dynamic Host Configuration Protocol</i> )	7
Configurer le routage	5
Configurer IPSec	10
Configurer un serveur DNS ( <i>Domain Name System</i> )	6
Configurer les zones DNS	6
Configurer les enregistrements DNS	6 et 7
Configurer la réPLICATION DNS	6
Configurer la résolution de noms pour des ordinateurs clients	5 et 6
Configurer l'accès à distance	10
Configurer la protection d'accès réseau (NAP)	10
Configurer l'authentification réseau	10
Configurer l'accès sans fil	10
Configurer les paramètres du pare-feu	10
Configurer un serveur de fichier	8
Configurer DFS ( <i>Distributed File System</i> )	8
Configurer le service des clichés instantanés	8
Configurer la sauvegarde et la restauration	8
Administrer les quotas sur les disques	8
Configurer et surveiller les services d'impression	9
Configurer des paramètres serveur WSUS ( <i>Windows Server Update Services</i> )	11
Collecter les données de performance	11
Surveiller les journaux des événements	11
Collecter des données réseau	11

# Comment se préparer

Passer un examen n'est pas une action anodine. L'anxiété, le stress dû à la préparation, votre appréhension face à un examen peuvent vous faire perdre tous vos moyens c'est la raison pour laquelle il est indispensable de prendre confiance en vous en vous entraînant un maximum avec des exercices théoriques et pratiques et en vous répétant intérieurement la théorie correspondante.

Pour commencer, il faut savoir que les compétences testées peuvent être modifiées à la discréction de Microsoft et que le format des questions peut évoluer dans le temps. La lecture du guide de préparation est un élément important mais prenons les différentes phases dans l'ordre.

## 1. Phase d'apprentissage

Durant cette phase, vous devez vous concentrer uniquement sur l'acquisition de la théorie en lisant le livre et en suivant les procédures présentées dans chaque chapitre ainsi qu'en effectuant des travaux pratiques.

Il vous faut comprendre ce que vous faites afin de le reproduire dans une situation réelle. L'utilisation d'Internet et particulièrement les sites consacrés aux livres blancs (*whitepaper*), le TechNet, le MSDN et les blogs des équipes de développement permettent de compléter votre apprentissage.

N'hésitez pas à créer vos propres scénarios et à les tester.

## 2. Phase d'entraînement

Vous disposez de la connaissance, il est temps maintenant d'évaluer vos compétences. Pour cela, entraînez-vous avec les questions du livre et les questions supplémentaires qui sont sur le site des Éditions ENI.

En tant que formateur, j'ai constaté que certaines personnes échouaient à l'examen car elles ne savaient pas LIRE la question. Étrange ! Pas tant que cela, en effet ces personnes recherchent la complexité en inventant des éventualités qui n'existent pas.

Les questions sont précises et décrivent en quelques lignes un cas de figure. Toute information qui n'est pas explicitement citée n'est pas utile et correspond à un paramétrage par défaut ! À partir de ces éléments, vous devez être capable de répondre. Il n'existe pas d'éléments cachés.

Lorsque vous lisez une question vous devez vous représenter mentalement l'environnement et le cas, sinon c'est qu'il vous manque soit de la théorie, et il vous faut la retravailler, soit un peu de pratique, donc n'hésitez pas à reproduire le scénario de la question. Avec un peu d'entraînement vous serez capable non seulement de vous représenter le scénario de la question mais également d'indiquer la réponse ou la meilleure réponse possible proposée.

Lorsque vous vous entraînerez avec les questions du site Web des Éditions ENI, soyez détendu et chronométrez le temps que vous mettez pour chaque question afin d'évaluer votre rapidité.

## 3. Informations sur les types de questions

Cette section est basée sur le guide de préparation pour passer un examen MCP de Microsoft. Concernant les types de questions que vous pouvez rencontrer :

- **Questions avec une ou plusieurs réponses** : il vous faut répondre en cliquant sur la(les) bonne(s) réponse(s). Dans certains cas, il est possible d'obtenir des points même si la réponse est partiellement correcte. D'autre part, il se peut qu'il existe plusieurs réponses correctes alors qu'une seule réponse est attendue, indiquez simplement votre réponse.
- **Questions de type sélection d'une zone** : il vous faut ici cliquer sur la zone correcte avec la souris.
- **Questions de type affichage actif** : vous devez ici sélectionner le bon texte et le placer dans le bon élément. Tous les éléments ne peuvent être sélectionnés.
- **Questions de type drag and drop** : vous devez sélectionner un objet source et le déplacer vers l'emplacement correct. Il se peut que certains objets sources soient inutiles et que certains objets sources puissent être réutilisés plusieurs fois en fonction de la question.

- **Questions de type construire et mettre dans le bon ordre une liste** : il vous faut ici sélectionner des objets sources et les placer dans le bon ordre dans la zone de destination.
- **Questions de type création d'une arborescence** : semblable à la liste ordonnée, il vous faut ici construire une arborescence d'au maximum cinq niveaux. Bien entendu vous pouvez avoir plusieurs enfants pour un nœud.
- **Format d'examen type étude de cas** : le type d'examen le plus complexe car un scénario vous est présenté et des questions s'y rapportant vous sont posées. Le temps est limité et généralement vous avez plusieurs études de cas dans un examen. Une fois que vous passez à l'étude suivante vous ne pourrez plus revenir sur l'étude précédente et le temps éventuellement restant n'est pas reporté sur l'étude suivante. L'objectif est d'examiner votre esprit d'analyse et de synthèse.

Il faut également savoir que :

- Aucun point ne vous est enlevé pour des réponses incorrectes.
- Certaines questions peuvent ne pas être prises en compte à la discréction de Microsoft.
- Pour réussir un examen vous devez faire un score d'au moins 700 points.
- Vous pouvez revenir sur les questions auxquelles vous avez déjà répondu.

## 4. L'inscription

L'inscription est relativement aisée, et peut se faire en ligne. Actuellement seul Prometrics est habilité par Microsoft à faire passer des examens. Bien entendu Prometrics travaille avec des centres de certification près de chez vous. Les dates d'examens sont flexibles et changent d'un centre à l'autre en fonction de leurs horaires d'ouverture. Il vous suffit de sélectionner une date et une heure qui vous convient et bien entendu de payer les frais d'examen pour être inscrit à l'aide d'une carte de crédit. Si vous n'en possédez pas, contactez directement le centre d'examen. En cas d'échec, il vous faudra repayer les frais d'examen sauf si une action seconde chance est en vigueur. Concernant la langue de l'examen, choisissez une langue dans laquelle vous êtes à l'aise. Le passage du français à l'anglais peut parfois être déroutant car certains idiomes ne sont pas les mêmes dans les deux langues.

## 5. Le jour de l'examen

Le jour de l'examen, soyez zen ! Le soir précédent, ne restez pas éveillé trop longtemps et reposez-vous afin d'être le plus détendu possible, et préparez les documents qui vous seront demandés. Le matin, en partant de chez vous, contrôlez que vous n'avez pas oublié les documents requis à présenter au centre d'examen. Soyez à l'heure, soit au moins 15 minutes avant le début de l'examen pour remplir les formulaires administratifs. Si besoin est, interrogez la personne de l'accueil sur les questions que vous vous posez encore.

La durée de l'examen comprend des sections explicatives avant l'examen proprement dit ainsi qu'après pour éventuellement commenter l'examen.

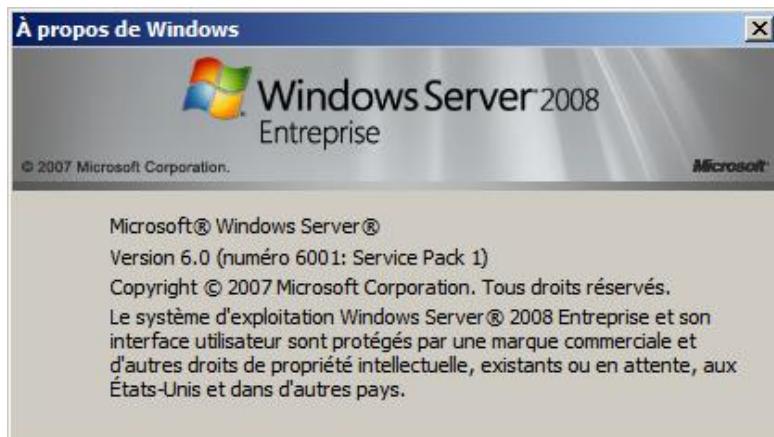
Lisez attentivement la question posée et répondez-y ou passez à la suivante. Répondez en priorité aux questions qui vous semblent faciles voire courtes puis revenez pour les questions longues ou qui vous semblent difficiles.

## 6. Gestion du temps

Gérer votre temps au mieux, pour cela lorsque la première question apparaît divisez le temps restant par le nombre de questions, de cette manière vous connaissez le temps maximum que vous pouvez passer par question. Généralement votre examen n'a qu'une seule section mais si vous vous apercevez que la durée est très inférieure à la durée annoncée, c'est qu'il y a probablement plusieurs sections. Cela signifie que vous ne pourrez pas revenir dans cette section lorsque vous serez passé à la suivante. Si vous bloquez sur une question, passez rapidement à la suivante en ayant pris soin de la noter pour y revenir par la suite. Cinq minutes avant la fin, il faudrait que vous reveniez sur les questions en suspens pour au moins y mettre une réponse. Il n'y a pas de points négatifs pour une réponse incorrecte.

# Généralités sur Windows Server 2008

Avant toute chose, voici la fenêtre **À propos de Windows** de la version sortie en février 2008. Vous remarquez que la version porte le numéro 6001, et que le Service Pack 1 est déjà présent !



Il faut savoir que Microsoft a fusionné le code du noyau de Windows Vista et de Windows Server 2008, d'où le Service Pack 1.

Microsoft a adapté Windows pour que la version 2008 réponde aux besoins et aux attentes des entreprises et des informaticiens, qu'ils soient programmeurs ou administrateurs.

Leur réflexion a montré qu'un service informatique a amélioré la productivité des utilisateurs d'où une augmentation des budgets informatiques mais également des pressions, comme des contraintes liées à la sécurité, à la mise en conformité des règles légales ou non, du changement de technologie, de la compétitivité de l'entreprise, de la réduction des coûts.

Environ 70 % du budget informatique est lié aux coûts administratifs du personnel, de la maintenance de l'infrastructure et à la résolution des problèmes. Seuls 30 % du budget permettent d'améliorer l'infrastructure de manière proactive, automatisée et efficiente.

Fort de ce constat, Windows a été adapté et l'architecture s'appuie sur les piliers suivants :

- **Une solide fondation**
- **La sécurité**
- **La virtualisation**
- **Le Web**

## 1. Une solide fondation

Par solide fondation, il faut comprendre un système d'exploitation flexible et robuste.

La flexibilité fait référence à la notion de rôles et de fonctionnalités introduites dans cette version mais également aux nouvelles possibilités de gestion comme avec **PowerShell**, **Windows Remote Shell** se basant sur des services Web ou les services de déploiement **WDS** par exemple. Par robuste, il faut entendre également fiable, ce qui est réalisé entre autres avec le *cluster failover*, la notion de **Server Core** ou la nouvelle architecture de la pile réseau.

## 2. La sécurité

Bien que Windows Server 2008 soit déjà le système d'exploitation le plus sécurisé créé par Microsoft, plusieurs de ses fonctionnalités lui permettent d'étendre la sécurité au niveau de l'environnement comme avec l'utilisation de contrôleurs de domaine en mode lecture seule, **RODC**, ou de garantir que l'accès au réseau ne se fait que grâce à des ordinateurs sains avec **NAP**, ou de fédérer des identités de manière sécurisée entre les entreprises avec **ADFS**.

## 3. La virtualisation

La virtualisation regroupe aussi bien l'utilisation de machines virtuelles que des outils de type Terminal Server. Aujourd'hui, la virtualisation se répand facilement car le modèle de licences de Microsoft facilite son utilisation. Les entreprises demandent également de pouvoir réduire le nombre des serveurs, de disposer d'un modèle d'administration plus simple. Les technologies de virtualisation répondent parfaitement à ces attentes.

## 4. Le Web

Le terme Web est intimement lié au serveur Web (**IIS** *Internet Information Server*). Ce dernier a été entièrement réécrit de manière à s'intégrer avec le système d'exploitation. Modulaire, il permet de réduire la surface d'attaque au minimum tout en fournissant le niveau de services souhaité. IIS sert également de fondation pour les services **SharePoint** V3 largement utilisés par les applications **Office** de Microsoft, de fondation pour le **WCF** (*Windows Communication Foundation*) du **Framework** 3.0 ainsi que pour le service de streaming.

## 5. L'option d'installation Server Core de Windows Server 2008

Avec Windows Server 2008, on voit apparaître un Server Core, soit une installation minimale qui ne contient qu'un nombre limité des fonctionnalités de l'installation complète. Leur noyau est identique mais les packages additionnels sont différents, ce qui interdit le passage d'un Server Core vers une installation complète par une simple mise à jour.

Par Core, il faut entendre les services d'entreprise minimum comme l'**AD**, le **DHCP**, etc. et non une version minimalistre sur laquelle on peut rajouter ses propres applications.

Le Server Core ne dispose pas ou ne peut installer entre autres :

- d'un bureau graphique, il dispose seulement d'une invite de commandes,
- du Framework.NET,
- du PowerShell,
- d'Internet Explorer,
- du panneau de contrôle.

---

► Il est quand même possible d'utiliser le bloc-notes (**notepad**) ou la base de registre (**regedit**), voire d'autres applications sous conditions.

---

Cela signifie que l'administration doit se faire soit à l'aide des commandes, soit à distance.

---

► Certains outils de type ligne de commandes ne sont pas disponibles sur le Server Core, d'autres portent des noms différents par rapport à l'installation complète ce qui ne simplifie pas l'administration !

---

Le Server Core est vraiment limité, ce qui a comme avantage de diminuer l'empreinte en mémoire vive (512 Mo sont suffisants), de limiter la place nécessaire sur le disque dur (1 Go à la place de 8 Go), de diminuer les coûts de maintenance comme l'application de patchs et également de diminuer la surface d'attaque.

---

► Pas de Framework.NET en installation minimale implique l'impossibilité d'utiliser des applications basées sur .NET telles que PowerShell, Servermanagercmd, ASP.NET...

---

► Le nombre de services installés sur un **Server Core** est d'environ 40 et seulement environ 30 sont exécutés, à comparer respectivement aux 75 et 50 services d'une installation complète.

---

## Présentation des éditions de Windows Server 2008

Le nombre des éditions de Windows Server 2008 est élevé et il n'est pas facile de s'y retrouver. Le tableau suivant résume les différentes éditions et versions qu'il est possible d'obtenir.

	<b>Standard</b>	<b>Enterprise</b>	<b>Datacenter</b>	<b>Itanium</b>	<b>Web</b>	<b>Foundation</b>	<b>HPC</b>
Version 32 bits disponible	x	x	x		x		
Version 64 bits disponible	x	x	x	x	x	x	x
Edition complète	x	x	x	x	x	x	x
Server Core	x	x	x		x		
Edition sans Hyper-V	x	x	x				

À ces éditions, il faut encore ajouter les éditions suivantes :

**HPC Server 2008** (*High Performance Computing*) est une édition orientée super calculateur permettant de réunir des nœuds afin qu'ils mettent à disposition du système leur puissance de calcul, elle fonctionne en 64 bits seulement. Il faut au minimum deux nœuds soit un nœud appelé **head node** et un nœud appelé **compute node**.

**Server foundation** est une édition vendue uniquement en tant que système d'exploitation préinstallé. Ses rôles sont limités. Il peut également être contrôleur de domaine mais le nombre d'utilisateurs est limité à quinze. Son utilisation est principalement prévue pour des petites entreprises devant partager des documents et n'ayant pas besoin de système de messagerie interne. Il est possible d'effectuer une mise à niveau vers Windows Server 2008.

**Windows Small Business Server 2008** est une version adaptée aux petites entreprises supportant jusqu'à 75 utilisateurs ou périphériques. Disponible en deux éditions, Standard ou Premium.

**Windows Essential Business Server 2008** est une version adaptée aux entreprises supportant jusqu'à 300 utilisateurs ou périphériques. Disponible en deux éditions, Standard ou Premium.

Le tableau suivant résume les logiciels inclus pour une édition Business :

	<b>Small Business Server</b>		<b>Essentiel Business Server</b>	
	<b>Standard</b>	<b>Premium</b>	<b>Standard</b>	<b>Premium</b>
Windows Server 2008 Standard	1	2	3	4
Exchange Server 2007 Standard	x	x	2	2
Windows Sharepoint Services 3.0	x	x	x	x
Microsoft ForeFront Security for Exchange Server Small Business Edition	x	x	x	x
Windows Live OneCare for Server	x	x		
Windows Server Update Services 3.0 SP1	x	x		
Integration with Microsoft Office Live Services Small Business	x	x		
System Center Essentiel 2007			x	x
Edge Security			x	x

SQL Server 2008 Standard		x		x
--------------------------	--	---	--	---

Le tableau suivant résume les limites et le matériel supporté en fonction des éditions principales.

 Remarquez que les versions 64 bits permettent de gérer plus de mémoire que les éditions 32 bits.

	<b>Standard</b>	<b>Enterprise</b>	<b>Datacenter</b>	<b>Itanium</b>	<b>Web</b>	<b>Foundation</b>	<b>HPC</b>
Nombre de processeurs X86	4	8	32		4		
Nombre de processeurs X64	4	8	64		4	1	4
Nombre de processeurs IA64				64			
RAM maximum OS 32 bits	4 Go	64 Go	64 Go		4 Go		
RAM Maximum OS 64 bits	32 Go	2 To	2 To	2 To	32 Go	8 Go	128 Go
Ajout de la mémoire à chaud		x	x	x			
Remplacement de la mémoire à chaud			x	x			
Ajout/remplacement du processeur à chaud			x	x			

Le tableau suivant montre les différences entre les éditions en terme de fonctionnalités :

	<b>Standard</b>	<b>Enterprise</b>	<b>Datacenter</b>	<b>Itanium</b>	<b>Web</b>	<b>Foundation</b>	<b>HPC</b>
Cluster failover (nombre de nœuds)		16	16	8			oui pour le head node
Synchronisation de la mémoire à tolérance de panne		x	x	x			
RéPLICATION Cross-File (DFS-R)		x	x	x			
Connexions d'accès distants (RRAS)	250	Illimité	Illimité	2		50	250
Connexions d'accès réseau (NPS)	50	Illimité	Illimité			10	

Passerelle Terminal Service	250	Illimité	Illimité	2		50	
Utilisation en tant qu'image virtuelle	1	4	Illimité	Illimité		non	1

Le tableau suivant montre quelle édition supporte quel(s) rôle(s) :

Rôle	Standard	Enterprise	Datacenter	Itanium	Web	Foundation	HPC
Services Web avec clients Internet sans installation avec l'option Core	x	x	x	x	x	x	x
Services Web avec clients AD	x	x	x	x	x	x	x
Serveur applicatif	x	x	x	x		x	
Services AD CS, Services de fichiers, Services NAP et Terminal Services en accès limité	x					x	x
Services AD CS, Services de fichiers, Services NAP et Terminal Services en accès complet		x	x				
Services AD FS		x	x				
Services UDDI	x	x	x			x	
Services d'impression	x	x	x			x	
Serveur de fax	x	x	x			x	
Services de gestion des clients AD RMS	x	x	x			x	
Autres rôles	x	x	x			x	

Le tableau suivant montre quelle édition supporte quel(s) rôle(s) avec l'option d'installation **Core** :

Rôle	Standard	Enterprise	Datacenter	Itanium	Web
Services Web sans ASP.NET	x	x	x		x
Services d'impression	x	x	x		
Services de domaine AD	x	x	x		

Services de domaine AD LDS	x	x	x		
Serveur DHCP	x	x	x		
Serveur DNS	x	x	x		
Services de fichiers limités	x				
Services de fichiers		x	x		
Hyper-V	x	x	x		

Le tableau suivant montre le matériel minimum requis et conseillé pour installer Windows Server 2008 :

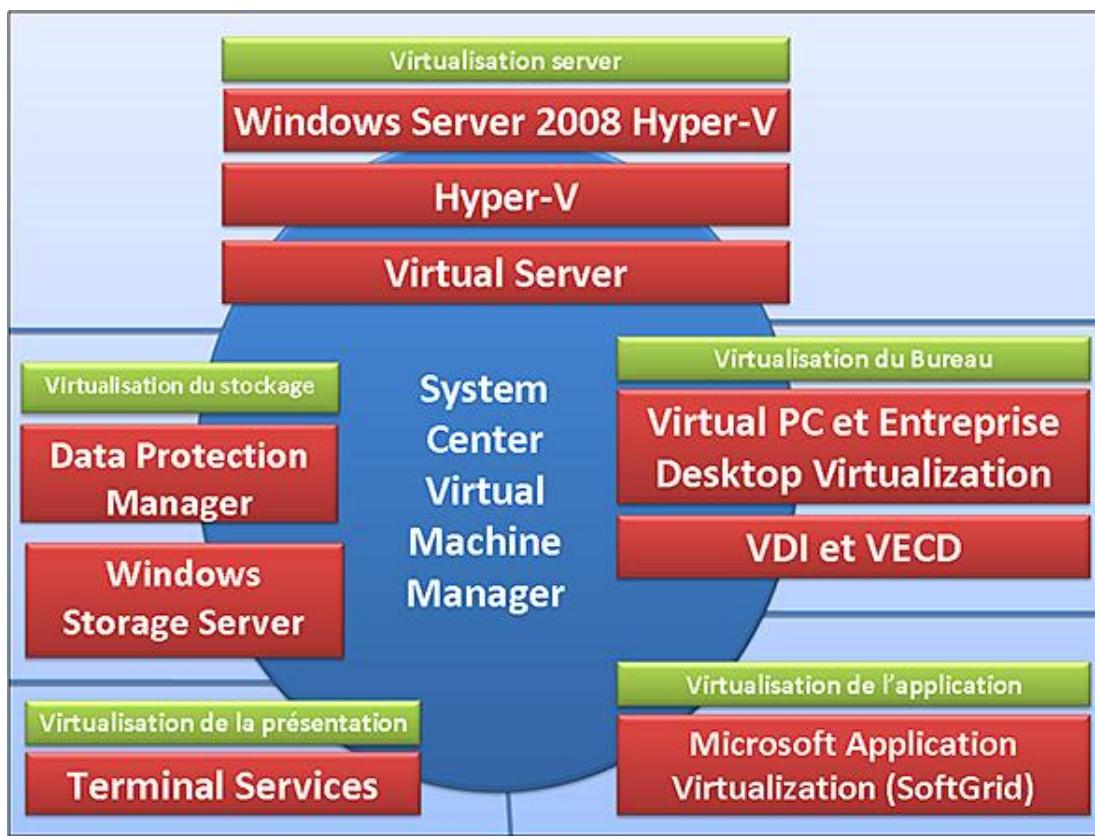
Processeur	X86	X64	Itanium	Foundation	HPC		
Nombre minimal de processeurs	1	1	2	1	1 x 64 bits		
Puissance minimale	1 GHz	1,4 Ghz		1,4 Ghz	1,4 Ghz		
Puissance conseillée	2 GHZ	2 GHz		2 Ghz	2 Ghz		
Mémoire minimale	512 MB	512 MB		512 MB	512 MB		
Mémoire conseillée	2 Go	2 Go		2 Go	2 Go		
Espace disque minimal	20 Go	20 Go	10 Go	10 Go	50 Go		
Espace disque conseillé	50 Go	50 Go	50 Go	50 Go			
Lecteur de DVD-ROM	Oui						
Carte graphique VGA (800x600)	Oui						
Clavier, souris	Oui						
Adaptateur réseau	Oui						

Windows Server 2008 est disponible en 19 langues mais seulement quelques-unes d'entre elles pour l'édition Itanium.

# Présentation de la virtualisation

La virtualisation est le **MOT** à la mode. Il faut connaître sa signification qui couvre en fait plusieurs technologies.

La figure suivante montre la vision Microsoft concernant la virtualisation.



## 1. Virtual PC

Virtual PC est l'outil idéal pour utiliser la virtualisation sur une station de travail. Il s'agit d'une application téléchargeable gratuitement qui permet de créer et d'utiliser d'autres ordinateurs (virtuels) sur votre bureau. Le prochain chapitre vous explique comment mettre en œuvre cette technologie.

## 2. Microsoft Enterprise Desktop Virtualization (MED-V)

MED-V ajoute quatre composants supplémentaires fonctionnant au-dessus de Virtual PC, à savoir :

- point centralisé de stockage et de distribution des images virtuelles ;
- surveillance et gestion centralisée ;
- contrôle de l'utilisation et du transfert des données à l'aide de stratégies ;
- intégration avec l'interface utilisateur pour utiliser ses connaissances.

MED-V n'est disponible qu'avec la Software Assurance sous la dénomination Microsoft Desktop Optimization pack.

## 3. Infrastructure de postes de travail virtualisés (VDI) et Windows Vista Enterprise Centralized Desktop (VECD)

Sous ces termes se cache un mode architectural pour VDI dans lequel les ordinateurs clients sont virtualisés et s'exécutent sur un serveur. Cela permet de disposer au niveau de l'ordinateur client d'un ordinateur léger. Le fonctionnement est semblable à Terminal Server et la différence se situe dans le fait que c'est le poste de travail qui est centralisé et pas uniquement la session.

Les composants requis pour mettre en place l'architecture VDI sont :

- Windows Server 2008 Hyper-V.
- System Center Virtual Manager 2008.
- Windows Vista Enterprise Centralized Desktop (VECD).

L'architecture VDI peut être complémentaire avec d'autres technologies comme Microsoft Application Virtualization (App-V), Windows Server 2008 Terminal Services RemoteApp.

Windows Vista Enterprise Centralized Desktop (VECD) correspond à la licence pour utiliser une architecture VDI.

## 4. Virtual Server

Virtual Server est un outil qui s'installe en tant que service. Il s'agit d'une application téléchargeable gratuitement. Son fonctionnement est similaire à celui de Virtual PC. Le format de l'image virtuelle VHD est identique, ce qui signifie que la même image peut fonctionner mais n'est pas optimisée sur l'une ou l'autre des plates-formes sans modification, voire en changeant quelques paramètres.

Virtual Server est l'outil idéal de virtualisation sur des versions de Windows antérieures à 2008.

Leurs différences principales sont les suivantes :

- Virtual PC fonctionne en tant qu'application autonome et Virtual Server en tant que service.
- Virtual PC gère également une carte son.
- Virtual Server gère également des disques virtuels au format SCSI.
- La gestion de Virtual Server se fait à l'aide d'une console Web alors que Virtual PC utilise une application.
- Virtual Server est conçu pour fonctionner sur un serveur et faire tourner en production des versions Server de Windows ou de Linux. Virtual PC est adapté pour une station de travail et pour effectuer des tests.

## 5. Hyper-V

Hyper-V est un moteur de virtualisation fonctionnant de manière autonome ou intégré au système d'exploitation Windows Server 2008. Il est basé sur la technologie **XEN** de l'université de Cambridge et ne fonctionne que sur une plate-forme matérielle 64 bits. Sorti 180 jours après le lancement officiel de Windows Server 2008, il est l'outil de virtualisation incontournable dans un environnement Windows Server 2008 par rapport à Virtual Server.

Le moteur Hyper-V requiert moins de ressources que Virtual PC ou Virtual Server pour fonctionner, donc les performances des machines virtuelles sont améliorées. Lorsque l'on virtualise un ordinateur, il faut prêter une attention particulière aux composants qui sont en contention comme la mémoire, le processeur, l'accès disque et l'accès réseau.

Le format des ordinateurs virtuels utilise également le format VHD. Lors de la migration d'un environnement virtualisé, il faut prêter une attention particulière à ce que les machines virtuelles aient été créées sur des versions de Virtual PC ou Virtual Server, car le simple transfert, même s'il fonctionne, ne garantit pas un fonctionnement optimal de l'ordinateur virtuel. La KB954958 montre les systèmes d'exploitation invités pris en charge sur Hyper-V.

La société VMWare propose entre autres un produit concurrent.

## 6. Windows Server 2008 Hyper-V

Dans Windows, Hyper-V se présente sous la forme d'un rôle.

## 7. Terminal Server

Terminal Server est l'outil de présentation de l'affichage Windows sur un ordinateur distant. En fait, aujourd'hui, toutes les sessions de Windows virtualisent l'affichage mais la plupart du temps l'affichage est redirigé sur la console locale. L'administration à distance, l'assistance à distance ou le partage du Bureau Windows utilisent également une technologie type Terminal Server sans en porter le nom. Pour un affichage distant, le protocole RDP est utilisé.

Le serveur supporte toute la charge des sessions clientes, l'ordinateur client n'a besoin lui que d'un client RDP pour afficher le Bureau distant ; il est donc possible d'utiliser un ordinateur client ayant une version de Windows différente de celle du Bureau distant et dont le matériel est très limité. On parle également de client léger.

Terminal Server peut être déployé dans de nombreux scénarios qui vont de la manière de travailler en entreprise aux utilisateurs itinérants.

Dans la version 2008, Terminal Server permet non seulement à des utilisateurs distants de se connecter, d'être gérés par un serveur de licences, mais également :

- De répartir la charge des clients et d'aider à la reconnexion dans une ferme de serveurs Terminal Server **TS Broker**.
- D'utiliser un mode appelé Application distante **RemoteApp** qui permet de n'afficher sur l'ordinateur client que l'application et non plus le Bureau.
- D'utiliser un site Web pour sélectionner les serveurs TS ou les applications distantes.
- Pour les utilisateurs provenant de l'Internet, de passer par un ordinateur servant de passerelle **TS Gateway** pour rediriger le client sur le bon serveur TS et éventuellement, d'encapsuler le protocole RDP du protocole HTTP/S.

La société Citrix propose entre autres un produit concurrent.

## 8. Microsoft Application Virtualization (SoftGrid)

Microsoft Application Virtualization est une plate-forme de déploiement d'application en temps réel. Avec ce type de virtualisation, l'application n'a plus besoin d'être installée sur l'ordinateur client, elle est simplement appellée par l'utilisateur et transférée à partir du serveur en temps réel ou via un média.

Microsoft Application Virtualization est composé d'un élément serveur qui distribue les packages pour les ordinateurs clients et d'une partie cliente qui appelle les packages et virtualise les éléments nécessaires au fonctionnement de l'application comme les composants COM, la base de registre, etc.

Microsoft Application Virtualization est parfaitement adapté dans un environnement d'entreprise pour les ordinateurs de bureau traditionnels.

La bande passante du réseau doit être importante et les ordinateurs clients doivent être compatibles avec l'application pour pouvoir la supporter.

La société Altiris propose entre autres un produit concurrent.

Il diffère de Terminal Server du fait que :

- Avec Terminal Server l'affichage, le clavier et la souris (éventuellement d'autres éléments) sont renvoyés sur l'ordinateur client.
- Avec Microsoft Application Virtualization, l'application tourne sur l'ordinateur client.
- Avec Microsoft Application Virtualization, il est possible de stocker localement le package sur l'ordinateur client et donc de travailler en l'absence d'un serveur.
- Dans Terminal Server, la bande passante nécessaire peut être faible, soit de l'ordre de 30 Kb/s.

## 9. System Center Data Protection Manager

Microsoft System Center Data Protection Manager (DPM) permet de mettre en œuvre une infrastructure de protection des disques y compris dans des environnements virtuels.

Il permet d'effectuer des sauvegardes des images virtuelles directement en ligne donc sans interruption de service.

## 10. Windows Storage Server

La version actuelle se base sur Windows Server 2003R2. En fait, il s'agit d'un serveur de fichiers et d'impression basé sur Windows pour consolider différents serveurs de fichiers y compris des serveurs de sauvegarde ou de réPLICATION. Son principal avantage est d'intégrer un service iSCSI target.

## 11. System Center Virtual Manager

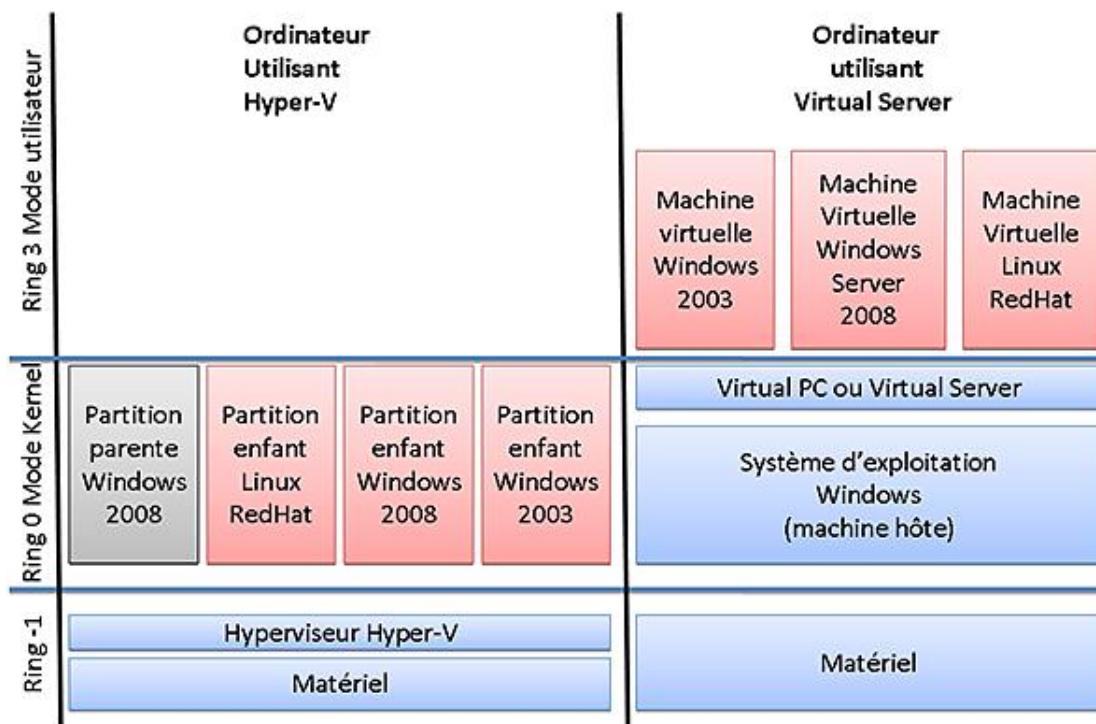
System Center Virtual Manager est un outil de gestion globalisée et de création de rapports pour gérer un environnement d'ordinateurs virtualisés.

System Center Virtual Manager 2008 permet de gérer les différentes plates-formes virtuelles, comme Hyper-V, Virtual Server, VMWare, etc. Il dispose également d'un convertisseur P2V (*Physical to Virtual*) rapide et fiable.

La société VMWare propose un produit concurrent.

## 12. Comparaison de l'architecture entre Virtual Server et Hyper-V

La figure suivante montre les différences d'architecture entre Virtual Server et Hyper-V :



Le noyau de l'Hyper-V est l'Hyperviseur qui est une couche mince (quelques centaines de Ko) dont le travail est de permettre un accès partagé au processeur, à la mémoire, etc., sans risquer de conflit.

Toute communication entre les différentes partitions utilise un bus appelé **VMBus** fonctionnant sur l'Hyperviseur, voire une émulation qui est plus lente que le VMBus si le système d'exploitation invité n'est pas supporté.

À l'inverse, Virtual PC fournit un environnement matériel qui émule un certain nombre de périphériques de l'ordinateur.

Le tableau suivant montre les différences principales entre Virtual Server et Hyper-V :

	Virtual Server	Hyper-V
--	----------------	---------

Ordinateur hôte 32 bits	x	
Ordinateur hôte 64 bits	x	x
Machine virtuelle 32 bits	x	x
Machine virtuelle 64 bits		x
Nombre de processeurs supportés pour la machine virtuelle	1	Jusqu'à 4, dépend de l'OS
Nombre de processus supportés par l'hôte	dépend de l'OS	24
Mémoire maximum supportée par la machine virtuelle	3.4 Go	64 Go
Mémoire maximum supportée par l'hôte	dépend de l'OS	1 To 32 Go pour l'édition standard
Nombre de contrôleurs SCSI	1	4
Sauvegarde basée sur des clichés instantanés si la machine virtuelle fonctionne		x
Hyperviseur basé sur la technologie Xen		x
Environnement émulé	x	

### 13. Équivalence entre les produits VMWare et Microsoft

Le tableau suivant montre les équivalences entre ces produits :

	<b>Microsoft</b>	<b>VMWare</b>
Virtualisation Server haute performance basée sur la technologie de l'Hyperviseur	Hyper-V	VMWare ESXi VMWare ESX
Virtualisation sur le serveur	Virtual Server	VMWare Server
Virtualisation sur la station de travail	Virtual PC	VMWare Workstation
Outil de gestion	System Center Virtual Manager	VMWare Virtual Center

Ce tableau ne tient pas compte des différences de caractéristiques existant entre les produits, ni des différences de coût, ni des produits additionnels permettant d'étendre les fonctionnalités de base comme VMWare VMotion.

## Présentation des rôles

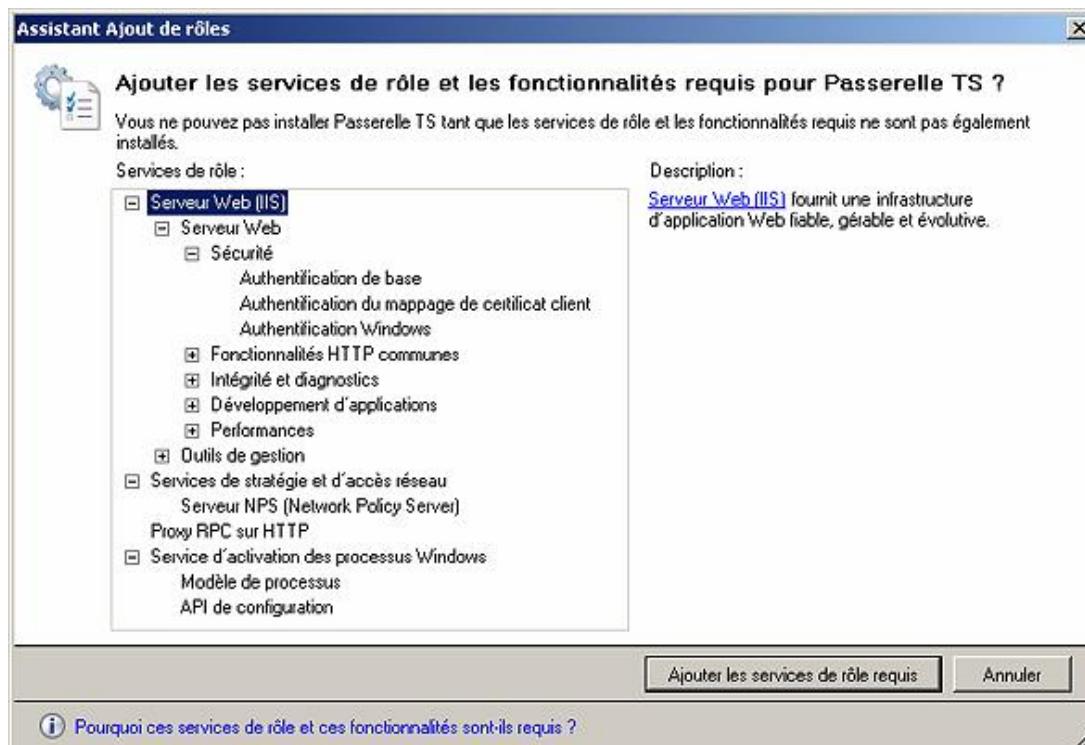
Un rôle regroupe un ou plusieurs composants permettant de réaliser une tâche spécifique sur le réseau. Bien que le rôle soit un artifice logique, il permet de simplifier la logique d'administration. Dans Windows Server 2008, Microsoft a défini 17 rôles par défaut. Disposant d'une architecture extensible, de nouveaux rôles apparaissent avec le temps comme le rôle **WSUS 3.0 SP1** (*Windows Server Update Services*).

Un **service de rôle** est un sous-ensemble d'un rôle donné. Dès qu'un rôle se compose de plusieurs services de rôle pouvant fonctionner de manière autonome, vous devez décider quel service de rôle installer.

Les services de rôle simplifient l'administration et réduisent la surface d'attaque du serveur.

À l'installation, aucun rôle n'est installé. Un rôle s'installe soit manuellement par l'intermédiaire de l'administrateur, soit automatiquement lors de l'installation d'un autre rôle ou d'une fonctionnalité.

Si des fonctionnalités ou des rôles sont manquants lors de l'installation d'une fonctionnalité ou d'un rôle, l'assistant vous propose d'installer les éléments requis comme le montre l'exemple de la figure suivante où on a voulu installer le rôle Terminal Service avec le service de rôle Passerelle TS.



Le tableau suivant résume les rôles que l'on peut installer sur les différentes installations complètes de Windows Server 2008.

Rôle	Standard	Enterprise	Datacenter	Itanium	Web
Serveur d'applications	x	x	x	x	
Serveur de télécopies	x	x	x		
Serveur DHCP	x	x	x		
Serveur DNS	x	x	x		
Serveur Web (IIS)	x	x	x	x	x
Services de domaine Active Directory AD DS	x	x	x		
Active Directory Lightweight Directory Services AD LDS	x	x	x		

Services de gestion des droits Active Directory AD RMS	x	x	x		
Services de fédération Active Directory AD FS		x	x		
Services de certificats Active Directory AD CS	Limité	x	x		
Services de déploiement Windows (WDS)	x	x	x		
Services d'impression	x	x	x		
Services de fichiers	Limité	x	x		
Services d'accès et de stratégie réseau	Limité	x	x		
Services Terminal Server TS	Limité	x	x		
Services UDDI ( <i>Universal Description Discovery and Integration</i> )	x	x	x		
Hyper-V™ (1)	x	x	x		
Services Windows Media (Streaming)	Limité	x	x		Limité

(1) Les éditions Standard, Entreprise et DataCenter sont disponibles sans la technologie Hyper-V.

Le tableau suivant résume les rôles que l'on peut installer sur les différentes installations minimales de Windows Server 2008.

Rôle	Standard	Enterprise	Datacenter	Web
Serveur Web (IIS) sans ASP.NET	x	x	x	x
Services d'impression	x	x	x	
Serveur DHCP	x	x	x	
Serveur DNS	x	x	x	
Services de fichiers	Limité	x	x	
Services de domaine Active Directory AD DS	x	x	x	
Services AD LDS ( <i>Active Directory Lightweight Directory Services</i> )	x	x	x	
Hyper-V™ (1)	x	x	x	
Services Windows Media (Streaming)	Limité	x	x	Limité

(1) Les éditions Standard, Entreprise et DataCenter sont disponibles sans la technologie Hyper-V.

## 1. Serveur d'applications

Le rôle de serveur applicatif permet d'installer facilement les fonctionnalités pouvant être requises par une application métier.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Serveur d'applications	Application-Server
Fondation du serveur d'applications	AS-AppServer-Foundation
Prise en charge du serveur Web IIS	AS-Web-Support
Accès au réseau COM+	AS-Ent-Services
Partage de port TCP	AS-TCP-Port-Sharing
Service d'activation des processus Windows	AS_WAS-Support
Activation HTTP	AS-HTTP-Activation
Activation Message Queuing	AS-MSMQ-Activation
Activation TCP	AS-TCP-Activation
Activation des canaux nommés	AS-Named-Pipes
Transactions distribuées	AS-Dist-Transaction
Transactions distantes entrantes	AS-Incoming-Trans
Transactions distantes sortantes	AS-Outgoing-Trans
Transactions WS-Atomic	AS-WS-Atomic

**Fondation du serveur d'applications** : est requis pour installer le rôle et installe le Framework 3.0.

**Prise en charge du serveur Web (IIS)** : installe le service Web (IIS).

**Accès au réseau COM+** : permet de communiquer à distance avec le protocole COM+.

**Partage de port TCP** : permet à plusieurs applications WCF (*Windows Communication Foundation*) de partager le même port.

**Service d'activation des processus Windows** : installe et active différents mécanismes de communication basés sur les protocoles HTTP, Message Queuing, TCP ou les canaux nommés.

**Transactions distribuées** : installe un mécanisme permettant de gérer une transaction sur plusieurs serveurs. Pour des transactions initiées localement à distance ou utilisant un service Web.

---

➤ Ce rôle n'est à installer que sur un serveur applicatif qui requiert un ou plusieurs composants décrits comme fondation d'une application métier.

---

➤ Rôle applicatif optionnel.

---

## 2. Serveur de télécopie

Ce rôle crée un serveur de télécopie permettant de :

- Configurer des périphériques de télécopie.
- Gérer des utilisateurs.
- Définir des règles pour les télécopies sortantes.

- Définir des stratégies de routage pour les télécopies entrantes.
- Configurer le serveur de télécopie.

Ce rôle dépend du serveur d'impression. De plus il faut disposer d'un fax modem et les imprimantes multifonctions ne sont pas supportées à moins qu'un pilote de fax modem ne soit fourni.

Le composant de ce rôle est :

Rôle ou service de rôle	Valeur de la commande
Serveur de télécopie	Fax

- 
- L'utilité de ce rôle diminue car il est de plus en plus remplacé par l'e-mail. S'il s'avère nécessaire, il faut planifier son installation sur un serveur qui joue également le rôle de serveur d'impression.
- 
- Rôle applicatif optionnel.
- 

### 3. Serveur DHCP (Dynamic Host Configuration Protocol)

Le serveur DHCP permet de centraliser la gestion et la distribution des adresses IP.

Le chapitre Configurations autour du protocole DHCP décrit en détail ce rôle.

Le composant de ce rôle est :

Rôle ou service de rôle	Valeur de la commande
Serveur DHCP	DHCP

Le composant de ce rôle sur un Server Core est :

Rôle ou service de rôle	Valeur de la commande
Serveur DHCP	DHCPServerCore

- 
- Au moins un serveur DHCP doit être installé dans un réseau.
- 
- Ce rôle d'infrastructure est requis mais peut être remplacé par un serveur DHCP provenant d'un matériel ou d'un autre système d'exploitation.
- 

### 4. Serveur DNS (Domain Name System)

Le serveur DNS permet de résoudre la résolution d'un nom en adresse IP. Il fournit également l'emplacement des services de l'Active Directory dans un réseau d'entreprise.

Le chapitre Configuration de la résolution de noms décrit en détail ce rôle.

Le composant de ce rôle est :

Rôle ou service de rôle	Valeur de la commande
Serveur DNS	DNS

Le composant de ce rôle sur un Server Core est :

Rôle ou service de rôle	Valeur de la commande
Serveur DNS	DNS-Server-Core-Role

➤ Au moins un serveur DNS doit être installé dans un réseau d'entreprise.

➤ Ce rôle d'infrastructure est requis dans une forêt Active Directory et est à préférer par rapport à d'autres types de serveurs DNS. Dans un réseau de type groupe de travail, un serveur DNS externe d'un FAI (fournisseur d'accès Internet) peut être suffisant.

## 5. Serveur Web IIS (Internet Information Service)

La nouvelle mouture du serveur Web IIS 7.0 permet de choisir parmi près de 40 modules ceux qui doivent être installés. Cette nouvelle méthode d'installation permet de réduire la surface d'attaque. Ce serveur sert de support pour plusieurs rôles ainsi que pour Windows SharePoint Services.

Sur un Server Core, il n'est pas possible d'utiliser ASP.NET car le Framework est absent.

C'est le seul rôle installable sur une édition Web.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Serveur Web IIS	Web-Server
Fonctionnalités HTTP communes	Web-Common-http
Contenu statique	Web-Static-Content
Document par défaut	Web-Default-Doc
Exploration de répertoire	Web-Dir-Browsing
Erreurs HTTP	Web-Http-Errors
Redirection HTTP	Web-Http-Redirect
Développement d'applications	Web-App-Dev
ASP.NET	Web-Asp-Net
Extensibilité.NET	Web-Net-Ext
ASP	Web-ASP
CGI	Web-CGI
Extensions ISAPI	Web-ISAPI-Ext
Filtres ISAPI	Web-ISAPI-Filter
Fichiers Include côté serveur	Web-Includes
Intégrité et diagnostics	Web-Health
Journalisation http	Web-Http-Logging

Outils de journalisation	Web-Log-Libraries
Observateur de demandes	Web-Request-Monitor
Suivi	Web-Http-Tracing
Journalisation personnalisée	Web-Custom-Logging
Journal ODBC	Web-ODBC-Logging
Sécurité d'IIS	Web-Security
Authentification de base	Web-Basic-Auth
Authentification Windows	Web-Windows-Auth
Authentification Digest	Web-Digest-Auth
Authentification du mappage de certificat client	Web-Client-Auth
Authentification de mappage de certificats clients d'IIS	Web-Cert-Auth
Autorisation URL	Web-Url-Auth
Filtrage des demandes	Web-Filtering
Restrictions IP et de domaine	Web-IP-Security
Performances	Web-Performance
Compression de contenu statique	Web-Stat-Compression
Compression de contenu dynamique	Web-Dyn-Compression
Outils de gestion	Web-Mgmt-Tools
Console de gestion d'IIS	Web-Mgmt-Console
Scripts et outils de gestion d'IIS	Web-Scripting-Tools
Service de gestion	Web-Mgmt-Service
Compatibilité de gestion IIS 6	Web-Mgmt-Compat
Compatibilité avec la métabase de données IIS 6	Web-Metabase
Compatibilité WMI d'IIS 6	Web-WMI
Outils de script IIS 6	Web-Lgcy-Scripting
Console de gestion IIS 6	Web-Lgcy-Mgmt-Console
Service de publication FTP	Web-Ftp-Publishing
Serveur FTP	Web-Ftp-Server
Console de gestion FTP	Web-Ftp-Mgmt-Console

Les composants de ce rôle sur un Server Core sont :

<b>Rôle ou service de rôle</b>	<b>Valeur de la commande</b>
Serveur Web IIS	WebServerRole
Server Web IIS	IIS-WebServer
Fonctionnalités HTTP communes	IIS-CommonHttpFeatures
Contenu statique	IIS-StaticContent
Document par défaut	IIS-DefaultDocument
Exploration de répertoire	IIS-DirectoryBrowsing
Erreurs HTTP	IIS-HttpErrors
Redirection HTTP	IIS-HttpRedirect
Développement d'applications	IIS-ApplicationDevelopment
ASP	IIS-ASP
CGI	IIS-CGI
Extensions ISAPI	IIS-ISAPIExtensions
ASP	IIS-ASP
Filtres ISAPI	IIS-ISAPIFilter
Fichiers Include côté serveur	IIS-ServerSideIncludes
Intégrité et diagnostics	IIS-HealthAndDiagnostics
Journalisation http	IIS-HttpLogging
Outils de journalisation	IIS-LoggingLibraries
Observateur de demandes	IIS-RequestMonitor
Suivi	IIS-HttpTracing
Journalisation personnalisée	IIS-CustomLogging
Journal ODBC	IIS-ODBCLogging
Performances	IIS-Performance
Compression de contenu statique	IIS-HttpCompressionDynamic
Compression de contenu dynamique	IIS-HttpCompressionStatic
Sécurité	IIS-Security
Authentification de base	IIS-BasicAuthentication
Authentification Windows	IIS-WindowsAuthentication
Authentification Digest	IIS-DigestAuthentication

Authentification du mappage de certificat client	IIS-ClientCertificateMappingAuthentication
Authentification de mappage de certificats clients d'IIS	IIS-IISCertificateMappingAuthentication
Autorisation URL	IIS-URLAuthorization
Filtrage des demandes	IIS-RequestFiltering
ASP	IIS-ASP
Restrictions IP et de domaine	IIS-IPSecurity
Outils de gestion	IIS-WebServerManagementTools
Scripts et outils de gestion d'IIS	IIS-ManagementScriptingTools
Compatibilité de gestion IIS 6	IIS-IIS6ManagementCompatibility
Outils de script IIS 6	IIS-LegacyScripts
Compatibilité avec la métabase de données IIS 6	IIS-Metabase
Serveur FTP	IIS-FTPServer
Outils de scripts IIS 6	IIS-LegacyScripts
Compatibilité WMI d'IIS 6	IIS-WMICompatibility
Outils de script IIS 6	IIS-LegacyScripts
Service de publication FTP	IIS-FTPPublishingService
Serveur FTP	IIS-FTPServer

**Fonctionnalités HTTP communes** : installe les modules de base pour gérer le serveur Web comme le support des fichiers statiques, le nom des documents par défaut si la demande ne contient pas de page spécifique, l'exploration de répertoire si elle peut être supportée, la personnalisation des pages d'erreur et la redirection des requêtes clients.

**Développement d'applications** : fournit l'infrastructure pour installer le support des technologies de développement suivantes : ASP.NET, le support des modules d'extensions .NET, les pages ASP, l'interface CGI (*Common Gateway Interface*), les extensions ISAPI, les filtres ISAPI et les fichiers Include côté serveur SSI.

**Intégrité et diagnostics** : ajoute les modules nécessaires pour créer des journaux et tracer les requêtes.

**Sécurité** : installe les modules pour gérer une authentification particulière et autoriser l'accès à une page selon différents critères.

**Performances** : installe le service pour activer la compression logicielle.

**Outils de gestion** : installe l'infrastructure de gestion et la console MMC. La compatibilité avec la version 6 est assurée afin de supporter des applications Web et leur mode de gestion sans modification.

**Services de publication FTP** : fournit l'infrastructure pour installer un serveur FTP et/ou la console MMC de gestion.

➤ À installer en fonction des besoins. Si un accès depuis Internet est autorisé, il faut prêter une attention particulière à la sécurité.

➤ Ce rôle d'infrastructure applicatif est optionnel.

## 6. Services de domaine Active Directory (AD DS)

C'est le rôle qui installe l'Active Directory. La configuration se fait toujours à l'aide de la commande **dcpromo**.

Le chapitre Crédation du bac à sable pour effectuer les ateliers montre comment installer une Active Directory.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services de domaine Active Directory	
Contrôleur de domaine Active Directory	ADDS-Domain-Controller
Gestion des identités pour Unix	ADDS-Identity-Mgmt
Serveur pour le service NIS ( <i>Network Information Services</i> )	ADDS-NIS
Synchronisation des mots de passe	ADDS-Password-Sync
Outils d'administration	ADDS-IDMU-Tools

Le composant de ce rôle pour un Server Core est :

Rôle ou service de rôle	Valeur de la commande
Services de domaine Active Directory	
Contrôleur de domaine Active Directory	DirectoryServices-DomainController-ServerFoundation

**Contrôleur de domaine Active Directory** : installe les services de domaine Active Directory sur le serveur pour en faire un contrôleur de domaine.

**Gestion des identités pour Unix** : installe les outils nécessaires pour intégrer des ordinateurs Windows dans des environnements Unix en permettant la synchronisation automatique des mots de passe et le mappage des entrées de l'Active Directory avec les domaines NIS.

- 
- Au moins un serveur Active Directory est requis pour créer un domaine dans un réseau d'entreprise. Ce rôle est inutile dans un groupe de travail.

---

  - Ce rôle d'infrastructure est requis ! L'expérience montre que le plus petit réseau peut être composé d'un serveur plus un client pour simplifier l'administration et être facilement évolutif en utilisant une édition Small Business Server par exemple.
- 

## 7. Active Directory Lightweight Directory Services (AD LDS)

Ce rôle installe un annuaire **LDAP** (*Lightweight Directory Access Protocol*) permettant à des applications spécifiques de prendre en charge des utilisateurs provenant de votre entreprise ou d'entreprises différentes sans compromettre la sécurité d'Active Directory.

Identique à l'Active Directory, excepté qu'il ne gère pas l'authentification des utilisateurs.

Le composant de ce rôle est :

Rôle ou service de rôle	Valeur de la commande
Services AD LDS ( <i>Active Directory Lightweight Directory Services</i> )	ADLDS

Le composant de ce rôle pour un Server Core est :

Rôle ou service de rôle	Valeur de la commande
Services AD LDS ( <i>Active Directory Lightweight Directory Services</i> )	DirectoryServices-ADAM-ServerCore

- Si vous planifiez l'utilisation d'une application qui fait appel à l'utilisation d'un annuaire LDAP, alors ce rôle est un excellent candidat potentiel.
  
- Ce rôle applicatif est optionnel.

## 8. Service de gestion des droits (AD RMS)

Ce rôle installe un service de gestion des droits d'accès du contenu des fichiers, au sein d'une forêt Active Directory. Les documents et les e-mails peuvent être protégés contre tout accès, ou utilisation non autorisés.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services AD RMS ( <i>Active Directory Rights Management Services</i> )	Ne peut être installé en mode ligne de commande
Active Directory Rights Management Server	Ne peut être installé en mode ligne de commande
Prise en charge de la fédération des identités	Ne peut être installé en mode ligne de commande

Le Service AD RMS est divisé en deux composants, le premier composant est le serveur lui-même et le second permet la prise en charge des identités fédérées à l'aide d'un serveur AD FS.

- Si vous planifiez une stratégie de gestion des droits d'accès aux documents, alors ce rôle est un excellent candidat potentiel.
  
- Ce rôle d'infrastructure de sécurité est optionnel.

## 9. Services de fédération Active Directory (ADFS)

Le rôle **ADFS** permet de fédérer l'authentification entre plusieurs entités en fournissant une technologie d'authentification Web unique **SSO** (*Single Sign On*) pour authentifier un utilisateur.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services ADFS ( <i>Active Directory Federation Services</i> )	
Service de fédération	ADFS-Federation
Proxy du service de fédération	ADFS-Proxy
Agent Web AD FS	ADFS-Web-Agents
Agent prenant en charge les revendications	ADFS-Claims
Agent basé sur les jetons Windows	ADFS-Windows-Token

**Service de fédération** : installe l'infrastructure pour autoriser l'accès à des ressources.

**Proxy du service de fédération** : collecte les demandes des applications Web clientes pour les transmettre au service de fédération au nom du client.

**Agent Web AD FS** : active l'authentification pour des clients Windows ou des applications.

➤ Si vous planifiez une stratégie d'authentification de type SSO, alors ce rôle est un excellent candidat. Cette fonctionnalité est apparue avec Windows Server 2003 R2.

➤ Ce rôle d'infrastructure de sécurité est optionnel.

## 10. Services de certificats Active Directory (ADCS)

Le rôle installe le nouveau serveur de certificats, qui permet de délivrer, gérer et révoquer des certificats au sein d'une entreprise.

L'édition Standard est limitée à l'installation du composant **Autorité de certification**.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services de certificats Active Directory	AD-Certificate
Autorité de certification	ADCS-Cert-Authority
Inscription de l'autorité de certification via le Web	ADCS-Web-Enrollment
Répondeur en ligne	ADCS-Online-Cert
Service d'inscription de périphériques réseau	ADCS-Device-Enrollment

**Autorité de certification** : est le serveur qui émet et garantit les certificats.

**Inscription de l'autorité de certification via le Web** : installe un site Web pour demander des certificats.

**Répondeur en ligne** : installe un serveur alternatif pour consulter la liste des certificats révoqués basés sur le protocole OCSP (*Online Certificate Status Protocol*).

**Service d'inscription de périphériques réseau** : installe un serveur de certificats permettant à des périphériques tels qu'un routeur de demander des certificats compatibles avec le protocole MSCEP (*Microsoft Simple Certificate Enrollment Protocol*).

➤ Il n'est pas nécessaire d'installer ce rôle car il est également possible d'acheter des certificats.

➤ Ce rôle ne doit être installé et géré que par des administrateurs qui maîtrisent une infrastructure de certificats.

➤ Ce rôle peut être requis par certaines technologies utilisées.

➤ Ce rôle d'infrastructure de sécurité est optionnel.

## 11. Services de déploiement Windows (WDS)

Le service WDS est le successeur du service **RIS** (*Remote Installation Service*) des anciennes versions. Il permet de d'effectuer des installations à distance pour des clients Windows Vista et Windows Server 2008 uniquement.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services de déploiement Windows	WDS

Serveur de déploiement	WDS-Deployment
Serveur de transport	WDS-Transport

**Serveur de déploiement** : installe le service WDS.

**Serveur de transport** : permet d'installer les éléments requis pour transmettre des données en utilisant le *multicasting*. Il peut fonctionner sans le serveur de déploiement.

- Si vous planifiez des stratégies de déploiement de masse ou de maintenance à travers le réseau, alors ce rôle est un excellent candidat.
  
- Ce rôle d'infrastructure est optionnel.

## 12. Services d'impression

Ce rôle permet d'installer une console de gestion centralisée des imprimantes, le service LPD (*Line Printer Daemon*) et le service d'impression Internet.

Le chapitre Mise en œuvre de l'impression décrit en détail ce rôle.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services d'impression	Print-Services
Serveur d'impression	Print-Server
Service LPD	Print-LPD-Service
Impression Internet	Print-Internet

Les composants de ce rôle pour un Server Core sont :

Rôle ou service de rôle	Valeur de la commande
Serveur d'impression	Printing-ServerCore-Role
Service LPD	Printing-LPDPrintService

**Serveur d'impression** : c'est le serveur d'impression qui gère les imprimantes et leurs pilotes.

**Service LPD** : il permet à des ordinateurs fonctionnant sous Unix d'imprimer sur le serveur d'impression.

**Impression Internet** : il permet de se connecter en utilisant le protocole HTTP pour imprimer ou gérer le serveur d'impression.

- Ce rôle d'infrastructure est requis dès qu'une imprimante est mise en réseau.

## 13. Services de fichiers

Le service de fichiers fournit plusieurs services pour gérer efficacement les fichiers de votre entreprise. L'édition Standard est limitée à une racine DFS autonome.

Le chapitre Mise en œuvre du serveur de fichiers décrit en détail ce rôle.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services de fichiers	
Serveur de fichiers	FS-FileServer
Système de fichiers distribués	FS-DFS
Espaces de noms DFS	FS-DFS-Namespace
RéPLICATION DFS	FS-DFS Replication
Gestion de ressources du serveur de fichiers	FS-Resource-Manager
Services pour NFS	FS-NFS-Services
Service de recherche Windows	FS-Search-Service
Services de fichiers Windows 2003	FS-Win2003-Services
Service de réPLICATION de fichiers	FS-Replication
Service d'indexation	FS-Indexing-Service

Les composants de ce rôle pour un Server Core sont :

Rôle ou service de rôle	Valeur de la commande
Système de fichiers distribués	DFSN-Server
RéPLICATION DFS	DFSR-Infrastructure-ServerEdition
Services pour NFS	ServerForNFS-Base
Client NFS	ClientForNFS-Base
Service de réPLICATION de fichiers	FRS-Infrastructure

**Serveur de fichiers** : c'est le serveur de fichiers.

**Système de fichiers distribués** : il permet de créer des arborescences logiques de partages serveurs qui peuvent être répliquées sur plusieurs serveurs.

**Gestion de ressources du serveur de fichiers** : c'est un ensemble d'outils d'administration.

**Services pour NFS** : il permet de partager des documents avec le protocole NFS principalement utilisé sous Unix.

**Service de recherche Windows** : c'est le système de recherche par indexation des fichiers de Windows.

**Services de fichiers Windows 2003** : il crée une compatibilité avec les serveurs sous Windows Server 2003.



Ce rôle d'infrastructure est requis.

## 14. Services de stratégie et d'accès réseau NAP

Le service NAP permet de créer des stratégies d'accès réseau garantissant que les ordinateurs sont conformes et sains.

L'édition Standard est limitée à 250 connexions RRAS, 50 connexions IAS et 2 groupes de serveur IAS.

Le chapitre Gestion et surveillance d'une infrastructure réseau présente ce rôle.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services de stratégie d'accès réseau	NPAS
Serveur NPS ( <i>Network Policy Server</i> )	NPAS-Policy-Server
	NPAS-RRAS-Services
	NPAS-RRAS
	NPAS-Routing
Autorité HRA ( <i>Health Registration Authority</i> )	NPAS-Health
HCAP ( <i>Host Credential Authorization Protocol</i> )	NPAS-Host-Cred

- Si vous planifiez une stratégie de gestion de l'accès réseau, alors ce rôle est un excellent candidat.

## 15. Services Terminal Server TS

Le service Terminal Server permet de centraliser les applications sur un serveur, ce qui simplifie la gestion des applications et permet de conserver des ordinateurs peu puissants comme poste de travail pour un utilisateur.

Ce service permet également d'améliorer grandement la sécurité des utilisateurs itinérants.

L'édition Standard est limitée à 250 connexions pour le service de passerelles.

Le chapitre Introduction présente ce rôle.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services Terminal Server	Terminal Server
Terminal Server	TS-Terminal-Server
	TS-Licensing
	TS-Session-Broker
	TS-Gateway
	TS-Web-Access

**Terminal Server** : c'est le service Terminal Server.

**Gestionnaire de licences TS** : c'est le gestionnaire de licences Terminal Server.

**Session Broker TS** : il permet de suivre les sessions utilisateur, y compris dans un environnement WNLB.

**Passerelle TS** : c'est le point d'entrée sur des serveurs TS pour tout client Internet.

**Accès Web TS** : il permet aux clients d'accéder aux sessions TS ou aux applications en mode **remote application** par l'intermédiaire d'un site Web.

- Dans une entreprise, à partir de 100 collaborateurs ou dès que des données doivent rester confidentielles, les utilisateurs itinérants ne devraient avoir accès aux applications qu'en mode TS.

- Ce rôle est adapté à toutes les entreprises qui veulent gérer de manière centralisée les applications.

 Ce rôle d'infrastructure est optionnel.

## 16. Services UDDI (Universal Description Discovery and Integration)

Les services Web sont de plus en plus nombreux. Comme ils sont susceptibles d'être utilisés par des applications développées en interne dans l'entreprise, il serait utile d'installer un serveur **UDDI** qui fédère la connaissance des services Web installés de l'entreprise ou de partenaires.

Les composants de ce rôle sont :

Rôle ou service de rôle	Valeur de la commande
Services UDDI	Ne peut être installé en mode ligne de commande
Base de données des services UDDI	Ne peut être installé en mode ligne de commande
Application Web des Services UDDI	Ne peut être installé en mode ligne de commande

 Ce rôle d'infrastructure est optionnel. Il n'est à installer qu'à la demande de développeurs internes à votre entreprise ou dans un cadre plus large auprès de partenaires.

## 17. Hyper-V™

Hyper-V est le moteur de virtualisation de Windows Server 2008 basé sur la technologie XEN.

Des éditions de Windows Server 2008 Standard, Enterprise et Datacenter sont disponibles sans Hyper-V.

 Exige une version 64 bits.

Le chapitre Introduction présente ce rôle.

Le composant de ce rôle est :

Rôle ou service de rôle	Valeur de la commande
Hyper-V	Hyper-V

Le composant de ce rôle pour un **Server Core** est :

Rôle ou service de rôle	Valeur de la commande
Hyper-V	Microsoft-Hyper-V

 C'est un rôle d'infrastructure. Si vous planifiez d'utiliser la virtualisation pour certains de vos serveurs à l'aide des technologies Microsoft, alors Hyper-V est un des premiers choix.

## 18. Streaming Media Services

Ce rôle est un rôle additionnel qu'il faut télécharger depuis le site de Microsoft (voir la KB934518). Il permet de distribuer de l'information en continu que ce soit des films, de la musique, de la TV sur IP (IPTV)... de manière fiable et sans surcharger le réseau.

Le composant de ce rôle est :

<b>Rôle ou service de rôle</b>	<b>Valeur de la commande</b>
Streaming Media Server	MediaServer

Le composant de ce rôle sur une édition Core est :

<b>Rôle ou service de rôle</b>	<b>Valeur de la commande</b>
Streaming Media Server	MediaServer

-  Ce rôle d'infrastructure est optionnel. Si vous planifiez d'utiliser un système de distribution de flux d'information, alors le rôle est un candidat potentiel.

## 19. Windows Server Update Services (WSUS)

La version 3SP1 du service WSUS peut être téléchargée et installée en tant que nouveau rôle (KB940518).

Le chapitre Configuration des services réseaux avancés montre ce rôle en détail.

<b>Rôle ou service de rôle</b>	<b>Valeur de la commande</b>
Windows Server Update Services	

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre indirectement les compétences évaluées à l'examen. Ce chapitre parle des rôles et des fonctionnalités. Leur connaissance s'avère donc indispensable.

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



## 3. Objectifs

Dans les versions précédentes, l'ajout de composants optionnels était basé sur une boîte de dialogue et un fichier statique. Un outil avait le même poids qu'une application. Avec Windows Server 2008, cette approche n'était plus adaptée et Microsoft a créé une nouvelle architecture appelée CBS (*Component Based Servicing*) qui capture toutes les dépendances et gère l'intégrité du service de manière dynamique. La notion de rôle et de fonctionnalité a été créée. Enfin, l'architecture CBS est évolutrice.

Étant donné le nombre élevé des éditions et des versions de Windows Server 2008, il n'est pas évident de savoir si le rôle ou la fonctionnalité est disponible pour une édition particulière.

Pour une bonne planification et une utilisation rationnelle et optimisée de Windows Server 2008, il est utile de connaître leur fonction et leur implication.

À la fin du chapitre, vous serez à même de décrire tous les rôles et toutes les fonctionnalités. Vous pourrez indiquer et planifier leur cadre d'utilisation. Enfin, vous saurez installer et désinstaller un rôle ou une fonctionnalité avec les trois outils, le **Gestionnaire de serveur**, la commande **ServerManagerCmd** et la commande **ocsetup**.

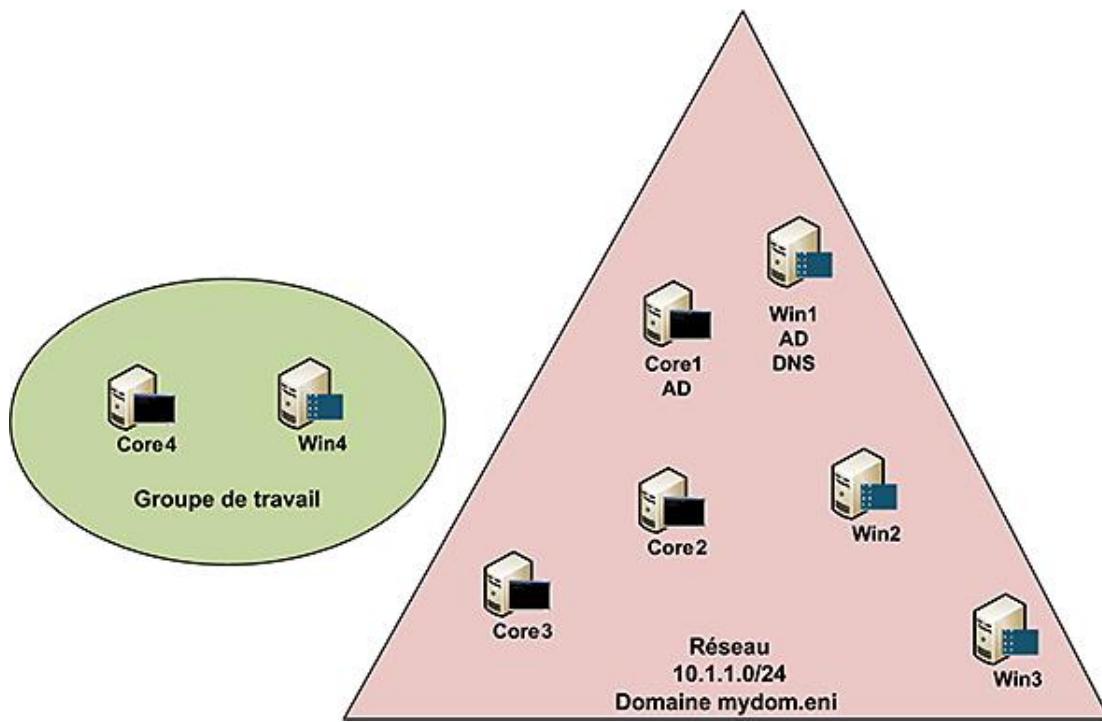
Vous pourrez également utiliser le **Gestionnaire de serveur** pour gérer les rôles ou les fonctionnalités sur une installation complète.

## Résumé du chapitre

Vous avez appris les avantages que vous pouvez tirer de la virtualisation pour la création d'un bac à sable. Ensuite, il vous a été présenté les procédures pas à pas à suivre pour créer des machines virtuelles que se soit pour une installation minimale ou complète. Enfin, vous avez créé le bac à sable Mises en pratique qui vous permettra de réaliser toutes les procédures présentées dans ce livre.

## Création du bac à sable Mises en pratique

Ce bac à sable est très simple à mettre en œuvre, car il se compose de 8 ordinateurs, soit 4 Windows Server 2008 en installation complète et 4 Windows Server 2008 en installation minimale pour représenter le réseau suivant :



Ce bac à sable est conçu de manière à ce que le lecteur puisse effectuer toutes les procédures décrites dans le livre même avec un ordinateur hôte peu puissant.

Les machines virtuelles sont appelées Win1, Win2, Win3 et Win4 pour les installations complètes et Core1, Core2, Core3 et Core4 pour les installations minimales.

À chaque procédure, ou titre dans les prochains chapitres, sera associée une icône vous indiquant sur quel ordinateur virtuel vous devez effectuer la procédure. Si le numéro de l'ordinateur n'est pas précisé, vous pouvez utiliser n'importe quelle machine virtuelle.

Il faut compter 60 minutes pour créer une machine virtuelle, néanmoins vous pouvez créer plusieurs machines virtuelles en même temps.

Vous pouvez télécharger une check-list depuis le site des Éditions ENI pour vérifier que vous avez réalisé toutes les étapes.

 Par défaut l'**UAC** (*User Account Control*) est activé. Dans le livre, il n'en est jamais tenu compte sauf s'il faut travailler en mode administrateur afin de ne pas surcharger les procédures. Ne soyez pas surpris si l'UAC vous demande votre consentement pour continuer.

### 1. Machine virtuelle Win1



#### a. Paramètres à utiliser pour la machine virtuelle Win1

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\practices\win1

Système d'exploitation		Windows Server 2008
Mémoire vive		<b>1 Go</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Enterprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Win1
Adressage IP	Statique 10.1.1.1 - 255.255.255.0
Domaine	Mydom.eni
Rôle	Active Directory
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Attribuer l'adresse IP et l'adresse du DNS de manière statique.
- Installer les compléments pour ordinateur virtuel.

### d. Comment installer l'Active Directory

La procédure suivante est à effectuer après avoir configuré le nom, l'adressage IP et avoir installé les compléments pour l'ordinateur virtuel.

- Téléchargez au préalable le fichier **WMyDomEni.txt** à partir du site des Éditions ENI.
- Connectez-vous en tant qu'administrateur puis saisissez la commande suivante : `dcpromo.exe /unattend:C:\WMyDomEni.txt`.

## 2. Machine virtuelle Win2



Win2

### a. Paramètres à utiliser pour la machine virtuelle Win2

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\practices\win2
Système d'exploitation		Windows Server 2008
Mémoire vive		1 Go
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut
Disques d'annulation	Activer les disques d'annulation	Case à cocher sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	Case à cocher sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Win2
Adressage IP	Statique 10.1.1.2 - 255.255.255.0 - DNS 10.1.1.1
Domaine	Membre du domaine Mydom.eni
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Attribuer l'adresse IP et l'adresse du DNS de manière statique.
- Rentrer dans le domaine Mydom.eni.
- Installer les compléments pour ordinateur virtuel.

### 3. Machine virtuelle Win3



#### a. Paramètres à utiliser pour la machine virtuelle Win3

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\practices\win3
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>1 Go</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher sélectionnée</b>
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher sélectionnée</b>

#### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Win3
Adressage IP	Statique 10.1.1.3 - 255.255.255.0 - DNS 10.1.1.1
Domaine	Membre du domaine Mydom.eni
Compléments virtuels	installés

#### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Attribuer l'adresse IP et l'adresse du DNS de manière statique.
- Rentrer dans le domaine Mydom.eni.

- Installer les compléments pour ordinateur virtuel.

## 4. Machine virtuelle Win4



### a. Paramètres à utiliser pour la machine virtuelle Win4

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\practices\win4
Système d'exploitation		Windows Server 2008
Mémoire vive		1 Go
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	Réseau partagé (NAT) ou local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Win4
Adressage IP	Non configuré, soit client DHCP
Domaine	Non configuré soit dans un groupe de travail
Compléments virtuels	installés

### c. Configuration post installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 5. Machine virtuelle Core1



### a. Paramètres à utiliser pour la machine virtuelle Core1

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\practices\Core1
Système d'exploitation		Windows Server 2008
Mémoire vive		Valeur par défaut
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut
Disques d'annulation	Activer les disques d'annulation	Case à cocher sélectionnée
Réseau	Carte 1	local seul
Son	Activer la carte audio	Case à cocher désélectionnée
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	Case à cocher sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (minimale)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Core1
Adressage IP	Statique 10.1.1.4 - 255.255.255.0
Domaine	Mydom.eni
Rôle	Active Directory
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Attribuer l'adresse IP et l'adresse du DNS de manière statique.
- Installer les compléments pour ordinateur virtuel.

Toute autre modification est optionnelle.

#### d. Comment installer l'Active Directory

La procédure suivante est à effectuer après avoir configuré le nom, l'adressage IP et avoir installé les compléments pour l'ordinateur virtuel.

- Téléchargez au préalable le fichier **CMyDomEni.txt** à partir du site des Éditions ENI.
- Connectez-vous en tant qu'administrateur puis saisissez la commande suivante :  
dcpromo.exe /unattend:C:\CMyDomEni.txt.

 Utilisez les dossiers partagés de Virtual PC pour transférer le fichier de configuration.

## 6. Machine virtuelle Core2



#### a. Paramètres à utiliser pour la machine virtuelle Core2

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\practices\Core2</b>
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>Valeur par défaut</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Son	Activer la carte audio	<b>Case à cocher</b> désélectionnée
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

#### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Minimale)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Core2
Adressage IP	Statique 10.1.1.5 - 255.255.255.0 - DNS 10.1.1.1
Domaine	Membre du domaine Mydom.eni
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Attribuer l'adresse IP et l'adresse du DNS de manière statique.
- Rentrer dans le domaine Mydom.eni.
- Installer les compléments pour ordinateur virtuel.

Toute autre modification est optionnelle.

## 7. Machine virtuelle Core3



### a. Paramètres à utiliser pour la machine virtuelle Core3

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\practices\Core3</b>
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>Valeur par défaut</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher sélectionnée</b>
Réseau	Carte 1	local seul
Son	Activer la carte audio	<b>Case à cocher</b>

		désélectionnée
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher sélectionnée</b>

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (minimale)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Core3
Adressage IP	Statique 10.1.1.6 - 255.255.255.0 - DNS 10.1.1.1
Domaine	Membre du domaine Mydom.eni
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Attribuer l'adresse IP et l'adresse du DNS de manière statique.
- Rentrer dans le domaine Mydom.eni.
- Installer les compléments pour ordinateur virtuel.

Toute autre modification est optionnelle.

## 8. Machine virtuelle Core4



### a. Paramètres à utiliser pour la machine virtuelle Core4

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\practices\Core4
Système d'exploitation		Windows Server 2008
Mémoire vive		Valeur par défaut
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut

Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	Réseau partagé (NAT) ou local seul
Son	Activer la carte audio	<b>Case à cocher</b> désélectionnée
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (minimale)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	Core4
Adressage IP	Non configuré, soit client DHCP
Domaine	Non configuré, soit dans un groupe de travail
Complément virtuels	installé

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

Toute autre modification est optionnelle.

---

 Utilisez les disques durs d'annulation pour ne pas enregistrer les modifications effectuées durant une procédure ou un chapitre.

---

# Création d'un bac à sable

Dans cette section, vous allez examiner comment créer un bac à sable basé sur Virtual PC 2007. Il est présupposé que vous avez téléchargé et installé Virtual PC 2007 SP1 sur votre ordinateur.

Il y a trois étapes à réaliser :

- Création et configuration de la machine virtuelle.
- Installation du système d'exploitation.
- Installation des compléments Virtual Machine addition.

## 1. Crédation et configuration d'une machine virtuelle

La procédure suivante montre la procédure pas à pas pour la création d'une machine virtuelle. Pour réaliser cette opération, il est nécessaire que Virtual PC 2007 SP1 soit installé.

- Affichez la console **Virtual PC** en cliquant sur **Démarrer** puis sur **Tous les programmes** puis sur **Microsoft Virtual PC**.
- Dans la console **Virtual PC**, cliquez sur **Fichier** puis **Assistant Nouvel ordinateur virtuel**.
- Sur la page **Bienvenue dans l'assistant Nouvel ordinateur virtuel** de l'assistant, cliquez sur **Suivant**.
- Sur la page **Options de l'assistant**, sélectionnez l'option **Créer un ordinateur virtuel** puis cliquez sur **Suivant**.
- Sur la page **Nom et emplacement de l'ordinateur virtuel**, saisissez ou sélectionnez le chemin où le fichier vmc doit être créé puis cliquez sur **Suivant**. Par défaut pour le bac à sable **Mises en pratique** de ce livre, le chemin correspond à **d:\eni** et le nom spécifique de la machine est **win1**.

---

 Chaque machine virtuelle est associée à au moins deux fichiers soit un fichier de configuration portant l'extension vmc que vous pouvez modifier avec un éditeur de texte et un fichier vhd qui contient l'image de la machine virtuelle. Un fichier vhd est portable d'un logiciel de virtualisation Microsoft à l'autre.

---

## Assistant Nouvel ordinateur virtuel

### Nom et emplacement de l'ordinateur virtuel

Le nom que vous spécifiez apparaîtra dans la liste des ordinateurs virtuels dans la Console Virtual PC.



Entrez le nom du fichier de l'ordinateur virtuel. Choisissez un nom qui vous permettra d'identifier la configuration matérielle ou logicielle de l'ordinateur virtuel, ou le système d'exploitation qu'il exécutera. Le fichier est automatiquement enregistré dans le dossier Mes ordinateurs virtuels. Pour choisir un emplacement différent, cliquez sur le bouton Parcourir.

Nom et emplacement :

d:\jeni\win1.vmc

Parcourir...

< Précédent

Suivant >

Annuler

- Sur la page **Système d'exploitation**, sélectionnez **Windows Server 2008** puis cliquez sur **Suivant**.

## Assistant Nouvel ordinateur virtuel

### Système d'exploitation

Sélectionnez le système d'exploitation que vous souhaitez installer sur l'ordinateur virtuel.



Le fait de sélectionner un système d'exploitation ici permet à l'Assistant de recommander les paramètres appropriés pour cet ordinateur virtuel. Si le système d'exploitation invité souhaité n'apparaît pas, sélectionnez un système d'exploitation nécessitant une quantité de mémoire équivalente, ou sélectionnez Autre.

Système d'exploitation :

Windows Server 2008 ▾

Sélection du matériel par défaut :

Mémoire :	512 Mo
Disque virtuel :	65'536 Mo
Audio :	compatible avec Vista
	Interne 16

< Précédent

Suivant >

Annuler

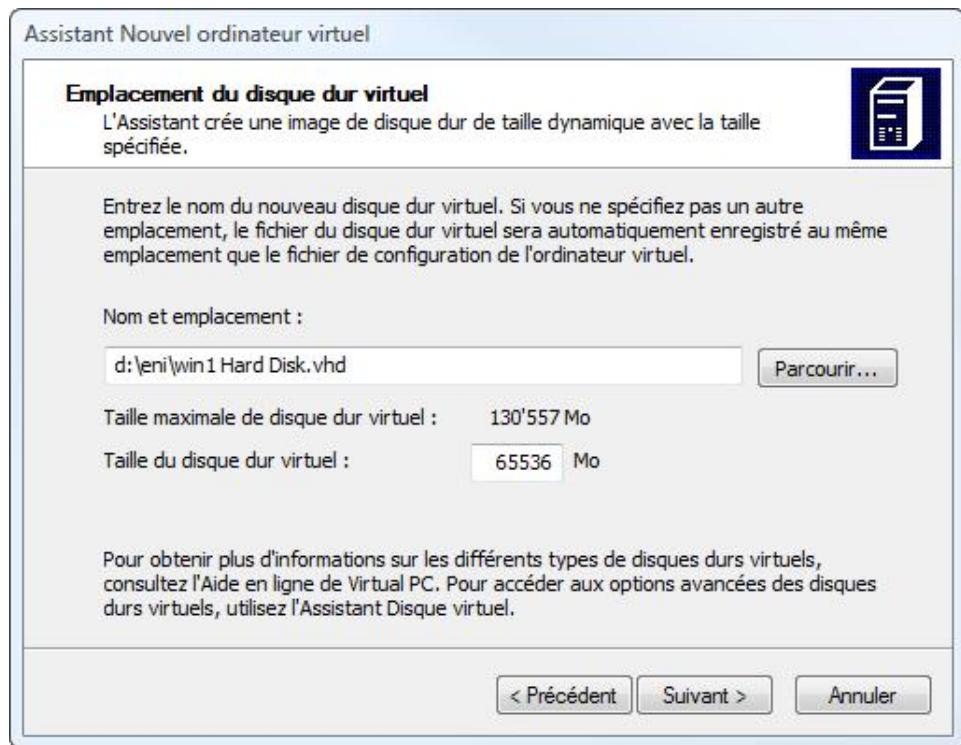
- Sur la page **Mémoire**, sélectionnez l'option **Réglant la mémoire vive** ; à l'aide du glisseur qui est apparu, choisissez une valeur comprise entre 800 Mo et 1,5 Go en fonction de la mémoire vive de votre ordinateur physique. Pour installer un Server Core, il est possible de lui attribuer uniquement 500 Mo. Par la suite, si cela s'avère nécessaire, il est toujours possible de modifier cette valeur. Ensuite cliquez sur **Suivant**.



La quantité de mémoire vive a une influence non négligeable sur la vitesse d'exécution de la machine virtuelle. Il est nécessaire de pouvoir y allouer au moins 1 Go. N'hésitez pas à arrêter des services ou des applications qui fonctionnent sur la machine physique pour libérer suffisamment de mémoire.

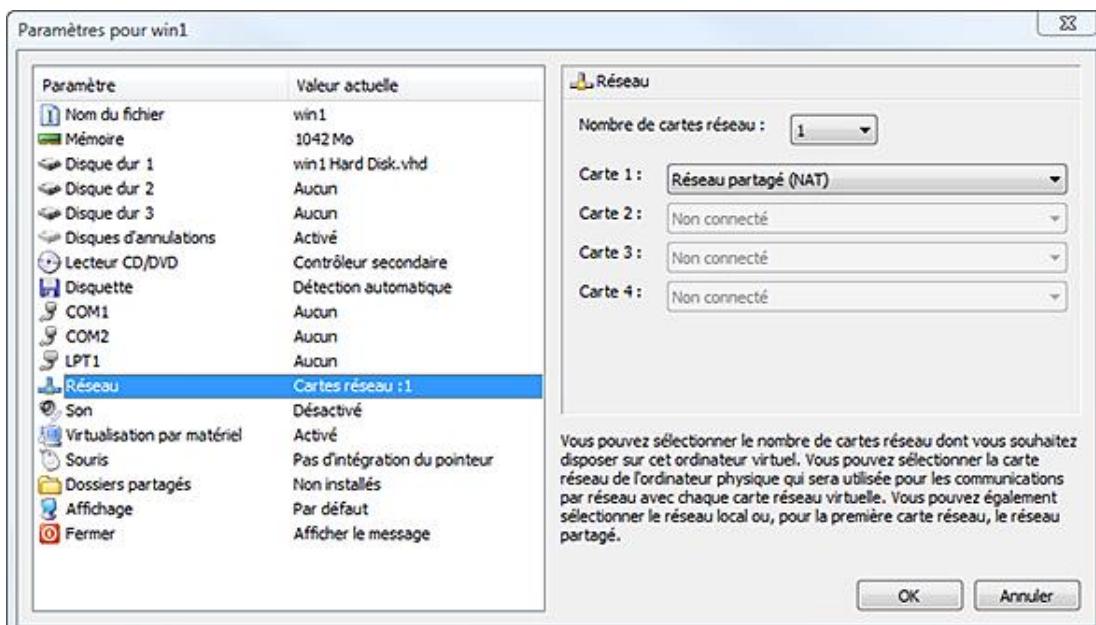
**► Afin d'éviter une dégradation importante des performances, laissez au moins 300 Mo de mémoire vive libres sur votre ordinateur hôte, soit à peu près 15 à 20 % pour 2 Go de RAM.**

- Sur la page **Options de disque dur virtuel**, sélectionnez **Un nouveau disque dur virtuel** puis cliquez sur **Suivant**.
- Sur la page **Emplacement du disque dur virtuel**, vous pouvez conserver la taille proposée pour le disque ainsi que le nom et l'emplacement. Il s'agit de l'image virtuelle dont le format est VHD (par défaut le chemin est le même que celui du fichier de configuration vmc). Puis cliquez sur **Suivant**.



- Sur la page **Fin de l'Assistant Nouvel ordinateur virtuel**, cliquez sur **Terminer**.

Votre machine virtuelle est maintenant prête, elle est ajoutée à la liste des ordinateurs virtuels. Maintenant, vous pouvez contrôler et modifier les paramètres de votre machine virtuelle en la sélectionnant dans la liste et en cliquant sur le bouton **Paramètres**.



Pour la suite du livre, lorsqu'il sera nécessaire de créer et configurer une machine virtuelle, les informations vous seront fournies dans un tableau sous la forme suivante :

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		
Système d'exploitation		
Mémoire vive		
Disque dur 1		
Taille du disque dur		
Disques d'annulation	Activer les disques d'annulation	
Réseau	Carte 1	
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	

Les disques durs d'annulation permettent de travailler et éventuellement de revenir à un état spécifique, c'est-à-dire celui de la dernière fusion entre les différents disques. Pour le réseau, vous avez la possibilité d'activer et de configurer jusqu'à 4 cartes réseaux par machine virtuelle. Généralement une carte réseau est suffisante. La virtualisation assistée par matériel devrait toujours être activée.

Pour les autres paramètres, vous pouvez les modifier en fonction de votre personnalisation.

Certains paramètres ne peuvent pas être modifiés tant que vous n'avez pas installé les compléments Virtual Machine addition dans la machine virtuelle invitée. D'autres paramètres ne peuvent pas être modifiés si la machine virtuelle fonctionne.

## 2. Installation du système d'exploitation

Virtual PC peut lire aussi bien un lecteur de CD-Rom/DVD qu'une image de disque au format ISO. Il faut savoir que le lecteur de CD-Rom/DVD est une ressource qui peut être utilisée soit par l'ordinateur hôte soit par l'ordinateur invité. Pour installer Windows, il faut au préalable capturer le lecteur de CD-Rom/DVD ou l'image ISO.

### Démarrage à partir du DVD

- Insérez le DVD de Windows Server 2008 dans l'ordinateur.
- Dans la console Virtual PC, sélectionnez la machine virtuelle **win1** et cliquez sur le bouton **Démarrer**. L'installation doit commencer, dans le cas contraire sélectionnez le lecteur DVD comme montré pour l'image ISO.

### Démarrage à partir d'une image ISO

-  L'image ISO doit être accessible depuis la console Virtual PC, évitez les chemins réseaux pour des raisons de performance.

- Dans la console **Virtual PC**, sélectionnez la machine virtuelle **win1** et cliquez sur le bouton **Démarrer**.
- Sélectionnez dans le menu **CD** de la fenêtre de la machine virtuelle qui vient de s'ouvrir l'image ISO qui contient Windows Server 2008 en utilisant la commande **Capturer l'image ISO...** comme le montre la figure suivante, notez que vous pouvez également choisir un lecteur CD/DVD spécifique.



### **Suite de l'installation (DVD et ISO)**

- Après le chargement des fichiers, choisissez la **Langue à installer**, le **Format de l'heure et de la monnaie** ainsi que le **Clavier ou méthode d'entrée** puis cliquez sur **Suivant**.



Sur l'écran suivant, vous pouvez consulter des informations supplémentaires sur l'installation en cliquant sur **A lire avant d'installer Windows**.

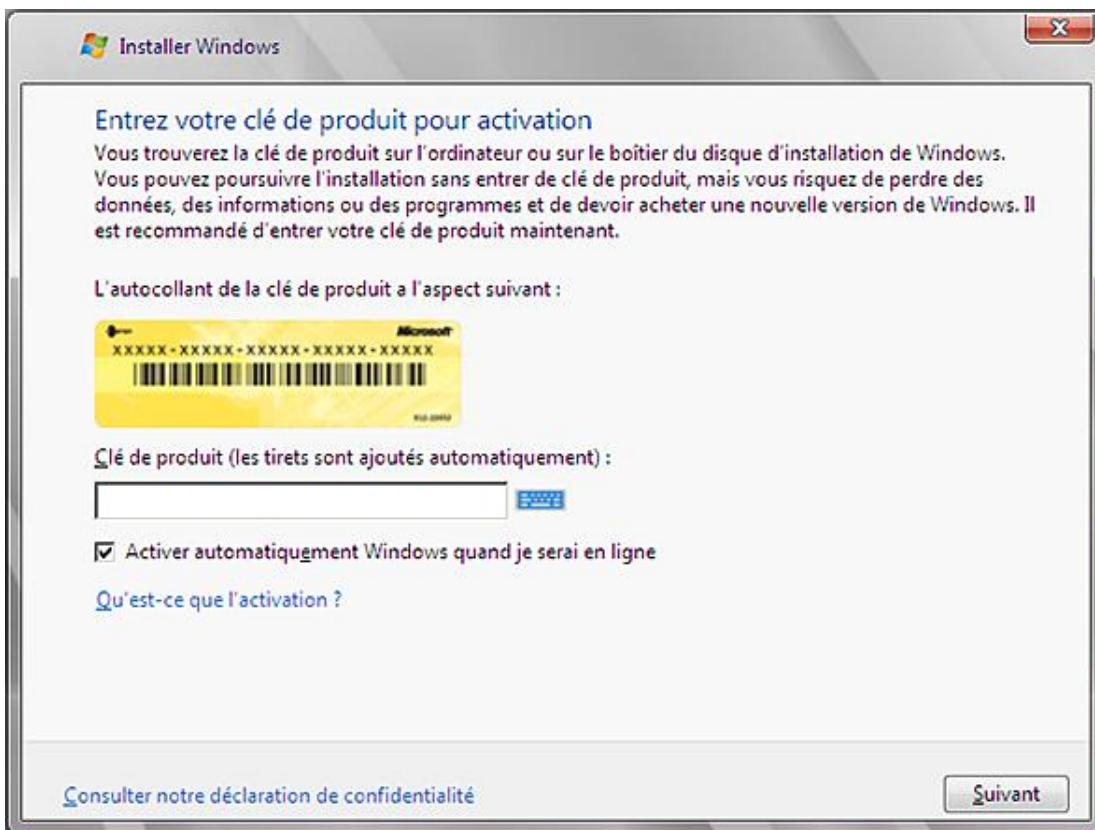
- Continuez l'installation en cliquant sur **Installer**.

S'il vous est demandé un numéro de licence uniquement :

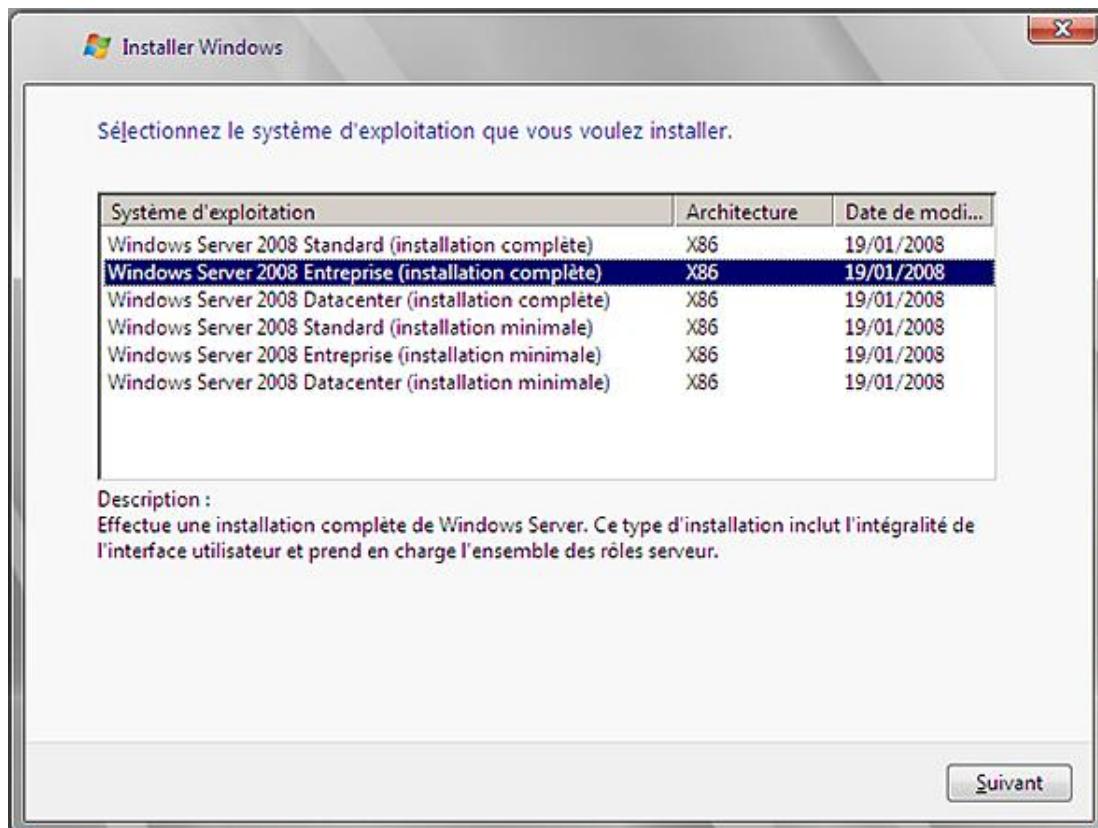
- Désélectionnez **Activer automatiquement Windows lorsque je serai en ligne** puis cliquez sur **Suivant** sans introduire un numéro de licence. Dans la boîte de dialogue **Installation de Windows** qui apparaît, cliquez sur **Non** ; vous pourrez utiliser au maximum 240 jours cette machine virtuelle sans lui donner un numéro de licence et

l'activer, ce qui est suffisant pour effectuer les tests. D'autre part, vous aurez la possibilité de sélectionner le système d'exploitation que vous voulez installer.

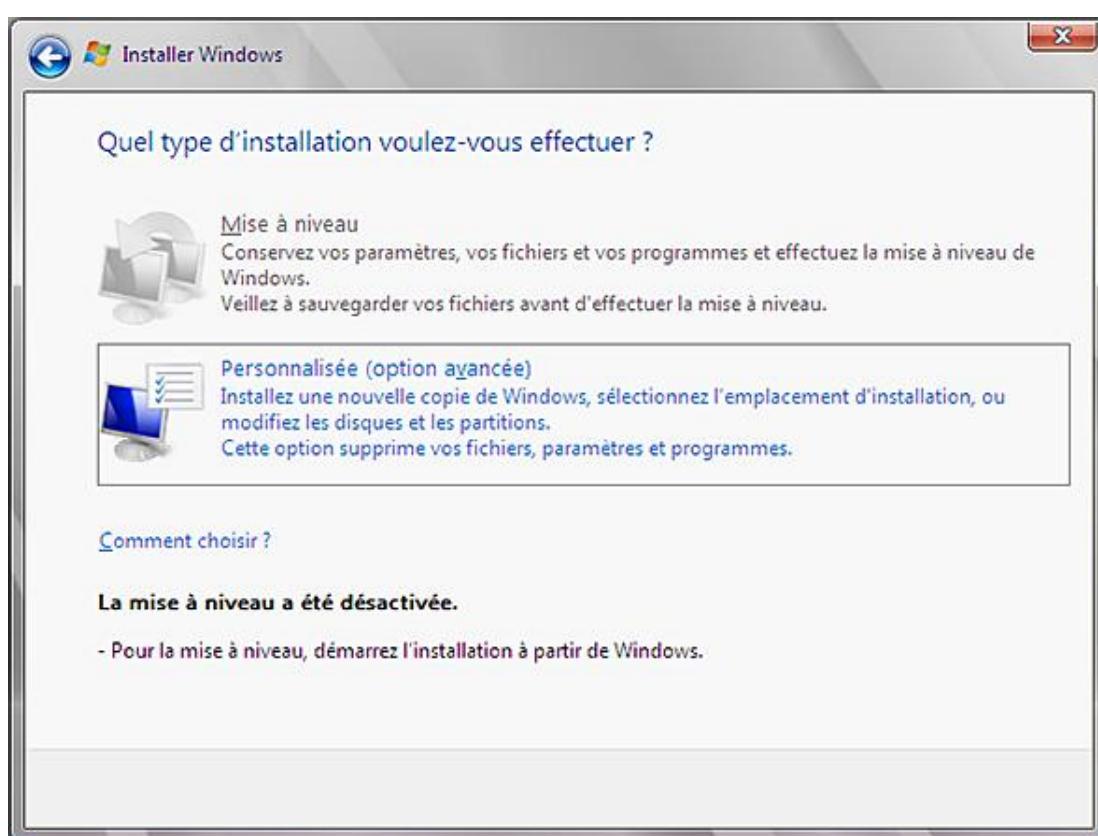
- Pour effectuer des tests, il est possible de ne pas introduire de clé, et de cliquer directement sur le bouton **Suivant**. Vous pouvez poursuivre l'installation et vous aurez 60 jours de période de grâce pour introduire une clé et activer votre serveur.
- Il est également possible d'étendre cette période de grâce trois fois et de l'étendre à 240 jours en utilisant la commande suivante dans une invite de commande en mode administrateur : `s1mgr -rearm`.
- Le fait de saisir une clé sélectionne automatiquement le système d'exploitation correspondant à ladite clé.



- Sur la page **Sélectionnez le système d'exploitation que vous voulez installer**, sélectionnez **Windows Server 2008 Entreprise (installation complète)** ou **Windows Server 2008 Entreprise (installation minimale)** puis cliquez sur **Suivant**.



- L'étape suivante consiste à accepter les termes de la licence en activant l'option **J'accepte les termes du contrat de licence**. Cliquez sur **Suivant**.
- Sur l'écran suivant, sélectionnez le type d'installation **Personnalisée (option avancée)** en cliquant dessus.



La dernière étape consiste à partitionner et sélectionner le disque dur sur lequel vous allez installer Windows. Le

formatage préalable de la partition n'est pas nécessaire ce qui réduit considérablement la durée de l'installation. Pour faire apparaître les commandes avancées, cliquez sur **Options de lecteurs (avancées)**. Ce mode permet d'ajouter des pilotes pour des contrôleurs de disque dur, de créer, détruire et formater des partitions.

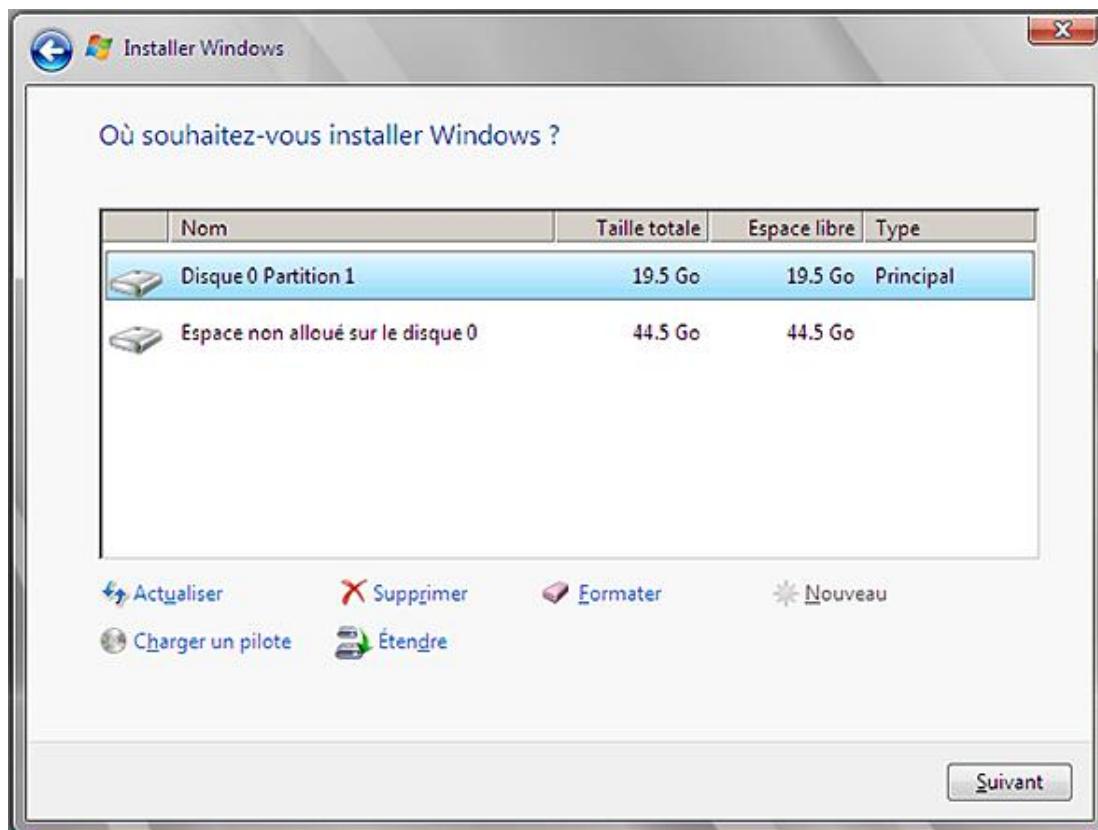
Pour ajouter un pilote de contrôleur de disque non reconnu par Windows, cliquez sur **Charger un pilote** ou appuyez sur [Ctrl] 6. Le pilote peut se trouver sur une disquette, un CD, un DVD ou une clé USB.

Windows Server 2008 ne crée que des partitions dites **primaires**, c'est-à-dire qui ne contiennent qu'un lecteur logique par partition et qui peuvent être **amorçables**. Il n'y a pas d'inconvénient à créer plusieurs partitions lors de l'installation.

➤ Pour les exercices du livre, chaque machine virtuelle dispose de deux partitions.

- Sélectionnez le disque et cliquez sur **Nouveau** pour créer une partition avec une taille de 20 Go ou 20 000 Mo puis cliquez sur **Suivant**.

➤ Sur un serveur de production, la taille de cette partition devrait être d'au moins 40 Go.



Votre travail est terminé, l'installateur va maintenant installer sur le disque tous les programmes et utilitaires dont l'administrateur a besoin.

➤ Tous les packages des rôles et des fonctionnalités sont stockés sur le disque et installés à la demande.

À la fin de l'installation, l'ordinateur redémarre.

#### a. Configuration initiale pour une installation complète

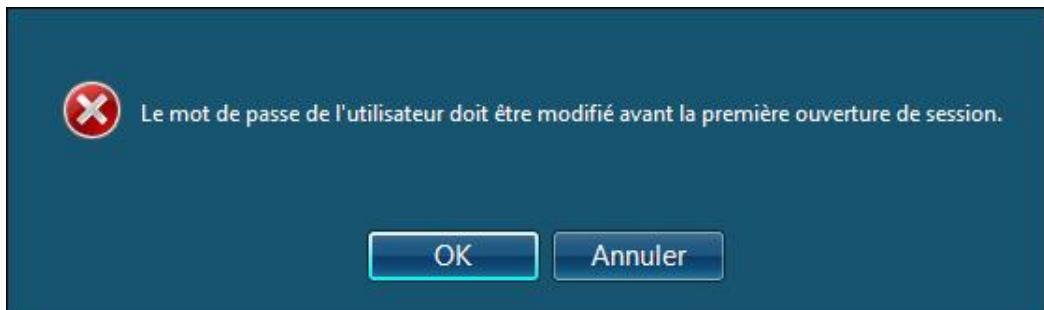
Après le redémarrage, Windows va finir l'installation. Pour ouvrir une session, il faut définir un mot de passe pour le compte administrateur local de l'ordinateur. Ce mot passe doit être complexe c'est-à-dire :

- Avoir une longueur d'au moins 6 caractères.
- Contenir des caractères d'au moins 3 des 4 catégories suivantes :

- majuscules A à Z ;
- minuscules a à z ;
- nombre 0 à 9 ;
- caractères non alphabétique (@, \$, !, %, &, ...).

➤ Cette règle des stratégies de sécurité est exécutée par défaut.

- Sur l'écran qui indique que le mot de passe de l'utilisateur doit être modifié, cliquez sur **OK**.



➤ La convention utilisée tout le long du livre concernant les mots de passe est d'utiliser le même mot de passe, à savoir **Pa\$\$word**, pour tous les utilisateurs.

- Saisissez deux fois **Pa\$\$word**, puis cliquez sur la flèche horizontale.



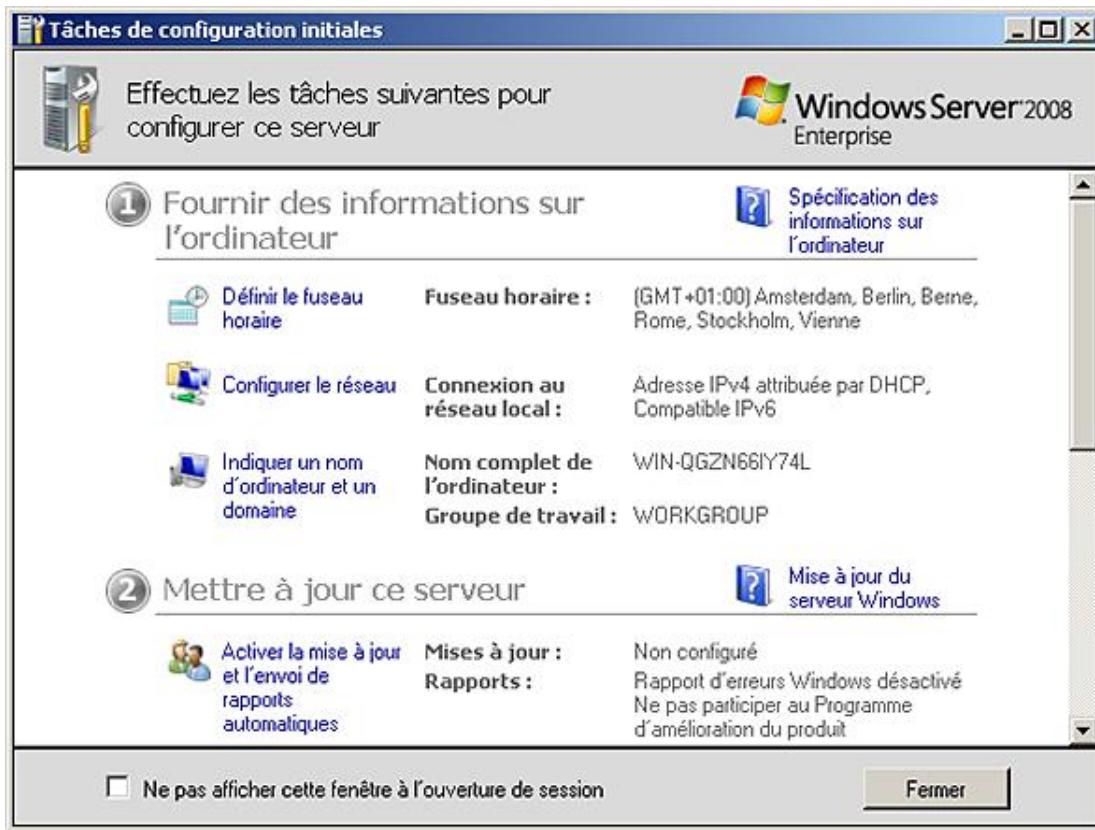
- Sur l'écran **Votre mot de passe a été changé**, cliquez sur **OK** pour vous loguer en tant qu'administrateur local.

Dès que le bureau est chargé, vous pouvez commencer la configuration initiale qui comprend trois parties :

- Informations à fournir à l'ordinateur.

- Mise à jour du serveur.
- Personnalisation du serveur.

Dans ce livre, seule la partie **Informations à fournir** nous intéresse car elle permet de modifier le nom de l'ordinateur, définir le fuseau horaire, configurer le réseau et indiquer un domaine.



### **Configurer l'adresse IP de la carte réseau**

Par défaut, le protocole IPv4 est configuré pour recevoir une adresse IP provenant d'un serveur DHCP. Pour lui attribuer une adresse IP statique, veuillez suivre la procédure suivante :

- Dans **Tâches de configuration initiales**, cliquez sur **Configurer le réseau**. Vous pouvez aussi directement saisir **ncpa.cpl** dans la zone **Rechercher** du menu **Démarrer**.
- Dans la fenêtre **Connexions réseau**, double cliquez sur l'icône représentant la carte réseau dont vous voulez modifier les paramètres IP.
- Sur l'onglet **Général** de la boîte de dialogue **Etat de connexion au réseau local**, cliquez sur **Propriétés**.
- Sur l'onglet **Gestion de réseau** de la boîte de dialogue **Etat de connexion au réseau local**, double cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
- Dans la boîte de dialogue **Propriétés de Protocole Internet version 4 (TCP/IPv4)**, sélectionnez l'option **Utiliser l'adresse IP suivante** puis remplissez les champs **Adresse IP**, **Masque de sous réseau** et éventuellement **Serveur DNS préféré**.
- Cliquez deux fois sur **OK** puis sur **Fermer** pour fermer les boîtes de dialogue. Enfin fermez la fenêtre **Connexions réseau**.

► Il est également possible d'utiliser la commande **netsh** comme indiqué plus loin pour un Server Core.

## **Modifier le nom de l'ordinateur**

- Dans **Tâches de configuration initiales**, cliquez sur **Indiquer un nom d'ordinateur et un domaine**. Vous pouvez aussi directement saisir **sysdm.cpl** dans **Rechercher** du menu **Démarrer**.
- Sur l'onglet **Nom de l'ordinateur** de la boîte de dialogue **Propriétés système**, cliquez sur le bouton **Modifier**.
- Remplacez le nom de la zone de texte **Nom de l'ordinateur** puis cliquez sur **OK** deux fois. Un redémarrage est requis pour que le nouveau nom soit opérationnel. Il est également possible de joindre directement un domaine sans quitter la boîte de dialogue.

---

 Il est également possible d'utiliser la commande **netdom** comme indiqué plus loin pour un Server Core.

---

## **Joindre un domaine**

- Dans **Tâches de configuration initiales**, cliquez sur **Indiquer un nom d'ordinateur et un domaine**. Vous pouvez aussi directement saisir **sysdm.cpl** dans la zone **Rechercher** du menu **Démarrer**.
- Sur l'onglet **Nom de l'ordinateur** de la boîte de dialogue **Propriétés système**, cliquez sur le bouton **Modifier**.
- Dans la zone **Membre d'un**, sélectionnez l'option **Domaine** puis saisissez le nom du domaine désiré dans la zone de texte avant de cliquer sur **OK**. Indiquez l'identité d'un utilisateur/administrateur du domaine pour faire rentrer l'ordinateur dans le domaine et attendez la boîte de dialogue qui vous indique que l'ordinateur a joint le domaine. Un redémarrage est requis.

---

 Il est également possible d'utiliser la commande **net join** comme indiqué plus loin pour un Server Core.

---

## **b. Configuration initiale d'une installation avec l'option Core**

Après le redémarrage, Windows va finir l'installation. Pour ouvrir une session, il faut définir un mot de passe pour le compte administrateur local de l'ordinateur. Ce mot passe doit être complexe c'est-à-dire :

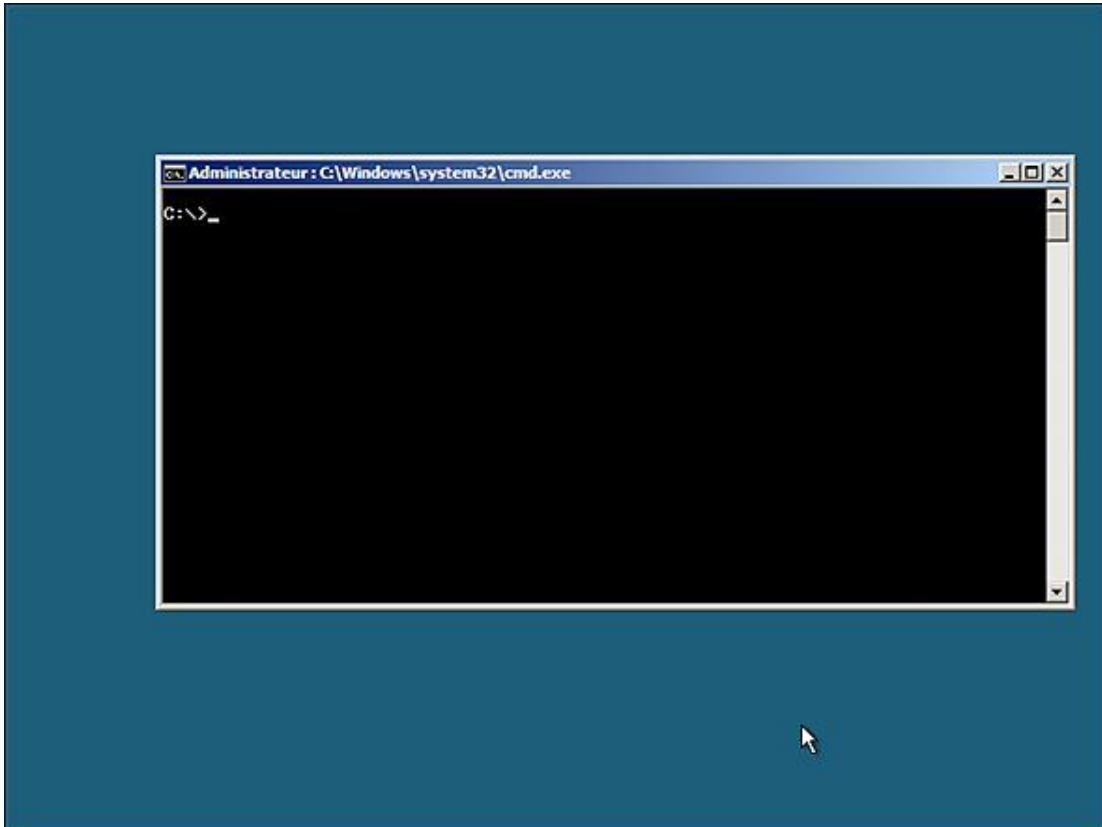
- avoir une longueur d'au moins 6 caractères ;
- contenir des caractères d'au moins 3 des 4 catégories suivantes :
  - majuscules A à Z ;
  - minuscules a à z ;
  - nombre 0 à 9 ;
  - caractères non alphabétique (@, \$, !, %, &, ...).

---

 Cette règle des stratégies de sécurité est exécutée par défaut.

---

L'image suivante montre le bureau d'une édition Entreprise installée avec l'option Core.



Avant de pouvoir utiliser votre serveur, il faut encore le configurer. Cette opération se fait manuellement via l'invite de commandes. La configuration consiste à modifier en priorité et si nécessaire les paramètres :

- du fuseau horaire ;
- de l'adressage IP ;
- d'activation de Windows Server 2008.
- du nom de l'ordinateur.
- de l'appartenance à un domaine ou un groupe de travail

Dans un second temps, elle consiste à activer les outils de gestion et à configurer le pare-feu afin d'utiliser des outils graphiques pour la gestion comme :

- le Bureau distant ;
- la gestion distante du pare-feu ;
- la gestion à distance via une console MMC ;
- l'activation de Windows RemoteShell.

Enfin certaines commandes sont utiles à connaître pour :

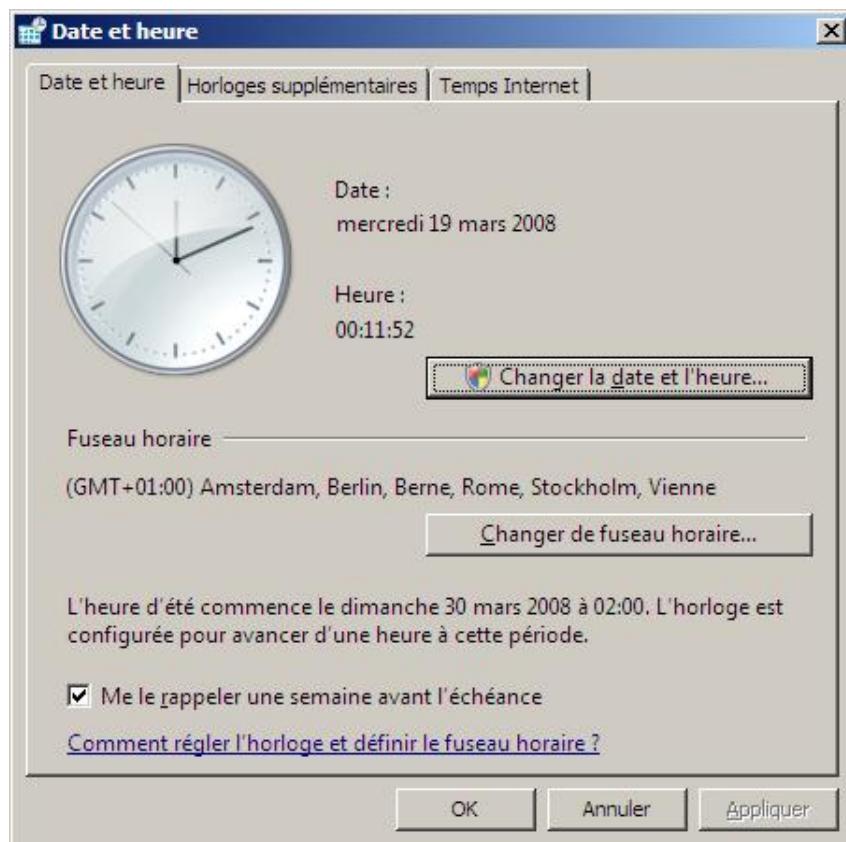
- Activer les mises à jour automatiques.
- Modifier le mot de passe de l'administrateur local.
- Modifier les paramètres régionaux.

- Se déconnecter du serveur.
- Redémarrer un serveur.
- Arrêter le serveur.

### **Configuration du fuseau horaire**

Par défaut, le fuseau horaire sélectionné est celui qui est défini avec le format de l'heure et de la monnaie lors de l'installation. Normalement, il n'est pas nécessaire de le modifier, dans le cas contraire il doit être modifié manuellement. Malheureusement il n'existe pas de commande pour le modifier, l'opération consiste à appeler l'applet du panneau de configuration permettant de modifier la date, l'heure et le fuseau horaire.

- Dans l'invite de commande, saisissez **control timedate.cpl** puis appuyez sur [Entrée].



- Dans la boîte de dialogue **Date et heure**, cliquez sur **Changer de fuseau horaire...**
- Dans la boîte de dialogue **Paramètres de fuseau horaire**, sélectionnez le bon fuseau horaire et cochez **Ajuster l'horloge pour l'observation automatique de l'heure d'été** si vous y êtes soumis, puis cliquez sur **OK** deux fois.

► Il est également possible de changer la date et l'heure pendant cette opération, ce qui est inutile si le serveur doit rejoindre un domaine.

### **Configuration de l'adressage IP**

Par défaut, l'adressage IP est configuré de manière à recevoir une **adresse IP** provenant d'un serveur **DHCP**.

S'il faut attribuer une **adresse IP statique au serveur**, il faut utiliser la commande `netsh`.

► Il n'est pas possible d'appeler l'applet correspondant **ncpa.cpl**.

- Pour configurer une adresse **IP statique** saisissez dans l'invite de commande :

```
Netsh interface ipv4 show interfaces
```

Le résultat affiche la liste des interfaces logiques et physiques. Notez la valeur **Idx** de la carte réseau dont vous voulez modifier l'adresse IP.

```
netsh interface ipv4 set address name=<Idx> source=static address=<adresseIP>
mask=<MasquedeSousRéseau> gateway=<PasserelleParDéfaut>
```

```
netsh interface ipv4 add dnsserver name=<Idx> address=<AdresseIPDNS>
index=<PositionDuServeurDNS>
```

Si vous n'avez qu'un seul serveur DNS, la valeur de l'index est égale à 1. Sinon ressaisissez cette dernière commande avec l'adresse du second serveur DNS en y incrémentant la valeur de l'index de 1.

```
C:\>netsh interface ipv4 show interface
Idx  Mét  MTU  État          Nom
2    10   1500  connected    Connexion au réseau local
1    50   4294967295  connected  Loopback Pseudo-Interface 1

C:\>netsh interface ipv4 set address name=2 source=static address=172.30.1.142 m
ask=255.255.255.0 gateway=172.30.1.1

C:\>netsh interface ipv4 add dnsserver name=2 address=172.30.1.1 index=1

C:>
```

Pour recevoir une adresse IP provenant d'un serveur DHCP :

```
netsh interface ipv4 show interfaces
```

Le résultat affiche la liste des interfaces logiques et physique. Notez la valeur **Idx** de la carte réseau à modifier.

```
netsh interface ipv4 set address name=<Idx> source=dhcp
netsh interface ipv4 delete dnsserver name=<Idx> all
```

### **Activation de Windows Server 2008**

Pour activer Windows Server 2008 via Internet depuis le serveur, saisissez dans l'invite de commande Slmgr.vbs -ato.

Pour activer Windows Server 2008 depuis une autre machine, saisissez la commande suivante :

```
Slmgr.vbs <NomDuServeur> <NomdeL'administrateur> <MotdePasse Administrateur>
-ato
```

### **Renommer l'ordinateur**

- Pour renommer l'ordinateur, saisissez les commandes suivantes dans l'invite de commande :

```
Netdom renamecomputer %hostname% /NewName :<NouveauNomDeL'Ordinateur>
```

- À la question de l'avertissement **Voulez-vous continuer (O ou N) ?**, saisissez **O**.

Il faut redémarrer l'ordinateur pour que le nouveau nom soit pris en compte : shutdown /r /t 0

```

C:\Administrator : C:\Windows\system32\cmd.exe
D:\>hostname
Mercure

D:\>netdom renamecomputer Mercure /NewName:Jupiter
Cette opération renommera l'ordinateur Mercure
en Jupiter.

Certains services, tels que l'Autorité de certification, sont basés sur un nom
d'ordinateur fixe. Si des services de ce type sont en cours d'exécution sur
Mercure, une modification du nom de l'ordinateur risque d'avoir
un impact négatif.

Voulez-vous continuer (O ou N) ?
o
Vous devez redémarrer l'ordinateur pour terminer l'opération.

L'opération s'est bien déroulée.

D:\>shutdown /r /t 0

```

## **Joindre un domaine**

Pour joindre un domaine, il faut saisir les commandes suivantes :

```
netdom join <NomDel'Ordinateur> /domain :<NomDuDomaine> /userd:<Nomde
l'Administrateur> /passwordd :<MotDePasse> ou *
```

- Pour le mot de passe, il est préférable d'utiliser l'étoile \* au lieu de saisir le mot de passe qui serait alors en clair. Le mot de passe vous sera demandé à l'exécution de la commande. Il est obligatoire de saisir l'option **/passwordd** sinon le résultat de la commande est en échec.

---

Il est possible de le placer directement dans une Unité d'Organisation avec l'option : **/OU :<CheminDel'Unitéd'Organisation>**.

Par défaut le serveur est placé dans le container Computer.

Il est possible de forcer l'ordinateur à redémarrer automatiquement à la fin de l'opération avec l'option **/Reboot :<DuréeEnSecondes>**.

- 
- Le groupe des administrateurs de domaine est automatiquement ajouté au groupe des administrateurs locaux.

```

C:\Administrator : C:\Windows\system32\cmd.exe
C:\>netdom join jupiter /domain:pffc /ou:ou=book,dc=pffc,dc=ch /userd:pffc\admin
istrator /passwordd:* /REBoot:30
Tapez le mot de passe associé à l'utilisateur du domaine :

L'opération s'est bien déroulée.

C:\>

    Vous allez être déconnecté.

        Arrêt en cours en raison d'une modification
        d'appartenance de domaine initiée par
        Administrateur.

        Fermer

```

Pour quitter un domaine :

```
netdom remove <NomDel'Ordinateur> /userD :<Nomdel'AdministrateurDeDomaine>
/passwordd :*
```

```
shutdown /r /t 0
```

## **Activation du bureau à distance**

Pour activer le bureau à distance, les commandes sont les suivantes :

```
cscript %windir%\system32\scregedit.wsf /ar 0
```

Active le bureau à distance, 0 signifie activation et 1 désactivation. L'accès est permis uniquement pour des clients distants Windows Server 2008 ou Windows Vista (RDP 6.1).

```
cscript %windir%\system32\scregedit.wsf /cs 0
```

Cette dernière commande permet également un accès avec des clients Windows Server 2003 ou Windows XP en utilisant le protocole RDP 6.0 qui est moins sécurisé.

 Il est recommandé d'activer le bureau à distance une fois que l'ordinateur a joint le domaine sinon il faut désactiver la règle du pare-feu **Bureau à distance (TCP-Entrée)** du profil **public** et ressaïsir la commande.

## **Autoriser la gestion du pare-feu à distance**

Afin de simplifier l'accès au Server Core, il peut être utile d'autoriser la gestion du pare-feu à distance. Cela permettra par la suite d'utiliser l'interface graphique au lieu de la commande netsh.

Pour autoriser l'accès à distance du pare-feu, saisissez la commande :

```
netsh advfirewall set currentprofile settings remotemanagement enable
```

## **Autoriser la gestion à distance à l'aide de la console MMC**

Par défaut, il n'est pas possible d'utiliser une console MMC pour gérer un Server Core, il est nécessaire d'autoriser la console MMC dans le pare-feu en tapant la commande suivante :

```
netsh advfirewall firewall set rule group="Administration distante"  
new enable=yes
```

 Il est possible d'utiliser l'interface graphique du pare-feu et d'activer les trois règles qui commencent par **Administration à distance**.

## **Activer Windows RemoteShell**

- Saisissez la commande suivante : winrm quickconfig

## **Activer les mises à jour automatiques**

Par défaut, le serveur n'est pas configuré pour aller chercher des mises à jour. Il faut saisir la commande `cscript %windir%\system32\scregedit.wsf /au 4` pour l'activer.

4 pour activer 1 pour désactiver les mises à jour automatiques

Si le serveur entre dans un domaine, ces paramètres devraient être configurés par une stratégie de groupe.

## **Modification du mot de passe administrateur**

- Pour modifier le mot de passe de l'administrateur local, saisissez la commande suivante : `net user administrateur * puis appuyez sur [Entrée]`.
- Saisissez le nouveau mot de passe puis appuyez sur [Entrée].
- Confirmez le mot passe en le retapant puis appuyez sur [Entrée].

## **Modifier les paramètres régionaux**

- S'il est nécessaire de modifier les paramètres régionaux, saisissez la commande control intl.cpl.

### **Déconnexion**

- Pour vous déconnecter, saisissez logoff.

### **Redémarrer le serveur**

- Pour redémarrer le Server Core, saisissez la commande shutdown /r /t 0. La valeur du paramètre /t indique le nombre de secondes avant le redémarrage.

### **Arrêter le serveur**

- Pour arrêter le Server Core, saisissez la commande shutdown /s /t 0.

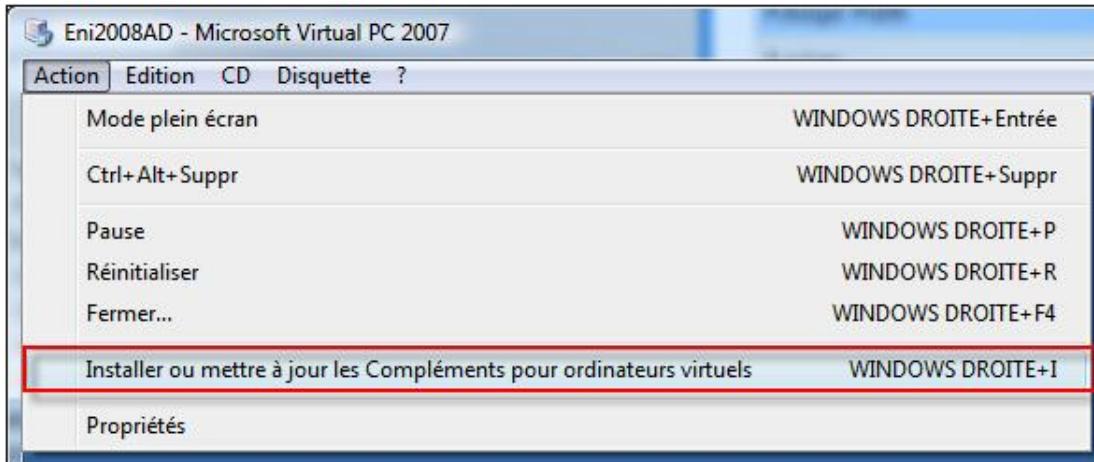
## **3. Installation des compléments pour ordinateurs virtuels**

Pour éliminer l'effet indésirable de la capture du curseur de la souris et améliorer la vitesse de réaction il est indispensable d'installer les compléments pour ordinateur virtuel. Ceux-ci sont développés par Microsoft et adaptés au système d'exploitation de l'ordinateur invité. Pour une liste complète des systèmes d'exploitation supportés, consultez la documentation en ligne de Microsoft. Parmi les améliorations apportées par les compléments pour ordinateur virtuel, on peut noter que :

- Il est possible d'effectuer des opérations de **copier/coller** entre l'ordinateur hôte et l'ordinateur virtuel.
- Il est possible d'effectuer des opérations de **glisser/déplacer** entre l'ordinateur hôte et l'ordinateur virtuel.
- L'horloge de l'ordinateur virtuel se synchronise par rapport à l'ordinateur hôte.
- Une amélioration sensible en terme de vitesse.
- Il est possible de paramétrier l'option **dossiers partagés**.

### **a. Installation des compléments pour ordinateurs virtuels pour une installation complète**

- Démarrez la machine virtuelle et connectez-vous.
- Dès que le Bureau de la machine virtuelle apparaît, appuyez sur la touche hôte de Virtual PC pour sortir de la machine virtuelle puis cliquez sur le menu **Action - Installer ou mettre à jour les Compléments pour ordinateurs virtuels** comme le montre la copie d'écran suivante :



- Sur la boîte de dialogue qui apparaît, cliquez sur **Continuer**.
- Sur la boîte de dialogue **Exécution automatique**, cliquez sur **Exécuter setup.exe**.
- Sur la page de bienvenue de l'assistant **Virtual Machine Additions**, cliquez sur **Next**.
- Sur la page **Setup Completed**, cliquez sur **Finish**.
- Sur la boîte de dialogue qui vous demande de redémarrer votre ordinateur, cliquez sur **Yes**.

### b. Installation des compléments pour ordinateurs virtuels pour une installation minimale

 Au préalable assurez-vous que la case à cocher **Activer la carte audio** du paramètre **son** a été désactivée dans les paramètres de la machine virtuelle.

- Démarrez la machine virtuelle et connectez-vous.
- Dès que l'invite de commande apparaît, appuyez sur la touche hôte de Virtual PC pour sortir de la machine virtuelle puis cliquez sur le menu **Action - Installer ou mettre à jour les Compléments pour ordinateurs virtuels**, l'assistant ne démarre pas ! Il faut le lancer manuellement.
- Dans l'invite de commande saisissez **d:** puis appuyez sur [Entrée].
- **cd windows** puis appuyez sur [Entrée].
- **FRAVirtualMachineAdditions.msi** puis appuyez sur [Entrée].
- Sur la boîte de dialogue qui apparaît, cliquez sur **Continuer**.
- Sur la boîte de dialogue **Exécution automatique**, cliquez sur **Exécuter setup.exe**.
- Sur la page de bienvenue de l'assistant **Virtual Machine Additions**, cliquez sur **Next**.
- Sur la page **Setup Completed**, cliquez sur **Finish**.
- Sur la boîte de dialogue qui vous demande de redémarrer votre ordinateur, cliquez sur **Yes**.

### c. Optimisation pour Virtual PC 2007 sans Service Pack uniquement

Une fois les **compléments pour ordinateurs virtuels installés**, il est possible d'améliorer l'affichage de l'ordinateur virtuel pour que le contenu d'une fenêtre déplacée soit toujours visible et que le curseur de la souris ne soit pas toujours visible à l'écran lorsque vous quittez l'ordinateur virtuel.

- Ces deux procédures ne s'appliquent que pour une édition complète.

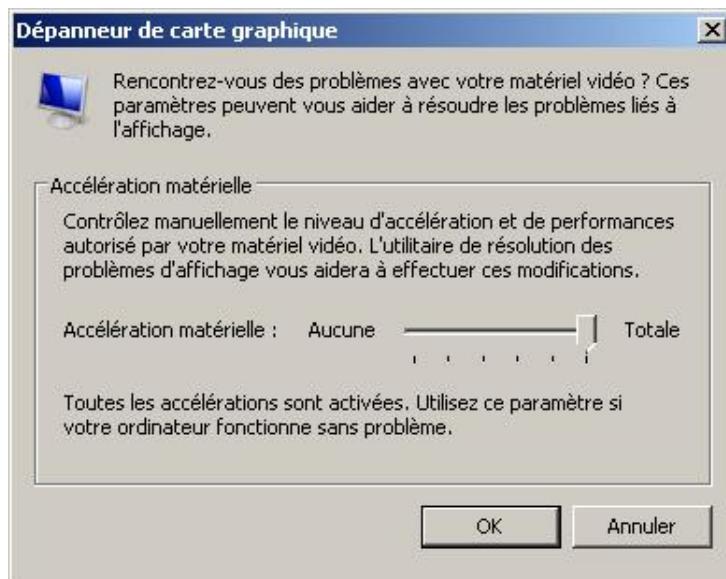
Pour modifier l'affichage du contenu de la fenêtre, il faut être connecté sur l'ordinateur invité.

- Cliquez sur **Démarrer**, puis sélectionnez **Ordinateur** puis avec le bouton droit de la souris faites apparaître le menu contextuel et cliquez sur **Propriétés**.
- Dans la boîte de dialogue **Système**, cliquez sur **Paramètres systèmes avancés**.
- Dans la boîte de dialogue **Propriétés système**, sur l'onglet **Paramètres systèmes avancés**, cliquez sur **Paramètres**.
- Dans la boîte de dialogue **Options de performances**, onglet **Effets visuels**, sélectionnez **Ajuster afin d'obtenir la meilleure apparence** ou gardez que l'option **Afficher le contenu des fenêtres pendant leur déplacement** est sélectionnée. Puis cliquez sur **OK**.

- Il est également possible pour des tests de modifier dans l'onglet **Avancé** de la boîte de dialogue **Options de performances** pour les **Performances des applications** la sélection sur **Les programmes** au lieu de **Les services d'arrière-plan**.

Pour modifier l'affichage du curseur de la souris, il faut être connecté sur l'ordinateur invité.

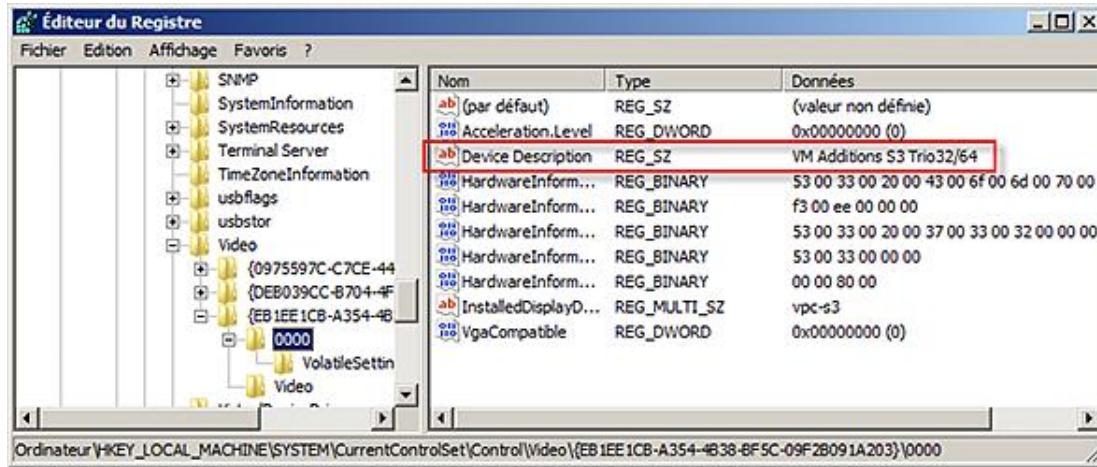
- Sur un espace vide du bureau, cliquez avec le bouton droit de la souris pour faire apparaître le menu contextuel puis cliquez sur **Personnaliser**.
- Dans la boîte de dialogue **Personnalisation**, cliquez sur **Paramètres d'affichage**.
- Dans la boîte de dialogue **Paramètres d'affichage**, cliquez sur **Paramètres avancés**.
- Dans la boîte de dialogue **Propriétés de (Ecran par défaut) et VM Additions S3 Trio32/64** sélectionnez l'onglet **Résolution des problèmes** puis cliquez sur **Modifier les paramètres**.
- Sur la boîte de dialogue **Dépanneur de carte graphique**, positionnez le curseur sur **Totale** comme le montre l'image suivante puis cliquez sur **OK** trois fois.



Sur une édition Core, il est seulement possible de modifier l'accélération matérielle de la carte graphique de la

manière suivante :

- Cliquez sur **Démarrer**, saisissez **regedit** dans la zone **Rechercher** puis appuyez sur [Entrée].
- Déplacez-vous jusqu'à **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Video**.
- Parmi les GUID recherchez celui qui affiche la valeur **VM Additions S3 Trio32/64** comme le montre l'image suivante :



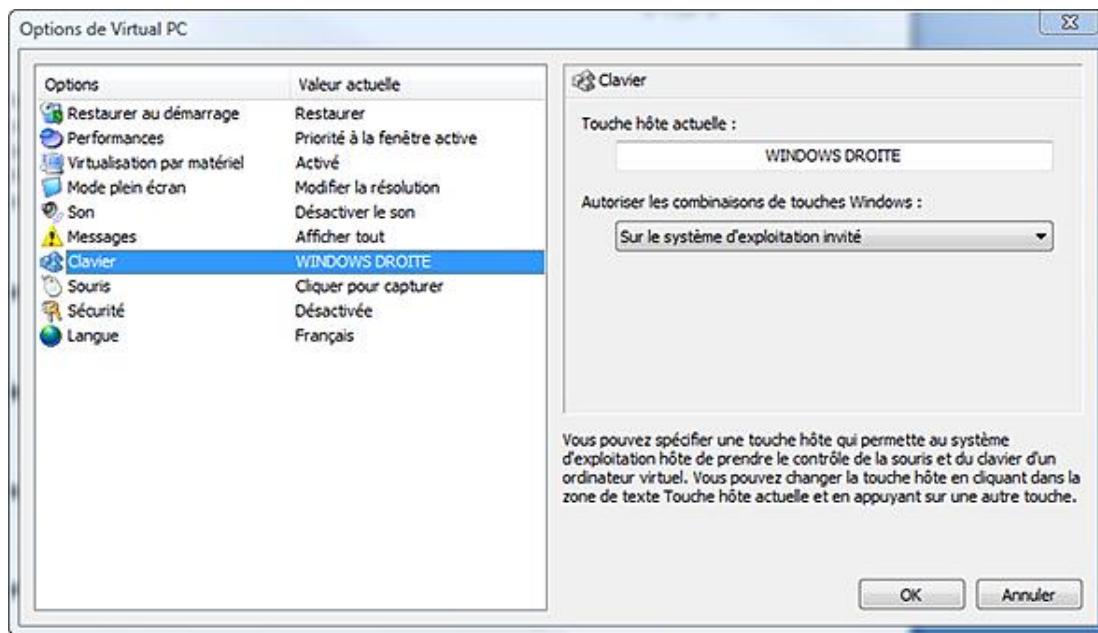
- Puis modifiez ou créez une clé appelée **Acceleration.Level** de type **REG\_DWORD** et assignez-lui une valeur de 0.
- Fermez **regedit**.
- Redémarrez votre ordinateur en tapant la commande `shutdown /r /f /t 0` suivie de [Entrée].

# Quelques astuces pour utiliser Virtual PC

## 1. La touche hôte

Il est nécessaire de connaître la touche hôte qui permet de simuler [Alt][Ctrl], par défaut il s'agit de la touche [Alt Gr]. En fonction des types de clavier, voire des personnes, il peut être utile de modifier la touche hôte grâce à la procédure suivante :

- Cliquez sur **Options** du menu **Fichier** de la console Virtual PC pour faire apparaître la boîte de dialogue suivante :



- Dans les **Options**, cliquez sur **Clavier**, puis cliquez dans la zone de texte appelée **Touche hôte actuelle** pour qu'elle dispose du focus. Ensuite appuyez sur une touche, pour ma part j'utilise la touche **Windows Droite** (le nom change), et appuyez sur **OK**.

## 2. Simuler [Alt][Ctrl][Suppr]

Pour simuler ces touches, appuyez sur la touche [hôte][Suppr].

## 3. Passer en mode plein écran ou en mode fenêtre

Il vous faut utiliser la touche [hôte][Entrée].

---

► Vous remarquez que le curseur de la souris ne peut sortir de la zone de l'ordinateur virtuel sans que vous appuyiez sur la *touche hôte* qui simule [Alt][Ctrl] dont on a parlé plus haut tant que vous n'avez pas installé les **compléments d'ordinateurs virtuels**.

---

## Bac à sable

Il peut paraître surprenant de parler de bac à sable dans un livre professionnel alors que cette expression est réservée aux enfants. Ce terme largement utilisé chez nos voisins anglo-saxons est moins rigoureux que banc de test et correspond mieux à l'idée que je me fais du lecteur, soit quelqu'un de curieux qui a besoin de pouvoir tester rapidement les nouvelles connaissances acquises et qui expérimente ses connaissances sur ses propres scénarios.

Pour effectuer tous les exercices et les démonstrations présentées dans ce livre, il est nécessaire de créer plusieurs bacs à sable soit :

- Un bac à sable appelé **Mises en pratique** dans ce livre pour effectuer les démonstrations et les procédures montrées dans la partie théorique.
- Un bac à sable appelé **Atelier** dans ce livre pour effectuer les exercices récapitulatifs du chapitre Travaux pratiques.

La création des bacs à sable est montrée pas à pas plus loin dans ce chapitre. Selon la complexité du scénario, il peut être nécessaire d'utiliser plusieurs ordinateurs, il est donc nécessaire de les virtualiser pour éviter de devoir disposer de plusieurs ordinateurs.

La virtualisation permet de faire tourner dans le même ordinateur physique des ordinateurs virtuels, donc elle permet de recréer un environnement réseau à bas coût. En contrepartie, il faut disposer d'un ordinateur puissant ayant beaucoup de RAM. Selon le logiciel de virtualisation utilisé, il est possible de créer des réseaux virtuels voire de virtualiser des systèmes d'exploitation 64 bits.

### 1. Mon propre bac à sable

Pour préparer mes séminaires, mes présentations et mes cours, etc. je dispose de plusieurs bacs à sable que je crée en fonction des situations et des besoins.

Ainsi pour l'écriture de ce livre j'utilise deux bacs à sable composés chacun de plusieurs machines virtuelles sous Windows Server 2008, Windows Vista, Windows XP et Windows 2003.

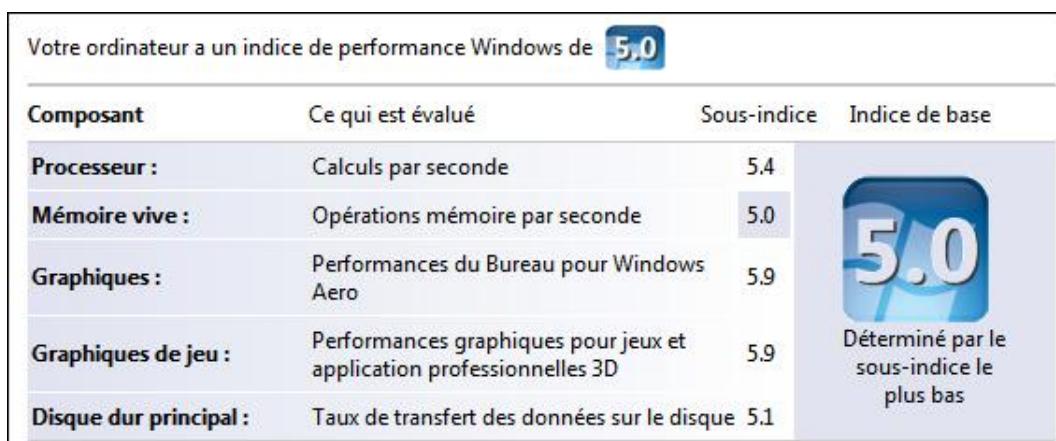
L'utilisation de la virtualisation m'a permis de réduire le nombre d'ordinateurs physiques à un seul. En dehors d'un coût d'infrastructure bas, d'une réduction de la facture d'électricité et d'un gain de place, le temps d'installation d'une machine virtuelle est réduit, son temps démarrage et son temps arrêt également.

Enfin il est également possible d'enregistrer l'état d'un ordinateur virtuel à un instant **T** puis de le recharger plus tard pour continuer à partir du point **T** enregistré.

L'utilisation d'un disque dur d'annulation permet également d'annuler toutes les modifications qui n'ont pas été enregistrées.

Mon environnement principal se compose d'un ordinateur personnalisé et assemblé en 2006 basé sur une carte mère Asus P5DWH avec un processeur Intel Core 2 Duo E6600, de 8 Go de RAM, d'un disque dur principal tournant à 7 200 tours réservé au système d'exploitation hôte (Windows Vista 64 bits), d'un second disque dur de grande capacité pour stocker mes ordinateurs virtuels et de 2 cartes graphiques reliées chacune à 2 écrans pour un total de 4 écrans.

Son indice de performance sous Windows Vista 64 bits est de 5.0 comme montré ci-dessous.



Le point sensible étant la mémoire car actuellement, il n'est pas évident de trouver des barrettes mémoire de grande capacité rapides à des prix abordables. D'autre part, l'ajout de mémoire a tendance à faire chuter l'indice Mémoire

vive sans explication. Cette configuration me semble idéale pour travailler avec un environnement virtualisé avec plusieurs machines concurrentes.

Pour mes présentations, j'utilise un ordinateur portable acheté en 2008 disposant d'un écran de 12 pouces dont la résolution max est de 1280\*800, d'un processeur Intel T9300, de 3 Go de RAM et d'un disque dur de 250 Go. Il tourne sous Windows Vista 64 bits. Cette configuration me semble être la configuration minimale pour utiliser convenablement un environnement virtualisé. Je stocke toutes mes machines virtuelles sur un disque dur USB externe de 2,5" d'une capacité de 500 Go tournant à 7 200 T/min car le disque est alimenté directement par le câble USB. Cette méthode me permet d'utiliser mes machines virtuelles aussi bien sur mon ordinateur portable que sur mon ordinateur de bureau.

## 2. Pour votre bac à sable

Pour votre propre bac à sable, il vous faut :

- un ordinateur si possible puissant ;
- un logiciel de virtualisation ;
- le logiciel Windows Server 2008.

### a. Un ordinateur puissant

Les recommandations suivantes sont indiquées uniquement dans le but de disposer d'un bac à sable rapide. Dans le cas où votre ordinateur ne dispose pas du minimum conseillé pour le processeur et la mémoire, vous pouvez toujours faire un test et, si le temps de réaction est lent, mettre à jour l'élément le plus approprié.

Concernant le processeur, les informations suivantes ne s'appliquent que pour utiliser Windows Server 2008 en tant qu'ordinateur virtuel. L'expérience montre que le processeur est l'élément qui joue le plus grand rôle pour faire tourner à une vitesse acceptable Windows Server 2008 en tant que machine virtuelle. C'est la raison pour laquelle je recommande au minimum un processeur de type Dual Core, Core 2 Duo d'Intel ou équivalent en précisant que je n'ai jamais eu l'occasion d'effectuer des tests avec les processeurs d'AMD. Les processeurs des générations précédentes ne disposant pas d'une aide à la **virtualisation assistée par le matériel** les temps de réaction sont parfois lents et aléatoires. Ce problème n'existe pas lorsque l'on installe Windows Server 2008 sur un ordinateur physique.

Pour la mémoire RAM, 2 Go est un minimum. Avec plus de RAM, vous pourrez disposer de plus de machines virtuelles concurrentes. Mon expérience indique que 4 Go ou plus semblent conseillés, mais dans ce cas, pour enlever la limite imposée par un système d'exploitation 32 bits, il est nécessaire d'utiliser un système d'exploitation 64 bits pour l'ordinateur physique et de veiller à ce que le BIOS de votre ordinateur supporte bien 4 Go ou plus.

Pour les disques durs, je recommande un disque rapide (minimum 7200 t/min) et de grande capacité. En effet, une machine virtuelle sous Windows Server 2008 utilise au minimum 8 Go d'espace disque.

Concernant les cartes vidéo, je trouve plus intéressant de pouvoir utiliser un écran supplémentaire que de disposer d'une carte graphique plus puissante.

### b. Un logiciel de virtualisation

Personnellement j'ai opté pour **Virtual PC 2007 SP1** qui est gratuit et téléchargeable depuis le site de Microsoft. **Virtual Server 2005 R2 SP1** est également un bon choix mais il tourne en tant que service. Enfin, rien ne vous empêche d'installer **Hyper-V** en tant qu'hôte ou plutôt partition principale.

D'autres logiciels de virtualisation pourraient être utilisés comme ceux proposés par VMWare mais ils ne sont pas traités dans ce livre.

## 3. Logiciels Windows

Si vous ne disposez pas d'une version de Windows Server 2008, il est toujours possible de télécharger une version d'évaluation de l'édition Entreprise (durée de 60 jours extensible à 240) sur le site de Microsoft.

Vous pouvez à la place télécharger une image virtuelle basée utilisable sur les logiciels de virtualisation cités mais elle est basée sur la Beta3 en anglais.

## **4. La configuration de l'ordinateur hôte**

Je recommande d'installer Windows XP ou mieux Windows Vista. Si vous disposez de 4 Go de RAM, il faut prévoir une version 64 bits de Windows Vista.

Si vous utilisez votre ordinateur personnel, généralement un certain nombre d'applicatifs et de services tournent en arrière-plan et consomment inutilement des ressources mémoire et processeur. Les désactiver et les réactiver peut devenir à la longue fastidieux. Si votre ordinateur est trop chargé, vous pouvez toujours acquérir un second disque ainsi qu'un système de tiroirs amovibles dont le coût est faible. L'avantage est de conserver votre disque personnel et de disposer d'un disque pour effectuer vos tests sans risquer de détruire par accident des données.

## Objectifs du chapitre

Une des grandes difficultés est de créer un environnement de test pour effectuer dans de bonnes conditions les différentes procédures ainsi que les travaux pratiques. Pour ces raisons, le début du chapitre introduit la notion de **bac à sable** puis vous explique et montre comment construire votre propre bac à sable pour effectuer les exercices et les travaux pratiques proposés dans le livre mais également pour tester vos propres scénarios, voire créer un environnement de test dans votre entreprise.

## Résumé du chapitre

Vous connaissez comment le livre est organisé, vous pouvez donc l'utiliser de manière efficiente selon vos besoins et connaissances.

De précieux conseils vous ont été dispensés pour préparer au mieux votre examen.

Il vous a été expliqué la philosophie introduite dans Windows Server 2008, puis les différentes éditions et leurs caractéristiques vous ont été décrites.

Les cinq aspects de la virtualisation vous ont été montrés et vous pouvez les décrire et conseiller sur leur cadre d'utilisation.

## Présentation des fonctionnalités

Une fonctionnalité est un composant optionnel permettant d'étendre les possibilités de Windows Server 2008. Dans Windows Server 2008, Microsoft a défini 35 fonctionnalités par défaut.

À l'installation, aucune fonctionnalité n'est installée. Une fonctionnalité s'installe soit manuellement par l'intermédiaire de l'administrateur, soit automatiquement lors de l'installation d'un rôle ou d'une autre fonctionnalité.

Si d'autres fonctionnalités ou rôles manquent pour installer correctement la fonctionnalité, l'assistant vous propose d'installer les éléments requis manquants.

Le tableau suivant résume les fonctionnalités que l'on peut installer sur une installation complète en fonction de Windows Server 2008.

Fonctionnalité	Standard	Enterprise	Datacenter	Itanium	Web
Assistance à distance	x	x	x	x	x
Base de données interne Windows	x	x	x	x	x
Chiffrement BitLocker	x	x	x	x	
Client d'impression Internet	x	x	x	x	x
Client Telnet	x	x	x	x	x
Client TFTP	x	x	x	x	
Clustering avec basculement		x	x	x	
Compression différentielle à distance RDC	x	x	x	x	
Équilibrage de la charge réseau WNLB	x	x	x	x	x
Expérience audio-vidéo haute qualité Windows (qWave)	x	x	x	x	x
Expérience utilisateur	x	x	x		x
Extension du serveur BITS	x	x	x	x	
Fonctionnalités .NET Framework 3.0	x	x	x	x	x
Fonctionnalités de sauvegarde de Windows Server	x	x	x	x	x
Gestion des stratégies de groupe	x	x	x	x	x
Gestionnaire de ressources système Windows	x	x	x	x	x
Gestionnaire de stockage amovible	x	x	x	x	
Gestionnaire de stockage pour réseau SAN	x	x	x		
Kit d'administration de Connection Manager	x	x	x		
Message Queuing	x	x	x	x	
Moniteur de port LPR	x	x	x		

MPIO ( <i>Multipath I/O</i> )	x	x	x	x	
Outils d'administration de serveur distant	x	x	x		x
Protocole PNRP ( <i>Peer Name Resolution Protocol</i> )	x	x	x	x	x
Proxy RPC sur HTTP	x	x	x	x	
Serveur iSNS ( <i>Internet Storage Name Server</i> )	x	x	x		x
Serveur SMTP	x	x	x	x	x
Serveur Telnet	x	x	x	x	x
Serveur WINS ( <i>Windows Internet Naming Service</i> )	x	x	x		
Service d'activation des processus Windows	x	x	x	x	x
Service de réseau local sans fil	x	x	x		
Services SNMP ( <i>Simple Network Management Protocol</i> )	x	x	x	x	x
Services TCP/IP simples	x	x	x	x	
Sous-système pour les applications UNIX Windows (SUA)	x	x	x	x	
Windows PowerShell	x	x	x	x	x

Le tableau suivant résume les fonctionnalités que l'on peut installer sur un Server Core en fonction de l'édition de Windows Server 2008.

Fonctionnalité	Standard	Enterprise	Datacenter	Web
Chiffrement BitLocker	x	x	x	
Client Telnet	x	x	x	x
Clustering avec basculement		x	x	
Équilibrage de la charge réseau WNLB	x	x	x	x
Expérience audio-vidéo haute qualité Windows (qWave)	x	x	x	x
Fonctionnalités de sauvegarde de Windows Server	x	x	x	x
Gestionnaire de stockage amovible	x	x	x	
MPIO ( <i>Multipath I/O</i> )	x	x	x	
Serveur WINS ( <i>Windows Internet Naming Service</i> )	x	x	x	
Services SNMP ( <i>Simple Network Management Protocol</i> )	x	x	x	x
Sous-système pour les applications UNIX Windows (SUA)	x	x	x	

## 1. Assistance à distance

L'assistance à distance permet à un expert d'aider un novice en visualisant ou partageant la session de travail du novice en utilisant un client RDP.

Le chapitre Gestion et surveillance d'une infrastructure réseau décrit en détail cette fonctionnalité.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Assistance à distance	Remote-Assistance

- Fonctionnalité d'administration pouvant être utile dans de grandes équipes.

## 2. Base de données interne Windows

La base de données interne Windows est une base de données uniquement utilisée par les services suivants :

- Service UDDI.
- AD RMS (*Active Directory Rights Management Services*).
- Service WSUS (*Windows Server Update Services*).
- Gestionnaire de ressources système Windows (WSRM pour *Windows System Resource Manager*).
- WSS V3 (*Windows SharePoint Service V3*).

Il s'agit en fait d'une version de SQL Server 2005 Embedded Edition.

Il est possible d'utiliser l'outil SQL Server Management Studio Express pour s'y connecter.

Cette fonctionnalité s'installe automatiquement dès qu'un service en fait la demande. Vous pouvez la détruire si plus aucun service ne l'utilise, mais ce n'est pas recommandé. La procédure suivante montre comment l'effacer, mais il peut subsister d'autres éléments qui sont propres à chaque application.

### Plate-forme 32 bits

```
Msieexec /x {CEB5780F-1A70-44A9-850F-DE6C4F6AA8FB} callerid=ocsetup.exe
```

### Plate-forme 64 bits

```
msiexec /x {BDD79957-5801-4A2D-B09E-852E7FA64D01} callerid=ocsetup.exe
```

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Base de données interne Windows	Windows-Internal-DB

- C'est une fonctionnalité d'infrastructure qu'il ne faut pas modifier.

## 3. Chiffrement de lecteur BitLocker

Le chiffrement BitLocker permet de chiffrer l'intégralité d'un volume disque et empêche tout accès non autorisé à ce

volume.

Le scénario le plus évident concerne l'ordinateur portable puisqu'il permet d'éviter, si l'ordinateur est volé, d'avoir accès aux données contenues sur son disque dur. Néanmoins, le scénario le plus intéressant pour les serveurs concerne les serveurs qui doivent être hautement sécurisés du fait de la nature très confidentielle des données qu'ils contiennent. Également des serveurs situés dans des lieux non protégés physiquement (pas de salle informatique, de local fermé ou d'accès contrôlé).

Le démarrage d'un serveur protégé par BitLocker ne peut avoir lieu si la clé de démarrage USB n'est pas insérée. De même, il n'est pas possible de modifier des données hors connexion.

BitLocker améliore la protection contre des attaques physiques au niveau du serveur.

- Il est nécessaire de laisser une partition au format NTFS ayant au moins 1,5 Go non chiffrée par le système BitLocker pour démarrer l'ordinateur, sans qu'il s'agisse de la partition système.

BitLocker peut utiliser une puce TPM version 1.2 ou supérieure pour améliorer la sécurité. Sinon, les clés sont stockées sur une clé USB. Pour utiliser BitLocker sans TPM, il est nécessaire de modifier la stratégie de groupe dépendant du fichier TPM.admx comprenant les paramètres suivants : **Configuration ordinateur - Modèles d'administration - Composants Windows - Chiffrement de lecteur BitLocker - Configuration du panneau de configuration : Activer les options de démarrage avancées**. Il faut au minimum un ordinateur exécutant Windows Vista.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Chiffrement de lecteur BitLocker	BitLocker

Les composants pour cette fonctionnalité sur un Server Core sont :

Fonctionnalité	Valeur de la commande
Chiffrement de lecteur BitLocker	BitLocker
Outil d'administration à distance BitLocker	BitLocker-RemoteAdminTool

- C'est une fonctionnalité de sécurité, à installer uniquement sur des serveurs qui doivent disposer d'un niveau de sécurité élevé.

## 4. Client d'impression Internet

Le client d'impression Internet utilise le protocole **IPP** (*Internet Printing Protocol*) et permet aux utilisateurs de pouvoir se connecter, gérer et imprimer des documents même lorsqu'ils sont en dehors de l'entreprise pour autant qu'un serveur Web IIS soit installé et configuré en tant que serveur d'impression.

Le chapitre Mise en œuvre de l'impression décrit en détail cette fonctionnalité.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Client d'impression Internet	Internet-Print-Client

- C'est une fonctionnalité utilisateur à réserver à un serveur disposant d'un rôle Terminal Server.

## 5. Client Telnet

Le client Telnet (*TELecommunication NETwork*) est un outil de gestion qui permet d'exécuter des commandes sur un hôte distant. Ce protocole est peu fiable car le login (nom et mot de passe) circule en clair sur le réseau. Pour offrir une meilleure sécurité au protocole Telnet, il est possible d'utiliser soit un client SSH (*Secure Shell*), soit le protocole IPSEC au lieu du protocole IP. Le projet **TeraTerm** sur [tssh2.sourceforge.jp](http://tssh2.sourceforge.jp) offre une bonne alternative au client

Telnet fourni par Microsoft.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Client Telnet	Telnet-Client

Le composant pour cette fonctionnalité sur un Server Core est :

Fonctionnalité	Valeur de la commande
Client Telnet	TelnetClient

- C'est une fonctionnalité d'administration à ne pas utiliser, lui préférer Windows Remote Shell. Néanmoins, vous pouvez utiliser le client Telnet à des fins de diagnostics de connectivité dans un réseau filtré comme par exemple "Telnet adresse IP port" permet de tester la connexion alors que l'ICMP est filtré. Une fois la fenêtre Telnet ouverte, on appuie sur [Ctrl] \$ sinon cela indique un problème de connexion.

## 6. Client TFTP (Trivial File Transfer Protocol)

Le client TFTP est une version triviale non sécurisée du protocole FTP car elle n'utilise pas d'authentification entre le client et le serveur et le protocole UDP utilisé est moins fiable que le protocole TCP. TFTP peut encore avoir sa raison d'être pour mettre à jour le système d'exploitation appelé **IOS** (*Internetwork Operating System*) du matériel Cisco dans un environnement sécurisé mais pas dans un autre environnement !

- TFTP est un protocole utilisé par le serveur de déploiement WDS et les clients PXE.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Client TFTP	TFTP-Client

- Fonctionnalité d'administration à installer uniquement en cas de besoin spécifique, telle que la mise à jour d'un microcode (firmware) sur un périphérique supportant ce protocole.

## 7. Clustering avec basculement

Le clustering avec basculement ou *clustering failover* permet d'installer les composants nécessaires à l'ordinateur afin de créer un système hautement disponible.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Clustering avec basculement	Failover-Clustering

Le composant pour cette fonctionnalité pour un Server Core est :

Fonctionnalité	Valeur de la commande
Clustering avec basculement	FailoverCluster-Core

- C'est une fonctionnalité d'infrastructure. Si vous concevez l'installation d'un serveur en haute disponibilité, alors cette fonctionnalité est à prendre en considération.

## 8. Compression différentielle à distance

La compression différentielle à distance (RDC : ici *Remote Differential Compression* et non *Remote Desktop Connection*) est un protocole client serveur de synchronisation apparu avec Windows Server 2003 R2 permettant à des applications utilisant les API (*Application Programmer Interface*) de transmettre efficacement sur des réseaux WAN des données.

L'objectif est de synchroniser des données entre le client et le serveur. Le protocole permet de détecter les parties d'un jeu de fichiers qui ont été modifiées (insertion, modification et/ou suppression) et de n'envoyer sur le réseau que ces modifications. La détection se fait à la volée et n'est pas dépendante d'une notion de version du fichier.

La compression différentielle à distance fonctionne très efficacement pour des fichiers dès 64 Ko subissant peu de modifications comme des fichiers au format Word (DOC), de messagerie (PST) ou de virtualisation (VHD).

En plus de l'installation du protocole, il est nécessaire d'avoir sur le serveur une application compatible avec ce protocole.

- Bien que la réplication DFS et l'Active Directory AD DS utilisent de manière interne le protocole RDC, il n'est pas nécessaire de l'installer.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Compression différentielle à distance	RDC

- C'est une fonctionnalité applicative, à installer avec une application qui requiert cette fonctionnalité.

## 9. Équilibrage de la charge réseau (NLB)

L'équilibrage de charge réseau ou WNLB (*Windows Network Load Balancing*) parfois appelé cluster NLB permet de répartir des requêtes entre plusieurs serveurs qui fonctionnent comme une seule entité. Cela permet d'augmenter la charge ainsi que de concevoir un système hautement disponible.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Équilibrage de la charge réseau	NLB

Le composant pour cette fonctionnalité pour un Server Core est :

Fonctionnalité	Valeur de la commande
Équilibrage de la charge réseau	NetworkLoadBalancingHeadlessServer

- C'est une fonctionnalité d'infrastructure, si vous concevez l'installation d'une ferme de serveur alors cette fonctionnalité est à prendre en considération.

## 10. Expérience audio-vidéo haute qualité Windows (qWave)

L'expérience audio-vidéo haute qualité Windows ou qWave (*Quality Windows Audio-Video Experience*) est la nouvelle plate-forme de qualité de services QOS (*Quality of Services*) incluant également les flux multimédia.

Ce protocole est adapté aussi bien aux réseaux domestiques utilisant des systèmes sans fil qu'à des entreprises.

Des API sont également disponibles pour les développeurs et les fabricants de matériel.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Expérience audio-vidéo haute qualité Windows	qWave

Le composant pour cette fonctionnalité pour un Server Core est :

Fonctionnalité	Valeur de la commande
Expérience audio-vidéo haute qualité Windows	QWAVE

-  C'est une fonctionnalité d'infrastructure, à installer avec une application qui requiert cette fonctionnalité.

## 11. Expérience utilisateur

L'expérience utilisateur permet d'ajouter des applications pour l'utilisateur afin de disposer d'un environnement de bureau plus riche ressemblant à Windows Vista.

Cette fonctionnalité est particulièrement prévue pour les utilisateurs de Terminal Server ainsi que dans le cas où un utilisateur travaillerait régulièrement sur un serveur, bien que ce dernier scénario ne soit pas recommandé.

Les applications installées sont :

- Calendrier Windows
- Windows Mail
- Lecteur Windows Media
- Windows Aero™ et autres thèmes du Bureau
- Video for Windows (prise en charge AVI)
- Galerie de photos Windows
- Windows SideShow™
- Windows Defender
- Nettoyage de disque
- Centre de synchronisation
- Magnétophone
- Table des caractères

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Expérience utilisateur	Desktop-Experience

-  C'est une fonctionnalité d'infrastructure, à n'installer que si un utilisateur régulier travaille sur le serveur ou si le rôle Terminal Server est installé.

## 12. Extensions du serveur BITS

Les extensions du serveur BITS (*Background Intelligent Transfer Service*) sont un service fonctionnant avec le serveur Web IIS qui permet de notifier les applications Web de l'arrivée de données sur un répertoire virtuel et de retourner une réponse adéquate.

Le transfert peut se faire dans les deux sens, le téléchargement ou le chargement, BITS se chargeant d'optimiser le transfert de fichiers entre le client et le serveur.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Extensions du serveur BITS	BITS

 C'est une fonctionnalité d'infrastructure applicative, à n'installer que si une application Web requiert cette fonctionnalité. Ne pas confondre avec le Service de transfert intelligent en arrière-plan utilisé entre autres par Windows Update.

## 13. Fonctionnalités .NET Framework 3.0

Le Framework est une interface entre le système d'exploitation et l'application, permettant de faire fonctionner des applications dans un environnement sécurisé et fiable indépendant du système d'exploitation et du processeur.

La base du Framework est constituée du CLR (*Common Language Runtime*) et de sa formidable bibliothèque de classes prêtes à l'emploi pour les développeurs. Les développeurs peuvent utiliser plus de 30 langages de programmation dont les plus connus sont **VB.Net** et **C#** mais également **PowerShell** ou **jScript.Net**.

L'application créée n'est pas entièrement compilée mais transcrive dans un langage intermédiaire appelé CIL (*Common Intermediate Language*). Généralement, c'est à l'exécution que le programme compile à la volée l'application sur la plate-forme 32 ou 64 bits du couple AMD/INTEL y compris les processeurs Intel Itanium.

Les DLLs (*Dynamic Link Library*) partagées appelées **Assemblies** s'installent dans le répertoire **%systemroot%\assembly** et pour une DLL donnée, plusieurs versions peuvent maintenant y résider côté à côté.

Il est désormais possible de faire tourner une application X en version 1 en même temps que la même application X mais en version 2, même si les DLLs dépendantes sont différentes.

Il existe même une version du Framework soutenue par Novell tournant sous Linux appelée **mono** ([www.monoproject.com](http://www.monoproject.com)) dont les fonctionnalités la situent entre la version 2.0 et 3.5 du Framework.

Certaines applications ont été conçues uniquement pour une version spécifique du Framework. Il n'y a pas de problèmes, car il est possible de faire fonctionner plusieurs versions du Framework côté à côté comme les versions 1.1 et 2.0. Par contre, les Framework 3.0 et 3.5 sont complémentaires et s'installent au-dessus de la version 2.0.

Année de sortie	2002	2003	2005	2007	2008
<b>Framework</b>	1.0	1.1	2.0	3.0	3.5
<b>Visual Studio.NET</b>	2002	2003	2005	+SDK	2008
<b>Fonctionnalités</b>	Common Langage Runtime WinForms Web Services ASP.NET			WCF WF WPF CardSpace	LinQ AJAX REST

Par défaut, le Framework 2.0 est installé, mais l'installation du service SharePoint 3.0 exige l'installation de la version 3.0. D'autres applications récentes nécessitent même la version 3.5 du Framework.

Les composants pour cette fonctionnalité sont :

Fonctionnalité	Valeur de la commande
Fonctionnalités .NET Framework 3.0	NET-Framework
NET Framework 3.0	NET-Framework-Core
Visionneuse XPS	NET-XPS-Viewer
Activation de Windows Communication Foundation	Net-Win-CFAC
Activation HTTP	NET-HTTP-Activation
Activation non HTTP	NET-Non-HTTP-Activ

**NET Framework 3.0** : installe le Framework.

**Visionneuse XPS** : installe la visionneuse de documents XPS

**Activation de Windows Communication Foundation** : active le type de communication sélectionné.

- 
- C'est une fonctionnalité d'infrastructure, il ne faut installer le Framework 3.0 ou supérieur que si une application requiert ces fonctionnalités afin de réduire la surface d'attaque.
- 

## 14. Fonctionnalités de sauvegarde de Windows Server

Il s'agit de l'utilitaire de sauvegarde de Windows Server 2008, il remplace l'utilitaire de sauvegarde appelé **NTBackup** des versions précédentes.

Le chapitre Mise en œuvre du serveur de fichiers décrit en détail cette fonctionnalité.

Les composants pour cette fonctionnalité sont :

Fonctionnalité	Valeur de la commande
Fonctionnalité de la sauvegarde de Windows Server	Backup-Feature
Utilitaire de sauvegarde de Windows Server	Backup
Outils en ligne de commande	Backup-Tools

Le composant pour cette fonctionnalité pour un Server Core est :

Fonctionnalité	Valeur de la commande
Utilitaire de sauvegarde de Windows Server	WindowsServerBackup

- 
- C'est une fonctionnalité d'infrastructure, si vous concevez une planification de la sauvegarde, alors cette fonctionnalité est à prendre en considération.
- 

## 15. Gestion des stratégies de groupe

Il s'agit du composant MMC permettant de gérer les stratégies de groupe pour l'entreprise.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Gestion des stratégies de groupe	GPMC

-  C'est une fonctionnalité d'administration installée automatiquement sur les contrôleurs de domaine.

## 16. Gestionnaire de ressources système Windows

Le gestionnaire de ressources systèmes Windows WSRM (*Windows System Resource Manager*) est un outil d'administration permettant de contrôler l'utilisation de ressources mémoire et processeur que l'on peut allouer à une application.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Gestionnaire de ressources système Windows	WSRM

-  C'est une fonctionnalité d'optimisation, à installer sur un serveur si l'on veut contrôler l'allocation des ressources.

## 17. Gestionnaire de stockage amovible

Cette fonctionnalité gère les médias amovibles tels que les bandes et les disques optiques. Ce gestionnaire est spécialement conçu pour gérer les librairies matérielles comme les robots de sauvegarde, les juke-box, les étiquettes et catalogues en garantissant des opérations fiables et sécurisées.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Gestionnaire de stockage amovible	Removable-Storage

Le composant pour cette fonctionnalité pour un Server Core est :

Fonctionnalité	Valeur de la commande
Gestionnaire de stockage amovible	Microsoft-Windows-RemovableStorageManagementCore

-  C'est une fonctionnalité d'infrastructure, à installer avec un matériel ou une application qui requiert cette fonctionnalité.

## 18. Gestionnaire de stockage pour réseau SAN

Le gestionnaire de stockage pour réseau SAN permet de gérer des numéros d'unité logique appelé LUN (*Logic Unit Number*) pour des SAN (*Storage Area Network*) ou des systèmes iSCSI (*Internet Small Computer System Interface*) qui prennent en charge le service des disques virtuels VDS (*Virtual Disk Service*).

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Gestionnaire de stockage pour réseau SAN	Storage-Mgr-SANS

-  C'est une fonctionnalité d'infrastructure, à installer avec un matériel ou une application qui requiert cette fonctionnalité.

## 19. Kit d'administration de Connection Manager

Le kit d'administration de Connection Manager est un assistant qui permet de créer des profils de numérotation et de connexion d'un réseau distant ou un réseau VPN (*Virtual Private Network*).

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Kit d'administration de Connection Manager	CMAK

- C'est une fonctionnalité d'administration. À installer si vous planifiez l'utilisation de VPN Microsoft ou client d'accès à distance.

## 20. Message Queuing

Message Queuing est une infrastructure de messagerie applicative asynchrone pour applications distribuées gérant des files d'attentes. Ce service présente des avantages comme une garantie de remise des messages, une amélioration de la sécurité et la possibilité de gérer des transactions.

Cette fonctionnalité s'installe avec une application ou fait partie des pré-requis pour installer l'application.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Message Queuing	MSMQ
Services Message Queuing	MSMQ-Services
Serveur Message Queuing	MSMQ-Server
Intégration du service d'annuaire	MSMQ-Directory
Déclencheurs Message Queuing	MSMQ-Triggers
Prise en charge HTTP	MSMQ-HTTP-Support
Prise en charge de la multidiffusion	MSMQ-Multicasting
Service de routage	MSMQ-Routing
Prise en charge des clients Windows 2000	MSMQ-Win2000
Proxy DCOM Message Queuing	MSMQ-DCOM

- C'est une fonctionnalité d'infrastructure. À n'installer qu'avec des applications qui requièrent cette fonctionnalité.

## 21. Moniteur de port LPR

Le moniteur de port LPR (*Line Printer Remote*) permet d'imprimer sur un ordinateur Unix ayant une imprimante de type LPD (*Line Printer Daemon*).

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Moniteur de port LPR	LPR-Port-Monitor

 C'est une fonctionnalité d'interopérabilité. Cette fonctionnalité n'est à installer que pour imprimer sur un serveur Unix. Si le serveur est de type Windows, il faut lui préférer le port d'imprimante TCP/IP standard car il est plus rapide.

---

## 22. MPIO (Multipath I/O)

La fonctionnalité MPIO permet de créer des routes redondantes (si plusieurs routes existent) pour les SAN ou les systèmes iSCSI afin d'améliorer la fiabilité.

Il est même possible de répartir la charge entre les différents chemins disponibles, ce qui améliore les temps de réponse globaux du serveur.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
MPIO (Multipath I/O)	Multipath-IO

Le composant pour cette fonctionnalité sur un Server Core est :

Fonctionnalité	Valeur de la commande
MPIO (Multipath I/O)	MultipathIo

 C'est une fonctionnalité d'infrastructure. À n'installer que s'il existe des routes SAN ou iSCSI redondantes.

---

## 23. Outils d'administration de serveur distant

Outils d'administration de serveur distant est un pack qui permet la gestion à distance de Windows Server 2008 ou Windows Server 2003 à partir d'un serveur exécutant Windows Server 2008.

Ce pack contient les logiciels composants enfichables pour gérer les rôles suivants :

- Services de certificats Active Directory AD CS.
- Services de domaine Active Directory AD DS.
- Services applicatifs Active Directory AD LDS.
- Services de gestion des droits Active Directory AD RMS.
- Serveur DHCP.
- Serveur DNS.
- Serveur de télécopie.
- Services de fichiers.
- Services de stratégies et d'accès réseau.

- Services d'impression.
- Services Terminal Server.
- Services UDDI.
- Serveur Web (IIS).
- Services de déploiement Windows WDS.

Ainsi que les fonctionnalités suivantes :

- Chiffrement de lecteur BitLocker.
- Extensions du serveur BITS.
- Clustering avec basculement.
- Équilibrage de la charge réseau WNLB.
- Serveur SMTP.
- Serveur WINS.

Les composants pour cette fonctionnalité sont :

<b>Fonctionnalité</b>	<b>Valeur de la commande</b>
Outils d'administration de serveur distant	RSAT
Outils d'administration de rôles	RSAT-Role-Tools
Outils des services de certificats Active Directory	RSAT-ADCS
Outils d'autorité de certification	RSAT-ADCS-Mgmt
Outils des répondeurs en ligne	RSAT-Online-Responder
Outils des services de domaine Active Directory	RSAT-ADDS
Outils de contrôleur de domaine Active Directory	RSAT-ADDC
Outils de Serveur pour NIS	RSAT-SNIS
Outils des services AD LDS ( <i>Active Directory Lightweight Directory Services</i> )	RSAT-ADLDS
Outils des services AD RMS ( <i>Active Directory Rights Management Services</i> )	RSAT-RMS
Outils du serveur DHCP	RSAT-DHCP
Outils du serveur DNS	RSAT-DNS-Server
Outils du serveur de télécopie	RSAT-Fax
Outils de services de fichiers	RSAT-File-Services
Outils du système de fichiers DFS	RSAT-DFS-Mgmt-Con

Outils de gestion de ressources du serveur	RSAT-FSRM-Mgmt
Outils des services pour NFS	RSAT-NFS-Admin
Outils de la stratégie réseau et des services d'accès	RSAT-NPAS
Outils des services d'impression	RSAT-Print-Services
Outils des services Terminal Server	RSAT-TS
Outils du serveur Terminal Server	RSAT-TS-RemoteApp
Outils de la passerelle TS	RSAT-TS-Gateway
Outils des licences Terminal Server	RSAT-TS-Licensing
Outils des services UDDI	RSAT-UDDI
Outils du serveur Web (IIS)	RSAT-Web-Server
Outils des services de déploiement Windows	RSAT-WDS
Outils Hyper-V	RSAT-Hyper-V
Outils d'administration de fonctionnalités	RSAT-Feature-Tools
Outils de chiffrement de lecteur BitLocker	RSAT-BitLocker
Outils d'extensions du serveur BITS	RSAT-Bits-Server
Outils de clustering avec basculement	RSAT-Clustering
Outils d'équilibrage de la charge réseau	RSAT-NLB
Outils du serveur SMTP	RSAT-SMTP
Outils du serveur WINS	RSAT-WINS

➤ C'est une fonctionnalité d'administration, à installer si nécessaire.

## 24. Protocole PNRP (Peer Name Resolution Protocol)

Le protocole PNRP est un protocole prévu pour permettre une résolution de noms sécurisée, évolutive et dynamique dans un environnement de groupe de travail.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Protocole de résolution de noms d'homologues	PNRP

➤ C'est une fonctionnalité d'infrastructure, à n'installer que si vous êtes en mode groupe de travail.

## 25. Proxy RPC sur HTTP

Le protocole RPC (*Remote Procedure Call*) exige de connaître l'adresse réelle de l'émetteur et du destinataire, ce qui empêche une application de traverser les pare-feu et autres systèmes NAT (*Network Address Translation*).

Le proxy RPC sur HTTP permet d'encapsuler le protocole RPC dans le protocole HTTP depuis le client jusque vers le serveur de destination.

Pour améliorer la sécurité, il est préférable d'utiliser des certificats SSL, donc le protocole HTTPS.

L'application la plus connue qui bénéficie de cette technologie est le logiciel de messagerie **Microsoft Outlook**. Elle permet à un client Outlook utilisant le protocole MAPI (*Messaging API*) qui utilise les RPC de se connecter vers le serveur Exchange, même si le client se trouve au-delà du pare-feu.

L'avantage pour le client Outlook est de pouvoir créer un mini VPN (*Virtual Private Network*) entre son emplacement et le serveur Exchange uniquement pour la connexion MAPI.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Proxy RPC sur HTTP	RPC-over-HTTP-Proxy

- C'est une fonctionnalité d'infrastructure, à n'installer que si des applications demandent ce protocole.

## 26. Serveur iSNS (Internet Storage Name Server)

Le serveur iSNS est un service d'annuaire pour les réseaux de stockage iSCSI et SAN si ces derniers utilisent une passerelle iFCP (*Internet Fibre Channel Protocol*).

Cet annuaire permet de centraliser en un point l'état des différents espaces de stockage. Ce service facilite la découverte des périphériques de stockage sur un réseau Ethernet.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Serveur iSNS (Internet Storage Name Server)	ISNS

- C'est une fonctionnalité d'infrastructure, à n'installer que si vous disposez de périphériques iSCSI.

## 27. Serveur SMTP

L'installation d'un serveur SMTP permet d'envoyer ou recevoir des messages au format e-mail. Cette fonctionnalité s'attache au serveur Web IIS. Elle s'adresse principalement aux applications qui peuvent recevoir ou envoyer des messages électroniques.

- Trop souvent, certaines entreprises mettent en œuvre des serveurs SMTP utilisant ce service non sécurisé avec lesquels il est possible d'envoyer des messages de spam en dehors de l'entreprise !

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Serveur SMTP	SMTP-Server

- C'est une fonctionnalité d'infrastructure. Ce service ne doit être installé que si une application requiert un serveur SMTP spécifique. Il faut prendre un soin particulier à le filtrer et le sécuriser.

## 28. Serveur Telnet

Le serveur Telnet est la fonctionnalité qui permet à des clients Telnet de se connecter sur le serveur Windows 2008 afin de le gérer via la ligne de commandes. Le serveur Telnet est fortement déconseillé.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Server Telnet	Telnet-Server

- C'est une fonctionnalité d'administration. Ce service ne devrait plus être installé. Windows Remote Shell le remplace de manière plus puissante et plus sécurisée.

## 29. Serveur WINS (Windows Internet Naming Service)

Le service WINS est un service de mappage de noms NetBIOS avec leur adresse IP correspondante. Il indique également le type de service fourni par l'ordinateur comme par exemple s'il s'agit d'un serveur ou d'une station de travail.

Depuis Windows 2000, ce service cohabite avec le service DNS pour permettre aux "vieux" ordinateurs exécutant Windows NT de cohabiter avec l'Active Directory. Certaines applications utilisent encore le protocole NetBIOS.

Dans un environnement idéal composé de serveurs Windows 2008, de clients Windows Vista et d'applications récentes, un service de noms NetBIOS est inutile.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Serveur WINS	WINS-Server

Le composant pour cette fonctionnalité sur un Server Core est :

Fonctionnalité	Valeur de la commande
Serveur WINS	WINS-SC

- C'est une fonctionnalité d'infrastructure réseau. Ce service ne devrait plus être utile, néanmoins certaines applications requièrent l'utilisation de noms NetBIOS.

## 30. Service d'activation des processus Windows

Le service d'activation des processus Windows est un service qui travaille en conjonction avec le Framework 3.0 ainsi que IIS7.

Il met à disposition des applications utilisant WCF (*Windows Communication Foundation*) des fonctionnalités qui sont propres à IIS.

Les composants pour cette fonctionnalité sont :

Fonctionnalité	Valeur de la commande
Service d'activation des processus Windows	WAS
Modèle de processus	WAS-Process-Model
Environnement .NET	WAS-NET-Environment
API de configuration	WAS-Config-APIs

Les composants pour cette fonctionnalité sur un Server Core sont :

Fonctionnalité	Valeur de la commande
Service d'activation des processus Windows	WAS-WindowsActivationService
Modèle de processus*	WAS-ProcessModel

\*Les dépendances n'ont pas été affichées.

➤ C'est une fonctionnalité d'infrastructure. Ce service s'installe automatiquement avec le Framework 3 et IIS 7.

## 31. Service de réseau local sans fil

Le service de réseau local sans fil active l'autoconfiguration WLAN (*Wireless Local Area Network*) et le fait démarrer.

➤ Bien que plus sécurisé que les versions précédentes, il est déconseillé d'utiliser ce service sur un serveur disposant d'une carte sans fil et de la configurer manuellement.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Service de réseau local sans fil	Wireless-Networking

➤ C'est une fonctionnalité d'administration réseau. À n'activer que si votre serveur dispose d'une carte sans fil et éventuellement en conjonction avec une politique d'accès réseau NAP.

## 32. Services SNMP (Simple Network Management Protocol)

Les services SNMP se composent de deux fonctionnalités pouvant s'installer séparément à savoir :

- Service SNMP.
- Fournisseur WMI SNMP.

Le service SNMP récupère les informations sur les périphériques à surveiller et envoie des rapports à la console de gestion.

Le fournisseur WMI SNMP affiche des variables SNMP et des tables en tant qu'instance WMI.

SNMP est un service de gestion universellement reconnu et supporté par de nombreux acteurs informatiques.

Tous les systèmes d'exploitation Microsoft intègrent des agents SNMP pouvant interagir avec des consoles de gestion.

➤ MOM (*Microsoft Operation Manager*) est une alternative à SNMP.

Les composants pour cette fonctionnalité sont :

Fonctionnalité	Valeur de la commande
Services SNMP	SNMP-Services
Service SNMP	SNMP-Service

Le composant pour cette fonctionnalité sur un Server Core est :

Fonctionnalité	Valeur de la commande
Service SNMP	SNMP-SC

-  C'est une fonctionnalité d'administration de surveillance, à n'installer que si une application requiert SNMP.

### 33. Services TCP/IP simples

Cette fonctionnalité ajoute des services de protocole TCP/IP décrites dans les RFC (*Request For Comment*) comme étant facultatifs.

Il s'agit de :

**Générateur de caractères chargé** : utilisé pour tester les imprimantes lignes, car il permet d'envoyer des caractères imprimables, soit 95 caractères différents.

**Heure du jour** : retourne des messages contenant des informations sur la date et l'heure du serveur.

**Ignorer** : utile pour créer un port nul, soit un port qui ignore tout message sans réponse ou accusé de réception.

**Echo** : utile pour dépanner un port réseau du serveur car il renvoie à l'émetteur tous les paquets reçus pour un port particulier.

**Citation du jour quote** : retourne une des citations du jour contenues dans le fichier %systemroot%\System32\Drivers\Etc\Quotes.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Services TCP/IP simplifiés	Simple-TCPPIP

-  C'est une fonctionnalité réseau. Sauf si vous avez une application qui requiert un de ces services, il ne faut pas les installer.

### 34. Sous-système pour les applications UNIX

Le sous-système pour les applications Unix permet d'assurer une excellente interopérabilité au niveau du code source de l'application UNIX devant s'exécuter sur Windows. L'effort à fournir pour transporter l'application est nul, voire minime.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Sous-système pour les applications UNIX	Subsystem-UNIX-Apps

Le composant pour cette fonctionnalité sur un Server Core est :

Fonctionnalité	Valeur de la commande
Sous-système pour les applications UNIX	SUACore

-  C'est une fonctionnalité d'interopérabilité, à installer avec les applications qui la requièrent.

## 35. Windows PowerShell

Windows PowerShell est l'interpréteur de commandes permettant d'exécuter des commandes et des scripts écrits en PowerShell.

- Les éditions Core ne peuvent pas installer la fonctionnalité PowerShell.

Ce langage dont la syntaxe ressemble à des commandes UNIX est en fait un nouveau langage objet orienté vers des tâches d'administration dont chaque commande gère des objets et dont le résultat est un objet.

L'interpréteur ressemble à l'invite de commandes sur laquelle on a rajouté plus de 130 commandes, appelées **cmdlets**. En fait, l'interpréteur de commandes PowerShell est totalement personnalisable et permet d'ajouter d'autres cmdlets regroupées en **snap-ins**. Cette modularité en fait un système totalement extensible en fonction des besoins d'administration.

La notion de **Provider** permet de créer des outils d'exploration pour des systèmes de fichiers, des bases de données, la base de registre, etc.

Il est plus puissant que le langage VBS (*Visual Basic Scripting*) ; comme le VBS, il permet d'utiliser des objets WMI (*Windows Management Interface*, ADSI (*Active Directory Service Interface*)... mais en plus, il permet d'utiliser toutes les fonctionnalités du Framework et de créer des scripts disposant d'une interface graphique.

Il est extensible, c'est-à-dire que les développeurs peuvent créer des extensions de gestion pour leur application comme il en existe déjà pour Exchange 2007, IIS7, MOM 2007 et SQL Server 2008.

À terme, il devrait remplacer l'interpréteur de commandes DOS (*Disk Operating System*) et les scripts écrits en VBS ou en batch.

► Pour les administrateurs non programmeurs, son apprentissage est un peu ardu mais une fois sa philosophie comprise, grâce à ses possibilités infinies, il devient le compagnon indispensable de l'administrateur.

► Le Repository du Script Center du site Technet de Microsoft contient plusieurs centaines d'exemples de scripts écrits en PowerShell prêts à l'emploi ainsi que plusieurs milliers de scripts écrits principalement en VBS.

La version packagée dans Windows Server 2008 est la version 1, néanmoins la version 2 est téléchargeable sur le site de Microsoft. Parmi les nouveautés, on peut citer :

- Exécution des scripts sur des ordinateurs distants.
- Débogage de scripts.
- Interface graphique de PowerShell.

Le composant pour cette fonctionnalité est :

Fonctionnalité	Valeur de la commande
Windows PowerShell	PowerShell

- C'est une fonctionnalité d'administration, à installer et à utiliser sans modération.

## Résumé du chapitre

Vous avez appris à utiliser le gestionnaire de serveur, utiliser et personnaliser une console MMC, à ajouter les snap-ins supplémentaires pour gérer un serveur Windows 2008 et à utiliser l'administration à distance.

Windows Remote Shell a été présenté de manière approfondie afin de vous faire découvrir ses énormes possibilités.

Le gestionnaire de serveur en mode ligne de commande appelé **ServerManagerCmd** utilisable sur une édition complète ou son homologue **ocsetup** pour un Server Core minimal ont été présentés.

La commande **netsh** a été démystifiée et ses possibilités d'utilisations ont été présentées.

Enfin le langage PowerShell a été présenté pour montrer son énorme potentiel.

Vous avez également appris quels sont les avantages et inconvénients de chacun des outils présentés.

## Travaux pratiques

Dans les travaux pratiques, pour les différents exercices, vous effectuerez l'opération suivante :

- Déploiement de rôles et de fonctionnalités soit en utilisant l'interface graphique soit à l'aide de l'invite de commandes.

# Les outils de type ligne de commandes

## 1. ServerManagerCmd



La commande **ServerManagerCmd** permet d'installer, de gérer et de supprimer des rôles ou des fonctionnalités. La figure suivante en montre la syntaxe.

```
C:\>servermanagercmd
Utilisation :

ServerManagerCmd.exe
Installe et supprime les rôles, les services de rôle et les fonctionnalités.
Affiche également la liste de tous les rôles, services de rôle et
fonctionnalités disponibles, et indique lesquels sont installés sur
l'ordinateur. Pour plus d'informations sur les rôles, les services de rôle
et les fonctionnalités qu'il est possible de spécifier à l'aide
de cet outil, consultez l'aide du Gestionnaire de serveur.

-query [<query.xml>] [-logPath <log.txt>]
-install <nom>
    [-resultPath <result.xml> [-restart] : -whatIf] [-logPath <log.txt>]
    [-allSubFeatures]
-remove <nom>
    [-resultPath <result.xml> [-restart] : -whatIf] [-logPath <log.txt>]
-inputPath <answer.xml>
    [-resultPath <result.xml> [-restart] : -whatIf] [-logPath <log.txt>]
-help : -?
-version
```

Cette commande n'est pas disponible sur un Server Core.

### a. Afficher la liste des rôles et fonctionnalités

```
C:\>servermanagercmd -query
..
----- Rôles -----
[ ] Serveur d'applications [Application-Server]
[ ] Fondation du serveur d'applications [AS-AppServer-Foundation]
[ ] Prise en charge du serveur Web (IIS) [AS-Web-Support]
[ ] Accès réseau COM+ [AS-Ent-Services]
[ ] Partage de port TCP [AS-TCP-Port-Sharing]
[ ] Prise en charge du service d'activation des processus Windows [AS-WAS-support]
    [ ] Activation HTTP [AS-HTTP-Activation]
    [ ] Activation Message Queuing [AS-MSMQ-Activation]
    [ ] Activation TCP [AS-TCP-Activation]
    [ ] Activation des canaux nommés [AS-Named-Pipes]
[ ] Transactions distribuées [AS-Dist-Transaction]
    [ ] Transactions distantes entrantes [AS-Incoming-Trans]
    [ ] Transactions distantes sortantes [AS-Outgoing-Trans]
    [ ] Transactions WS-Atomic [AS-WS-Atomic]
[X] Serveur de télécopie [Fax]
[ ] Serveur DHCP [DHCP]
[ ] Serveur DNS [DNS]
```

Les rôles ou les fonctionnalités apparaissent dans des couleurs différentes en fonction de leur état d'installation.

## b. Créer un fichier des rôles et fonctionnalités

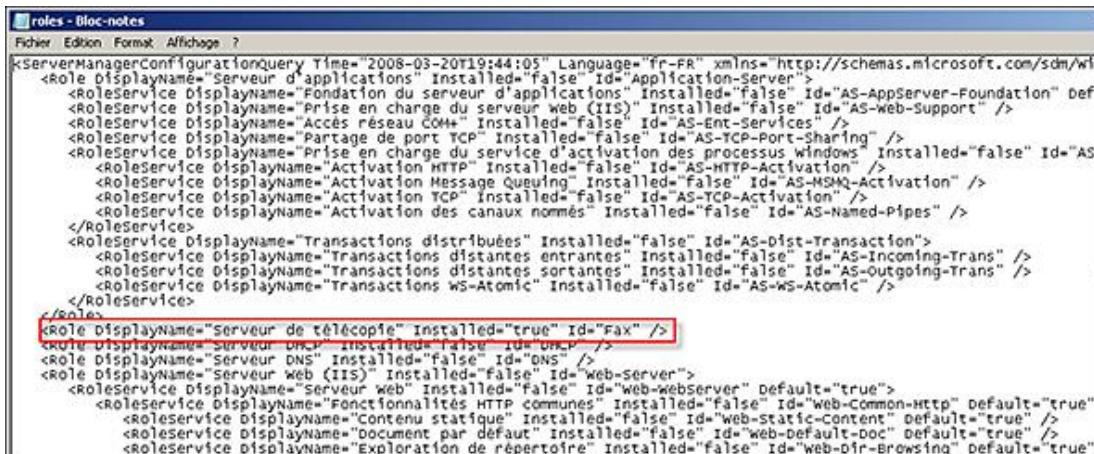


```
C:\>servermanagercmd -query roles.xml
--
```

Le fichier créé s'appelle roles.xml et se trouve dans le répertoire actif à moins d'y spécifier un chemin complet.

L'image suivante montre une partie du fichier généré. Sa lecture peut être un peu déroutante, vous verrez plus loin, dans la section consacrée à PowerShell, comment améliorer sa présentation.

Notez que le service de télécopie est installé.



```
<ServerManagerConfigurationQuery Time="2008-03-20T19:44:05" Language="fr-FR" xmlns="http://schemas.microsoft.com/sdm/wf">
<Role DisplayName="Serveur d'applications" Installed="false" Id="Application-Server">
  <RoleService DisplayName="Fondation du serveur d'applications" Installed="false" Id="AS-AppServer-Foundation" def="true"/>
  <RoleService DisplayName="Prise en charge du serveur Web (IIS)" Installed="false" Id="AS-Web-Support"/>
  <RoleService DisplayName="Accès réseau COM+" Installed="false" Id="AS-Ent-Services"/>
  <RoleService DisplayName="Partage de port TCP" Installed="false" Id="AS-TCP-Port-Sharing"/>
  <RoleService DisplayName="Prise en charge du service d'activation des processus Windows" Installed="false" Id="AS-Activation"/>
  <RoleService DisplayName="Activation HTTP" Installed="false" Id="AS-HTTP-Activation"/>
  <RoleService DisplayName="Activation Message Queuing" Installed="false" Id="AS-MSMQ-Activation"/>
  <RoleService DisplayName="Activation des canaux nommés" Installed="false" Id="AS-Named-Pipes"/>
</RoleService>
<RoleService DisplayName="Transactions distribuées" Installed="false" Id="AS-Dist-Transaction"/>
  <RoleService DisplayName="Transactions distantes entrantes" Installed="false" Id="AS-Incoming-Trans"/>
  <RoleService DisplayName="Transactions distantes sortantes" Installed="false" Id="AS-Outgoing-Trans"/>
  <RoleService DisplayName="Transactions WS-Atomic" Installed="false" Id="AS-WS-Atomic"/>
</RoleService>
</Role>
<Role DisplayName="Serveur de télécopie" Installed="true" Id="Fax" />
<Role DisplayName="Serveur DNS" Installed="false" Id="DNS" />
<Role DisplayName="Serveur Web (IIS)" Installed="false" Id="Web-server">
  <RoleService DisplayName="Serveur Web" Installed="false" Id="Web-WebServer" Default="true"/>
    <RoleService DisplayName="Fonctionnalités HTTP communes" Installed="false" Id="Web-Common-Http" Default="true"/>
      <RoleService DisplayName="Contenu statique" Installed="false" Id="Web-Static-Content" Default="true"/>
      <RoleService DisplayName="Document par défaut" Installed="false" Id="Web-Default-Doc" Default="true"/>
    <RoleService DisplayName="Exploration de répertoire" Installed="false" Id="Web-Dir-Browsing" Default="true"/>
  </RoleService>
</Role>
```

## c. Ajouter un rôle ou une fonctionnalité à partir d'un fichier

Il serait tentant d'utiliser le fichier XML généré plus haut pour le modifier. Malheureusement ce n'est pas si simple, car bien que le format soit du XML, les schémas utilisés sont différents.

 Il n'est pas possible d'installer certains rôles avec l'invite de commandes comme les rôles **UDDI** et **AD-RMS**.

Néanmoins, il est possible d'effectuer cette conversion. Pour cela, il faut télécharger depuis le site de Microsoft un utilitaire qui s'appelle **msxsl.exe** et effectuer plusieurs transformations fastidieuses. Il est plus simple de créer un fichier XML comme celui de l'image suivante :



```
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Install"
  xmlns="http://schemas.microsoft.com/sdm/windows/ServerManager/Configuration/2007/1"
  xmlns:xs="http://www.w3.org/2001/XMLSchema">

  <Role Id="Web-Server" />
  <Feature Id="Backup" />

</ServerManagerConfiguration>
```

Nommez-le **addroles.xml**.

La figure suivante montre quels sont les rôles, rôles de services et fonctionnalités touchés par cette installation. Pour cela il faut ajouter **-whatif** à la fin de la commande :

```
C:\>servermanagercmd -inputPath addroles.xml -whatif
.
.
.
DÉMARQUE L'exécution en mode « WhatIf ».
Spécifié pour l'installation : [Fonctionnalités de la Sauvegarde de Windows Server] Utilitaire de sauvegarde de Windows Server
Spécifié pour l'installation : [Serveur Web <IIS>] Outils de gestion
Spécifié pour l'installation : [Serveur Web <IIS>] Serveur Web
Spécifié pour l'installation : [Serveur Web <IIS>] Console de gestion d'IIS
Spécifié pour l'installation : [Serveur Web <IIS>] Performances
Spécifié pour l'installation : [Serveur Web <IIS>] Fonctionnalités HTTP communes
Spécifié pour l'installation : [Serveur Web <IIS>] Sécurité
Spécifié pour l'installation : [Serveur Web <IIS>] Intégrité et diagnostics
Spécifié pour l'installation : [Serveur Web <IIS>] Journalisation HTTP
Spécifié pour l'installation : [Serveur Web <IIS>] Compression de contenu statique
Spécifié pour l'installation : [Serveur Web <IIS>] Contenu statique
Spécifié pour l'installation : [Serveur Web <IIS>] Erreurs HTTP
Spécifié pour l'installation : [Serveur Web <IIS>] Exploration de répertoire
Spécifié pour l'installation : [Serveur Web <IIS>] Filtrage des demandes
Spécifié pour l'installation : [Serveur Web <IIS>] Document par défaut
Spécifié pour l'installation : [Serveur Web <IIS>] Observateur de demandes
Spécifié pour l'installation : [Service d'activation des processus Windows] Modèle de processus
Spécifié pour l'installation : [Service d'activation des processus Windows] API de configuration
Vous devrez peut-être redémarrer ce serveur à la fin de l'installation.
C:\>_

```

Enfin pour procéder à l'installation :

```
C:\>servermanagercmd -inputPath addroles.xml
.

.
.
DÉMARRER L'INSTALLATION...
[Installation], réussite : [Serveur Web <IIS>] Outils de gestion.
[Installation], réussite : [Serveur Web <IIS>] Serveur Web.
[Installation], réussite : [Serveur Web <IIS>] Fonctionnalités HTTP communes.
[Installation], réussite : [Serveur Web <IIS>] Intégrité et diagnostics.
[Installation], réussite : [Serveur Web <IIS>] Performances.
[Installation], réussite : [Serveur Web <IIS>] Sécurité.
[Installation], réussite : [Fonctionnalités de la Sauvegarde de Windows Server] Utilitaire de sauvegarde
[Installation], réussite : [Service d'activation des processus Windows] Modèle de processus.
[Installation], réussite : [Service d'activation des processus Windows] API de configuration.
[Installation], réussite : [Serveur Web <IIS>] Console de gestion d'IIS.
[Installation], réussite : [Serveur Web <IIS>] Erreurs HTTP.
[Installation], réussite : [Serveur Web <IIS>] Filtrage des demandes.
[Installation], réussite : [Serveur Web <IIS>] Compression de contenu statique.
[Installation], réussite : [Serveur Web <IIS>] Contenu statique.
[Installation], réussite : [Serveur Web <IIS>] Journalisation HTTP.
[Installation], réussite : [Serveur Web <IIS>] Document par défaut.
[Installation], réussite : [Serveur Web <IIS>] Exploration de répertoire.
[Installation], réussite : [Serveur Web <IIS>] Observateur de demandes.
<100/100>

RÉUSSITE : installation réussie.

```

#### d. Supprimer un ou plusieurs rôles

Pour supprimer plusieurs rôles, il est possible d'utiliser un fichier XML identique à celui de l'installation (addroles.xml). Pour cela, vous devez modifier **action = "Install"** en **action = "Remove"** et également renommer en **RemoveRoles.xml** par exemple.

```
RemoveRoles - Bloc-notes
Fichier Edition Format Affichage ?
<?xml version="1.0" encoding="utf-8" ?>
<ServerManagerConfiguration Action="Remove"
xmlns="http://schemas.microsoft.com/sdm/windows/ServerManager/Configuration/2007/1"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
    <Role Id="Web-Server" />
    <Feature Id="Backup" />
</ServerManagerConfiguration>
```

Puis il faut saisir la commande **ServerManagerCmd -inputPath c:\removeroles.xml**.

#### e. Avantages et inconvénients

Les inconvénients sont :

- Ne peut être utilisé sur un Server Core.
- Utilisable localement uniquement.
- Requiert la connaissance du format XML.
- Tous les rôles ne peuvent être installés en mode ligne de commandes.

Les avantages sont :

- Utilisable pour créer des scripts d'installation de rôles ou de fonctionnalités.
- Paramètre **Whatif** pour simuler l'exécution et voir le résultat.
- Les commandes peuvent être incluses dans des scripts pour automatiser les tâches.

## 2. PowerShell



PowerShell est l'outil par excellence pour les administrateurs qui veulent créer des scripts sans devenir programmeur. PowerShell est une fonctionnalité qu'il faut installer avant de pouvoir l'utiliser.

► PowerShell ne peut s'installer officiellement sur un Server Core. Le service pack 2 de Windows Server 2008 devrait toutefois l'accepter. Dans tous les cas, la version R2 de Windows Server 2008 disposera de la version 2 de PowerShell. En attendant, il toujours possible de recourir à la console **WMIC** qui offre un accès simplifié aux classes WMI. Exemple : WMIC SERVICE WHERE « STATE LIKE 'RUNING' » LIST BRIEF.

Au lieu d'en décliner les avantages et de refaire un cours sur PowerShell, il semble plus utile de montrer comment l'utiliser en interaction avec des commandes afin d'améliorer le rendu de l'information. La syntaxe pour lancer PowerShell est la suivante. Remarquez qu'il est possible de personnaliser l'affichage et les snap-ins chargés dans la console.

C:\ Administrateur : Invite de commandes

```

C:\>powershell /?
powershell[.exe] [-PSConsoleFile <file>] [-Version <version>]
  [-NoLogo] [-NoExit] [-NoProfile] [-NonInteractive]
  [-OutputFormat <Text | XML>] [-InputFormat <Text | XML>]
  [-Command <- : <bloc_script> [-args <tableau_arguments>]
           : <chaine> [<paramètres_commande>] > ]
powershell[.exe] -Help : -? : /?

-PSConsoleFile
  Charge le fichier console de Windows PowerShell spécifié. Pour créer
  un fichier console, utilisez Export-Console dans Windows PowerShell.

-Version
  Démarrer la version de Windows PowerShell spécifiée.

-NoLogo
  Masque la bannière de copyright au démarrage.

-NoExit
  Ne quitte pas après exécution des commandes de démarrage.

-NoProfile
  N'utilise pas le profil utilisateur.

-Noninteractive
  Ne présente pas d'invite interactive à l'utilisateur.

-OutputFormat
  Indique comment la sortie de Windows PowerShell est mise en forme. Les
  valeurs valides sont "Text" <chaînes de texte> ou "XML" <format CLIXML
  sérialisé>.

-InputFormat
  Décris le format des données envoyées à Windows PowerShell. Les valeurs
  valides sont "Text" <chaînes de texte> ou "XML" <format CLIXML sérialisé>.

-Command
  Exécute les commandes spécifiées (et tous paramètres) comme si elles avaient
  été tapées à l'invite de commandes de Windows PowerShell, puis quitte sauf
  si NoExit est spécifié. La valeur de Command peut être "-", une chaîne ou
  un bloc de script.

  Si la valeur de Command est "-", le texte de la commande est lu à partir de
  l'entrée standard.

  Les blocs de script doivent être entre accolades <>. Vous ne pouvez
  spécifier un bloc de script qu'en exécutant PowerShell.exe dans Windows
  PowerShell. Les résultats du script sont retournés à l'environnement parent
  en tant qu'objets XML déserialisés, et non en direct.

  Si la valeur de Command est une chaîne, Command doit être le dernier
  paramètre de la commande, car tous les caractères tapés après la commande
  sont interprétés comme des arguments de commande.

  Pour écrire une chaîne qui exécute une commande Windows PowerShell, utilisez
  le format :
    "& <<commande>>"
  dans lequel les guillemets indiquent une chaîne et l'opérateur d'appel (&)
  entraîne l'exécution de la commande.

-Help, -?, /?
  Affiche ce message. Si vous tapez une commande powershell.exe dans Windows
  PowerShell, faites précéder les paramètres de commande d'un trait d'union
  <->, et non d'une barre oblique </>. Vous pouvez utiliser un trait d'union
  ou une barre oblique dans Cmd.exe.

EXEMPLES
powershell -psconsolefile sqlsnapin.psc1
powershell -version 1.0 -nologo -inputformat text -outputformat XML
powershell -command {get-eventlog -logname security}
powershell -command "& {get-eventlog -logname security}"

```

## a. Formatage d'un fichier XML

Avec la commande ServerManagerCmd, vous avez créé un fichier de réponse appelé rôles.xml. Le langage XML n'est pas abordable pour tous. Dans l'exemple suivant vous allez améliorer la présentation du contenu XML en affichant clairement quels rôles ou fonctionnalités sont installés.

Il faut savoir que la racine XML s'appelle **ServerManagerConfigurationQuery** et que des éléments s'appellent **role** et **feature**. Consultez le fichier XML pour vous en rendre compte.

```

Windows PowerShell
PS C:\> $roles = [xml](get-content c:\roles.xml)
PS C:\> $roles.ServerManagerConfigurationQuery.role

```

DisplayName	Installed	Id	RoleService
Serveur d'application	false	Application-Server	<AS-AppServer-Fo...
Serveur de téléphonie	true	Fax	
Serveur DHCP	false	DHCP	
Serveur DNS	false	DNS	
Serveur Web (IIS)	false	Web-Server	<Web-WebServer, ...
Services AD LDS	false	ADLDS	
Services AD RMS	false		<Active Director...
Services ADFS (A...)	false		<ADFS-Federation...
Services d'impression	true	Print-Services	<Print-Server, P...
Services de certificat	false	AD-Certificate	<ADCS-Cert-Autho...
Services de déploiement	false	WDS	<WDS-Deployment,...
Services de domaine	false		<ADDS-Domain-Con...
Services de fichiers	false		<FS-FileServer, ...
Services de stratégies	false	NPAS	<NPAS-Policy-Ser...
Services Terminal Services	false	Terminal-Services	<TS-Terminal-Ser...
Services UDDI	false		<Base de données...

```

PS C:\> $roles.ServerManagerConfigurationQuery.feature

```

DisplayName	Installed	Id
Assistance à distance	false	Remote-Assistance
Base de données interne	false	Windows-Internal-DB
Chiffrement de lecteur	false	BitLocker
Client d'impression Internet	false	Internet-Print-Client
Client Telnet	false	Telnet-Client
Client IFIP	false	IFIP-Client
Clustering avec basculement	false	Failover-Clustering
Compression différentielle	false	RDC
Équilibrage de la charge	false	NLB
Expérience audio-vidéo	false	qWave
Expérience utilisateur	false	Desktop-Experience
Extensions du serveur BITS	false	BITS
Fonctionnalités .NET Framework	false	.NET-Framework
Fonctionnalités de la sécurité	true	Backup-Features
Gestion des stratégies	false	GPMC
Gestionnaire de ressources	false	WSRM
Gestionnaire de stockage	false	Removable-Storage
Gestionnaire de stockage SANS	false	Storage-Mgr-SANS
Kit d'administration de l'infrastructure	false	CMK
Message Queuing	false	MSMQ
Moniteur de port LPR	false	LPR-Port-Monitor

## b. Affichage des services

Pour afficher la liste des services qui sont démarrés :

```
get-service | where-object {$_.status -eq "Running"}
```

## c. Affichage des processus

Pour afficher la liste des processus :

```
get-process
```

## d. Avantages et inconvénients

Les inconvénients sont :

- Ne peut être utilisé actuellement sur un Server Core.
- Apprentissage d'une philosophie.
- Apprentissage d'un nouveau langage.
- La version 1 n'exécute pas de scripts distants.

Les avantages sont :

- Langage d'administration puissant orienté objet.
- Extensible selon des contextes.
- Langage évolutif.
- Invite de commande personnalisable.
- Existence d'éditeurs graphiques.
- Commandes simples mais puissantes.
- Création de scripts réutilisables.
- Accès aisés aux classes WMI.
- Plusieurs applications possèdent des extensions pour PowerShell.

### 3. Invite de commandes



L'invite de commandes est l'outil le plus connu, il permet d'exécuter des centaines de commandes et d'exécuter des scripts batch ou vbs.

➤ Pour créer des scripts, vous pouvez utiliser le Bloc-notes qui fonctionne bien excepté lorsqu'il faut utiliser des caractères accentués dans les commandes. Dans ce cas, il vous faut utiliser le wordpad et sauvegarder votre fichier en tant que **Document texte MS-DOS**.

➤ Elle est le bureau de tout Server Core.

#### a. Avantages et inconvénients

Les inconvénients sont :

- Langage de script vieillissant et pauvre.
- Langage peu adapté à l'administration.

Les avantages sont :

- Disponible sur toutes versions et éditions.
- Permet de lancer toutes les commandes.
- Permet de créer des scripts.
- Langage largement répandu chez les administrateurs.

### 4. ocsetup et pkgmgr



**Ocsetup** est le successeur de **sysocmgr**, il permet d'installer ou de supprimer des packages MSI (*Microsoft System Installer*) ou des composants optionnels.

**Pkgmgr** permet d'installer, de supprimer ou de mettre à jour des packages.

Ils ne remplacent pas le gestionnaire de serveur, car ces commandes sont plus difficiles à mettre en œuvre et les erreurs sont plus difficiles à résoudre.

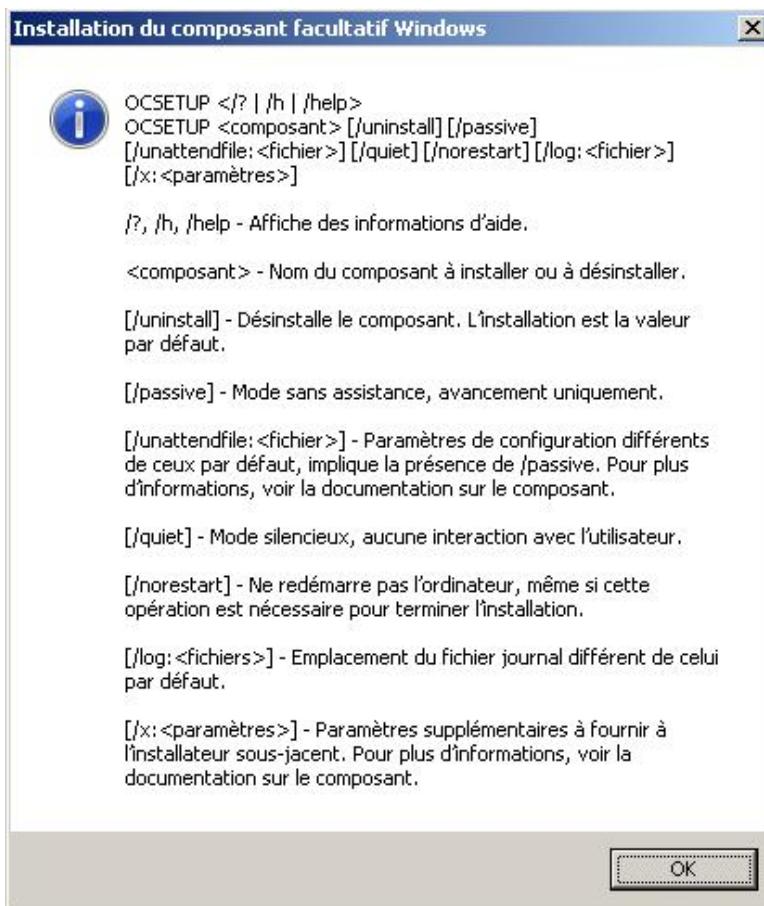
Pourtant ces deux commandes sont les seuls moyens d'installer des rôles et des fonctionnalités sur un Server Core. La commande **ocsetup** est la méthode préférée pour installer et désinstaller des rôles ou des fonctionnalités.

L'image suivante montre un exemple de commande pour installer et désinstaller le rôle DNS. Il faut respecter la casse pour le nom du rôle.

```
C:\>start /w ocsetup DNS-Server-Core-Role
C:\>start /w ocsetup DNS-Server-Core-Role /uninstall
```

- La commande **oclist** disponible uniquement sur un Server Core permet d'afficher si les rôles ou les fonctionnalités sont installés.

La syntaxe pour **ocsetup** est :



Le même exemple mais en utilisant **pkgmgr**.

```

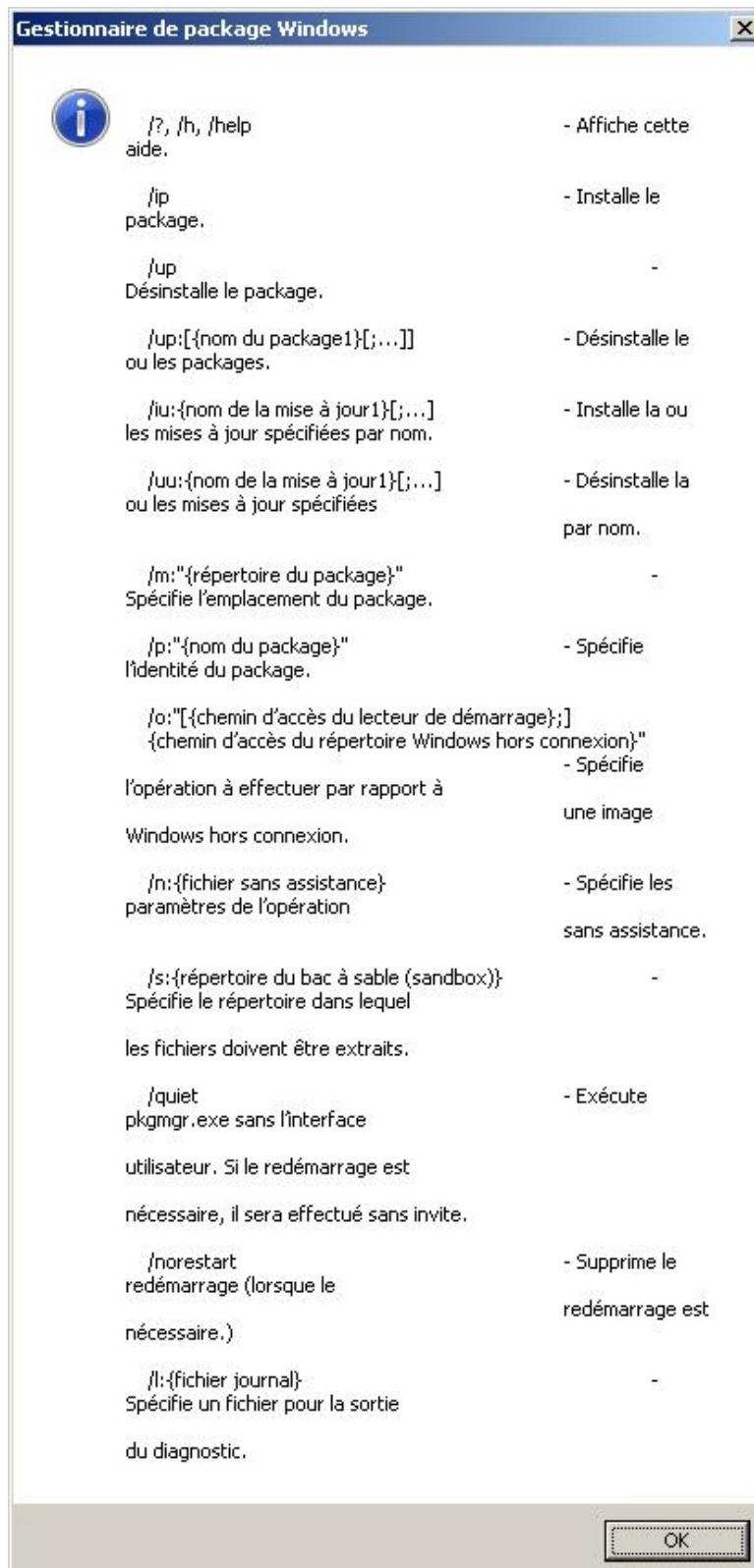
Administrator : C:\Windows\system32\cmd.exe

C:\>start /w pkgmgr /iu:DNS-Server-Core-Role
C:\>start /w pkgmgr /uu:DNS-Server-Core-Role

```

Si le rôle doit installer des services de rôle, il faut les ajouter à la fin de la ligne de commandes en les séparant par un point-virgule.

La syntaxe de **pkgmgr** est :



## a. Avantages et inconvénients d'ocsetup

Les inconvénients sont :

- La commande associée **oclist** ne peut être utilisée que sur un Server Core.
- Utilisable localement uniquement.
- Tous les rôles ne peuvent être installés en mode ligne de commandes.
- L'installation du rôle et des services de rôle est plus complexe qu'avec la commande **ServerManagerCmd**.

Les avantages sont :

- C'est une des deux méthodes possibles pour installer une fonctionnalité ou un rôle sur un Server Core.
- Permet d'installer ou d'enlever un composant.
- Peut être scriptable.

## b. Avantages et inconvénients de pkgmgr

Les inconvénients sont :

- Utilisable localement uniquement.
- Tous les rôles ne peuvent être installés en mode ligne de commandes.
- L'installation du rôle et des services de rôle est plus complexe qu'avec la commande **ServerManagerCmd**.

Les avantages sont :

- C'est une des deux méthodes possibles pour installer une fonctionnalité ou un rôle sur un Server Core.
- Permet d'installer ou d'enlever un composant.
- Peut être scriptable.

## 5. netsh



L'outil **netsh** est un outil ligne de commandes extensible utilisé pour configurer et surveiller des ordinateurs locaux ou distants.

Netsh accepte de créer de longues commandes pouvant être incluses dans des scripts.

Il dispose de commandes contextuelles vous permettant de vous déplacer dans l'application. Son mode de fonctionnement est le suivant :

- Dans une invite de commandes par exemple, commencez par saisir **netsh** pour entrer dans le premier niveau de l'application.

- Comme vous ne savez pas où vous diriger, saisissez **h** ou **help**, il n'est pas nécessaire de saisir la commande entière s'il n'existe pas d'ambiguïtés avec d'autres commandes.

Syntaxes et commandes de contextes de la commande **netsh** :

```

Administrator : Invite de commandes
C:\>netsh /?

Utilisation : netsh [-a Fichier_alias] [-c Contexte] [-r Ordinateur_distant]
               [-u [Nom_domaine\]Nom_utilisateur] [-p Mot_passe ; *]
               [Commande : -f Fichier_script]

Les commandes suivantes sont disponibles :

Commandes dans ce contexte :
?                               - Affiche une liste de commandes.
add                            - Ajoute une entrée de configuration à une liste d'entrées.
adufirewall                   - Modifications pour le contexte 'netsh adufirewall'.
bridge                         - Modifications pour le contexte 'netsh bridge'.
delete                         - Supprime une entrée de configuration d'une liste d'entrées.
dhcp                           - Modifications pour le contexte 'netsh dhcp'.
dhcpclient                     - Modifications pour le contexte 'netsh dhcpclient'.
dump                           - Affiche un script de configuration.
exec                           - Exécute un fichier script.
firewall                       - Modifications pour le contexte 'netsh firewall'.
help                           - Affiche une liste de commandes.
http                           - Modifications pour le contexte 'netsh http'.
interface                      - Modifications pour le contexte 'netsh interface'.
ipsec                          - Modifications pour le contexte 'netsh ipsec'.
lan                            - Modifications pour le contexte 'netsh lan'.
nap                           - Modifications pour le contexte 'netsh nap'.
netio                          - Modifications pour le contexte 'netsh netio'.
ras                           - Modifications pour le contexte 'netsh ras'.
rpc                           - Modifications pour le contexte 'netsh rpc'.
set                           - Met à jour les paramètres de configuration.
show                          - Affiche les informations.
winhttp                        - Modifications pour le contexte 'netsh winhttp'.
wins                          - Modifications pour le contexte 'netsh wins'.
winsock                        - Modifications pour le contexte 'netsh winsock'.

Les sous-contextes suivants sont disponibles :
adufirewall bridge dhcp dhcpclient firewall http interface ipsec lan nap netio ras rpc winh

Pour consulter l'aide d'une commande, entrez la commande, suivie par un
espace, et ensuite
entrez ?.

```

- Saisissez **interface** pour entrer dans le second niveau suivi de **h**. Vous remarquez que les commandes ont maintenant changé car vous n'êtes plus dans le même contexte que le niveau précédent. Vous ne pouvez pas remonter d'un niveau mais vous pouvez vous déplacer dans un autre contexte en utilisant soit les commandes du contexte actuel soit celles du contexte hérité.
- Saisissez **bye** ou **exit** pour quitter netsh.

Si vous connaissez le contexte dans lequel vous aimeriez aller, saisissez simplement **netsh -c Contexte** où **Contexte** est le nom du contexte.

L'intérêt de netsh est également de pouvoir créer des commandes qui peuvent être scriptées.

L'exemple suivant montre une commande netsh (netsh dhcp server show scope) qui a été stockée dans un fichier de script nommé showscopehcp.bat puis exécutée à partir de l'invite de commandes.

Adresse étendue	Masque sous-rés.	Etat	Nom étendue	Commentaire
172.30.1.0	- 255.255.255.0	-Actif	-Etendue4	-commentaire de
192.168.1.0	- 255.255.255.0	-Actif	-test	-
192.168.10.0	- 255.255.255.0	-Actif	-MonEtendue	-NouvelleEtendu

Nb total d'étendues = 3  
La commande s'est terminée correctement.

Comme les commandes sont contextuelles, c'est-à-dire qu'il existe des contextes applicatifs, ces contextes ne

— s'installent qu'avec des applications comme le contexte DHCP ou DNS. Il arrive comme effet indésirable que des commandes ne peuvent être lancées sur tous les ordinateurs car le contexte correspondant n'est pas installé.

---

### a. Avantages et inconvénients

L'inconvénient principal est :

- Apprentissage d'une philosophie de l'outil basé sur des contextes.

Les avantages sont :

- Les contextes peuvent être étendus grâce aux applications installées.
- Permet d'exécuter des commandes à distance.
- Peut être scriptable.
- Commandes orientées configuration et gestion de composants réseau.
- Aide en ligne contextuelle bien faite.
- Utilisation de commandes raccourcies si netsh peut identifier sans ambiguïté la commande par rapport à une autre.

## 6. Windows Remote Shell (WinRS) et Windows Remote Management (WinRM)

Windows Remote Shell est un outil de type ligne de commandes qui permet d'exécuter des commandes sur un ordinateur distant sur lequel est activé WinRM.

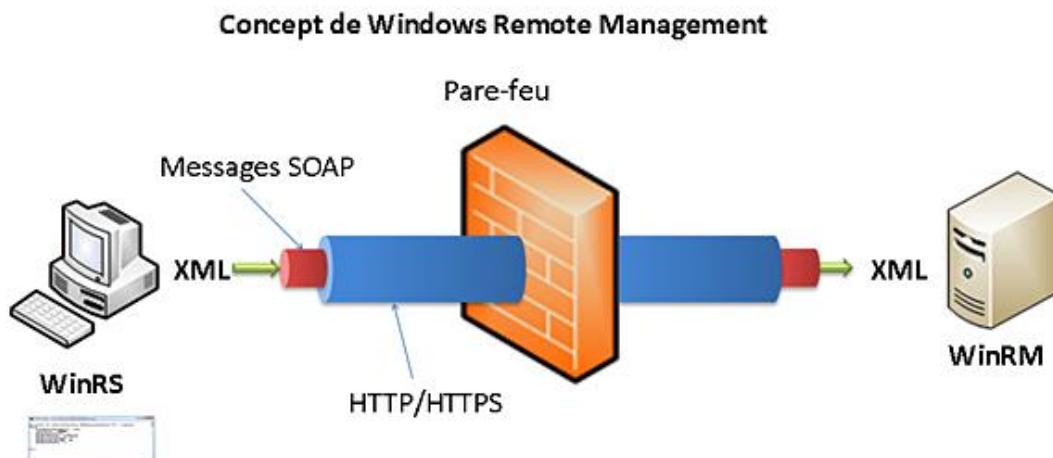
Windows Remote Management représente à la fois un outil qui permet de gérer et configurer un ordinateur localement ou à distance, ainsi que le Service Web correspondant.

---

► Le choix des noms est malheureux car WinRM signifie à la fois un protocole, un outil et un service Web !

---

Au lieu de se baser sur des échanges RPC, il utilise un protocole appelé WinRM (*Windows Remote Management*) qui est l'implémentation Microsoft de WS-Management (*Web Service Management*) du DMTF (*Distributed Management Task Force*) basé sur un protocole orienté service SOAP (*Simple Object Access Protocol*).



Le protocole WinRM peut être utilisé par des administrateurs pour créer des scripts, par des programmeurs pour créer des applications de gestion, et par d'autres acteurs informatiques. Par exemple, la notion de gestion distante de PowerShell V2 utilise WinRM.

Conceptuellement, un client envoie des requêtes HTTP ou HTTPS vers un service Web d'un serveur. Les pare-feu ne sont pas un obstacle et il n'est pas nécessaire d'installer un serveur Web sur le côté serveur. Concernant la sécurité, différents mécanismes d'authentification sont utilisés y compris le protocole Kerberos. Il est également possible d'ajouter les informations de connexions à une requête.

Windows Vista et Windows 2008 disposent dès l'installation de la partie serveur appelée **winrm** qui doit être activée pour l'utiliser. En téléchargeant winrm, il est également possible de l'installer sur Windows XP dès le SP2 et Windows Server 2003 dès le SP1.

Winrs est l'outil client que l'on exécute dans une invite de commandes qui envoie une commande vers le serveur sur lequel on a activé un service Web.

- La commande doit être une commande existante sur le serveur distant.

WinRS s'installe automatiquement sur les ordinateurs Windows Vista et Windows Server 2008.

- WinRS remplace de manière sécurisée et fiable un client Telnet ou un client SSH. WinRS est à utiliser comme une invite de commande alors que winrm permet de configurer winrm et de gérer le serveur avec des requêtes WMI.

La figure suivante montre la syntaxe de la commande **winrm** :

The screenshot shows a Windows Command Prompt window titled "Administrateur : Invite de commandes". The command entered is "C:\>winrm /?". The output provides detailed information about the WinRM command-line interface, including its purpose (managing Windows services over the network), usage (syntax for operations like GET, SET, CREATE, DELETE, etc.), specific operation help (like quickconfig, configSSDL, helpmsg), and help for related topics (URIs, aliases, configuration, certmapping, customremoteshell, remotening, help auth, help input, help switches).

```
C:\>winrm /?
Outil de ligne de commande de la Gestion à distance de Windows

La Gestion à distance de Windows (WinRM) est l'implémentation Microsoft du
protocole de gestion des services Web qui permet des communications sécurisées
avec les ordinateurs locaux et distants utilisant des services Web.

Utilisation :
  winrm OPÉRATION URI_RESSOURCE [-COMMUTATEUR:VALEUR [-COMMUTATEUR:VALEUR] ...]
  [(-CLÉ=VALEUR;CLÉ=VALEUR)...]

Pour obtenir de l'aide sur une opération spécifique :
  winrm g[et] -?      Récupérer des informations de gestion.
  winrm s[et] -?     Modifier des informations de gestion.
  winrm c[reate] -?   Créer des instances de ressources de gestion.
  winrm d[elete] -?   Supprimer une instance d'une ressource de gestion.
  winrm e[numerate] -? Lister toutes les instances d'une ressource de gestion.
  winrm i[nvoke] -?   Exécuter une méthode sur une ressource de gestion.
  winrm i[dentify] -? Déterminer si la gestion des services Web
                        s'exécute sur l'ordinateur distant.
  winrm q[uick]config -? Configurer l'ordinateur pour accepter les demandes de
                        gestion des services Web des autres ordinateurs.
  winrm configSSDL -? Modifie un descripteur de sécurité existant pour un URI.
  winrm h[elp]msg -?   Affiche un message d'erreur pour le code d'erreur.

Pour obtenir de l'aide sur les rubriques connexes :
  winrm help uris     Construction des URI de ressource.
  winrm help aliases   Abréviations des URI.
  winrm help config    Configuration du client WinRM et du service.
  winrm help certmapping Configure l'accès au certificat client.
  winrm help customremoteshell Configure un exécutable d'environnement et
                        les arguments correspondant à un URI d'environnement.
  winrm help remotening Accès aux ordinateurs distants.
  winrm help auth       Informations d'identification pour l'accès à distance.
  winrm help input      Entrées permettant de créer, de définir et d'appeler.
  winrm help switches   Autres commutateurs (format, options, etc.)

C:\>_
```

### a. Activation de Windows Remote Shell

La commande suivante est à exécuter sur le serveur que vous voulez administrer à distance. Elle va créer et activer le point d'entrée du service Web sur l'ordinateur distant appelé **écouteur**.

```
Winrm quickconfig
```

```
C:\>winrm quickconfig
WinRM n'est pas configuré pour la gestion à distance de cet ordinateur.
Les modifications suivantes doivent être effectuées :

Créez un écouteur WinRM sur HTTP://* pour accepter les demandes de la gestion de
ses services Web sur toutes les adresses IP de cet ordinateur.
Activez l'exception de pare-feu WinRM.

Effectuer ces modifications [y/n] ? y
WinRM a été mis à jour pour la gestion à distance.

Écouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestion des se
rvices Web sur toutes les adresses IP de cet ordinateur.
Exception de pare-feu WinRM activée.

C:\>
```

Cette commande paramètre l'utilisation du protocole HTTP qui utilise le port 80.

- Winrm permet également de lancer des commandes de configuration et des commandes WMI. Winrm est l'outil idéal pour retourner des informations WMI sans devoir utiliser un script sur un Server Core.

### b. Utiliser la commande winrm pour retourner des informations

La commande suivante récupère des informations de gestion :

```
Winrm get wmicimv2/win32_OperatingSystem -r :localhost
```

- **-r :serveur** indique le nom du serveur cible.

Les commandes suivantes listent les instances d'une ressource de gestion :

```
Winrm enumerate wmi/root/cimv2/win32_CacheMemory -r :localhost
```

```
Winrm enumerate wmi/root/cimv2/win32LogicalDisk -r :localhost
```

```
Winrm get wmi/root/cimv2/win32LogicalDisk?DeviceID=D: -r :localhost
```

Pour plus de souplesse, la commande suivante permet d'utiliser un filtre qui utilise le langage naturel d'interrogation de WMI appelé **WQL** (*WMI Query Language*).

La commande suivante liste tous les services qui sont démarrés :

```
Winrm enumerate wmicimv2/* -filter:"select * from win32_Service where state =
'running'"
```

### c. Afficher la configuration de winrm

```
Winrm get winrm/config
```

Le résultat de la commande précédente affiche les paramètres de configuration de WinRM que vous pouvez voir sur l'image suivante.

```
t - Bloc-notes
Fichier Edition Format Affichage ?
Config
  MaxEnvelopeSizekb = 150
  MaxTimeoutms = 60000
  MaxBatchItems = 20
  MaxProviderRequests = 25
Client
  NetworkDelayms = 5000
  URLPrefix = wsmans
  AllowUnencrypted = false
  Auth
    Basic = false
    Digest = true
    Kerberos = true
    Negotiate = true
    Certificate = true
  DefaultPorts
    HTTP = 80
    HTTPS = 443
  TrustedHosts
Service
  RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;GR;;;ER)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
  MaxConcurrentOperations = 100
  EnumerationTimeouts = 60000
  MaxConnections = 5
  AllowUnencrypted = false
  Auth
    Basic = false
    Kerberos = true
    Negotiate = true
    Certificate = false
  DefaultPorts
    HTTP = 80
    HTTPS = 443
  IPv4Filter = *
  IPv6Filter = *
Winrs
  AllowRemoteShellAccess = true
  IdleTimeout = 900000
  MaxConcurrentUsers = 5
  MaxShellRunTime = 2147483647
  MaxProcessesPerShell = 5
  MaxMemoryPerShellMB = 80
  MaxShellsPerUser = 2
```

#### d. Modifier un paramètre de configuration

La copie d'écran suivante montre une commande winrm lancée depuis Windows Vista et modifiant la configuration winrm d'un serveur Windows 2008 Server Core.

```
Administrator : Invite de commandes
C:\>winrm set winrm/config/Winrs @<MaxConcurrentUsers="6"> -r:jupiter
Winrs
  AllowRemoteShellAccess = true
  IdleTimeout = 900000
  MaxConcurrentUsers = 6
  MaxShellRunTime = 2147483647
  MaxProcessesPerShell = 5
  MaxMemoryPerShellMB = 80
  MaxShellsPerUser = 2

C:\>
```

#### e. Avantages et inconvénients de winrm

Les inconvénients sont :

- Configuration avancée complexe.
- Documentation des scénarios possibles encore limitée.
- Différentes versions de winrm existent avec des fonctionnalités différentes (Windows 2003).

- Confusion possible au niveau du nom entre le protocole, l'outil et le concept.
- Apprentissage et connaissance requise des classes WMI et du langage WQL.

Les avantages sont :

- Installation et configuration basique facile.
- Utilisable sur un ordinateur distant.
- Aide compréhensible.
- Les commandes peuvent facilement être intégrées dans un script.
- Outil d'administration adapté pour retourner des informations WMI.
- Utilise comme couche de transport des services Web et de ce fait n'est pas sensible aux pare-feu.
- Permet de travailler dans des contextes de sécurité différents.

## f. Utiliser l'outil **winrs**

L'outil **winrs** permet d'exécuter des commandes à distance en passant par un écouteur winrm. La syntaxe est la suivante :

```
Winrs -r :<NomDuServeur> <commande>
```

La figure suivante montre la syntaxe complète :

C:\>winrs /?

**Syntaxe**

=====

<MAJUSCULES = valeurs à fournir par l'utilisateur.>

winrs [</COMMUTATEUR[:VALEUR]>] COMMANDE

**COMMANDE** – Chaîne exécutable en tant que commande dans l'environnement cmd.exe.

**COMMUTATEURS**

=====

<La forme courte ou longue est acceptée pour tous les commutateurs. Par exemple, -r et -remote sont tous les deux valides.>

-r[remote]:POINT\_DE\_TERMINAISON – point de terminaison cible utilisant un nom NetBIOS ou l'URL de connexion standard : [TRANSPORT://]CIBLE:PORT]. À défaut, -r:localhost est utilisé.

-un[encrypted] – Les messages destinés à l'environnement distant ne sont pas chiffrés. Cela est utile pour résoudre les problèmes ou lorsque le trafic réseau est déjà chiffré avec ipsec, ou encore lors de la mise en œuvre d'une sécurité physique. Par défaut, les messages sont chiffrés avec des clés Kerberos ou NTLM. Ce commutateur est ignoré lorsque le transport HTTPS est sélectionné.

-u[username]:NOM\_UTILISATEUR – nom d'utilisateur sur la ligne de commande. À défaut, l'outil utilise l'authentification négociée ou demande d'entrer un nom. Si -username est spécifié, -password doit l'être également.

-p[password]:MOT\_DE\_PASSE – Mot de passe sur la ligne de commande. Si -password n'est pas spécifié contrairement à -username, l'outil demande d'entrer le mot de passe. Si -password est spécifié, -user doit l'être également.

-t[timeout]:SECONDES – Délai d'attente en secondes. Délai maximal d'exécution de la commande. Par défaut, le délai est illimité.

-d[directory]:CHEMIN – Répertoire de démarrage de l'environnement distant. À défaut, l'environnement distant démarre dans le répertoire d'accueil de l'utilisateur défini par la variable d'environnement USERPROFILE%.

-env[ironment]:CHAÎNE=VALEUR – Variable d'environnement unique à définir au démarrage de l'environnement, ce qui permet de changer l'environnement par défaut. Plusieurs occurrences de ce commutateur sont nécessaires pour spécifier plusieurs variables d'environnement.

-noe[cho] – L'écho est désactivé. Cela permet de s'assurer que les réponses de l'utilisateur aux messages distants ne sont pas affichées localement. Par défaut, l'écho est activé.

-nop[rofile] – Indique que le profil de l'utilisateur ne doit pas être chargé. Par défaut, le serveur tentera de charger le profil de l'utilisateur. Si l'utilisateur distant n'est pas un administrateur local du système cible, cette option sera nécessaire (la valeur par défaut engendrerait une erreur).

-? – Aide

Pour terminer la commande distante, l'utilisateur peut entrer Ctrl+C ou Ctrl+Pause, qui est envoyé à l'environnement distant. Un second Ctrl+C force l'arrêt de winrs.exe.

Pour gérer les environnements distants actifs ou la configuration WinRS, l'utilisateur dispose de l'outil winRM. L'alias d'URI pour gérer les environnements actifs est shell/cmd. L'alias d'URI pour la configuration WinRS est winrm/config/winrs.

Un exemple de syntaxe est disponible dans l'outil WinRM en tapant "WinRM -?".

La copie d'écran suivante montre un ordinateur exécutant Windows Vista affichant la liste des rôles et fonctionnalités installés sur un serveur Windows 2008 Server Core.

```
C:\>winrs -r:jupiter oclist
Utilisez les noms mis à jour avec Ocsetup.exe pour installer ou désinstaller un rôle de serveur ou une fonction en option.

L'ajout ou la suppression du rôle Active Directory avec OCSetup.exe n'est pas pris en charge. Cela peut laisser votre serveur dans un état instable. Utilisez toujours DCPromo pour installer ou désinstaller Active Directory.

=====
Microsoft-Windows-ServerCore-Package
Non installé :BitLocker
Non installé :BitLocker-RemoteAdminTool
Non installé :ClientForNFS-Base
Non installé :DFSMN-Server
Non installé :DFSR-Infrastructure-ServerEdition
Non installé :DHCPServerCore
Non installé :DirectoryServices-ADAM-ServerCore
Non installé :DirectoryServices-DomainController-ServerFoundation
Non installé :DNS-Server-Core-Role
Non installé :FailoverCluster-Core
Non installé :FRS-Infrastructure
Non installé :IIS-WebServerRole
:
--- Non installé :IIS-FTPPublishingService
```

### g. Avantages et inconvénients de winrs

L'inconvénient principal est :

- Il faut que sur le serveur distant winrm soit installé et activé.

Les avantages sont :

- Permet d'exécuter des commandes à distance.
- Aide compréhensible.
- Peut être scriptable.
- Utilise comme couche de transport des services Web et de ce fait n'est pas sensible aux pare-feu.
- Permet de travailler dans des contextes de sécurité différents.
- Utilisable sur d'autres versions de Windows.

### h. Créer des scripts VBS utilisant WinRM

L'exemple suivant montre juste comment créer un script en VBS en utilisant WinRM.

```
'ordinateur distant
strComputer = "Jupiter"

'Query
'Retourne la liste de tous les processus dont la priorité > 8
strQuery = "select * from win32_Process where Priority > 8"

'Ressources
strRes = "http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/*"
strDial = "http://schemas.microsoft.com/wbem/wsman/1/WQL"

'Objet utilisé
Set wsman = CreateObject("wsman.Automation")

'Création d'une session
Set Session = wsman.CreateSession ("http://" & strComputer)

'Recherche toutes les instances
set Reponse = Session.Enumerate(strRes, strQuery, strDial)

'Formatte et affiche chaque instance dans une boîte de dialogue
Do until Reponse.AtEndofStream
    Set xmlFile = CreateObject( "MSXML2.DOMDocument.3.0" )
    Set xslFile = CreateObject( "MSXML2.DOMDocument.3.0" )
    xmlFile.LoadXML(Reponse.ReadItem)
    xslFile.Load( "WsmTxt.xsl" )
    Wscript.Echo xmlFile.TransformNode( xslFile )
Loop
```

➤ Les scripts VBS peuvent également initier des requêtes winrm et pallier l'absence du langage PowerShell sur un Server Core.

## 7. WMIC

WMIC (*Windows Management Instrumentation Command-line*) est un outil de type ligne de commande qui permet d'interroger à l'aide d'une interface simple et relativement intuitive des objets WMI car il utilise des alias. Son principal avantage est qu'il est déjà installé donc il n'y a pas besoin de le télécharger et de l'installer sur l'ordinateur où l'on désire effectuer quelques interrogations. Il supporte l'imPERSONNALISATION et l'INTERROGATION DES ORDINATEURS DISTANTS.

Son fonctionnement est semblable à netsh, c'est-à-dire soit vous fonctionnez en mode script et saisissez toute la commande, soit vous travaillez en mode interactif en tapant wmic puis, pour connaître les commandes et alias disponibles, /?

➤ À l'inverse de netsh, il est nécessaire de saisir la commande comme indiqué dans la syntaxe.

Pour afficher le nom des utilisateurs locaux :

```
Wmic useraccount get name
```

Pour disposer de l'aide sur un alias :

```
Wmic useraccount /?
```

Pour connaître les propriétés accessibles en écriture :

```
Wmic useraccount set /?
```

Pour afficher la liste des services et toutes ses propriétés :

```
Wmic service
```

## **Avantages et inconvénients de WMIC**

Les inconvénients sont :

- Méthode peu conventionnelle pour accéder à WMI.
- Fait double emploi avec PowerShell.
- Limité à WMI.

Les avantages sont :

- Plus facile et intuitif à utiliser que WMI.
- Fonctionne sur un Server Core.
- Peut être intégré dans un script.
- Outils standards.

## **8. Quelle stratégie mettre en œuvre pour configurer et gérer Windows Server 2008 ?**

Quelle meilleure plate-forme pour gérer Windows Server 2008 qu'une autre plate-forme Windows Server 2008 ! En effet, les outils graphiques comme le gestionnaire de serveur ou les consoles MMC ont été conçus pour ne fonctionner que sur Windows Server 2008. Seuls les outils en ligne de commandes comme **RemoteShell** et **winrm** permettent d'utiliser d'autres plates-formes Windows.

 Dans tous les cas, l'utilisation intelligente des stratégies de groupes permet de limiter au maximum la configuration et la gestion d'un serveur.

Dans un environnement d'entreprise normal, pour configurer et gérer n'importe quelle édition Windows Server 2008 complète, il faut utiliser l'administration à distance pour se connecter sur un serveur Windows 2008, puis utiliser le gestionnaire de serveur et les consoles MMC.

Dans un environnement d'entreprise normal pour configurer et gérer n'importe quelle édition Windows Server 2008 Core, il faut :

- Se connecter localement pour terminer les opérations de post-installation comme cela a été décrit dans le chapitre consacré à l'installation.
- Utiliser soit l'administration à distance avec l'invite de commandes soit le **Windows Remote Shell** pour configurer le serveur.
- Utiliser à partir d'une édition complète de Windows Server 2008, les consoles MMC. Si une console est absente, il est toujours possible de l'installer avec la fonctionnalité **Outils d'administration à distance**.

Dans tous les cas, l'automatisation des tâches répétitives à l'aide des commandes de type ligne de commandes que vous placez dans des fichiers que l'on appelle des scripts vous permettent de gagner du temps ainsi que diminuer les erreurs d'inattention, voire de saisie !

 La création de nombreux scripts basés sur WinRM permet à un administrateur de disposer d'une bibliothèque utilisable de manière plus simple et plus fiable que d'écrire la commande.

 Utilisez les scripts partout où vous pouvez.

Un script peut être composé d'une seule commande ou de plusieurs commandes.

# Microsoft Outils disposant d'une interface graphique

Cette catégorie se divise en trois outils, à savoir :

- le Gestionnaire de serveur,
- la console MMC et les composants logiciels enfichables,
- l'accès distant.

## 1. Le Gestionnaire de serveur

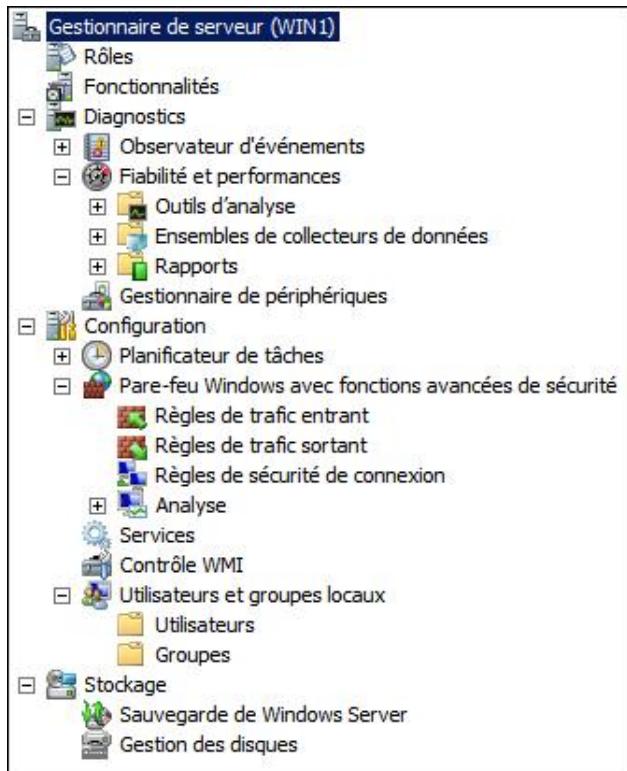
Le Gestionnaire de serveur est l'outil principal de l'administrateur sous Windows Server 2008. Il permet de configurer et de gérer avec un seul outil l'ensemble des tâches qui lui sont dévolues.

 Il n'est pas possible d'utiliser cet outil sur un Server Core.

Voici les tâches qu'un administrateur peut effectuer à l'aide du Gestionnaire de serveur :

- Configurer le serveur.
- Ajouter ou supprimer un rôle ou une fonctionnalité.
- Déterminer l'état d'un rôle ou d'un service et le configurer.
- Afficher les événements associés à un rôle ou tous les événements.
- Gérer les pilotes et le matériel.
- Déterminer les goulets d'étranglement et optimiser le serveur.
- Gérer le stockage.
- Gérer la sécurité du pare-feu.
- Planifier des tâches.
- Gérer des utilisateurs locaux.
- Dépanner des problèmes.

 Le Gestionnaire de serveur ne fonctionne qu'en mode local.



### a. Lancer le Gestionnaire de serveur



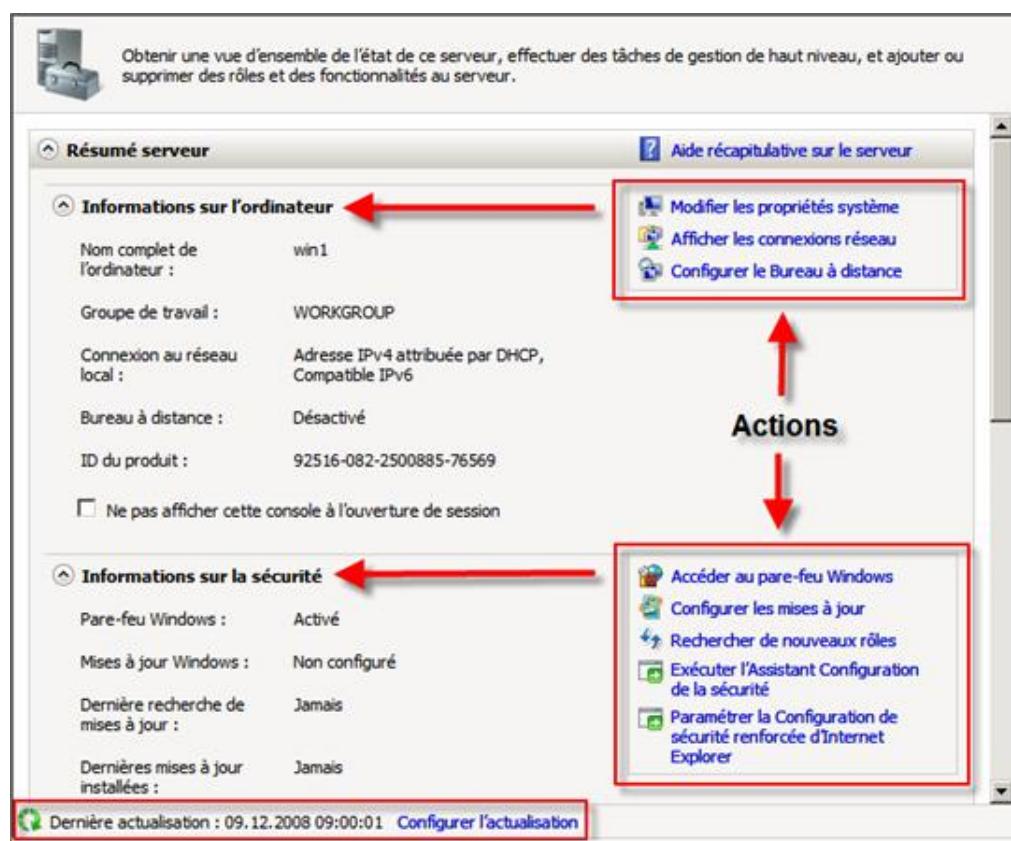
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.

À l'ouverture, la fenêtre principale affiche la zone résumé contenant les éléments de configuration actuels du serveur.

- 
- Si la zone résumé n'est pas visible, cliquez dans l'arborescence de la console sur **Gestionnaire de serveur**.
-



Chaque sous-section affiche les informations de manière claire et concise. Si vous désirez modifier un ou plusieurs de ces paramètres, vous pouvez utiliser directement les liens qui sont affichés sur la droite, que l'on appelle **actions**, pour faire apparaître l'outil de configuration correspondant.



Sur l'image précédente, **Configurer l'actualisation** permet de définir la fréquence d'actualisation des données. Par défaut la valeur est de 2 minutes, vous pouvez la modifier voire la désactiver.

La zone résumé se compose de 4 sous-sections regroupant logiquement des paramètres de configuration à savoir :

- Résumé du serveur
- Informations sur l'ordinateur

- Informations sur la sécurité
- Résumé des rôles
  - Rôles
- Résumé des fonctionnalités
  - Fonctionnalités
- Ressources et support

La section **Information sur l'ordinateur** contient les paramètres suivants :

Information	Contenu
Nom complet de l'ordinateur	Nom FQDN sur serveur. Action : <b>Modifier les propriétés système</b>
Nom du domaine ou du groupe de travail	Nom DNS du domaine ou du groupe de travail. Action : <b>Modifier les propriétés système</b>
Nom de la connexion réseau	Une ligne par carte réseau, indiquant le ou les protocoles activés et si l'adresse IP est statique ou dynamique. Action : <b>Afficher les connexions réseau</b>
État du bureau à distance	<b>Activé</b> ou <b>Désactivé</b> Action : <b>Configurer le bureau à distance</b>
ID du produit	Ce n'est pas la clé produit Windows mais un identifiant créé lors de l'installation.
Ne pas afficher cette console à l'ouverture de session	<input type="checkbox"/> <b>Activé</b> ou <b>Désactivé</b> Vous pouvez également modifier la clé de la base de registre suivante : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Server Manager La valeur 0 (défaut) indique que la fenêtre s'ouvre à l'ouverture de session, sinon y placer la valeur 1.

La section **Information sur la sécurité** contient les paramètres suivants :

Information	Contenu
État du pare-feu	<b>Activé</b> ou <b>Désactivé</b> Action : <b>Accéder au pare-feu</b>
État de Windows Update	<b>Configuré</b> ou <b>Non configuré</b> Action : <b>Configurer les mises à jour</b>
Dernière recherche de mise à jour	<b>Date</b> ou <b>Jamais</b>
Dernières mises à jour installées	<b>Date</b> ou <b>Jamais</b>
Configuration de sécurité renforcée d'Internet Explorer	<b>Activer ou désactiver pour les administrateurs</b> <b>Activer ou désactiver pour les utilisateurs</b>

Les deux actions dont aucun résultat n'est affiché sont :

- Rechercher de nouveaux rôles.
- Exécuter l'Assistant de configuration de la sécurité.

**Rechercher de nouveaux rôles** va rechercher sur Internet s'il existe de nouveaux rôles, leur téléchargement s'effectuera via Windows Update. Il existe au moins un nouveau rôle.

 Cette action serait mieux placée dans la section Résumé des rôles.

**Exécuter l'Assistant Configuration de la sécurité** est un assistant précieux qui permet de personnaliser la sécurité des rôles, des services de rôles et fonctionnalités. Un assistant similaire est apparu avec Windows Server 2003 SP1.

 Il est dommage que le Gestionnaire de serveur n'affiche pas des informations sur le dernier lancement de l'**Assistant de configuration de la sécurité** et sur la date des dernières modifications, voire si un fichier de configuration a été utilisé.

La section **Ressources et support** permet les actions suivantes :

Action	Conséquence
Participer au programme d'amélioration du produit	Permet de participer au programme d'amélioration du produit en envoyant régulièrement de manière anonyme des informations statistiques.  Aucune information permettant de vous identifier, vous ou votre entreprise, n'est recueillie.  Il n'est malheureusement pas possible de consulter les données recueillies avant leur envoi.
Activer le rapport d'erreurs de Windows	Permet d'activer votre participation au programme d'amélioration Microsoft en leur envoyant automatiquement des informations en cas d'erreur.  Si vous désirez recevoir une réponse, vous ne pourrez pas être anonyme.
Windows Server TechCenter	Renvoie à une page Internet de Microsoft Technet concernant le Gestionnaire de serveur consacré à Windows Server 2008. C'est un point de départ pour consulter d'autres informations sur le Technet.
Centre de la communauté Windows Server	Renvoie une page Internet qui centralise des liens pour accéder à des blogs, des groupes de discussion, des forums, des groupes d'utilisateurs, des webcasts, des sites communautaires et des discussions instantanées techniques concernant Windows Server 2008.  <b>Attention</b> , cette page est en anglais.
Envoyer des commentaires à Microsoft	Permet d'envoyer via un formulaire Internet des suggestions ou des feedbacks en anglais concernant Windows Server 2008.

## b. Avantages et inconvénients

Les inconvénients sont :

- Ne fonctionne que sur un serveur Windows 2008.
- Ne gère que des serveurs Windows 2008.
- Ne permet de gérer que le serveur local.

- L'affichage des informations sur la sécurité est laconique.
- Ne peut s'utiliser avec un Server Core.

Les avantages sont :

- Reconstruit automatiquement la base de données des rôles et des fonctionnalités si elle est corrompue.
- Outil bien conçu.
- Intègre également certains composants logiciels enfichables. Il n'est pas nécessaire de les lancer séparément.

## 2. Console MMC

La console **MMC** est une coquille vide qu'il faut remplir avec des programmes spéciaux appelés **composants logiciels enfichables** ou **snap-ins** en anglais. Un snap-in est un logiciel qui fonctionne à l'intérieur d'un autre logiciel.

 L'utilisation d'un snap-in est toujours identique, il faut utiliser l'arborescence pour se déplacer d'un élément à un autre et le clic droit pour faire apparaître le menu contextuel des actions possibles. La fenêtre centrale est réservée principalement à l'affichage.

Le snap-in fonctionne selon un mode client/serveur, c'est-à-dire qu'il faut une application serveur capable de répondre aux requêtes du snap-in client.

 Pour un Server Core, seule la partie serveur d'un snap-in peut être installée. La partie cliente doit obligatoirement se trouver sur un ordinateur distant. En d'autres termes, il n'est pas possible d'y installer l'outil **console MMC**.

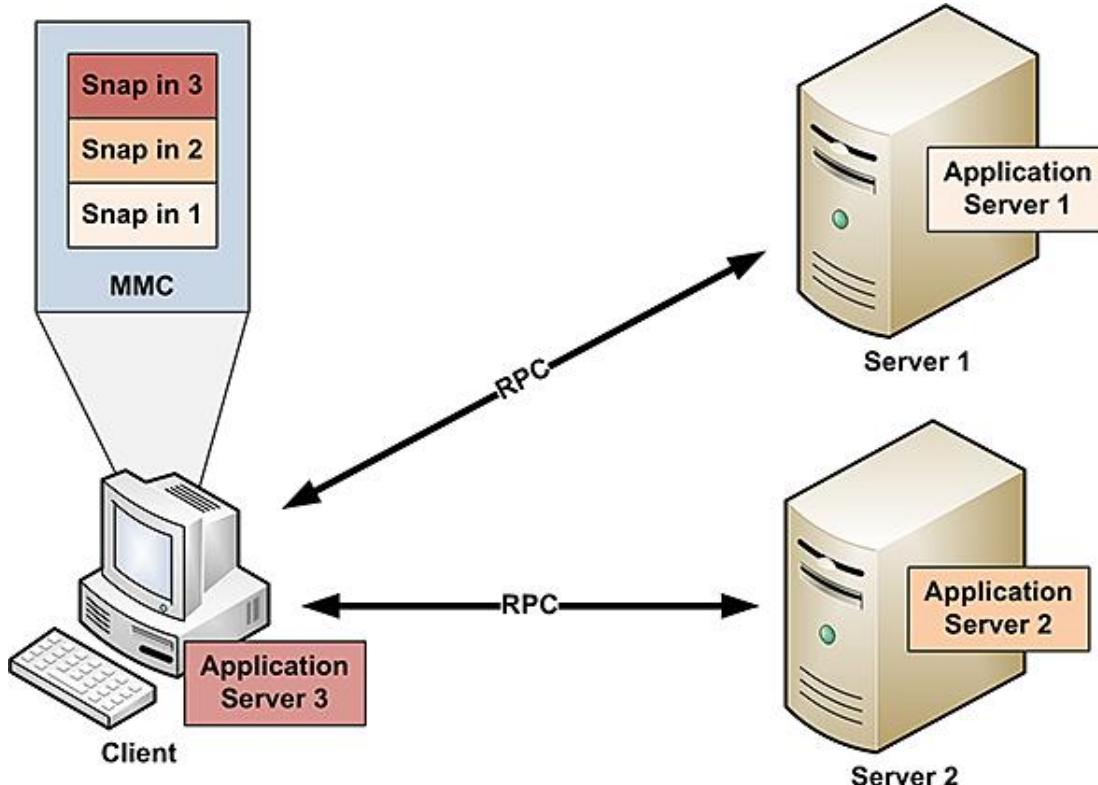
Les snap-ins utilisent entre autres le protocole RPC (*Remote Procedure Call*) pour communiquer entre le client et le serveur. Les applications clientes doivent être enregistrées auprès de la base de registre à l'aide de la commande **regsvr32**.

L'exemple suivant permet d'enregistrer la DLL de l'application cliente pour gérer le schéma dans une Active Directory. Il est nécessaire que le fichier DLL se trouve sur l'ordinateur.



```
C:\>regsvr32 %systemroot%\system32\schmmgmt.dll
```

La figure suivante montre le schéma de fonctionnement. Bien entendu, les fichiers DLLs correspondant aux snap-ins sont bien enregistrés dans la base de registre de l'ordinateur client :



La console MMC est un outil totalement personnalisable permettant la création de consoles adaptées aux niveaux des collaborateurs d'un département informatique.

- ➊ Certains snap-ins disponibles sur d'anciennes versions de Windows peuvent être compatibles avec Windows Server 2008. Néanmoins, il est possible que les nouvelles fonctionnalités ne soient alors pas disponibles.

### a. Création d'une console personnalisée en lecture seule



- Cliquez sur **Démarrer** puis saisissez **mmc** dans la zone **Rechercher** et appuyez sur [Entrée].
- Une fois la console ouverte, cliquez sur le menu **Fichier** puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
- Dans la boîte de dialogue **Ajouter ou supprimer un composant logiciel enfichable**, sélectionnez les composants de la liste de gauche pour les ajouter à la liste de droite :

**Gestion de l'ordinateur**, dans la boîte de dialogue sélectionnez **Ordinateur local**.

**Gestion des disques**, dans la boîte de dialogue qui apparaît, sélectionnez **Cet Ordinateur** et **Bureaux à distance**, enfin cliquez sur **OK**.

Les autres boutons de la boîte de dialogue sont :

**Supprimer** : permet de supprimer de la liste de droite le composant sélectionné.

**Monter** : permet de déplacer vers le haut le composant sélectionné.

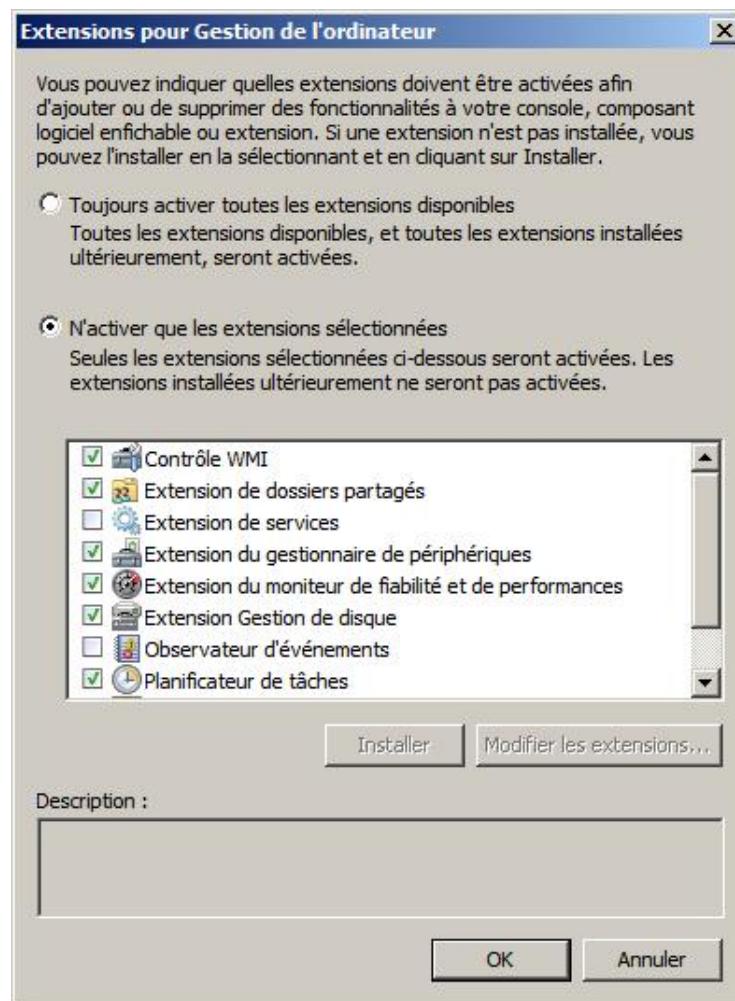
**Descendre** : permet de déplacer vers le bas le composant sélectionné.

**Avancé** : permet de créer des hiérarchies complexes en plaçant des composants enfants d'autres composants. Pour l'activer, il faut cocher la case de la boîte de dialogue avant de cliquer sur **OK** comme le montre l'image suivante :

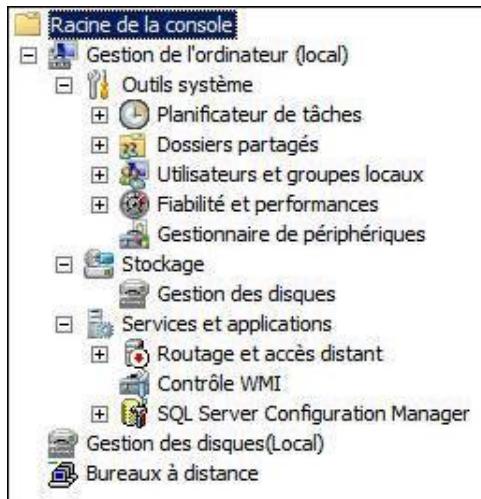


**Modifier les extensions** : certains composants disposent de plusieurs fonctionnalités appelées extensions que l'on peut sélectionner et installer afin de ne disposer que des outils dont on a besoin. Vous ne pouvez pas utiliser une extension tant qu'elle n'est pas installée.

- Dans la liste de droite, veuillez sélectionner **Gestion de l'ordinateur** puis cliquez sur **Modifier les extensions**, ensuite cliquez sur **N'activer que les extensions sélectionnées** et désélectionnez les extensions comme le montre la figure suivante. Enfin, cliquez deux fois sur **OK**.



Finalement la console ressemble à la capture d'écran suivante, veuillez noter que l'**Extension de services** et l'**Observateur d'événements** ont été retirés de **Gestion de l'ordinateur**, de même que **Gestion des disques** se trouve deux fois :



- Cliquez sur le menu **Fichier** puis sur **Options**.



L'onglet **Nettoyage de disque** permet de supprimer du profil de l'utilisateur qui a utilisé la console MMC les fichiers qui contiennent les modifications de l'affichage.

Dans l'onglet **Console**, le bouton **Changer l'icône** permet de choisir une icône spécifique pour votre console. Le texte qui affiche **Console1** peut être modifié. Il s'agit du nom de la console.

La liste déroulante **Mode de console** permet de sélectionner comment la console peut être modifiée.

- Le **mode auteur** est le mode par défaut lorsque vous ouvrez une nouvelle console MMC vide ; dans ce mode on peut tout faire.
- Le **mode utilisateur - accès total** est identique au mode auteur mais il n'est pas possible d'ajouter ou de supprimer un composant ou de modifier les options de la console, de créer des favoris ou de créer une liste des tâches.

- Le **mode utilisateur - accès limité, fenêtre multiple** donne accès uniquement aux parties de l'arborescence qui étaient visibles lorsque la console a été créée et permet également de créer de nouvelles fenêtres, mais pas de fermer les fenêtres existantes.
- Le **mode utilisateur - accès limité, fenêtre unique** permet de se déplacer uniquement dans la partie de l'arborescence visible.

La case à cocher **Ne pas enregistrer les modifications apportées à cette console** n'enregistre pas les modifications apportées au cours de la session. À utiliser en conjonction avec un mode utilisateur.

 Attention, si cette option est sélectionnée, vous ne pouvez plus modifier et enregistrer ces modifications. Il faut toujours conserver une console originale et activer cette option sur une copie ou saisir la commande suivante : **mmc /a maconsole.msc**.

La case à cocher **Autoriser l'utilisateur à personnaliser les vues** permet d'accéder à la boîte de dialogue **Personnalisation de l'affichage** en passant par le menu **Affichage - Personnaliser**. A utiliser en conjonction avec un mode utilisateur.

- Le nom de la console doit être **Ma super console**. Le mode console suivant doit être sélectionné : **mode utilisateur - accès limité, fenêtre unique**. La case à cocher **Ne pas enregistrer les modifications apportées à cette console** doit être sélectionnée. Enfin cliquez sur **OK**.
- Cliquez sur le menu **Fichier - Enregistrer**.
- Dans la boîte de dialogue **Enregistrer sous**, sélectionnez un emplacement et un nom pour la console comme par exemple le Bureau et MaConsole puis cliquez sur **Enregistrer**.
- Fermez la console.

 Notez que la console s'enregistre dans un fichier avec une extension **msc**.

Voilà, vous venez de créer une console personnalisée. Pour l'utiliser, il suffit de cliquer sur le fichier msc.

## b. Déploiement d'une console MMC

L'avantage d'une console MMC personnalisée est de pouvoir ensuite la rappeler à tout moment, voire de la distribuer aux autres membres de l'équipe.

Il faut être attentif au fait que la console MMC utilise deux éléments à savoir :

- Le fichier msc qui contient les éléments à afficher dans la console et les paramètres de présentation.
- Les fichiers exécutables DLLs (*Dynamic Link Library*) qui sont les programmes snap-ins dont la console a besoin.

Dans de grandes équipes, les fichiers msc personnalisés et enregistrés en mode utilisateur non modifiable sont placés sur un partage et utilisés par les membres de l'équipe.

 C'est une excellente pratique de créer des consoles MMC personnalisées et de les envoyer à un administrateur distant afin de résoudre un problème spécifique en limitant les extensions visibles.

Dans tous les cas, soyez vigilant à ce que les fichiers exécutables du snap-in se trouvent sur le serveur où sera exécutée la console MMC et sont également enregistrés dans la base de registre avant de distribuer vos fichiers msc.

## c. Rafraîchissement manuel d'une console MMC

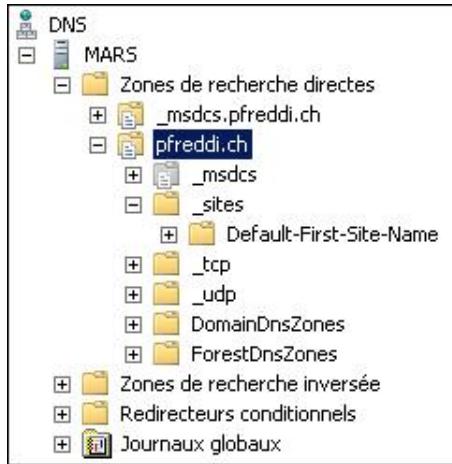
Un problème fréquemment rencontré avec les consoles MMC concerne le rafraîchissement des informations. Souvent on constate qu'une information que l'on vient d'ajouter n'apparaît pas dans l'arborescence de la console.

Effectivement, la console MMC ne réactualise pas toujours ces informations, il est donc nécessaire de la réactualiser manuellement.

C'est un problème largement connu, dont ne souffrent pas les consoles MMC de Windows Server 2008.

Si vous y êtes confronté, il faut prêter une attention toute particulière à l'endroit sélectionné dans l'arborescence, car le rafraîchissement interviendra à partir du nœud sélectionné et se propagera uniquement vers les éléments enfants de ce nœud.

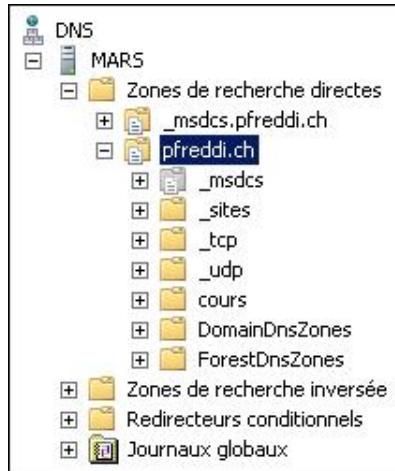
L'exemple suivant décrit le problème de réactualisation. Sur votre console MMC **Gestionnaire DNS**, le nœud sélectionné est **pfreddi.ch** qui correspond à une zone de recherche directe.



Un autre administrateur à l'aide d'une autre console MMC sur son ordinateur a créé une nouvelle zone directe appelée eni.fr sur le même serveur DNS. Il a également ajouté un sous-domaine appelé cours au domaine pfreddi.ch.

Comme il serait possible de le constater, la console MMC **Gestionnaire DNS** n'a pas réactualisé le contenu de l'arborescence de la console et ressemble toujours à la figure précédente.

Si vous rafraîchissez votre console en laissant le nœud pfreddi.ch sélectionné comme montré sur la figure précédente, seul le contenu du nœud pfreddi.ch est actualisé comme c'est le cas de la figure suivante. Seul le sous-domaine créé **cours** apparaît, mais pas la nouvelle zone eni.fr.



Pour réactualiser le contenu et faire apparaître la zone eni.fr, il faut sélectionner au moins le nœud **Zones de recherches directes**, voire le nœud **MARS** ou **DNS**. Dans ces deux derniers cas, il est nécessaire de se déplacer dans l'arborescence.



#### d. Création d'une console personnalisée disposant d'une vue de la liste des tâches



Win4

La délégation de l'administration passe également par l'utilisation d'outils adaptés au niveau du technicien ou de l'administrateur ainsi qu'au rôle qu'il joue.

La création d'une console personnalisée est intéressante, restreindre les extensions est encore mieux mais pas suffisant. Il serait intéressant de faciliter l'accès aux actions pour l'utilisateur de la console. Pour cela, il faut créer une vue de la liste des tâches.

Dans l'exemple suivant, vous allez créer une console qui permet uniquement de gérer les périphériques du Gestionnaire de périphérique ainsi que d'ajouter et gérer des utilisateurs locaux. L'exemple présenté ici est une des méthodes possible pour effectuer cette personnalisation, il a été retenu pour son côté pédagogique.

- Cliquez sur **Démarrer** puis saisissez **mmc** dans la zone **Rechercher** et appuyez sur [Entrée].
- Une fois la console ouverte, cliquez sur le menu **Fichier** puis sur **Ajouter/Supprimer un composant logiciel enfichable**.
- Dans la boîte de dialogue **Ajouter ou supprimer des composants logiciels enfichables**, sélectionnez et ajoutez **Gestion de l'ordinateur (ordinateur local)**.
- Sélectionnez **Gestion de l'ordinateur** puis cliquez sur **Modifier les extensions**.
- Dans la boîte de dialogue **Extensions pour Gestion de l'ordinateur**, activez l'option **N'activez que les extensions sélectionnées** et ne laissez sélectionnées que **Extension du gestionnaire de périphériques** et **Utilisateurs et groupes locaux**, puis cliquez sur **OK** deux fois.

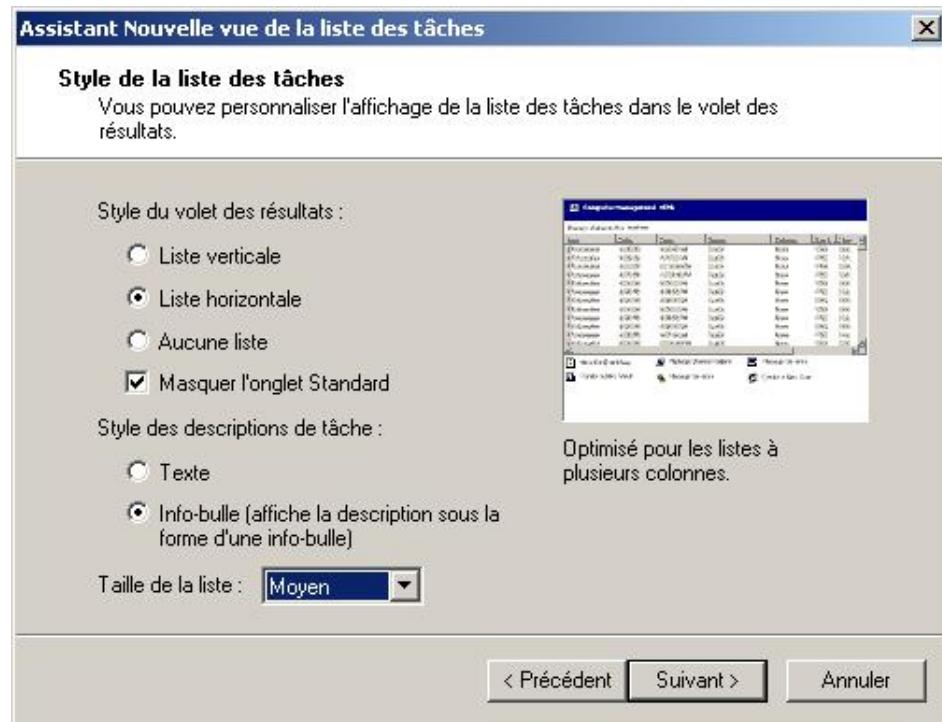
La console créée doit ressembler à celle présentée ci-après :



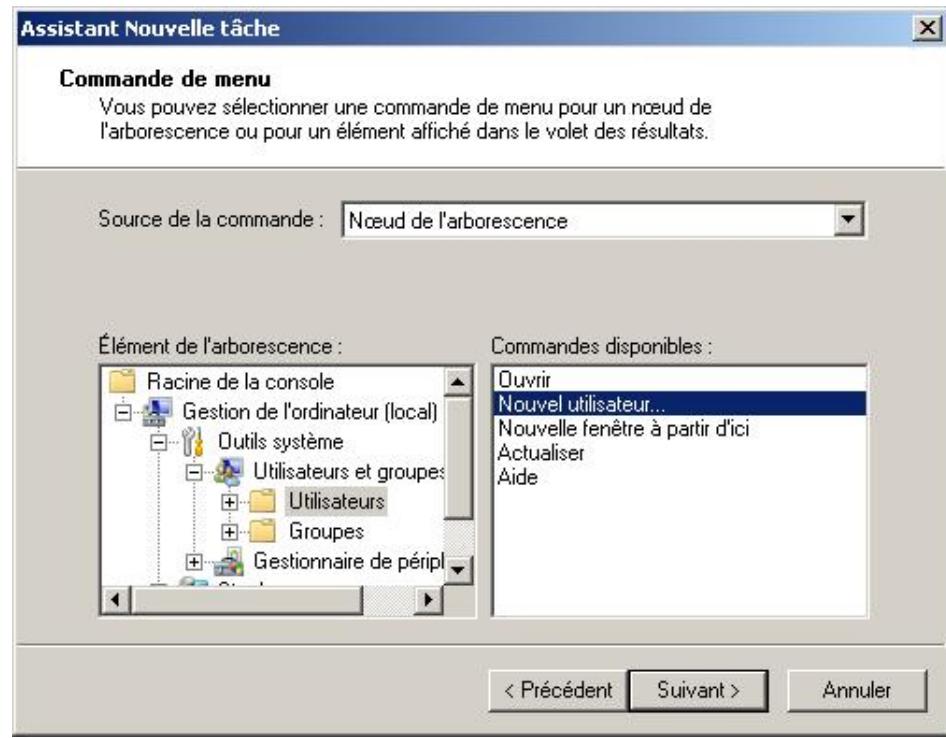
Vous remarquez que les nœuds **Stockage** et **Services et applications** sont vides.

- Cliquez avec le bouton droit de la souris sur le nœud **Outils système** puis sur **Nouvelle fenêtre à partir d'ici**.
- Dans la nouvelle fenêtre, cliquez avec le bouton droit de la souris sur le nœud **Outils système** puis sur **Nouvelle vue de la liste des tâches**.
- Sur la page **Assistant Nouvelle vue de la liste des tâches** de l'assistant, cliquez sur **Suivant**.

- Sur la page **Style de la liste des tâches**, configurez les options comme indiqué sur l'image suivante puis cliquez sur **Suivant**.

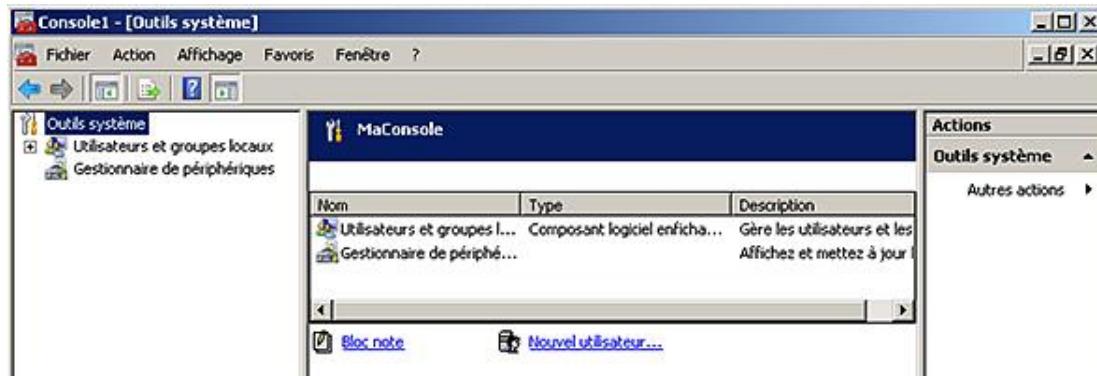


- Sur la page **Réutilisation de la liste des tâches**, cliquez sur **Suivant**.
- Sur la page **Nom et description**, saisissez **MaConsolePerso** pour le nom puis cliquez sur **Suivant**.
- Sur la page **Fin de l'Assistant Nouvelle vue de la liste des tâches** de l'assistant, assurez-vous que la case à cocher est bien sélectionnée puis cliquez sur **Terminer**.
- Sur la page **Assistant Nouvelle tâche** de l'assistant, cliquez sur **Suivant**.
- Sur la page **Type de commande** de l'assistant, sélectionnez **Commande de menu** puis cliquez sur **Suivant**.
- Sur la page **Commande de menu** de l'assistant, sélectionnez pour la source de la commande **Nœud de l'arborescence** ; dans **Elément de l'arborescence**, sélectionnez **Utilisateurs**, puis dans **Commandes disponibles** sélectionnez **Nouvel utilisateur** avant de cliquer sur **Suivant**.



- Sur la page **Nom et description de l'assistant** cliquez sur **Suivant**.
- Sur la page **Icône de la tâche** sélectionnez une icône parmi les icônes fournies par MMC puis cliquez sur **Suivant**.
- Sur la page **Fin de l'Assistant Nouvelle tâche**, cochez **Relancer l'assistant après avoir cliqué sur Terminer** puis cliquez sur **Terminer**.
- Sur la page **Assistant Nouvelle tâche** de l'assistant, cliquez sur **Suivant**.
- Sur la page **Type de commande** de l'assistant, sélectionnez **Commande de l'environnement** puis cliquez sur **Suivant**.
- Sur la page **Ligne de commande** saisissez **notepad** dans la zone de texte **Commande** puis cliquez sur **Suivant**.
- Sur la page **Nom et description**, saisissez **Bloc note** pour le nom puis cliquez sur **Suivant**.
- Sur la page **Icône de la tâche** de l'assistant, sélectionnez une icône parmi les icônes fournies par MMC puis cliquez sur **Suivant**.
- Sur la page **Fin de l'Assistant Nouvelle tâche** de l'assistant, cliquez sur **Terminer**.

Votre console ressemble maintenant à l'image suivante :



- Désélectionnez le panneau gauche et le panneau droit, en cliquant sur les icônes correspondantes dans la barre d'outils.
- Modifiez les options de la console de manière à être en **mode utilisateur - accès limité, fenêtre unique** sans pouvoir enregistrer les modifications ni autoriser l'utilisateur à personnaliser les vues.
- Enregistrez votre console et répondez **Oui** à la boîte de dialogue d'avertissement.

Vous venez de créer une console qui permet à l'utilisateur de créer rapidement un nouvel utilisateur en cliquant sur la tâche ou d'ouvrir le bloc-notes. Il a toujours la possibilité de gérer les périphériques ou les utilisateurs en sélectionnant les éléments dans la console.

### e. Avantages et inconvénients

Les inconvénients sont :

- Utilise le protocole RPC qui ne peut passer les pare-feu.
- Les mécanismes de sécurité exigent d'être dans le même contexte de sécurité que les serveurs distants.
- L'application cliente snap-in doit être enregistrée dans la base de registre.

Les avantages sont :

- Utilisable à partir d'une autre version de Windows, éventuellement en mode limité.
- Méthodologie consistante de travail entre les snap-ins.
- Les consoles peuvent être très facilement personnalisables.
- Grand nombre de snap-ins disponibles.
- Peut être utilisé pour administrer un Server Core.

## 3. Outils d'administration de serveur distant (RSAT)

Les outils d'administration de serveur distant sont des snap-ins utilisables pour la gestion à distance de serveur Windows 2008 ou Windows 2003 à partir de Windows Server 2008. Cette fonctionnalité remplace l'adminpak des versions précédentes.



Il n'est pas possible d'utiliser cet outil à partir d'un Server Core.

Il est possible d'administrer une partie de Windows Server 2008 à partir de Windows Vista SP1 en téléchargeant les Outils d'administration de serveur distant de la KB941314. Si l'adminpak est déjà installé, veuillez consulter la KB941314 pour connaître la procédure correcte d'installation.

Il s'agit d'une fonctionnalité qu'il faut installer dont la granularité est l'outil. La liste suivante montre les outils disponibles avec la fonctionnalité ainsi que les outils disponibles pour Windows Vista.

Outils	Windows Server 2008	Windows Vista SP1
Rôles		
Outils des services de certificat Active Directory	x	x
Outils d'autorité de certification	x	x

Outils des répondeurs en ligne	x	x
<b>Outils des services de domaine Active Directory</b>	x	x
Outils de contrôleur de domaine Active Directory	x	x
Outils de Serveur pour NIS	x	x
<b>Outils des services AD LDS</b>	x	x
<b>Outils des services AD RMS</b>	x	
<b>Outils du serveur DHCP</b>	x	x
<b>Outils du serveur DNS</b>	x	x
<b>Outils du serveur de télécopie</b>	x	
<b>Outils de services de fichiers</b>	x	x
Outils du système de fichiers DFS	x	x
Outils de Gestion de ressources du serveur	x	x
Outils des services pour NFS	x	
Outils de gestion du partage et du stockage		x
<b>Outils de la stratégie réseau et des services</b>	x	
<b>Outils des services d'impression</b>	x	
<b>Outils des services Terminal Server</b>	x	x
Outils du serveur Terminal Server	x	
Outils de la passerelle Terminal Server	x	
Outils des licences Terminal Server	x	
<b>Outils des services UDDI</b>	x	x
<b>Outils du serveur Web (IIS)</b>	x	
<b>Outils des services de déploiement Windows</b>	x	
<b>Outils Hyper-V</b>	x	
<b>Fonctionnalités</b>		
<b>Outils de chiffrement BitLocker</b>	x	x
<b>Outils d'extensions du serveur BITS</b>	x	
<b>Outils de clustering avec basculement</b>	x	x
<b>Outils d'équilibrage de la charge réseau</b>	x	x
<b>Outils du serveur SMTP</b>	x	x

<b>Outils du serveur WINS</b>	x	
<b>Outils de gestion Stratégie de groupe</b>		x
<b>Outils du gestionnaire de stockage pour réseau SAN</b>		x
<b>Outils du gestionnaire de ressources système Windows</b>		x

➤ Sur Windows Server 2008, il est recommandé d'utiliser un serveur dévolu aux tâches d'administration accessible en mode d'administration distante sur lequel les Outils d'administration de serveur distant sont installés.

### a. Installation des outils d'administration



Win4

- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur **Fonctionnalités**.
- Sur la fenêtre principale, cliquez sur **Ajouter des fonctionnalités**.
- Sur la page **Fonctionnalités** de l'assistant **Ajout de fonctionnalités**, sélectionnez le ou les outils dont vous avez besoin du noeud **Outils d'administration de serveur distant** puis cliquez sur **Suivant**.

➤ Les **outils des services Terminal Server**, **outils du serveur Web (IIS)**, **outils d'extensions du serveur BITS** et **outils du serveur SMTP** exigent également d'installer sur le serveur local le rôle serveur Web (IIS).

- Sur la page **Confirmation** de l'assistant **Ajout de fonctionnalités**, contrôlez la liste des outils qui seront installés puis cliquez sur **Installer**.

La page suivante montre l'état d'avancement. À la fin, vous pouvez être appelé à redémarrer le serveur. Sinon la page résultat s'affiche vous indiquant la réussite ou l'échec de l'installation.

Tous les outils sont maintenant disponibles dans les outils d'administration.

### b. Avantages et inconvénients

L'inconvénient est :

- Tous les snap-ins d'administration ne sont pas réunis dans cette fonctionnalité.

Les avantages sont :

- La granularité d'installation est le snap-in d'administration.
- Méthodologie consistante de travail entre les snap-ins.
- Création de console MMC personnalisable.
- Certains snap-ins peuvent être utilisés pour administrer un Server Core.

## 4. Administration à distance

L'administration à distance est simplement une version Terminal Server réservée à l'administration. Sur un serveur, deux administrateurs peuvent se connecter en même temps. Il n'est pas nécessaire d'acquérir des licences supplémentaires.

Une fois connecté, l'administrateur a accès à tout le serveur et le fonctionnement est identique à un fonctionnement interactif excepté qu'il se trouve à distance.

Travailler à distance permet de placer les serveurs dans des emplacements sécurisés. Toujours dans le but de garantir une meilleure sécurité, Microsoft a amélioré le protocole de transport utilisé pour l'affichage distant appelé RDP (*Remote Desktop Protocol*) et le serveur peut exiger que le client utilise ce nouveau protocole.

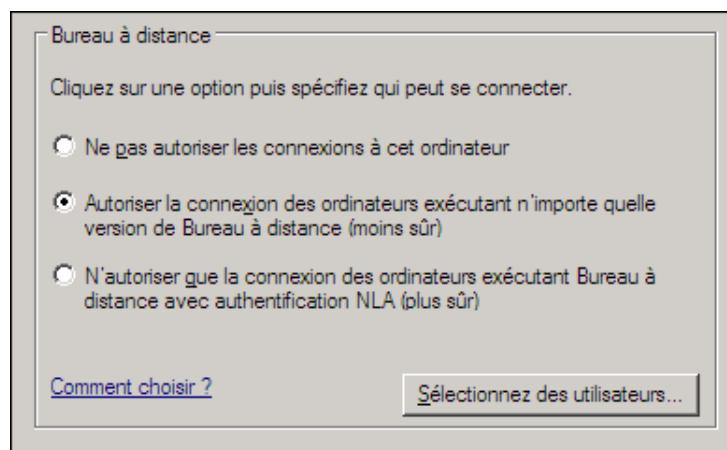
Pour travailler à distance, il est nécessaire d'activer cette fonctionnalité sur le serveur, puis il faut un outil client. Par défaut Windows XP et Windows 2003 utilisent le protocole RDP 6.0. Il faut disposer du Service pack 3 de Windows XP pour utiliser le protocole RDP 6.1 ou acheter un client RDP. Les clients Windows Vista et Windows Server 2008 utilisent le protocole RDP 6.1.

### a. Activation du Bureau distant



L'activation peut se faire lors de la configuration initiale du serveur ou à l'aide de la procédure suivante :

- Cliquez sur **Démarrer**, puis avec le bouton droit de la souris, cliquez sur **Ordinateur** pour faire apparaître le menu contextuel, et enfin cliquez sur **Propriété**.
- Dans la boîte de dialogue **Système**, cliquez sur **Paramètres d'utilisation à distance**.
- Dans la boîte de dialogue **Propriétés Système**, cliquez sur **Autoriser la connexion des ordinateurs exécutant n'importe quelle version du Bureau à distance (moins sûr)**, puis cliquez sur **OK**.
- Fermez la boîte de dialogue **Système**.



**Ne pas autoriser les connexions à cet ordinateur** empêche toute connexion vers cet ordinateur quel que soit l'outil utilisé.

**Autoriser la connexion des ordinateurs exécutant n'importe quelle version du Bureau à distance (moins sûr)** autorise les connexions distantes quels que soient l'outil et la version de l'outil.

**N'autoriser que la connexion des ordinateurs exécutant Bureau à distance avec authentification NLA (plus sûr)** autorise les connexions distantes pour autant que l'outil supporte le protocole NLA.

### b. Activation du Bureau distant sur un Server Core



Core4

Pour activer le bureau à distance :

- Dans l'invite de commande, saisissez **cscript %windir%\system32\scregedit.wsf /ar 0**

Pour activer le Bureau à distance, le paramètre **/ar** peut prendre les valeurs **0** pour activation et **1** pour désactivation. L'accès est autorisé uniquement pour des clients distants Windows Server 2008 ou Windows Vista (RDP 6.1).

- Puis la commande suivante **cscript %windir%\system32\scregedit.wsf /cs 0**

Pour permettre également un accès avec des clients Windows Server 2003 ou Windows XP (RDP 6.0), donc moins sécurisé.

 Il est recommandé d'activer le bureau à distance une fois que l'ordinateur a joint le domaine sinon il faut désactiver la règle **Bureau à distance (TCP-Entrée)** du profil **public** et ressaisir la commande.

### c. L'outil Connexion Bureau à distance



Win4

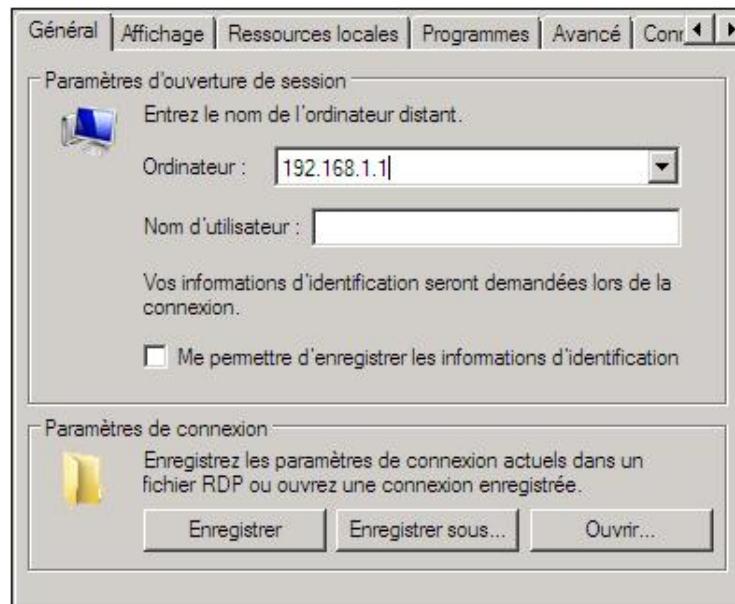
- Cliquez sur **Démarrer - Tous les programmes - Accessoires** puis sur **Connexion Bureau à distance**.

Par défaut, il suffit simplement de saisir le nom du serveur distant ou son adresse IP puis de cliquer sur **Connexion** :



Il est possible de configurer, voire d'enregistrer des connexions, pour cela, il faut cliquer sur le bouton **Options**.

### d. Onglet Général



**Ordinateur** permet de saisir un nom ou une adresse IP ; les anciennes valeurs sont conservées et peuvent être réutilisées. La valeur <parcourir...> permet de retrouver des serveurs TS dans un groupe de travail ou un domaine.

**Nom de l'utilisateur** vous permet d'entrer votre nom d'utilisateur, jamais le mot de passe.

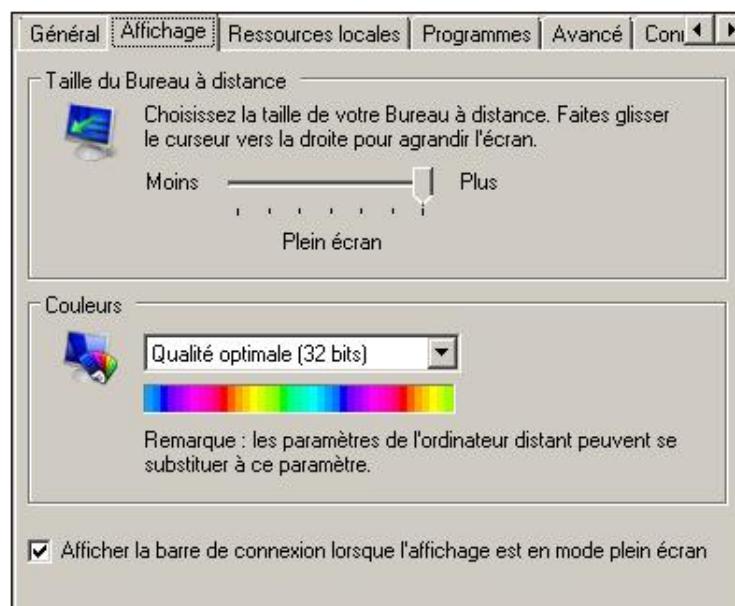
**Enregistrer** : enregistre un profil avec l'extension RDP.

**Enregistrer sous** : enregistre un profil avec l'extension RDP.

**Ouvrir** permet d'ouvrir un profil RDP.

**Me permettre d'enregistrer les informations d'identification** est une case à cocher qui s'affiche dès que vous entrez un nom pour l'ordinateur. Dans ce cas, les informations d'identification sont enregistrées pour que la prochaine fois l'ouverture de la session se fasse automatiquement.

#### e. Onglet Affichage

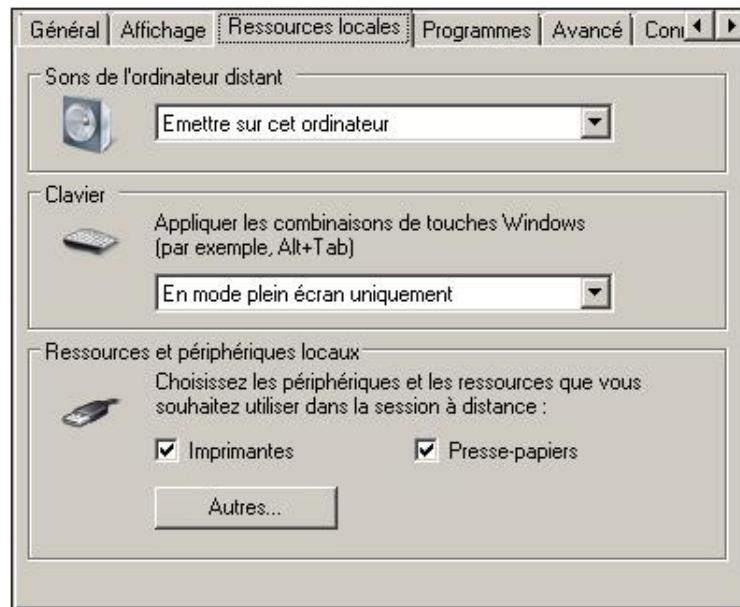


**Taille du Bureau à distance** permet de sélectionner la taille utilisée par la fenêtre du bureau distant.

**Couleurs** détermine le nombre de couleurs que vous désirez afficher.

- Ces paramètres dépendent également des possibilités de la carte graphique du serveur distant.

## f. Onglet Ressources locales



**Sons de l'ordinateur distant** : les sons peuvent être conservés sur l'ordinateur distant, redirigés sur l'ordinateur local ou désactivés.

**Clavier** : permet de sélectionner la façon dont les combinaisons de touches sont redirigées soit :

- sur la session locale ;
- la session distante ;
- en mode plein écran sur la session distante.

**Imprimante** : permet d'utiliser les imprimantes locales sur la session distante.

**Presse-papiers** : permet de passer des informations vers la session distante à l'aide du presse-papier.

**Autres** : permet de mapper des lecteurs locaux pour la session distante voire des périphériques plug-and-play qui utilisent des protocoles MTP (*Media Transfer Protocol*) ou PTP (*Picture Transfer Protocol*).

## g. Onglet Programmes

**Démarrer le programme suivant lors de la connexion** : permet de remplacer le Bureau par une application.

**Chemin d'accès au programme et nom du fichier** : indique le nom du programme à démarrer.

**Démarrer dans le dossier suivant** : définit le dossier pour le programme.

Cet onglet n'est pas vraiment utile pour administrer un serveur Windows 2008.

## h. Onglet Avancé

La liste déroulante permet de sélectionner automatiquement certaines fonctionnalités en fonction de la vitesse du réseau.

Ne perdez pas de temps à personnaliser ces valeurs, sélectionnez simplement la vitesse de connexion. Il faut juste noter que le lissage des polices coûte du temps processeur.

La case à cocher **Rétablissement la connexion si elle est interrompue** est intéressante car elle permet de rétablir les connexions en cas de micro coupures réseaux.

## i. Onglet Connexion

Cet onglet est plus utile dans le cadre d'une connexion Terminal Server que pour une connexion Bureau à distance.

- Comme il n'existe pas de boutons pour se déconnecter d'un Server Core, il est fortement recommandé de saisir **logoff** en fin de session afin d'éviter que des ressources soient gaspillées inutilement par une session ouverte.

C'est une excellente pratique que de créer des fichiers RDP qui sont autant de raccourcis personnalisés pour se connecter à des serveurs ou d'utiliser la console **Bureaux à distance** proposée en tant que snap-in.

La console **Bureaux à distance** permet d'enregistrer dans le snap-in plusieurs fichiers de configuration pour se connecter à différents serveurs. Ces paramètres de configuration sont semblables à ceux présentés pour le Bureau à distance.

## j. Avantages et inconvénients

L'inconvénient est :

- Ne peut pas démarrer physiquement un ordinateur distant sauf si celui-ci supporte le Wake on Lan.

Les avantages sont :

- Diminution de la surface d'attaque par une désactivation du service.
- Amélioration de la sécurité en exigeant des clients compatibles avec la dernière version du protocole RDP.
- Accès aux ressources comme un accès local.
- Peut passer à travers les pare-feu.
- Fonctionne même sur une connexion lente d'environ 30Kb/s.
- Utilisable pour administrer un Server Core.

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre indirectement les compétences évaluées à l'examen car il traite des outils qui seront utilisés dans les autres chapitres.

Les questions d'examens qui peuvent s'y rapporter concernent le choix d'un outil par rapport à un autre ou, pour une partie pratique, comment effectuer une tâche spécifique.

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes



## 3. Objectifs

Le choix des outils de configuration et de gestion n'est pas une chose aisée, c'est la raison pour laquelle un chapitre entier est consacré aux principaux outils de configuration et de gestion utilisés pour gérer un environnement Windows Server 2008. Les outils présentés utilisent soit une interface graphique soit une ligne de commandes.

Il faut savoir que tous les outils d'administration sont installés lors de l'installation de Windows Server 2008 et que Microsoft a revu à la baisse le nombre d'outils utilisables par l'administrateur en faisant disparaître la notion d'outils discrets au profit d'outils multi-applications dont l'apprentissage ne s'effectue qu'une seule fois.

Une excellente connaissance des outils permet à un administrateur de gagner du temps notamment en réduisant le temps d'exécution de certaines tâches. Chaque outil présenté est accompagné d'exemples permettant de l'utiliser pleinement.

À la fin du chapitre vous serez capable de décrire et d'utiliser tous les outils présentés. Vous saurez quel outil choisir et dans quel cadre d'utilisation que ce soit sur une installation minimale (Server Core) ou une installation complète.

# Validation des acquis : questions/réponses

## 1. Questions

### Questions triviales

- 1** Expliquez la différence entre un rôle et un service de rôle.
- 2** Citez quatre rôles existant pour un Server Core.
- 3** Citez un rôle qui n'est pas présent sur une **édition standard**.
- 4** Quel(s) rôle(s) est/sont disponible(s) sur une **édition Itanium** ?
- 5** Citez au moins un rôle qui n'est pas fourni avec le DVD de Windows Server 2008.
- 6** À quoi sert le rôle de serveur applicatif ?
- 7** Quel rôle faut-il installer pour configurer le service NAP ?
- 8** Citez au moins trois fonctionnalités en relation avec le stockage.
- 9** Quel est le principal défaut du client Telnet ?
- 10** Citez le nom d'une application pour installer un rôle ou une fonctionnalité sur un Server Core.
- 11** Citez le nom d'au moins deux applications pouvant s'exécuter sur une **installation complète**"...pour installer un rôle ou une fonctionnalité".
- 12** Est-il possible de gérer des serveurs de fichiers Windows 2003 à l'aide du rôle **Services de fichiers** ?
- 13** Est-il possible d'installer plusieurs composants en même temps sur un Server Core ?

### Questions de compréhension

- 14** Vous devez installer un **serveur Web (IIS)** pour héberger une application écrite en ASP.NET, quel type d'installation allez-vous exécuter sachant qu'il faut minimiser l'empreinte disque ?
- 15** Un de vos collègues doit installer un serveur hautement disponible comme serveur de base de données. Il propose d'utiliser la fonctionnalité WNLB. Que lui répondez-vous ?
- 16** Une de vos collègues s'interroge sur l'intérêt que peut avoir la fonctionnalité **Expérience utilisateur**. Quelle est votre réponse ?
- 17** Vous utilisez l'invite de commande pour installer le **service de rôle Web-Common-http**, est-ce que cela inclut également l'installation des **ASP.NET** ?
- 18** Comment installez-vous le Framework 3.5 ?
- 19** On vous demande de permettre l'impression Internet sur le serveur 2008. Installez-vous un rôle ou une fonctionnalité ?

### Questions de mise en œuvre

- 20** Votre collègue du bureau distant vous demande de l'aide pour installer correctement le rôle de Service de gestion des droits AD RMS en préparant un script qu'il n'aurait qu'à exécuter. Quelle serait votre réponse ?
- 21** Votre nouveau collègue vient d'installer un serveur Windows 2008 et il essaie d'effectuer une sauvegarde, malheureusement sans succès, pourquoi ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /21

Pour ce chapitre, votre score minimum doit être de 16 sur 21.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

### **3. Réponses**

#### **Questions triviales**

- 1** Expliquez la différence entre un rôle et un service de rôle.

*Un rôle peut être composé de plusieurs services appelés Services de rôle optionnels pour que le rôle fonctionne.*

- 2** Citez quatre rôles existant pour un Server Core.

*Vous pouvez citer les rôles suivants : Serveur Web (IIS), Services d'impression, Serveur DHCP, Serveur DNS, Services de fichiers, Services de domaine Active Directory AD DS, Services Active Directory Lightweight Directory Services AD LDS, Hyper-V et Services Windows Media (Streaming).*

- 3** Citez un rôle qui n'est pas présent sur une **édition standard**.

*Le service de fédération Active Directory AD FS.*

- 4** Quel(s) rôle(s) est/sont disponible(s) sur une **édition Itanium** ?

*Vous pouvez seulement installer les rôles suivants : Serveur d'application et Serveur Web (IIS).*

- 5** Citez au moins un rôle qui n'est pas fourni avec le DVD de Windows Server 2008.

*Vous pouvez citer Services Windows Media (Streaming) et Windows Server Update Services.*

- 6** À quoi sert le rôle de serveur applicatif ?

*Le rôle serveur applicatif installe des fonctionnalités pouvant être requises par une application métier.*

- 7** Quel rôle faut-il installer pour configurer le service NAP ?

*Il faut installer le rôle Services de stratégie et d'accès réseau.*

- 8** Citez au moins trois fonctionnalités en relation avec le stockage.

*Vous pouvez citer le Chiffrement de lecteur BitLocker, le Gestionnaire de stockage amovible, le Gestionnaire de stockage pour réseau SAN et Serveur iSNS.*

- 9** Quel est le principal défaut du client Telnet ?

*Le nom et le mot de passe circulent en clair sur le réseau. Pour le sécuriser, vous pouvez utiliser le protocole IPSEC.*

- 10** Citez le nom d'une application pour installer un rôle ou une fonctionnalité sur un Server Core.

*Vous pouvez citer **ocsetup** et **pkgmgr**.*

- 11** Citez le nom d'au moins deux applications pouvant s'exécuter sur une installation complète pour installer un rôle ou une fonctionnalité.

*Vous pouvez citer le Gestionnaire de serveur et ServerManagerCmd.*

- 12** Est-il possible de gérer des serveurs de fichiers Windows 2003 à l'aide du rôle Services de fichiers ?

*Oui.*

- 13 Est-il possible d'installer plusieurs composants en même temps sur un Server Core ?

*Bien entendu, en voici quelques exemples :*

**pkgmgr /iu :SUACore ;WINS-SC ou ocsetup SUACore ;WINS-SC.**

#### **Questions de compréhension**

- 14** Vous devez installer un serveur Web (IIS) pour héberger une application écrite en ASP.NET, quel type d'installation allez-vous exécuter sachant qu'il faut minimiser l'empreinte disque ?

*Il faut effectuer une installation complète car le Server Core ne supporte pas les ASP.NET et le Framework est requis.*

- 15** Un de vos collègues doit installer un serveur hautement disponible comme serveur de base de données. Il propose d'utiliser la fonctionnalité WNLB. Que lui répondez-vous ?

*La fonctionnalité WNLB peut être utilisée pour rendre hautement disponible des serveurs Web mais pas un serveur de base de données. Dans ce cas, une solution serait d'installer la fonctionnalité de **clustering avec basculement**.*

- 16** Une de vos collègues s'interroge sur l'intérêt que peut avoir la fonctionnalité Expérience utilisateur. Quelle est votre réponse ?

*Cette fonctionnalité peut s'utiliser en conjonction avec les services **Terminal Server** afin que les utilisateurs bénéficient d'une interface utilisateur plus conviviale. Elle peut également améliorer l'interface pour un utilisateur qui utiliserait Windows Server 2008 en tant que station de travail !*

- 17** Vous utilisez l'invite de commande pour installer le **service de rôle Web-Common-http**, est-ce que cela inclut également l'installation des **ASP.NET** ?

*Non car ASP.NET ne dépend pas du service de rôle Web-Common-http.*

- 18** Comment installez-vous le **Framework 3.5** ?

*Une solution serait de télécharger le Framework 3.5 depuis le site de Microsoft et de l'installer, une autre serait de passer par **Windows Update**.*

- 19** On vous demande de permettre l'impression Internet sur le serveur 2008. Installez-vous un rôle ou une fonctionnalité ?

*Il faut installer un rôle car c'est la partie serveur qu'il faut installer. La fonctionnalité ne concerne que la partie cliente.*

#### **Questions de mise en œuvre**

- 20** Votre collègue du bureau distant vous demande de l'aide pour installer correctement le rôle de Service de gestion des droits AD RMS en préparant un script qu'il n'aurait qu'à exécuter. Quelle serait votre réponse ?

*Malheureusement, il n'est pas possible d'installer ce rôle via la ligne de commande. La meilleure solution consiste à utiliser le bureau distant.*

- 21** Votre nouveau collègue vient d'installer un serveur Windows 2008 et il essaie d'effectuer une sauvegarde, malheureusement sans succès, pourquoi ?

*Car la sauvegarde qui est une fonctionnalité n'est pas installée par défaut.*

## Résumé du chapitre

Dans ce chapitre, vous avez appris la définition d'un rôle et d'une fonctionnalité puis une description vous a été donnée pour chaque rôle et chaque fonctionnalité, sa fonction et son utilité dans un réseau d'entreprise.

Il vous est même possible de planifier l'utilisation d'un rôle ou d'une fonctionnalité dans votre entreprise ainsi que l'édition à choisir.

Enfin, vous avez appris comment installer ou désinstaller un rôle avec le Gestionnaire de serveur, la commande **ServerManagerCmd**, la commande **ocsetup** et la commande **pkgmgr** et quel est leur cadre d'utilisation.

Vous savez également comment gérer un rôle ou une fonctionnalité à l'aide du Gestionnaire de serveur.

## Travaux pratiques

Il n'y a pas d'exercice spécifique pour la gestion d'un rôle ou d'une fonctionnalité mais presque tous les exercices font appel à ces notions.

# Installer/désinstaller un rôle ou une fonctionnalité

Utilisez les outils comme indiqué dans le tableau suivant :

Outil	Cadre d'utilisation
Gestionnaire de serveur	Installation complète
ServerManagerCmd	Script installation complète
ocsetup	Server Core
pkgmgr	Server Core

➤ Malheureusement les outils à utiliser entre une installation complète et un Server Core sont différents.

## 1. Installation avec le Gestionnaire de serveur



Pour installer un rôle ou une fonctionnalité avec le gestionnaire de serveur, vous devez vous trouver sur une installation complète.

➤ Si l'assistant d'installation ou de désinstallation demande un redémarrage du serveur, alors le serveur se trouve dans un état considéré comme instable jusqu'au redémarrage et il n'est plus possible de réutiliser l'assistant d'ajout ou de suppression.

### a. Installation d'un rôle

- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.  
À l'ouverture, la fenêtre principale affiche la zone **Résumé** contenant les éléments de configuration actuels du serveur.
- Dans l'arborescence de la console, cliquez sur **Rôles**.
- Dans la fenêtre principale contenant la page **Rôles**, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** de l'**Assistant Ajout de rôles** apparaît, cliquez sur **Suivant**.
- Sur la page **Sélectionner des rôles de serveurs** de l'**Assistant Ajout de rôles**, sélectionnez le ou les rôles que vous voulez installer.

➤ Il est possible d'installer plusieurs rôles en même temps. Les rôles déjà installés sont grisés.

- Ensuite, cliquez sur **Suivant** et continuez en sélectionnant les options dont vous avez besoin jusqu'à la page **Confirmation** puis cliquez sur **Installer**.
- Si un rôle dépend d'un autre rôle ou d'une fonctionnalité, un message l'indique et vous ne pouvez continuer l'installation que si vous confirmez l'installation des composants pré-requis comme le montre la figure

suivante.



- Si un rôle peut engendrer des risques pour la sécurité, l'assistant vous demande votre autorisation pour continuer.

- Si besoin, redémarrez le serveur pendant la phase **État d'avancement**. Ensuite, attendez la page **Résultats** qui indique si l'installation a réussi.

## b. Installation d'une fonctionnalité



- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur **Fonctionnalités**.
- Dans la fenêtre principale contenant la page **Fonctionnalités**, cliquez sur **Ajouter des Fonctionnalités**.
- Sur la page **Sélectionnez des fonctionnalités** de l'**Assistant Ajout de fonctionnalités**, sélectionnez la ou les fonctionnalités que vous voulez installer.

- Il est possible d'installer plusieurs fonctionnalités en même temps.

- Ensuite, cliquez sur **Suivant** et continuez en sélectionnant les options dont vous avez besoin jusqu'à la page **Confirmation**, puis cliquez sur **Installer**.

- Si une fonctionnalité dépend d'un autre rôle ou d'une fonctionnalité, un message vous l'indique et vous ne pouvez continuer l'installation que si vous confirmez l'installation des composants pré-requis.

- Si besoin, redémarrez le serveur pendant la phase **État d'avancement**. Ensuite, attendez la page **Résultats** qui indique si l'installation a réussi.

## 2. Désinstallation avec le Gestionnaire de serveur

### a. Suppression d'un rôle



Win

- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.  
À l'ouverture, la fenêtre principale affiche la zone **Résumé** contenant les éléments de configuration actuels du serveur.
- Dans l'arborescence de la console, cliquez sur **Rôles**.
- Dans la fenêtre principale contenant la page **Rôles**, cliquez sur **Supprimer des rôles**.
- Si la page **Avant de commencer** de l'**Assistant Suppression de rôles** apparaît, cliquez sur **Suivant**.
- Sur la page **Sélectionnez des rôles de serveurs** de l'**Assistant Suppression de rôles**, sélectionnez le ou les rôles que vous voulez enlever puis cliquez sur **Suivant**.



Il est possible de supprimer plusieurs rôles en même temps.

- Sur la page **Confirmer les sélections pour la suppression**, contrôlez et prenez note des avertissements puis cliquez sur **Supprimer**.
- Si besoin, redémarrez le serveur pendant la phase **État d'avancement**. Ensuite, attendez la page **Résultats**, pour consulter le résultat de la suppression.



La suppression d'un rôle ayant requis des dépendances de rôle ou de fonctionnalité ne les supprime pas automatiquement.

### b. Suppression d'une fonctionnalité



Win

- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.  
À l'ouverture, la fenêtre principale affiche la zone **Résumé** contenant les éléments de configuration actuels du serveur.
- Dans l'arborescence de la console, cliquez sur **Fonctionnalités**.
- Dans la fenêtre principale contenant la page **Fonctionnalités**, cliquez sur **Supprimer des fonctionnalités**.
- Si la page **Avant de commencer** de l'**Assistant Suppression de fonctionnalités** apparaît, cliquez sur **Suivant**.
- Sur la page **Sélectionnez des fonctionnalités de serveurs** de l'**Assistant Suppression de fonctionnalités**, sélectionnez la ou les fonctionnalités que vous voulez enlever puis cliquez sur **Suivant**.



Il est possible de supprimer plusieurs fonctionnalités en même temps.

---

- Sur la page **Confirmer les sélections** pour la suppression, contrôlez et prenez note des avertissements puis cliquez sur **Supprimer**.
- Si besoin, redémarrez le serveur pendant la phase **État d'avancement**. Ensuite attendez la page **Résultats** pour consulter le résultat de la suppression.

### 3. Gestion d'un rôle à l'aide du Gestionnaire de serveur

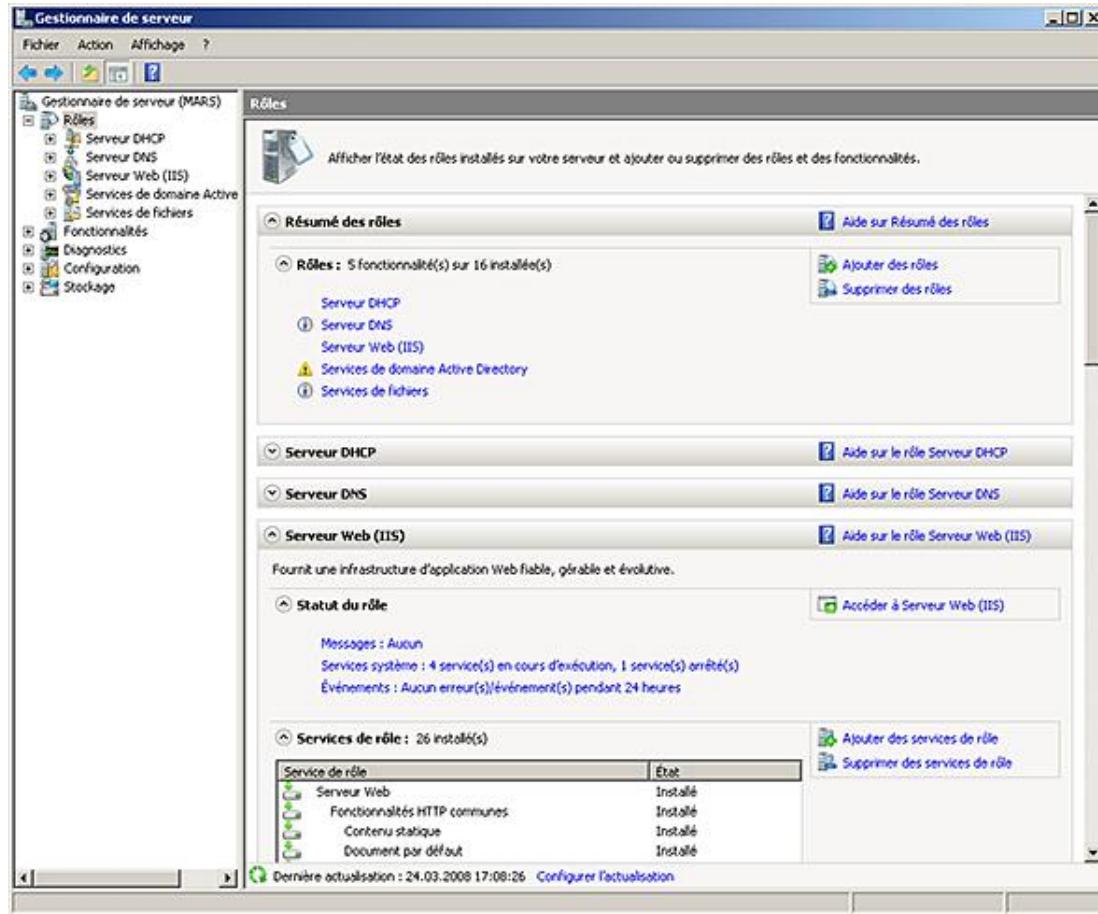
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.

À l'ouverture, la fenêtre principale affiche la zone **Résumé** contenant les éléments de configuration actuels du serveur.

- Dans l'arborescence de la console, cliquez sur **Rôles**.

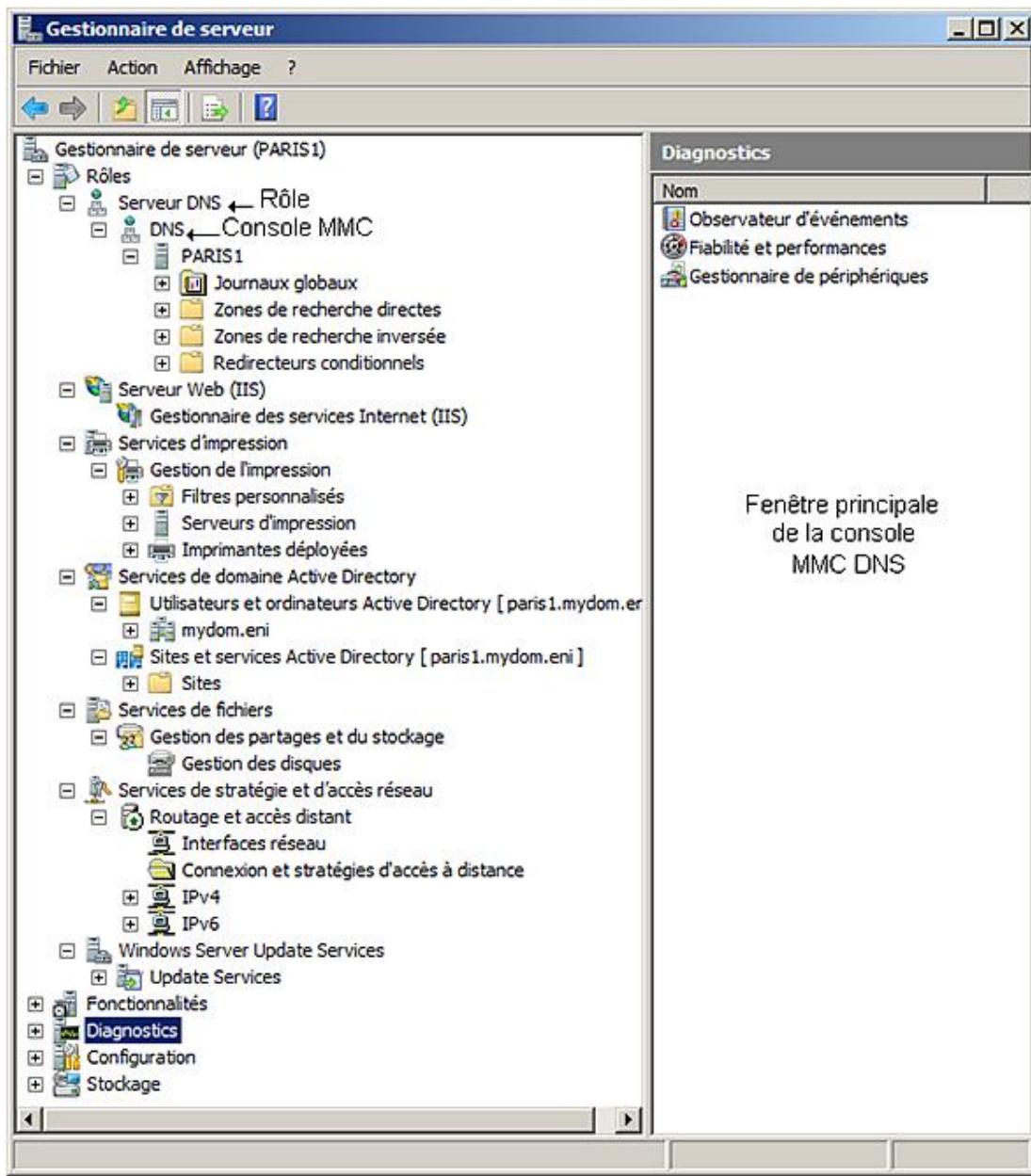
À partir de la fenêtre principale contenant la page **Rôles**, vous pouvez :

- Ajouter ou supprimer des rôles.
- Consulter la liste des rôles installés et visualiser leur état.
- Recevoir de l'aide.
- Pour chaque rôle :
  - Connaître le statut du rôle.
  - Accéder à la console d'administration du rôle du Gestionnaire de serveur.
  - Savoir quels services de rôles sont installés.
  - Ajouter ou supprimer un service de rôle.
  - Lire la description du rôle.

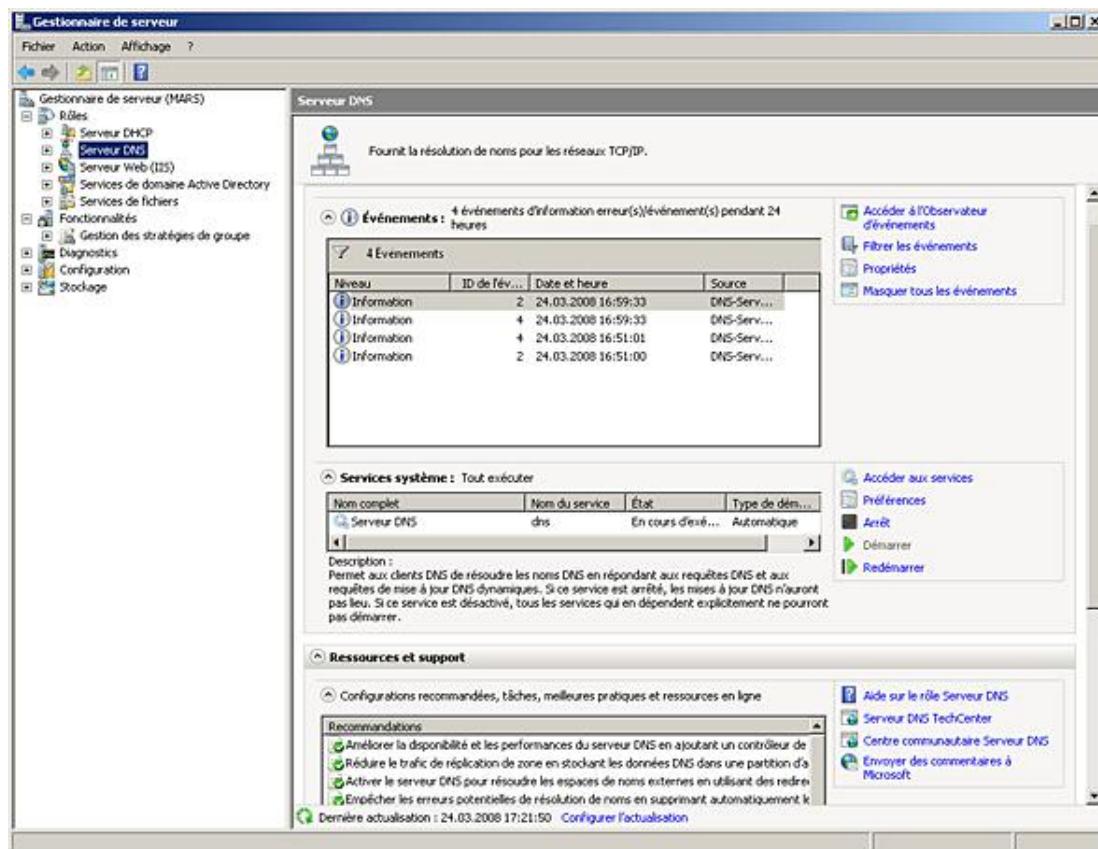


- Dans l'arborescence de la console, cliquez sur le nœud **Rôles** pour faire apparaître la liste des rôles installés.

Remarquez qu'il est possible de développer un niveau supplémentaire qui donne accès à la console MMC du rôle comme le montre la figure suivante :



- Sélectionnez un rôle. Le contenu de la fenêtre principale ressemble à la figure suivante.



**Événements** : cette section affiche tous les événements relatifs au rôle survenus durant les 24 dernières heures par défaut. Dans cette section, les actions possibles sont :

- Démarrer la console **Observateur d'événements**.
- **Filtrer les événements**, comme le montre l'image suivante :



- Afficher le contenu de l'événement sélectionné dans la liste en cliquant sur **Propriétés**.
- Effacer de la liste tous les événements en cliquant sur **Masquer tous les événements**.

**Services système** : cette section affiche la liste des services du rôle et leur état. Les actions disponibles sont :

- **Accéder aux services** qui affiche la console MMC services pour une gestion complète des services.
- **Préférences** qui permet de sélectionner dans la liste des services ceux qui doivent être affichés.
- **Arrêt** pour arrêter le service.
- **Démarrer** pour démarrer le service sélectionné.
- **Redémarrer** pour redémarrer le service sélectionné.

**Ressources et support** : cette section affiche une liste de recommandations qu'il est possible de consulter pour le rôle. Les actions disponibles sont :

- **Aide sur le rôle du serveur sélectionné** : affiche l'aide locale sur le sujet.
- **Rôle sur TechCenter** : renvoie une page sur le site Microsoft qui concerne le rôle sélectionné.
- **Centre communautaire concernant le rôle** : renvoie à une page Internet en anglais sur les communautés de type blogs, newsgroups, Webcasts... sur les technologies Microsoft.
- **Envoyer des commentaires à Microsoft** : renvoie à une page en anglais destinée à envoyer des suggestions ou des retours d'expérience sur Windows Server 2008.

## 4. Gestion d'une fonctionnalité à l'aide du Gestionnaire de serveur



Win

- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.

À l'ouverture, la fenêtre principale affiche la zone **Résumé** contenant les éléments de configuration actuels du serveur.

- Dans l'arborescence de la console, cliquez sur **Fonctionnalités**.

Vous pouvez :

- Ajouter ou supprimer des fonctionnalités.
- Consulter la liste des fonctionnalités installées.
- Recevoir de l'aide.

Dans l'arborescence de la console, certaines fonctionnalités apparaissent si elles disposent d'une interface de gestion de type console MMC comme la console **Gestion des stratégies de groupes** de la figure précédente.

## 5. Installation et désinstallation avec la commande ServerManagerCmd



Win

Toutes les commandes suivantes sont à exécuter dans une invite de commandes ou à inclure dans un script de type batch.

Pour afficher tous les rôles et fonctionnalités ainsi que leur état (installé ou non) :

```
ServerManagerCmd -query
```

Pour simuler une opération avec **-whatif** :

```
ServerManagerCmd -install Dhcp -whatif
```

Pour forcer le redémarrage à la fin de l'opération **-restart** :

```
ServerManagerCmd -install Dhcp -restart
```

Pour installer ou désinstaller plusieurs rôles ou fonctionnalités (doivent être séparés par des espaces) :

```
ServerManagerCmd -remove Dhcp Dns
```

Pour installer ou désinstaller un rôle ainsi que le service de rôles :

```
ServerManagerCmd -install Web-Server -allSubFeatures
```

Pour enregistrer le résultat de l'opération dans un fichier **-resultpath <FichierRésultat.xml>** :

```
ServerManagerCmd -install Dhcp -resultPath c:\result.xml
```

En utilisant un fichier de réponses édité à l'aide du bloc-notes, cela donne :

Le fichier de réponses doit ressembler à celui-ci :

```
<ServerManagerConfiguration Action="Install"  
xmlns="http://schemas.microsoft.com/sdm/windows/ServerManager/Configuration/2007/1">  
    <Role Id="web-Server" InstallAllSubFeatures="true" />  
</ServerManagerConfiguration>
```

**Action** : indique si l'on installe ou supprime le rôle.

**Role Id** : indique le nom de la commande ; indiquez une commande par ligne. Vous pouvez placer un rôle, un service de rôle ou une fonctionnalité.

**InstallAllSubFeatures** : est optionnel et vous permet d'installer les services de rôle associés ; sinon, ajoutez une ligne par service de rôle en omettant cet attribut.

- Ensuite, vous pouvez lancer la commande suivante :

```
ServerManagerCmd -InputPath c:\install.xml
```

## 6. Installation et désinstallation avec la commande ocsetup



Toutes les commandes suivantes sont à exécuter dans une invite de commandes ou à inclure dans un script de type batch.m

- Sur un Server Core, saisissez **oclist** pour voir la liste des rôles et des fonctionnalités et si elles sont installées.
- Sur un Server Core, saisissez **start /w** devant les commandes.

Pour installer un composant :

```
ocsetup SUACore
```

 La casse des noms de commande est importante.

Pour installer plusieurs composants et enregistrer un fichier de logs :

```
ocsetup SUACore ; WINS-SC /log :c:\t.log
```

Pour supprimer un composant :

```
ocsetup SUACore /Uninstall
```

## 7. Installation et désinstallation avec la commande pkgmgr



Toutes les commandes suivantes sont à exécuter dans une invite de commandes ou à inclure dans un script de type batch.

 Sur un Server Core, saisissez **start /w** devant les commandes.

Pour installer un composant :

```
pkgmgr /iu:SUACore
```

Pour installer plusieurs composants :

```
pkgmgr /iu :SUACore;WINS-SC
```

Pour supprimer un composant :

```
pkgmgr /uu:SUACore
```

# Validation des acquis : questions/réponses

## 1. Questions

### Questions triviales

- 1 Citez au moins 5 outils faisant partie du Gestionnaire de serveur.
- 2 Citez une méthode rapide pour modifier la configuration d'une carte réseau.
- 3 Citez une méthode pour indiquer l'état du pare-feu.
- 4 Citez un des inconvénients de l'assistant de configuration de la sécurité.
- 5 Indiquez un avantage de WinRM.

### Questions de compréhension

- 6 Un de vos collaborateurs recherche en vain le Gestionnaire de serveur, que pouvez-vous lui répondre ?
- 7 Comment feriez-vous pour administrer à distance un serveur Windows 2008 à partir d'une station de travail Windows XP ?
- 8 Comment feriez-vous pour administrer à distance un serveur Windows 2008 à partir d'une station de travail Windows Vista ?
- 9 Votre collègue a installé les outils d'administrations distants (RSAT) sur sa station de travail malheureusement, il n'arrive pas à gérer le serveur de télécopie, pourquoi ?
- 10 Vous aimerez installer plusieurs rôles et fonctionnalités à l'aide d'un script. Vous écrivez une commande mais vous aimerez la tester avant de l'exécuter. Comment feriez-vous ?
- 11 Votre collègue vous fournit un script écrit en PowerShell pour gérer votre serveur Windows 2008. Malheureusement, il ne fonctionne pas sur votre ordinateur, quelle pourrait en être la raison ?
- 12 Votre collègue vous fournit un script qui utilise uniquement la commande **ocsetup** pour l'installation du rôle Serveur DHCP. Malheureusement, il ne fonctionne pas sur votre serveur 2008, quelle pourrait être la raison ?
- 13 Un de vos collègues aimeraient gérer un Server Core à l'aide de l'utilitaire Telnet mais plusieurs de vos autres collègues sont contre, quel est votre avis ?
- 14 Quel est l'outil qu'il faut installer sur un ordinateur Windows XP pour exécuter la commande `winrs -r:<NomDuServeur> <Commande>` ?

### Questions de mise en œuvre

- 15 Votre collègue doit administrer le serveur DNS d'un de vos clients à partir de sa station de travail. Il n'y arrive pas, quelle solution lui proposez-vous pour l'aider ?
- 16 Votre collègue localisé dans une autre ville vous demande de l'aide pour gérer son serveur. Il est peu à l'aise avec tous les outils possibles. Comment pourriez-vous l'aider ?
- 17 Vous venez d'installer et avez configuré le rôle **serveur DHCP** sur un serveur 2008. Vous utilisez la commande **netsh** pour contrôler que les étendues sont correctes et transmettez cette information à votre chef. Ce dernier veut également contrôler ces informations à l'aide de la commande netsh mais sans succès, pourquoi ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /17

Pour ce chapitre, votre score minimum doit être de 13 sur 17.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

## 3. Réponses

## Questions triviales

**1** Citez au moins 5 outils faisant partie du Gestionnaire de serveur.

*Vous pouvez citer Rôles, Fonctionnalités, Observateurs d'événements, Fiabilité et performances, Gestionnaire de périphériques, Planificateur de tâches, pare-feu Windows avec fonctions avancées de sécurité, Services, Contrôle WMI, Utilisateurs et groupes locaux, Sauvegarde de Windows Server et Gestion des disques.*

**2** Citez une méthode rapide pour modifier la configuration d'une carte réseau.

*Vous pouvez citer l'utilisation du Gestionnaire de serveur et utiliser l'action **Afficher les connexions réseau**. Vous pouvez également saisir **ncpa.cpl** ou utiliser **netsh**.*

**3** Citez une méthode pour indiquer l'état du pare-feu.

*Vous pouvez utiliser le Gestionnaire de serveur ou passer par l'outil d'administration **pare-feu Windows avec fonctions avancées de sécurité**.*

**4** Citez un des inconvénients de l'assistant de configuration de la sécurité.

*Il n'affiche pas les informations sur le dernier lancement de l'Assistant de la sécurité et la date des dernières modifications, voire si un fichier de configuration a été utilisé.*

**5** Indiquez un avantage de WinRM.

*Vous pouvez citer un des avantages suivants :*

- *Installation et configuration basique facile.*
- *Utilisable sur un ordinateur distant.*
- *Aide compréhensible.*
- *Peut être scriptable.*
- *Outil d'administration adapté pour retourner des informations WMI.*
- *Ne peut exécuter des commandes.*
- *Utilise comme couche de transport des services Web et de ce fait n'est pas sensible aux pare-feu.*
- *Permet de travailler dans des contextes de sécurité différents.*

## Questions de compréhension

**6** Un de vos collaborateurs recherche en vain le Gestionnaire de serveur, que pouvez-vous lui répondre ?

*Il est sûrement connecté à distance sur un Server Core.*

**7** Comment feriez-vous pour administrer à distance un serveur Windows 2008 à partir d'une station de travail Windows XP ?

*Il faut utiliser un outil d'administration à distance comme le snap-in **Bureaux à distance** ou l'outil **Connexion bureau à distance**. Les outils du pack d'administration adminpak.msi ne prennent pas en compte les nouvelles fonctionnalités de Windows 2008.*

**8** Comment feriez-vous pour administrer à distance un serveur Windows 2008 à partir d'une station de travail Windows Vista ?

*En fonction des outils dont on a besoin, il est possible d'utiliser les **Outils d'administrations de serveur distant (RSAT)** ou il faut utiliser un outil d'administration à distance comme le snap-in **Bureaux à distance** ou l'outil **Connexion bureau à distance**. Les outils du pack d'administration **adminpak.msi** ne prennent pas en compte les nouvelles fonctionnalités de Windows 2008.*

**9** Votre collègue a installé les outils d'administrations de serveur distant (RSAT) sur sa station de travail malheureusement, il n'arrive pas à gérer le serveur de télécopie, pourquoi ?

*Cet outil n'est pas inclus dans RSAT. Il faut utiliser un outil d'administration à distance comme le snap-in **Bureaux à distance** ou l'outil **Connexion bureau à distance**. Les outils du pack d'administration **adminpak.msi** ne prennent pas en compte les nouvelles fonctionnalités de Windows 2008.*

**10** Vous aimerez installer plusieurs rôles et fonctionnalités à l'aide d'un script. Vous écrivez une commande mais vous aimerez la tester avant de l'exécuter. Comment feriez-vous ?

*Il faut bien entendu utiliser la commande **ServerManagerCmd** et rajouter à la fin de la commande le paramètre **-whatif** qui simule l'exécution de la commande et nous montre le résultat.*

- 11** Votre collègue vous fournit un script écrit en PowerShell pour gérer votre serveur Windows 2008. Malheureusement, il ne fonctionne pas sur votre ordinateur, quelle pourrait en être la raison ?  
*Il n'est pas possible d'installer PowerShell sur un Server Core avant la version Windows Server 2008 R2. PowerShell n'est pas supporté officiellement par Microsoft.*
- 12** Votre collègue vous fournit un script qui utilise uniquement la commande **ocsetup** pour l'installation du rôle Serveur DHCP. Malheureusement, il ne fonctionne pas sur votre serveur 2008, quelle pourrait être la raison ?  
*Si le script utilise la commande **ocsetup** ou **pkcmgr**, l'incompatibilité provient de la méthode d'installation de Windows, dans un cas il s'agit d'une installation complète, dans l'autre d'une installation minimale. Le nom des rôles et des fonctionnalités sont différents car les packages sont différents.*  
*Si le script utilise la commande **ServerManagerCmd**, cet utilitaire n'est pas supporté sur un Server Core.*
- 13** Un de vos collègues aimeraient gérer un Server Core à l'aide de l'utilitaire Telnet mais plusieurs de vos autres collègues sont contre, quel est votre avis ?  
*Telnet n'est pas sécurisé est l'argument principal. Il est préférable d'utiliser un outil d'administration à distance comme le snap-in **Bureaux à distance** ou l'outil **Connexion bureau à distance**. On peut également remplacer l'utilitaire Telnet par l'utilitaire WinRM.*
- 14** Quel est l'outil qu'il faut installer sur un ordinateur Windows XP pour exécuter la commande **winrs -r:<NomDuServeur> <Commande>** ?  
**winrs** qui est l'outil client de WinRM.

#### **Questions de mise en œuvre**

- 15** Votre collègue doit administrer le serveur DNS d'un de vos clients à partir de sa station de travail. Il n'y arrive pas, quelle solution lui proposez-vous pour l'aider ?  
*La console DNS est un snap-in. Un snap-in utilise les RPC qui ne peuvent passer les pare-feu. En supposant qu'il existe un VPN vers le client, il faut également que le collègue soit logué en utilisant un login se trouvant sur le domaine du client, donc que l'ordinateur soit approuvé ce qui peut poser des problèmes de sécurité. En résumé, le plus simple est d'utiliser un outil d'administration à distance comme le snap-in **Bureaux à distance** ou l'outil **Connexion bureau à distance** puis lancer la console DNS.*
- 16** Votre collègue localisé dans une autre ville vous demande de l'aide pour gérer son serveur. Il est peu à l'aise avec tous les outils possibles. Comment pourriez-vous l'aider ?  
*Vous lui proposez de créer des consoles MMC personnalisées.*
- 17** Vous venez d'installer et avez configuré le rôle **serveur DHCP** sur un serveur 2008. Vous utilisez la commande **netsh** pour contrôler que les étendues sont correctes et transmettez cette information à votre chef. Ce dernier veut également contrôler ces informations à l'aide de la commande netsh mais sans succès, pourquoi ?  
*Comme le serveur DHCP est installé sur le serveur, les commandes netsh correspondantes ont été ajoutées au serveur, ce qui n'est pas le cas de la station de travail du chef.*

## Travaux pratiques

Dans les travaux pratiques pour les exercices 1, 2 et 3, vous devrez effectuer les opérations suivantes :

- Définir les plages d'adresses utilisables en IPv4 (Exercice 1).
- Configurer des interfaces réseaux (Exercice 2).
- Activer et configurer le routage (Exercice 2).
- Tester voire dépanner votre réseau (Exercice 3).
- Mettre en œuvre l'adressage IPv6 (Exercice 3).

# Présentation du dépannage

## 1. Ce qu'il faut savoir

Le dépannage réseau d'un ordinateur doit être rigoureux. Il faut toujours vérifier que notre ordinateur fonctionne et rechercher ensuite le problème en s'éloignant vers la destination. Cette procédure peut être remplacée par une procédure dichotomique plus efficace comme le montre le diagramme plus bas.

Le premier point de tout dépannage réseau commence par s'assurer que la couche réseau fonctionne entre les deux ordinateurs pour s'occuper ensuite d'un éventuel problème applicatif dû au DNS, à l'application, etc.

## 2. Quelques outils



### ipconfig (invite de commande)

La commande `ipconfig /all` montre la configuration actuelle de votre ordinateur.

### ping (invite de commande)

La commande `ping` permet de tester la connectivité entre votre ordinateur et la cible, en envoyant un paquet ICMP de type ECHO et en recevant une réponse appelée ECHO REPLY.

- 
-  Afin de garantir une connectivité au niveau IP (couche 3 du modèle OSI), pinguez une adresse IP et pas le nom de l'ordinateur distant.
- 

### tracert ou pathping (invite de commande)

Ces deux outils permettent d'effectuer un traçage en montrant les routeurs rencontrés. Bien qu'ils ne soient pas fiables à 100% en raison des routeurs qui ne répondent pas, leur réponse permet d'identifier rapidement où se situe le problème.

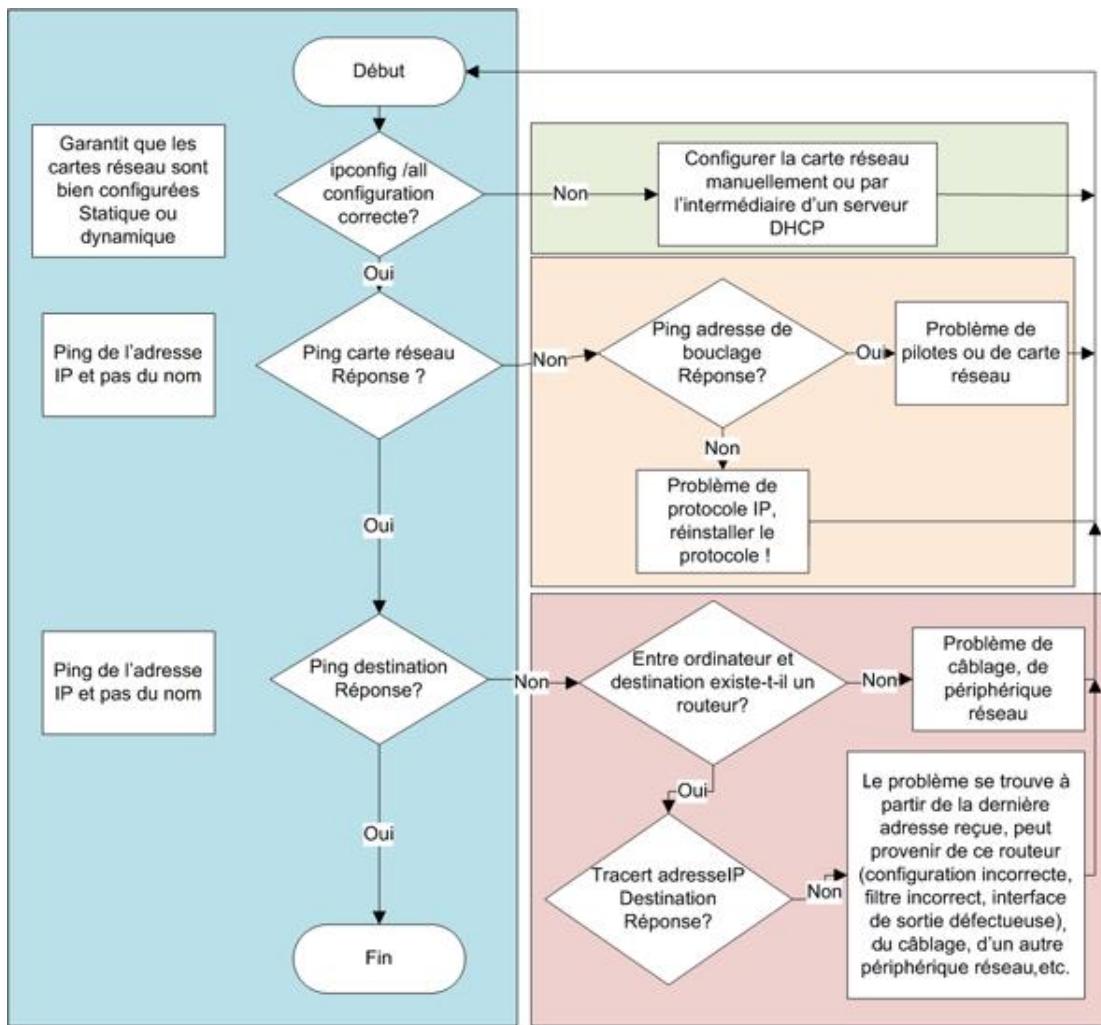
La commande est `tracert <adresseIPDestination>` ou `pathping <adresseIPDestination>`.

### netsh (invite de commande)

La commande `netsh` permet de consulter et de configurer les cartes réseau ainsi que les pare-feu.

## 3. Procédure de dépannage pour garantir un fonctionnement au niveau de la couche 3 du modèle OSI

La procédure suivante est dichotomique et vous garantit qu'en peu d'étapes vous pouvez identifier la source d'un problème réseau.



➤ Tous les outils s'utilisent avec une adresse IP et pas un nom.

➤ Cette procédure s'applique aussi bien au protocole IPv4 qu'IPv6.

# Présentation du routage

Depuis le milieu des années 90, les réseaux d'entreprises ont évolué d'abord pour accepter un plus grand nombre d'hôtes, puis en efficacité et en rapidité.

Cette évolution s'est faite en scindant les réseaux en sous-réseaux et en les reliant à l'aide de routeurs. Chaque sous-réseau représente un domaine de diffusion (domaine de broadcast), en d'autres termes les messages de diffusion sont limités au sous-réseau.

Le routeur est un appareil réseau fonctionnant au niveau de la couche 3 du modèle OSI permettant de relier plusieurs sous-réseaux contigus et de sélectionner le meilleur itinéraire pour les sous-réseaux distants.

Sur les routeurs modernes, des fonctionnalités comme le filtrage des paquets font partie intégrante du routeur.

La famille des serveurs Windows peut également agir en tant que routeur. Son activation est des plus simples. Néanmoins, ensuite, il faut créer des routes soit manuellement ou plus efficacement à l'aide d'un protocole de routage dynamique. Parmi les protocoles de routage existants, Windows Server 2008 supporte uniquement le protocole RIP (*Routing Internet Protocol*), largement répandu. Il peut donc interagir avec d'autres routeurs matériels. Concernant le protocole OSPF présent dans les versions précédentes, Microsoft l'a retiré de Windows Server 2008 car il était peu utilisé.

**RIPv2** est un protocole de routage adapté aux petits réseaux et facile à mettre en œuvre. Notez qu'OSPF est plus adapté dans des configurations WAN, sa mise en œuvre étant également plus complexe.

Le protocole RIP utilise un algorithme dit à vecteur de distance pour calculer la route la moins chère lorsque la topologie offre plusieurs routes. Chaque routeur annonce à ces voisins les routes qu'il connaît en y ajoutant un coût défini par l'administrateur, par l'intermédiaire de paquets UDP sur le port 0520. Ce coût est ensuite utilisé pour calculer la meilleure route. Le nombre maximum de hops (sauts) soit le passage de routeurs, est de 15.

Les problèmes principaux du protocole RIP sont qu'il utilise la notion de classes A, B et C et ne permet pas de travailler avec les suffixes. L'autre problème concerne les boucles. En effet, comme l'apprentissage d'une route ouverte ou fermée peut prendre quelques minutes, le protocole RIP peut décider d'utiliser une route moins efficace. Pour éviter ces problèmes, il faut préférer l'utilisation de RIPv2 qui remplace les messages de diffusion par l'adresse 224.0.0.9. Le protocole OSPF utilise un algorithme dit à lien d'état, le coût est fixe et on ajoute une information indiquant si la route est bonne ou non.

---

 La création et la gestion de routes manuelles ne sont pas forcément inappropriées, mais nécessitent de maîtriser la topologie du réseau.

---

Dans Windows Server 2008, le routage fait partie du rôle **Services de stratégie et d'accès réseau** et plus particulièrement du service de rôle **Services de routage et d'accès à distance**. Il n'est pas possible d'installer ce rôle sur un Server Core.

---

 En terme de performances, le routeur logiciel est moins performant qu'un vrai routeur, par contre il peut avoir son utilité dans de petites entreprises ou des départements où l'on peut ajouter le service de routage à un serveur existant pour un coût minime, celui d'une carte réseau.

---

## 1. Activation du routage par modification de la valeur de la clé de registre IpEnableRouter

Il est possible d'activer le routage en modifiant la valeur de la clé du registre IPEnableRouter de 0 (défaut) qui signifie désactivé à 1 qui signifie activé.

Le chemin est HKLM\ SYSTEM\ CurrentControlSet\ Services\ Tcpip\ Parameters. Un redémarrage est nécessaire.

Les paquets sont envoyés sur toutes les interfaces réseaux connectées. Le fonctionnement diffère de la méthode utilisant le routage et l'accès distant du fait qu'il n'est pas possible :

- d'ajouter un protocole de routage ;
- d'utiliser des filtres.

C'est une méthode simple pour activer le routage entre plusieurs segments de réseau comme par exemple dans un scénario simple utilisant un serveur se trouvant au centre de plusieurs segments réseaux ou un scénario complexe utilisant l'équilibrage de charge NLB et plusieurs cartes réseaux.

## 2. Ajout du service de routage et d'accès distant



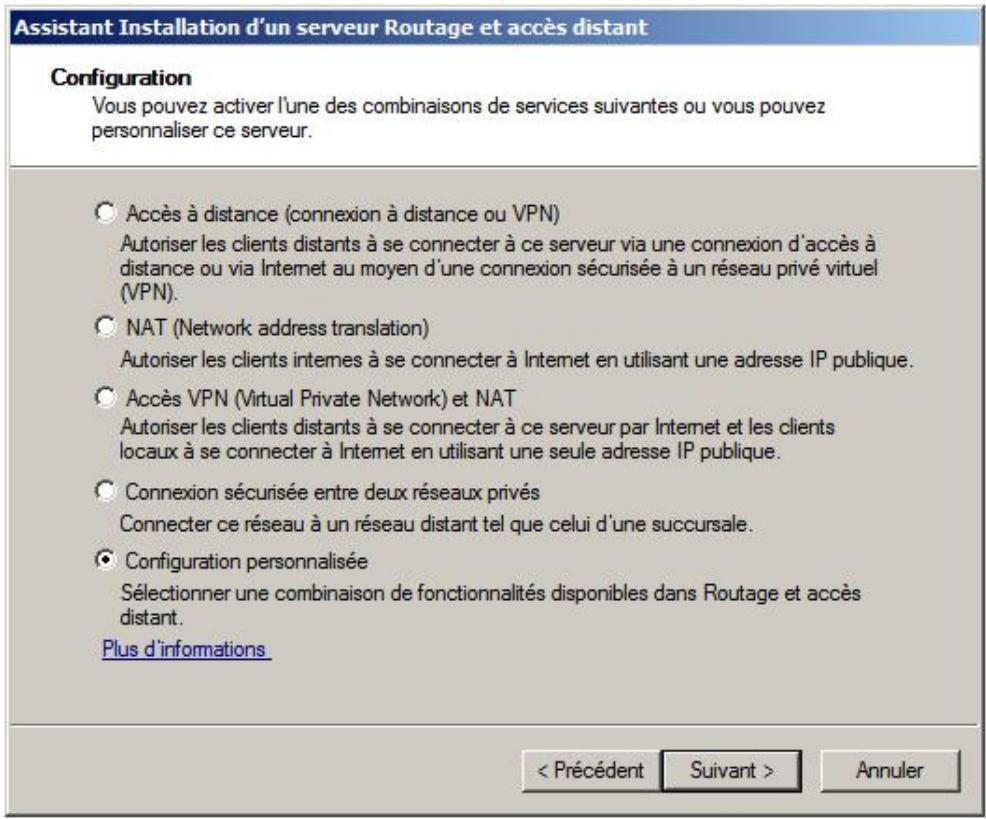
Si le service de rôle n'est pas encore installé :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur **Rôles**.
- Dans la fenêtre principale de **Rôles**, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez **Services de stratégie et d'accès réseau** puis cliquez sur **Suivant**.
- Sur la page **Stratégies et accès réseau**, cliquez sur **Suivant**.
- Sur la page **Services de rôle**, sélectionnez **Routage**.
- Dans la boîte de dialogue **Assistant Ajout de rôles**, cliquez sur le bouton **Ajouter les services de rôle requis**.
- Sur la page **Service de rôle**, cliquez sur **Suivant**.
- Sur la page **Confirmation**, cliquez sur **Installer**.
- Dès que la page **Résultats** apparaît, contrôlez que le rôle est bien installé, puis cliquez sur **Fermer**.

## 3. Activation du service de routage



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez avec le bouton droit de la souris sur **Routage et accès distant**, puis cliquez sur **Configurer et activer le routage et l'accès distant**.
- Sur la page **Bienvenue** de l'assistant, cliquez sur **Suivant**.
- Sur la page **Configuration**, sélectionnez l'option **Configuration personnalisée** puis cliquez sur **Suivant**.



**Accès à distance (connexion à distance ou VPN)** : permet de créer un serveur VPN pour des connexions entrantes.

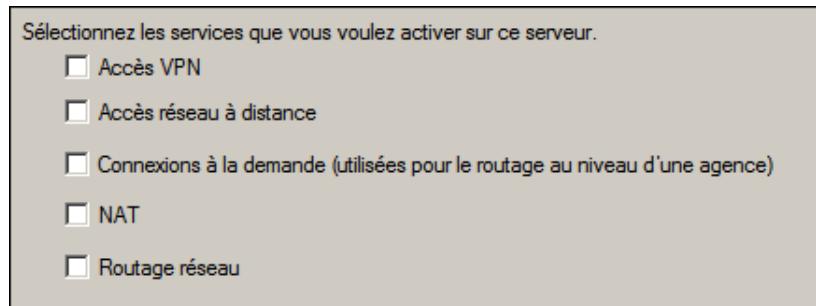
**NAT (Network address translation)** : permet d'activer NAT pour partager un accès Internet avec le réseau local.

**Accès VPN (Virtual Private Network) et NAT** : active VPN et NAT.

**Connexion sécurisée entre deux réseaux privés** : permet de créer un tunnel VPN entre deux points.

**Configuration personnalisée** : permet de sélectionner les options voulues.

- Sur la page **Configuration personnalisée**, sélectionnez **Routage réseau** puis cliquez sur **Suivant**.



**Accès VPN** : permet de créer un serveur VPN pour des connexions entrantes via Internet.

**Accès réseau à distance** : permet de créer un serveur VPN pour des connexions entrantes via un modem ou un autre équipement d'accès à distance.

**Connexions à la demande** : permet de créer ou recevoir des connexions à la demande.

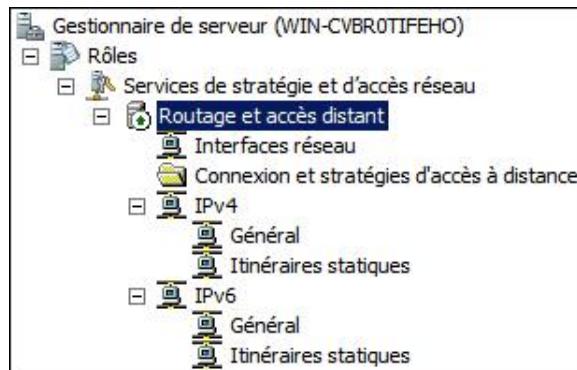
**NAT** : permet d'activer NAT pour partager un accès Internet avec le réseau local.

**Routage réseau** : permet d'activer le routage.

- Sur la page **Fin de l'Assistant Installation d'un serveur de routage et d'accès à distance**, cliquez sur **Terminer**.

- Dans la boîte de dialogue **Routage et accès distant**, cliquez sur **Démarrer le service**.

La console **Routage et accès distant** ressemble à l'image suivante :



Votre serveur est transformé en routeur.

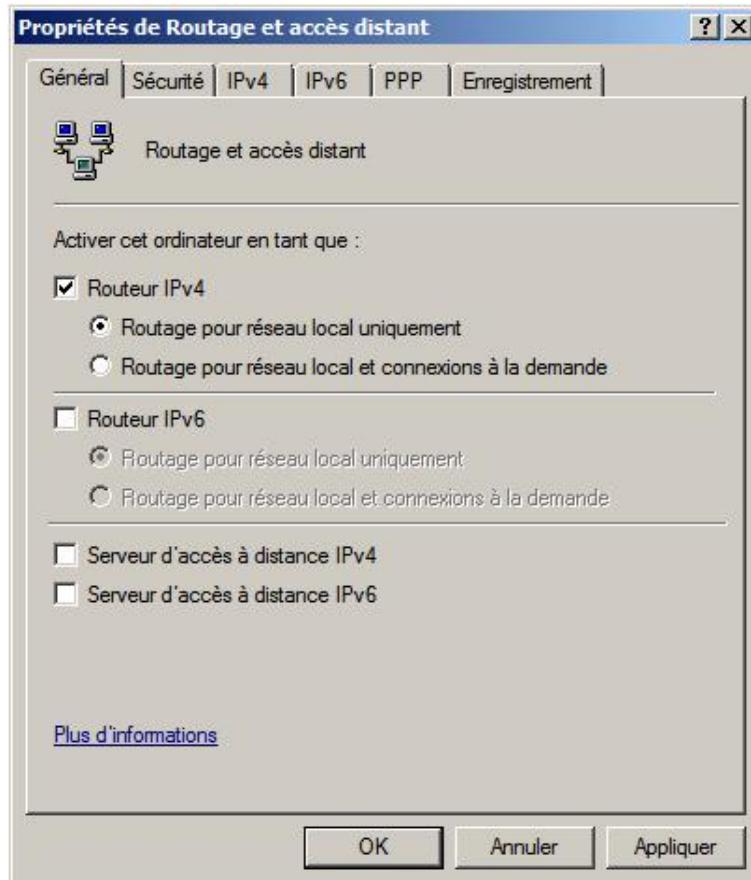
## 4. Configuration du routage



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez avec le bouton droit de la souris sur **Routage et accès distant** puis sur **Propriétés**.

La boîte de dialogue **Propriétés de Routage et accès distant** apparaît.

### Onglet Général



**Routeur IPv4** spécifie si le serveur est activé en tant que routeur IPv4 soit sur le réseau local uniquement (défaut), soit sur le réseau local et les connexions à la demande.

**Routeur IPv6** spécifie si le serveur est activé en tant que routeur IPv6 soit sur le réseau local uniquement, soit sur le réseau local et les connexions à la demande. Par défaut, le routage IPv6 est désactivé.

### Onglet IPv4

La sélection de la case à cocher indique que le routage IPv4 est activé.

### Onglet IPv6

**Activer le transfert IPv6** : active le routage IPv6.

**Activer les annonces de routage par défaut** : indique si un itinéraire par défaut est annoncé sur ce serveur.

**Affectation de préfixe IPv6** : indique le préfixe pour les clients d'accès distant.

### Onglet Enregistrement

Cet onglet permet de sélectionner quelles informations sont enregistrées dans le journal Système de l'Observateur d'événements.

La case à cocher permet d'enregistrer des informations supplémentaires pour les connexions PPP dans le fichier **%systemroot%\tracing\ppp.log**.

## 5. Afficher une table de routage

### Via l'invite de commandes



Win4

Dans une invite de commandes, saisissez **route print** puis appuyez sur [Entrée]. La commande affiche la table de

routage IPv4 et IPv6.

```
C:\>route print
=====
Liste d'Interfaces
 13 ...00 03 ff cd 6a cf ..... Carte Fast Ethernet PCI à base de Intel 21140 (é
mulée) #3
 12 ...00 03 ff cc 6a cf ..... Carte Fast Ethernet PCI à base de Intel 21140 (é
mulée) #2
 10 ...00 03 ff c4 6a cf ..... Carte Fast Ethernet PCI à base de Intel 21140 (é
mulée)
  1 ..... Software Loopback Interface 1
 16 ...00 00 00 00 00 00 e0 isatap.{BDBCF67A-C250-4D8D-A96F-34BD3631F591}
 11 ...02 00 54 55 4e 01 ..... Teredo Tunneling Pseudo-Interface
 14 ...00 00 00 00 00 00 e0 isatap.{E062DA77-A957-4421-B5D0-0BB7096EAEFE}
 15 ...00 00 00 00 00 00 e0 isatap.{DEEFA7CB-D1D0-44EB-AF62-0D0DB6498C4A}
=====

IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau   Masque réseau   Adr. passerelle   Adr. interface   Métrique
  0.0.0.0           0.0.0.0       172.30.1.254    172.30.1.23      21
  127.0.0.0         255.0.0.0     On-link          127.0.0.1       306
  127.0.0.1         255.255.255.255  On-link          127.0.0.1       306
 127.255.255.255  255.255.255.255  On-link          127.0.0.1       306
  172.30.1.0        255.255.255.0   On-link          172.30.1.105    276
  172.30.1.0        255.255.255.0   On-link          172.30.1.23     276
  172.30.1.23       255.255.255.255  On-link          172.30.1.23     276
 172.30.1.105      255.255.255.255  On-link          172.30.1.105    276
 172.30.1.255      255.255.255.255  On-link          172.30.1.105    276
 172.30.1.255      255.255.255.255  On-link          172.30.1.23     276
  224.0.0.0          240.0.0.0     On-link          127.0.0.1       306
  224.0.0.0          240.0.0.0     On-link          d              276
  224.0.0.0          240.0.0.0     On-link          172.30.1.23     276
  224.0.0.0          240.0.0.0     On-link          172.30.1.105    276
 255.255.255.255  255.255.255.255  On-link          127.0.0.1       306
 255.255.255.255  255.255.255.255  On-link          d              276
 255.255.255.255  255.255.255.255  On-link          172.30.1.23     276
 255.255.255.255  255.255.255.255  On-link          172.30.1.105    276
=====

Itinéraires persistants :
  Adresse réseau   Masque réseau   Adresse passerelle   Métrique
  0.0.0.0           0.0.0.0       172.30.1.254      1
=====

IPv6 Table de routage
=====
Itinéraires actifs :
If Metric Network Destination      Gateway
 1  306 ::1/128                 On-link
 13 276 fe80::/64                On-link
 12 276 fe80::/64                On-link
 10 276 fe80::/64                On-link
 13 276 fe80::81:77b8:9079:b13e/128
                                     On-link
 10 276 fe80::100d:188f:ea34:5315/128
                                     On-link
 12 276 fe80::ac86:bd8a:60f6:4e0d/128
                                     On-link
  1 306 ff00::/8                 On-link
 13 276 ff00::/8                 On-link
 12 276 ff00::/8                 On-link
 10 276 ff00::/8                 On-link
=====

Itinéraires persistants :
  Aucun
=====

C:\>
```

### Via la console Routage et accès distant



Win4

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le noeud **Rôles**.
- Cliquez sur le noeud **Services de stratégie et d'accès distant**.

- Cliquez sur le nœud **Routage et accès distant**.
- Cliquez sur le nœud **IPv4** ou **IPv6** pour faire apparaître la table de routage correspondante.
- Cliquez avec le bouton droit de la souris sur **Itinéraires statiques** puis choisissez **Afficher la table de routage IP**.

WIN-CVBR0TIFEHO - Table de routage IP						
Destination	Masque de réseau	Passerelle	Interface	Métrique	Protocole	
ff00::	8	::	Extranet	276	Gestion réseau	
ff00::	8	::	Internet	276	Gestion réseau	
ff00::	8	::	Intranet	276	Gestion réseau	
fe80::ac86:bd8a:60f6:4e0d	128	::	Internet	276	Gestion réseau	
fe80::ac86:bd8a:60f6:4e0d	128	::1000	Boucle de ra...	50	Locale	
fe80::100d:188fea34:5315	128	::	Extranet	276	Gestion réseau	
fe80::100d:188fea34:5315	128	::1000	Boucle de ra...	50	Locale	
fe80::81:77b8:9079:b13e	128	::	Intranet	276	Gestion réseau	
fe80::81:77b8:9079:b13e	128	::1000	Boucle de ra...	50	Locale	
fe80::	64	::	Extranet	276	Gestion réseau	
fe80::	64	::	Internet	276	Gestion réseau	
fe80::	64	::	Intranet	276	Gestion réseau	
::1000	128	::1000	Boucle de ra...	50	Locale	

# Configuration du Centre de réseau et partage

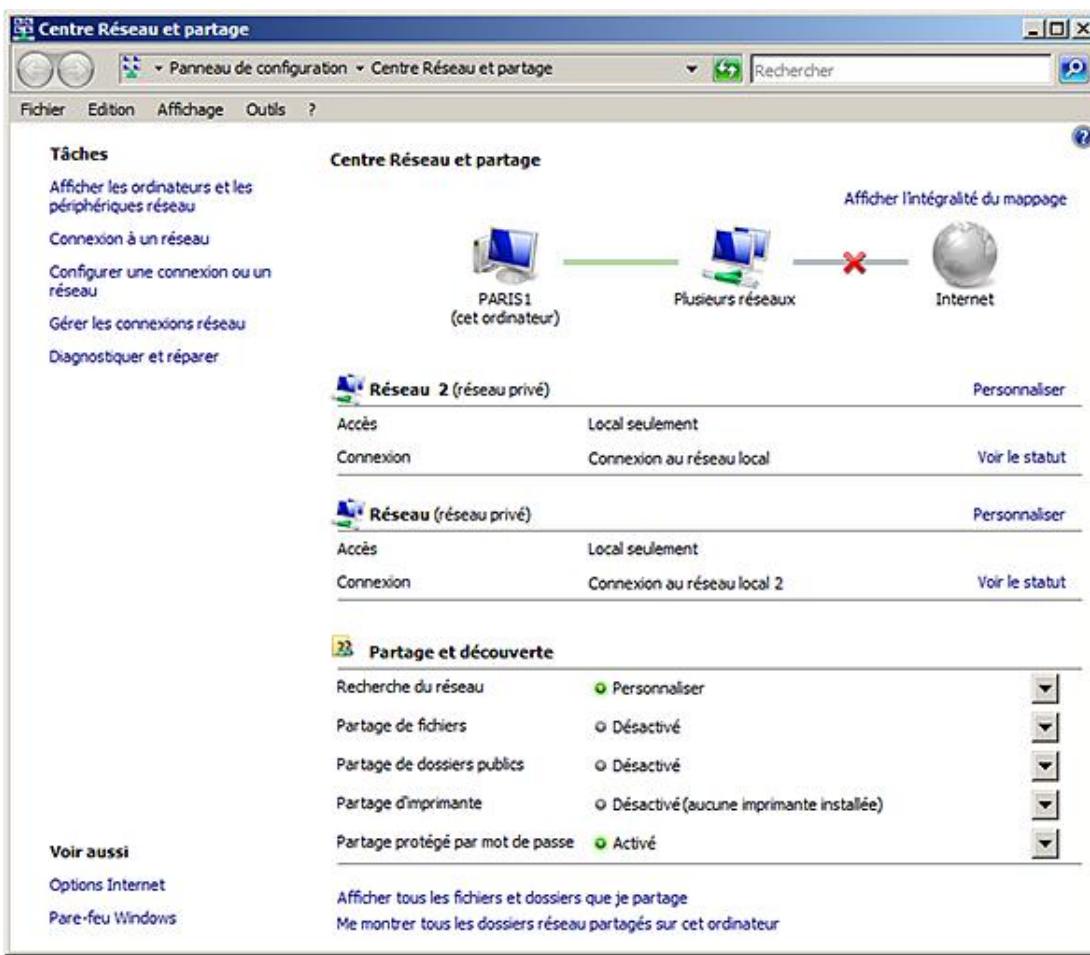


Le Centre réseau et partage apparu avec Windows Vista est un outil orienté utilisateur final qui permet de contrôler la connectivité réseau. Il permet de gérer simplement non seulement le type d'accès réseau (filaire, sans fil, VPN, etc.) mais également la visibilité d'éléments qui peuvent être partagés. Son interface graphique a alourdi beaucoup d'opérations par rapport aux anciennes versions de Windows Server 2008.

## 1. Ouvrir le Centre réseau et partage

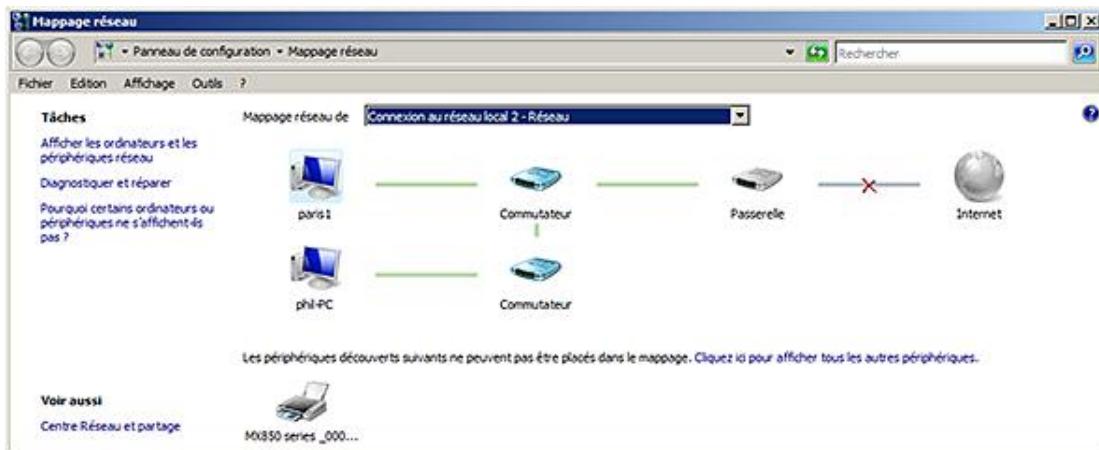
Pour ouvrir le Centre réseau et partage, suivez cette procédure :

- Sur le **Bureau**, dans la **zone de notification**, cliquez sur l'icône suivante .
- Sur la boîte de dialogue qui apparaît, cliquez sur le lien **Centre réseau et partage**. La fenêtre suivante apparaît :



### a. Mappage réseau

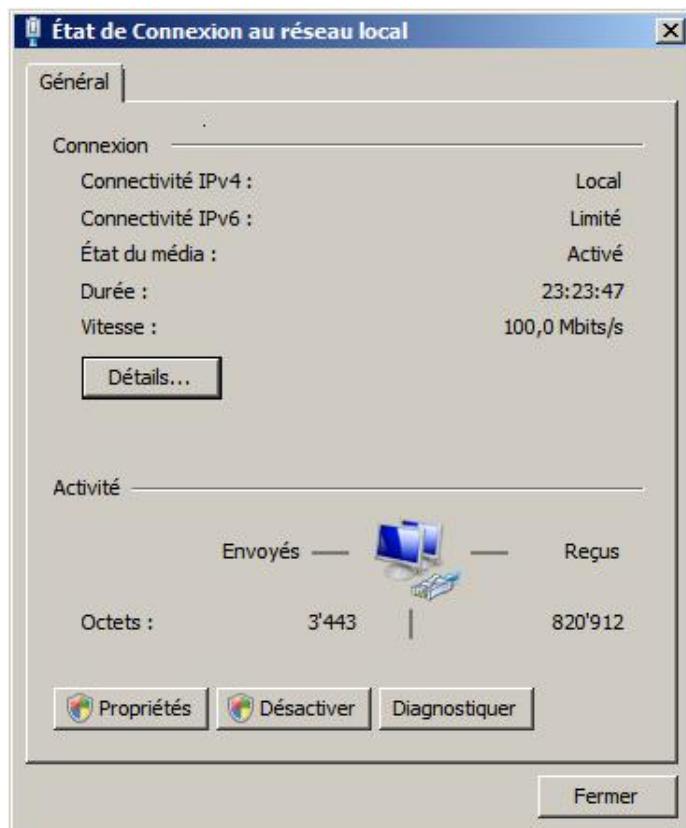
La zone du mappage réseau située en haut à droite représente graphiquement la connexion actuelle du réseau. Elle utilise le protocole LLTD (*Link Layer Topology Discovery*) pour déterminer et afficher la topologie réseau. Sur l'image précédente, vous pouvez remarquer que l'ordinateur paris1 se trouve connecté à plusieurs réseaux et n'est pas connecté à Internet. Un manque de connexion à Internet signifie généralement que l'adresse de la passerelle par défaut n'est pas définie. Si vous cliquez sur **Afficher l'intégralité du mappage** pour autant que l'ordinateur se trouve sur un type d'emplacement réseau qui n'est pas public et que le mappage réseau est activé, alors vous pouvez faire apparaître le mappage existant comme le montre l'image suivante :



## b. Connexion réseau

Sur la fenêtre du **Centre Réseau et partage**, en dessous de la zone de mappage réseau, vous trouvez les informations concernant l'accessibilité et la connexion de chacune des cartes réseaux. En cliquant sur le lien **Personnaliser**, vous pouvez modifier le nom du réseau, le type d'emplacement (public/privé), modifier l'icône représentant le réseau ainsi que fusionner des emplacements réseaux, c'est-à-dire définir un réseau composé de plusieurs emplacements réseaux.

En cliquant sur **Voir le statut**, vous faites apparaître la boîte de dialogue **Statut** de la fenêtre **Etat de la connexion au réseau local** comme le montre l'image suivante :



Le bouton **Détails** permet d'afficher les détails de la connexion.

Le bouton **Propriétés** permet d'afficher la boîte de dialogue **Propriétés** qui permet entre autres de modifier l'adressage IPv4 et IPv6 comme l'a montré la section précédente.

Le bouton **Désactiver** permet de désactiver l'interface réseau.

Le bouton **Diagnostiquer** permet de lancer l'outil de diagnostic pour vous indiquer une solution en cas de problème réseau.

### c. Partage et découverte

Sur la fenêtre du **Centre Réseau et partage**, dans la zone **Partage et découverte** vous pouvez modifier l'état (Activé/Désactivé/Personnaliser) de certains éléments réseaux comme l'explique la prochaine section.

## 2. Types d'emplacements réseau

Le type d'emplacement réseau agit automatiquement sur les règles du pare-feu. Il est nécessaire de définir correctement le type d'emplacement lorsque Windows le demande, c'est-à-dire à chaque changement de réseau lorsque la notification invite l'utilisateur à définir le nouvel emplacement. Bien que cette fonctionnalité soit très utile pour un utilisateur nomade, elle trouve son intérêt pour un serveur, si ce dernier doit être déplacé en définissant des règles très strictes lorsque l'ordinateur se situe sur un réseau autre que le réseau de domaine.

Windows Server 2008 peut se trouver dans l'un des types d'emplacements réseaux suivants :

- **Domaine** : un emplacement réseau qui est reconnu comme faisant partie du réseau de domaine.
- **Privé ou professionnel** : un emplacement réseau que l'utilisateur ou l'administrateur considère comme étant suffisamment sécurisé. Microsoft recommande de se trouver au moins derrière un pare-feu réseau ou un traducteur d'adresses réseau (NAT).
- **Public** : représente tous les autres emplacements.
- **Non identifié** : un emplacement réseau qui n'est pas encore défini. Les règles de l'emplacement public s'appliquent.

Le tableau suivant montre les différences des règles du pare-feu et les emplacements réseaux.

Partage ou découverte (règles du pare-feu)	Emplacement de domaine	Emplacement privé ou professionnel	Emplacement public
Recherche du réseau	Désactivé	Activé	Désactivé
Partage de fichiers	Désactivé	Activé	Désactivé
Partage de dossiers publics	Activé	Désactivé	Désactivé
Partage d'imprimante	Activé*	Activé*	Désactivé
Partage protégé par mot de passe	Non disponible	Activé	Activé

\* Seulement si une imprimante partagée est définie sur l'ordinateur.

 Il faut savoir que Windows conserve une trace de chaque réseau sur lequel l'ordinateur se sera connecté afin de rétablir le cas échéant la connexion en utilisant les paramètres de la dernière connexion sur ce réseau. En utilisant la commande **netsh**, il est possible de gérer la liste des réseaux visités.

## 3. Les tâches

Dans le **Centre Réseau et partage**, les tâches sont situées à gauche.

Le lien **Afficher les ordinateurs et les périphériques réseau** affiche une fenêtre avec le nom des ordinateurs et périphériques découverts sur le réseau. Si un des services dnscache (client DNS), fdrespub (Publication des ressources de découverte de fonctions), ssdpsrv (Découverte SSDP) et upnphost (Hôte de périphérique UPnP) ou une exception du pare-feu commençant par **Découverte** est manquante, l'état n'est pas activé mais personnalisé. Le fait d'activer la découverte réseau n'agit que sur les règles du pare-feu en les activant et en démarrant les services nécessaires mais en aucun cas, il ne modifie l'état de démarrage des services nécessaires. Cette fonctionnalité n'utilise pas le service Browser (Explorateur d'ordinateurs).

Le lien **Connexion à un réseau** permet, s'il existe plusieurs réseaux, de se connecter à un réseau spécifique. Généralement, cette tâche permet à un utilisateur nomade de sélectionner un réseau sans fil.

Le lien **Configurer une connexion ou un réseau** permet d'afficher l'assistant pour se connecter à un réseau. Un exemple d'utilisation est montré dans le chapitre Configuration des services réseaux avancés.

Le lien **Gérer les connexions réseau** affiche la fenêtre **Connexions réseau** déjà montrée dans une section précédente (ncpa.cpl).

Le lien **Diagnostiquer et réparer** lance l'outil diagnostic réseau de Windows.

Le lien **Options Internet** permet de modifier les propriétés d'Internet Explorer.

Le lien **Pare-feu Windows** démarre le pare-feu Windows.

# Configuration de la carte réseau

Cette section présente les étapes pour configurer la carte réseau avec les protocoles IPv4 et IPv6.

Il est à noter que le nom des cartes réseau est logique et dépend du protocole réseau. Chaque carte physique a au moins deux noms logiques, un pour le protocole IPv4 et un pour le protocole IPv6.

 Il n'est pas possible de supprimer les protocoles IPv4 et IPv6. Seule leur désactivation est permise.

## 1. Configuration via l'invite de commande



### a. Adresse IPv4 statique

- Ouvrez une invite de commande.
- Saisissez `netsh interface ipv4 show interface` pour connaître le nom des différentes interfaces puis appuyez sur [Entrée].
- Saisissez `netsh interface ipv4 set address name="NomCarteRéseau" source=static address=172.30.1.180 mask=255.255.255.0 gateway=172.30.1.254` puis appuyez sur [Entrée].
- Saisissez `netsh interface ipv4 set dnsserver name="NomCarteRéseau" source=static address=172.30.1.254` puis appuyez sur [Entrée] pour ajouter une adresse d'un serveur DNS.

 Il peut être utile de renommer la carte réseau non seulement pour une utilisation plus aisée de l'invite de commandes, mais également pour mieux identifier l'interface réseau.

### b. Adresse IPv4 dynamique

- Ouvrez une invite de commande.
- Saisissez `netsh interface ipv4 show interface` pour connaître le nom des différentes interfaces puis appuyez sur [Entrée].
- Saisissez `netsh interface ipv4 set address name="NomCarteRéseau" source=dhcp` puis appuyez sur [Entrée].
- Saisissez `netsh interface ipv4 set dnsserver name="NomCarteRéseau" source=dhcp` puis appuyez sur [Entrée] pour ajouter une adresse d'un serveur DNS.

### c. Adressage IPv6 manuel

- Ouvrez une invite de commande.
- Saisissez `netsh interface ipv6 show interface` pour connaître le nom des différentes interfaces puis appuyez sur [Entrée].

 Vous pouvez soit ajouter une nouvelle adresse : **add address**, soit modifier une adresse existante : **set address**.

- 
- Saisissez netsh interface ipv6 add address interface="NomCarteRéseau" address=<AdresseIPv6> type=<unicast | anycast> store=<active | persistent> puis appuyez sur [Entrée] pour ajouter une adresse IPv6.
  - Saisissez netsh interface ipv6 add route prefix= ::/0 interface="NomCarteRéseau" Nexthop=<AdresseRouteurIPv6> puis appuyez sur [Entrée] pour ajouter une passerelle par défaut.
  - Saisissez netsh interface ipv6 set dnsserver name="NomCarteRéseau" source=<dhcp | static> address=<AdresseIPv6> register=<non | primary | both> puis appuyez sur [Entrée] pour ajouter un serveur DNS IPv6.

#### d. Adresse IPv6 client DHCP

- Ouvrez une invite de commande.
- Saisissez netsh interface ipv6 show interface pour connaître le nom des différentes interfaces puis appuyez sur [Entrée].
- Saisissez netsh interface ipv6 set interface interface="NomCarteRéseau" advertise=enabled managedAddress=enabled puis appuyez sur [Entrée].

## 2. Configuration via l'interface graphique



#### a. Protocole IPv4

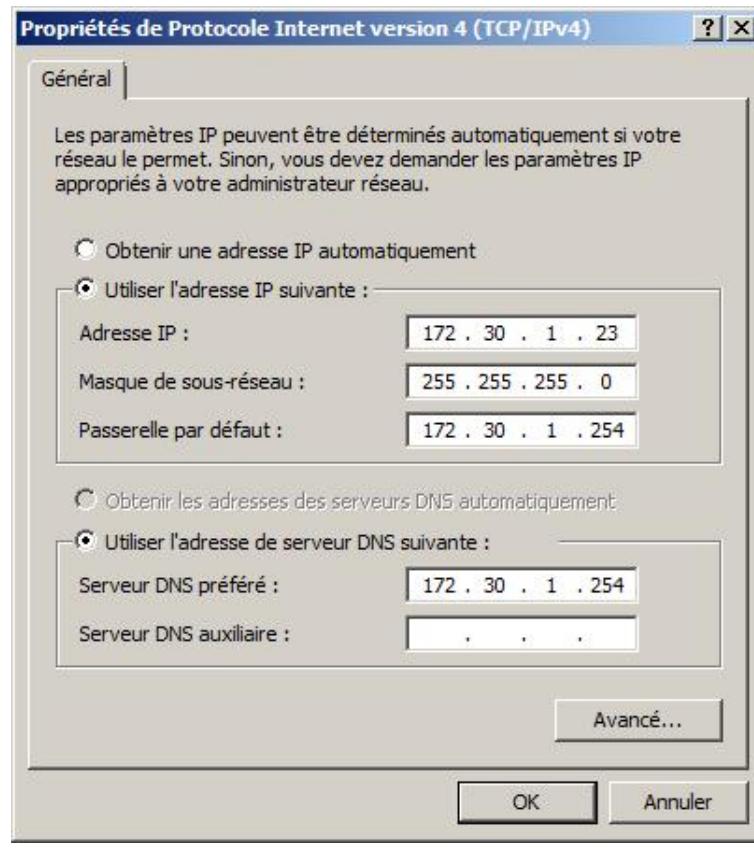
- Pour ouvrir les Connexions réseau, le plus simple est de saisir **control ncpa.cpl** dans la zone **Rechercher** du menu **Démarrer**.



Il est également possible de passer par Centre réseau et partage puis de cliquer sur **Gérer les connexions réseau**.

---

- Cliquez avec le bouton droit de la souris sur la carte à modifier et cliquez sur **Propriétés** dans le menu contextuel.
- Dans la liste de la boîte de dialogue suivante, sélectionnez **Protocole Internet version 4 (TCP/IPv4)** puis cliquez sur le bouton **Propriétés**.



**Obtenir une adresse IP automatiquement** : permet de recevoir une adresse IP provenant d'un serveur DHCP. Cela a pour effet de griser le contenu de **Utiliser l'adresse IP suivante**, d'activer **Obtenir les adresses des serveurs DNS automatiquement** et d'afficher un onglet nommé **Configuration alternative**.

**Utiliser l'adresse IP suivante** : permet d'indiquer une adresse IP statique en inscrivant l'adresse IP et le masque de sous-réseau. La passerelle par défaut est optionnelle.

**Obtenir les adresses des serveurs DNS automatiquement** : permet de recevoir les adresses des serveurs DNS par l'intermédiaire du serveur DHCP.

➤ Notez que ces réglages sont dissociés : vous pouvez stipuler des adresses statiques pour les serveurs DNS tout en conservant un adressage dynamique.

**Utiliser l'adresse de serveur DNS suivante** : permet de spécifier les adresses des serveurs DNS à utiliser dans l'ordre défini. Pour ajouter d'autres serveurs DNS, utilisez le bouton **Avancé** puis l'onglet **DNS**.

Le bouton **Avancé** affiche la boîte de dialogue de configuration avancée des paramètres TCP/IP.

#### Onglet Configuration alternative

Permet de définir comment assigner une adresse si aucun serveur DHCP n'est disponible.

#### Adresse IP privée automatique

Assigne automatiquement une adresse dans les adresses APIPA (169.254.y.z). Attention, le serveur ne reçoit pas de passerelles par défaut ni de serveurs Wins ou DNS sauf s'ils ont été définis dans les propriétés avancées.

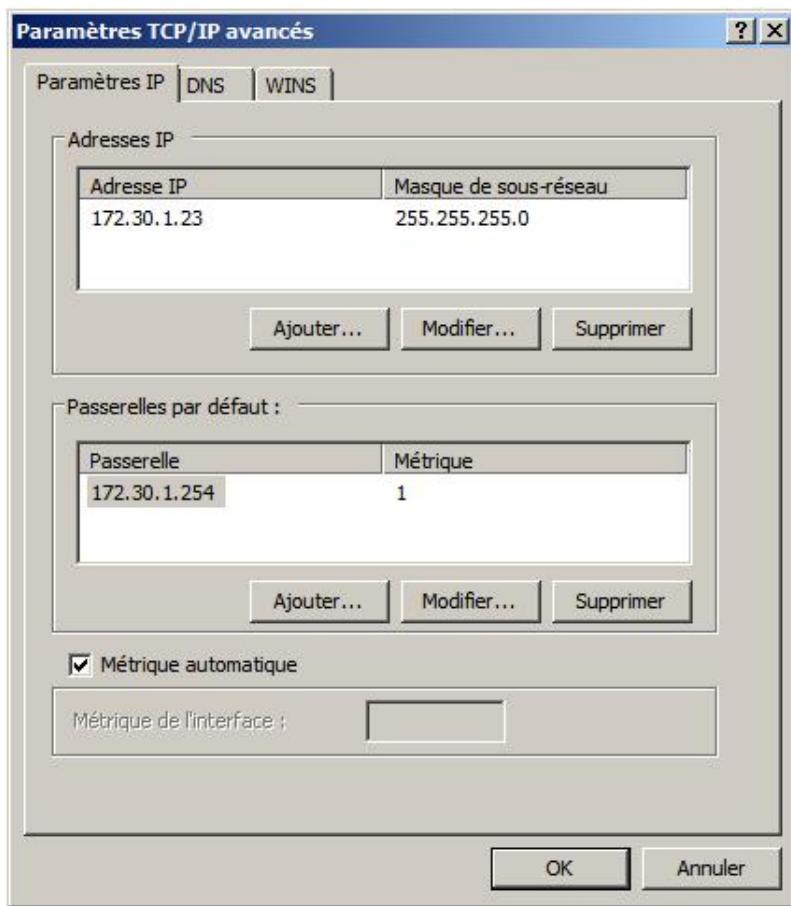
#### Spécifiée par l'utilisateur

Permet de définir une adresse IP statique, un masque ainsi qu'une passerelle par défaut. Vous pouvez également stipuler jusqu'à deux serveurs DNS et deux serveurs WINS. À l'instar de l'APIPA, ces paramètres sont pris en compte en l'absence de réponse d'un serveur DHCP.

➤ La configuration alternative (APIPA ou Utilisateur) est un mode de fonctionnement temporaire. Un test de détection de serveur DHCP est effectué toutes les 5 minutes et cette configuration est abandonnée au profit d'une réponse provenant d'un serveur DHCP.

 Pour désactiver APIPA sur toutes les cartes réseau, utilisez **regedit** pour modifier la valeur **IPAutoconfigurationEnabled** (**DWORD**) à **0** de la clé **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters**.

### Paramètres TCP/IP avancés - onglet Paramètres IP

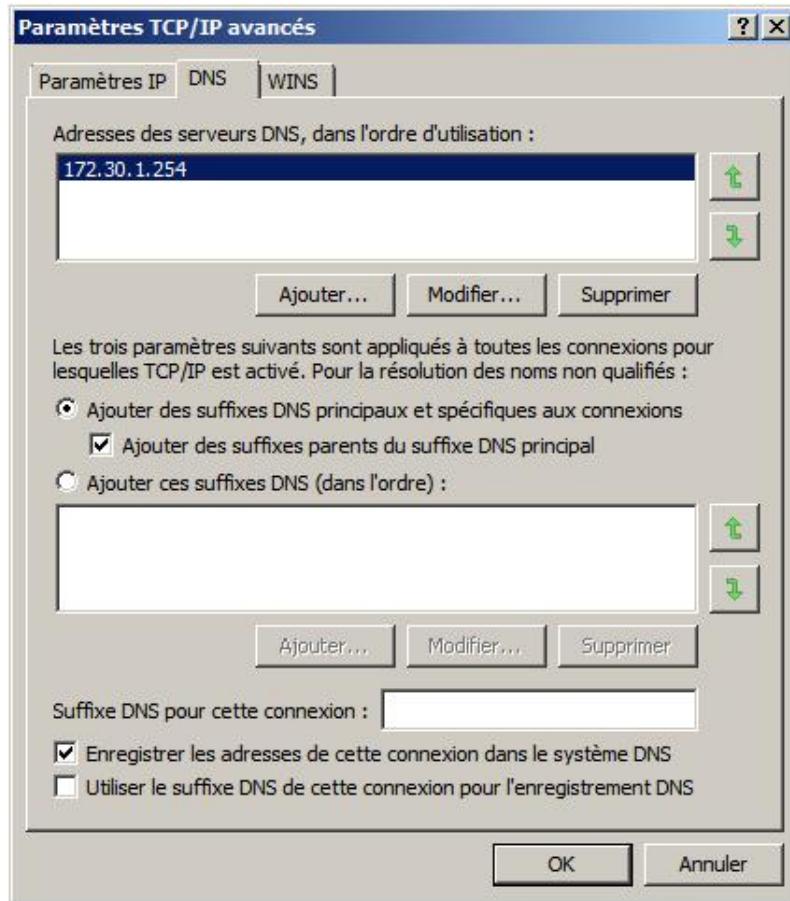


Dans la section **Adresse IP**, si l'adresse IP est statique il est possible d'ajouter d'autres adresses IP à la carte réseau. Pour cela, cliquez sur **Ajouter** puis saisissez l'adresse IP et son masque de sous-réseau. Il est également possible de modifier ou de supprimer une adresse IP sélectionnée. Les scénarios utilisant plusieurs adresses IP sur la même carte concernent généralement la simulation et les tests dans le cas où plusieurs sous-réseaux IP doivent partager le même réseau physique. Dans ce dernier cas, il n'y a pas besoin de passer par un routeur pour accéder au serveur.

Dans la section **Passerelles par défaut**, il est possible d'ajouter d'autres passerelles par défaut. Depuis Windows Server 2008, la notion de *failover* est supportée. Si la première passerelle n'est plus disponible, alors le serveur utilise la suivante dans la liste (*failover*). Le *failover* intervient lorsque le serveur va tenter de se reconnecter sur la première passerelle par défaut indiquée. Il peut être avantageux de déléguer cette notion de *failover* aux routeurs physiques.

L'option **Métrique automatique** permet d'indiquer une valeur de coût pour l'interface ; plus le coût est faible plus la chance d'utiliser l'interface est grande. À ne pas toucher sauf pour des cas spécifiques et d'optimisation.

### Paramètres TCP/IP avancés - onglet DNS



La section **Adresses des serveurs DNS, dans l'ordre d'utilisation** permet d'ajouter des serveurs et de gérer la liste des serveurs DNS si vous en avez plusieurs.

En utilisant les flèches vertes **Haut** et **Bas** situées à droite, il est possible de définir l'ordre d'utilisation des serveurs DNS pour la connexion.

L'ajout des **suffixes DNS** dans l'ordre permet d'utiliser les noms raccourcis (monOrdinateur) des ordinateurs au lieu de leur FQDN (monOrdinateur.pfreddi.ch). Dans le cas où la forêt Active Directory est composée de plusieurs domaines et sous-domaines, il peut être fastidieux d'utiliser les FQDN pour se connecter à un serveur. Il faut garantir que le nom raccourci est unique au sein de l'entreprise.

Dans la zone de texte **Suffixe DNS pour cette connexion**, il est possible de spécifier un suffixe différent pour cette connexion. La case à cocher **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS** est à utiliser conjointement.

La case à cocher **Enregistrer les adresses de cette connexion dans le système DNS** met à jour les informations DNS de cette connexion.

#### Paramètres TCP/IP avancés - onglet WINS

Dans la section **Adresses WINS, dans l'ordre d'utilisation**, vous trouvez les adresses des serveurs WINS. Il est possible d'ajouter les adresses IP des serveurs WINS en cliquant sur **Ajouter** puis en saisissant l'adresse IP. Il est également possible de modifier ou supprimer une adresse IP sélectionnée. En utilisant les flèches vertes **Haut** et **Bas** situées à droite, il est possible de définir l'ordre d'utilisation des serveurs WINS pour la connexion.

La case à cocher **Activer la recherche LMHOSTS** indique s'il faut utiliser ledit fichier pour résoudre les noms NetBIOS.

Le bouton **Importer LMHOSTS** permet de remplacer le fichier LMHOSTS d'origine situé dans le répertoire %SystemRoot%\System32\Drivers\Etc par votre fichier.

Dans la section **Paramètre NetBIOS**, vous pouvez choisir si la résolution de nom NetBIOS est activée et comment elle est configurée :

- **Par défaut** : s'utilise lorsque l'interface reçoit une adresse via un serveur DHCP.
- **Activer NetBIOS sur TCP/IP** : s'utilise lorsque l'interface dispose d'une adresse IP statique ou ne reçoit pas son adresse d'un serveur DHCP.

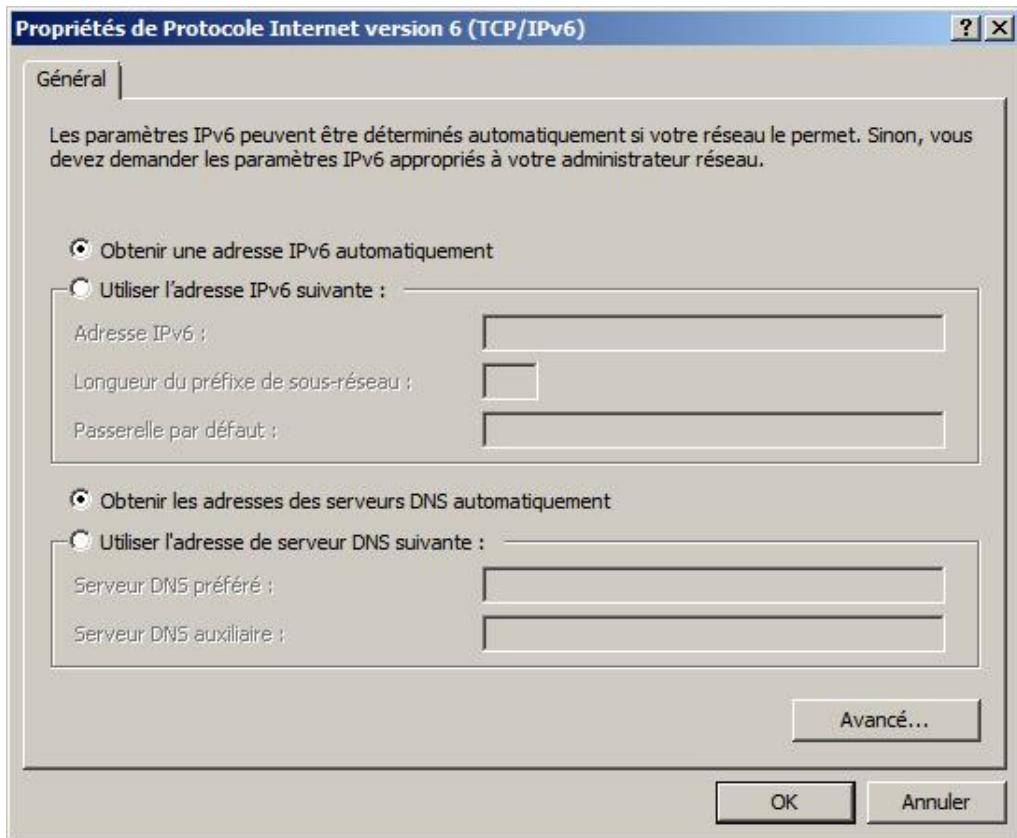
- **Désactiver NetBIOS sur TCP/IP** : désactive la résolution NetBIOS.

## b. Protocole IPv6



Win4

- Pour ouvrir les Connexions réseau, le plus simple est de saisir **control ncpa.cpl** dans la zone **Rechercher** du menu **Démarrer**.
- Cliquez avec le bouton droit de la souris sur la carte à modifier et cliquez sur **Propriétés** dans le menu contextuel.
- Dans la liste de la boîte de dialogue des propriétés, sélectionnez **Protocole Internet version 6 (TCP/IPv6)** puis cliquez sur le bouton **Propriétés**.



Pour l'adresse, vous pouvez soit saisir une adresse manuellement, soit laisser l'ordinateur en acquérir une automatiquement (défaut).

Si vous sélectionnez **Obtenir une adresse IPv6 automatiquement**, vous pouvez soit recevoir les adresses de serveurs DNS automatiquement, soit les saisir manuellement.

Si vous sélectionnez **Utiliser l'adresse IPv6 suivante**, il vous faut saisir une adresse IPv6 valide et la **Longueur du préfixe de sous-réseau**. La **Passerelle par défaut** et les serveurs DNS sont des valeurs optionnelles. Dans cet état, vous ne pouvez pas recevoir les adresses des serveurs DNS automatiquement.

Le bouton **Avancé** fait apparaître les paramètres TCP/IP avancés.

Les formulaires des deux onglets sont semblables à leur homologue TCP/IPv4.

### Paramètres TCP/IP avancés - onglet Paramètres IP

Dans la section **Adresse IP**, si l'adresse IP est statique il est possible d'ajouter d'autres adresses IP à la carte réseau. Pour cela, cliquez sur **Ajouter** puis saisissez l'adresse IP et son masque de sous-réseau. Il est également possible de modifier ou supprimer une adresse IP sélectionnée. Les scénarios utilisant plusieurs adresses IP sur la même carte concernent généralement la simulation et les tests dans le cas où plusieurs sous-réseaux IP doivent partager le même réseau physique. Dans ce dernier cas, il n'y a pas besoin de passer par un routeur pour accéder

au serveur.

Dans la section **Passerelles par défaut**, il est possible d'ajouter d'autres passerelles par défaut. Depuis Windows Server 2008, la notion de *fallback* est supportée. Si la première passerelle n'est plus disponible, alors le serveur utilise la suivante dans la liste (*failover*). Le *fallback* intervient lorsque le serveur va tenter de se reconnecter sur la première passerelle par défaut indiquée. Il peut être avantageux de déléguer cette notion de *failover* aux routeurs physiques.

L'option **Métrique automatique** permet d'indiquer une valeur de coût pour l'interface ; plus le coût est faible plus la chance d'utiliser l'interface est grande. À ne pas toucher, sauf pour des cas spécifiques et d'optimisation.

#### Paramètres TCP/IP avancés - onglet DNS

La section **Adresses des serveurs DNS, dans l'ordre d'utilisation** permet d'ajouter des serveurs et de gérer l'ordre des serveurs DNS si vous en avez plus de deux.

L'ajout des suffixes DNS permet d'utiliser les noms raccourcis (monOrdinateur) des ordinateurs au lieu de leur FQDN (monOrdinateur.pfreddi.ch). Dans le cas où la forêt Active Directory est composée de plusieurs domaines et sous-domaines, il peut être fastidieux d'utiliser les FQDN pour se connecter à un serveur. Il faut garantir que le nom raccourci est unique au sein de l'entreprise.

Dans la zone de texte **Suffixe DNS pour cette connexion**, il est possible de spécifier un suffixe différent pour cette connexion. La case à cocher **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS** est à utiliser conjointement.

La case à cocher **Enregistrer les adresses de cette connexion dans le système DNS** met à jour les informations DNS de cette connexion.

## 3. Activation/désactivation d'un protocole IP



### a. Activer ou désactiver le protocole IPv4

- Ouvrez une invite de commande.
- Saisissez `netsh interface ipv4 install |uninstall` puis appuyez sur [Entrée].
- Redémarrez le serveur.

### b. Activer ou désactiver le protocole IPv6

- Cliquez sur **Démarrer** et saisissez **regedit** dans la zone **Rechercher** puis appuyez sur [Entrée].
- Déplacez-vous vers **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\**.
- Donnez à **DisabledComponents** (DWORD32) une des valeurs suivantes :
  - 0 pour activer
  - 0xffffffff pour désactiver tous les composants IPv6 excepté l'interface de bouclage
  - 0x20 pour utiliser IPv4 au lieu d'IPv6 dans les préfixes
  - 0x10 pour désactiver les interfaces natives Ipv6
  - 0x01 pour désactiver tous les tunnels Ipv6
  - 0x11 pour désactiver les interfaces IPv6 excepté l'interface de bouclage
- Redémarrez le serveur.

- 
-  Il est fortement conseillé de désactiver le protocole IP qui n'est pas utilisé. Néanmoins certaines applications peuvent requérir les deux protocoles pour fonctionner correctement comme par exemple Exchange Server 2007 exige la présence du protocole IPv6 pour pouvoir utiliser le protocole IPv4.
  -  Si vous désactivez les protocoles en les décochant via les propriétés de la carte réseau, le protocole n'est pas entièrement désactivé.
-

# Introduction à l'adressage IPv6

L'adressage IPv6 devrait permettre de s'affranchir des limitations du nombre d'adresses du modèle IPv4. IPv6 a surtout été conçu pour répondre aux besoins des réseaux modernes dont les principales fonctionnalités sont :

- Nouveau format de l'en-tête (il devient plus efficace).
- Espace d'adressage plus important ( $3.4 \cdot 10^{38}$ ).
- Configuration des adresses en mode *stateful* et *stateless*.
- Sécurité intégrée (IPsec obligatoire).
- Infrastructure de routage hiérarchique efficiente.
- Amélioration du support de la priorité des paquets.
- Extensibilité

Pour l'introduction du protocole IPv6 dans les entreprises, il faut non seulement que les versions des systèmes d'exploitation disposent d'une pile IPv6, mais également que tout matériel réseau travaillant au moins au niveau de la couche 3 du modèle OSI utilise et gère ce protocole.

Windows supporte le protocole IPv6 depuis Windows NT4, mais c'est à partir de Windows XP SP1 qu'il est possible d'utiliser IPv6 dans un environnement de production. Windows Server 2008 apporte également l'infrastructure réseau nécessaire pour une implémentation dans de bonnes conditions, comme le support d'IPv6 dans les serveurs DNS et DHCP.

Les améliorations apportées avec Windows Server 2008 sont :

- IPv6 est installé et activé par défaut.
- Double pile IP (IPv4 et IPv6).
- Configuration possible à l'aide d'une interface graphique.
- Améliorations pour le protocole Teredo.
- Support d'IPsec intégré.
- Support pour la résolution de nom multicast link-local LLMNR.
- IPv6 sur PPP.
- Support du DHCPv6.
- Identificateur d'interface aléatoire pour les adresses IPv6.
- Support du Multicast Listener Discovery version 2 (MLDv2).

---

 Le mode *stateful/stateless* fait référence à la manière dont l'adresse IP a été obtenue. En mode *stateful*, l'adresse IP est acquise par l'intermédiaire d'un serveur DHCP. En mode *stateless*, l'ordinateur s'autoconfigure automatiquement pour autant qu'un routeur puisse annoncer le réseau IPv6.

---

## 1. L'adressage IPv6

Une adresse IPv6 se compose de 128 bits, soit 16 octets. Sa représentation utilise la notation hexadécimale.

Voici quelques exemples d'adresses valides :

- FE80::DSEC:AD14:FEC:FB14
- 2001:8B4

---

 Remarquez que les 0 peuvent être remplacés par ::.

---

### **La règle de compression des 0**

Soit :

- 1 bloc = 16 bits
- 8 blocs de 16 bits = 128 bits
- :: représente n blocs ne contenant que des 0
- Nb = nombre de blocs non vides
- Ne = nombre de blocs ne contenant que des 0
- Ne = 8 - Nb
- Nombre de bits représentés = Ne \* 16

Prenons par exemple l'adresse FE08::45

Il existe 2 blocs, soit le bloc FE08 et le bloc 45.

Il existe 8 blocs dans une adresse IP.

Donc il reste 6 blocs, soit 8 - 2, ce qui représente 96 bits car chaque bloc est composé de 16 bits.

### **Quelques adresses IPv6**

#### **Compatibilité avec les adresses IPv4**

0:0:0:0:0:172.30.1.101 ou ::172.30.1.101

#### **Adresse de bouclage**

0:0:0:0:0:1 ou ::1

#### **Liaison locale**

FE80::2822:E68:53E1:FE97

#### **Adresse mappée IPv4**

::FFFF.192.168.1.1

#### **Teredo**

2001:0:D5C7:A2CA:2822:E68:53E1:FE97

## **2. Préfixes IPv6**

Le préfixe correspond aux nombres de bits de l'adresse IPv6 utilisés par le sous-réseau et s'écrit en utilisant la notation CIDR soit : **Adresse-IPv6 /LongueurDuPrefixeEnBits**. 2001: AAC3:12DD::/48 en est un exemple où les 48 premiers bits définissent le sous-réseau.

### 3. Types d'adresses IPv6

Il existe 3 types d'adresses :

- **Unicast** (monodiffusion) : identifie une interface unique. Le paquet est envoyé à un ordinateur spécifique.
- **Multicast** (multidiffusion) : identifie entre 0 et n interfaces. Le paquet est envoyé à un groupe d'ordinateurs. Le premier octet est toujours **FF** suivi par une étendue, généralement la liaison locale **02**, le site local **05** et l'étendue globale **0E**. Le multicast remplace la diffusion IPv4 (*Broadcast*).
- Une adresse **anycast** est associée à plusieurs interfaces. La communication va de l'émetteur vers l'adresse anycast la plus proche en terme de distance de routage donc vers une seule interface.

### 4. Identification des types d'adresses

**Adresse non spécifiée** : soit l'absence d'adresse IPv6 comme par exemple lorsque le nœud arrive sur le réseau et qu'il attend pour recevoir une adresse. Sa notation est **::/128**.

**Adresse de bouclage** : l'adresse de bouclage est **::1/128**.

**Adresse multicast** : cette adresse commence toujours par **FF00::/8**.

**Adresse de liaison locale unicast** : cette adresse commence toujours par **FE80::/10**.

**Adresse globale unicast** : toutes les autres adresses.

**Adresse anycast** : est prise dans l'espace d'adressage Unicast et ne peut syntaxiquement être distinguée par rapport à une adresse Unicast.

### 5. Blocs d'adresses

#### a. Adresses non utilisables sur Internet

**Adresses dont la portée est le nœud** : **::/128** (adresse non spécifiée, RFC 4291) et **::1/128** (adresse de bouclage, RFC4291).

**Adresse IPv4 mappée** : soit **0:0:0:0:FFFF:x.y.z.w/96** ou **::FFFF.x.y.z.w /96** est utilisée pour des applications réseaux durant la période de transition sur un nœud disposant d'une double pile (RFC4038).

**Adresse compatible IPv4** : soit **0:0:0:0:0:w.x.y.z/96** ou **::w.x.y.z/96** est utilisée pour encapsuler une adresse IP v4 dans IPv6. Ces adresses sont dépréciées et ne devraient plus être utilisées (RFC4291).

**Adresse Liaison locale** : elle permet une communication locale entre interfaces sur le même lien. Elle commence toujours par **FE80::/10** et la longueur de l'interface est de 64 bits. Les routeurs ne communiquent jamais avec cette adresse. Il faut noter que toutes les interfaces d'un nœud peuvent disposer d'une adresse de liaison locale (RFC4291).

**Adresse unicast unique local IPv6** : permet d'éliminer l'éventuelle redondance d'adresses provenant des adresses Site Local et simplifie l'adressage dans des organisations complexes. Elle commence par **FC00 ::/7** et la longueur de l'interface est de 64 bits (RFC4193).

**Adresse Site local** : n'est pas routable en dehors du site. Elle doit être assignée. Elle commence toujours par **FCE0::/10** et la longueur de l'interface est de 64 bits. Ce type d'adresse est déprécié et ne devrait plus être utilisé (RFC4193).

**Préfixe de documentation** : commence par **2001 :DB8 ::/32**. Il est utilisé pour documenter des manuels, des RFCs, etc. (RFC3849).

**Adresse ORCHID** : soit *Overlay Routable Cryptographic Hash Identifiers* utilise le bloc 2001 :10 ::/28 (RFC4843). Ce type d'adresse est utilisé en tant qu'identificateur.

## b. Adresses utilisables sur Internet

**Adresse Unicast globale** : équivalente à l'adresse IPv4 d'un ordinateur. Elle est unique sur l'Internet IPv6. Elle commence toujours avec un **2000::/3** et la longueur de l'interface est de 64 bits.

**Adresse 6to4** : est utilisée pour une communication entre deux nœuds exécutant IPv6 sur une infrastructure IPv4. Elle commence toujours par **2002::/16** avec une adresse de type IPv4. C'est du tunneling du protocole IPv6 sur de l'IPv4 (RFC3056). Attention, le passage sur du NAT n'est pas garanti.

**Adresse Teredo** : est un protocole de tunneling utilisé pour encapsuler le protocole IPv6 dans les paquets de type IPv4 des datagrammes UDP qui peuvent passer les routeurs NAT (RFC4380). L'adresse Teredo commence toujours par **2001::/32**.

**Route par défaut** : **::/0** correspond à l'adresse de la route par défaut.

**Adresse multicast** : commence par **FF00::/8**. Seules les adresses dont l'étendue est globale en utilisant les 4 bits prévus à cet effet peuvent être utilisables sur Internet. (RFC4291).

## c. L'indice de zone

L'indice de zone est utilisé par les adresses de liaison locale lorsque plusieurs interfaces existent sur un ordinateur relié à plusieurs réseaux physiques et permettant de supprimer l'ambiguïté de n'être apparemment relié qu'à un seul réseau physique. À la fin de l'adresse, le signe **%<IdDeZone>** est ajouté comme le montre l'adresse suivante **FE80::B1D8:9AD4:9CA:61F2%10**. Dans Windows 2008, l'IdDeZone représente le numéro de l'interface.

## d. Divers

ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) définit une méthode utilisée dans Windows Server 2008 pour générer et déployer des adresses IPv6 de liaison locale à partir de l'adresse IPv4 et d'un mécanisme de découverte des voisins (RFC5214).

Le basculement vers IPv6 en entreprise va se faire mais en douceur. Comme il existe des passerelles IPV4/IPv6, il est possible de ne migrer qu'une partie du réseau de l'entreprise. De même, les FAI peuvent utiliser de manière transparente pour l'entreprise de l'IPv6 en VPN entre les sites de l'entreprise.

# Introduction à l'adressage IPv4 (Internet Protocol version 4)

## 1. Modèle OSI et pile IP

Le modèle OSI (*Open Systems Interconnection*) décrit de manière abstraite une communication en couche entre les périphériques réseaux et les logiciels. Le modèle OSI se compose de 7 couches, à savoir physique, liaison, réseau, transport, session, présentation et application. Le modèle TCP/IP quant à lui, se compose de 4 couches.

La couche **physique** correspond au média, au signal et à la transmission binaire.

La couche **liaison** correspond à l'adressage physique comme la **Mac Address** ainsi qu'à la trame.

La couche **réseau** détermine le chemin entre l'émetteur et le destinataire en utilisant l'adressage logique comme l'adressage IP.

La couche **transport** gère le type de connexion entre l'émetteur et le destinataire et s'occupe de la fiabilité.

La couche **session** gère la session entre l'émetteur et le destinataire.

La couche **présentation** prépare la représentation et éventuellement le chiffrement des données.

La couche **application** présente les données à l'application selon le protocole défini. Attention, il ne s'agit pas de l'application mais de l'interface avec cette dernière.

Le tableau suivant montre les 7 couches et leur correspondance avec le modèle OSI, le modèle TCP/IP, des exemples et des périphériques largement utilisés.

	Modèle OSI	Information	Suite IP	Exemples de protocoles TCP/IP	Types de périphériques
7	Application	Données	Application	NNTP, HTTP, FTP, SMTP, TELNET, DHCP, etc.	Pare-feu
6	Présentation				
5	Session				
4	Transport	Segment	Transport	TCP, UDP	Routeur
3	Réseau	Paquet	Internet	IP, IPSec, ICMP	
2	Liaison	Trame	Réseau	L2TP, PPP, PPTP	Switch, hub
1	Physique	Bits		Carte réseau, câbles,	Câbles

## 2. L'adressage IPv4

Une adresse IPv4 se compose de 32 bits, soit 4 octets ou 4 294 967 296 adresses théoriques. Sa représentation utilise la notation décimale pointée. En d'autres termes, chaque octet est séparé par un point et peut prendre n'importe quelle valeur comprise entre 0 et 255.

0.255 • 0.255 • 0.255 • 0.255

L'adresse IP représente deux éléments, à savoir l'adresse du réseau sur lequel se trouve l'hôte, et l'adresse de l'hôte sur ce réseau.

 Un hôte est un appareil se trouvant sur un réseau comme un ordinateur, un routeur, un pare-feu, etc.

Le masque de sous-réseau permet de distinguer l'adresse de l'hôte et l'adresse du réseau.

La RFC 791 ([www.rfc-editor.org](http://www.rfc-editor.org)) définit des classes d'adresses utilisables facilement reconnaissables grâce à l'identification du premier octet. Chaque classe est associée à un masque de sous-réseau. La figure suivante les montre :

Classe	Premier octet, en binaire	Premier réseau	Dernier réseau	Nombre de réseau	Masque de sous-réseau	Nombre d'hôtes par réseau
A	00000000	1.0.0.0	126.0.0.0	126	255.0.0.0	16777214
B	10000000	128.0.0.0	191.255.0.0	16384	255.255.0.0	65534
C	11000000	192.0.0.0	223.255.255.0	2097152	255.255.255.0	254
D	11100000	224.0.0.0				
E	11110000	240.0.0.0				

Seules les classes A, B et C peuvent être utilisables, la classe D est réservée et utilisée pour des adresses de type multicast et la classe E est réservée. Certaines implémentations de Windows ne supportent pas cette dernière, comme Windows 2000.

D'autre part, il n'est pas possible d'utiliser les adresses suivantes :

- L'adresse du réseau commençant par 0 signifie *This network* ou "ce réseau" (RFC 1122).
- L'adresse du réseau commençant par 127 signifie une adresse de bouclage et permet de tester la pile réseau (RFC 1122).
- L'adresse ne peut avoir tous les bits à 1 soit 255.255.255.255 car cette adresse est utilisée pour la diffusion générale (*broadcast*).

En 1993, la RFC 1519 définit un système d'adresses sans classe CIDR (*Classless Inter-Domain*) auxquelles un suffixe est ajouté pour indiquer le nombre de bits utilisés pour le réseau donc le masque de sous-réseau. Les objectifs étaient de réduire la taille des tables de routage, de diminuer le gaspillage d'adresses induit par la notion de classes qui oblige à réserver une classe entière même si l'on n'a besoin que de quelques adresses, enfin peut-être certains prévoient-ils déjà la pénurie d'adresses IP.

Comme dans les exemples suivants :

172.30.1.0/24 représente le réseau 172.30.1.0 dont le masque de sous-réseau est 255.255.255.0, soit 24 bits, ce qui permet d'utiliser 254 adresses sur ce réseau allant de 1 à 254.

Alors que 172.30.1.0/28 représente le réseau 172.30.1.0 dont le masque de sous-réseau est 255.255.255.240, soit 28 bits, ce qui permet d'utiliser 14 adresses sur ce réseau allant de 1 à 14.

Alors que 172.30.1.64/28 représente le réseau 172.30.1.64 dont le masque de sous-réseau est 255.255.255.240, soit 28 bits, ce qui permet d'utiliser 14 adresses sur ce réseau allant de 65 à 79.

---

 Dans les deux derniers exemples, l'adresse 172.30.1.65 ne se trouve pas dans le même réseau que 172.30.1.1 !

---

Il n'est pas possible d'utiliser n'importe quelle adresse IP. Il est important de choisir des adresses provenant des adresses dites privées basées sur la RFC 1918 qui vous permettent d'utiliser sans restriction toutes les adresses suivantes :

- 10.0.0.0 à 10.255.255.255
- 172.16.0.0 à 172.31.255.255
- 192.168.0.0 à 192.168.255.255

---

 Les adresses IP privées couvrent tous les besoins internes des entreprises.

---

Si vous voulez utiliser des adresses publiques, il est possible de les louer auprès de votre fournisseur d'accès Internet voire RIPE en Europe.

L'**IANA** (*Internet Assigned Numbers Authority*) est l'organisme qui gère les espaces d'adresses IPv4 et IPv6 (voir

- N'utilisez pas des adresses publiques tant que vous ne les avez pas louées car vous ne pourriez pas atteindre sur Internet des ordinateurs se trouvant sur le même réseau par exemple.

Enfin, il existe une plage privée spécifique appelée lien local ou APIPA (*Automatic Private IP Addressing*) qui permet aux ordinateurs clients d'un serveur DHCP de s'attribuer automatiquement une adresse IP si ce dernier n'est pas disponible. L'adresse obtenue se trouve dans la plage 169.254.0.0 à 169.254.255.255.

- Toute adresse commençant par 127 a une signification spéciale comme 127.0.0.1 qui est l'adresse de bouclage (loopback).

Le tableau suivant montre les adresses réservées actuellement :

Bloc d'adresses CIDR	Description	Référence RFC
0.0.0.0/8	Identification locale	1122 page 30
10.0.0.0/8	Réseau privé	1918
127.0.0.0/8	Adresse de bouclage	1122 page 31
169.254.0.0/16	Liaison locale ; APIPA	3330
172.16.0.0/12	Réseau privé	1918
192.0.2.0/24	Réservée pour Test-Net	3330
192.88.99.0/24	Réservée pour 6to4 Relay unicast	3068
192.168.0.0/16	Réseau privé	1918
198.18.0.0/15	Réservée pour des tests de performance	2544
224.0.0.0/4	Utilisé pour la multidiffusion ( <i>Multicasting</i> )	3171
240.0.0.0/4	Réservée pour un usage futur	1112 page 3
255.255.255.255	Adresse de diffusion ( <i>Broadcast</i> )	

### 3. Le calcul des réseaux

En théorie, il n'est pas nécessaire d'effectuer le calcul des sous-réseaux. Si vous devez les calculer, vous pouvez :

- rechercher un calculateur IP gratuit,
- utiliser le calcul binaire,
- utiliser le calcul décimal.

La méthode recommandée utilise uniquement le calcul décimal et des formules simples.

Le calcul décimal est très simple, il suffit de connaître et d'utiliser les règles suivantes applicables si devez partager un réseau d'au maximum 254 hôtes utilisables. Cette règle peut être adaptée facilement pour des réseaux plus grands.

Il faut savoir que :

- Le nombre d'hôtes d'un réseau est toujours une puissance de 2.

- Nombre magique = 256 soit  $2^8$ .
- Masque de sous-réseau = 255.255.255.256 - nombre théorique d'hôtes.
- Nombre théorique d'hôtes = nombre d'hôtes utilisables + 2
- Nombre de sous-réseaux possibles = nombre magique (256) / nombre théorique d'hôtes par sous-réseau.

 Il n'est pas possible d'utiliser la première et la dernière adresse d'un réseau. La première adresse est le nom du réseau et la dernière adresse est l'adresse de diffusion locale de ce réseau.

Prenons comme exemple un réseau sur lequel vous devez disposer de 15 adresses utilisables pour votre sous-réseau. Indiquons également que vous pouvez prendre n'importe quelle adresse dans une plage allant de 172.30.1.0 à 172.30.1.256. Comment allons-nous diviser notre plage d'adresses ? Telle est la question, triviale !

La réponse est la suivante : comme il faut 15 hôtes utilisables, il faut donc ajouter 2 adresses pour connaître le nombre théorique d'hôtes.

17 étant le nombre théorique d'adresses, il nous faut trouver la puissance de 2 égale ou supérieure à 17, soit 32, ou 2 puissance 5, pour connaître le **nombre d'hôtes d'un réseau**. Ce qui signifie que dans notre exemple, il y aura 15 adresses qui ne serviront à rien mais que l'on doit quand même attribuer à notre réseau.

Pour le calcul du masque, il faut utiliser un masque qui a comme dernier octet 224 car  $256 - 32 = 224$  (nombre magique moins le nombre d'hôtes d'un réseau).

Pour le choix de la plage d'adresses, il faut se rappeler que le nombre de sous-réseaux possibles = 256 (nombre magique) / nombre théorique d'hôtes par sous-réseau, soit 8 ( $256/32$ ) sous-réseaux ou plages d'adresses disponibles. Le tableau suivant résume les plages que l'on peut utiliser.

Adresse de réseau	Première adresse disponible	Dernière adresse disponible	Adresse de diffusion locale
172.30.1.0	172.30.1.1	172.30.1.30	172.30.1.31
172.30.1.32	172.30.1.33	172.30.1.62	172.30.1.63
172.30.1.64	172.30.1.65	172.30.1.94	172.30.1.95
172.30.1.96	172.30.1.97	172.30.1.126	172.30.1.127
172.30.1.128	172.30.1.129	172.30.1.158	172.30.1.159
172.30.1.160	172.30.1.161	172.30.1.190	172.30.1.191
172.30.1.192	172.30.1.193	172.30.1.222	172.30.1.223
172.30.1.224	172.30.1.225	172.30.1.254	172.30.1.255

Vous pouvez utiliser n'importe quelle plage parmi celles calculées précédemment.

Pour être complet, il nous faut encore trouver le suffixe. Il suffit également d'utiliser une règle de 3.

- Il y a 8 bits dans un octet.
- $256 =$  un octet soit 8 bits.
- $256$  (nombre magique) = nombre d'hôtes d'un réseau \* nombre de réseaux
- Nombre d'hôtes d'un réseau est une puissance de 2.
- Nombre de réseaux est une puissance de 2.

- Nombre de bits utilisés par le réseau = racine enième du nombre de réseaux.
- $24 = 3$  octets à 255 (255.255.255) soit 24 bits.
- Suffixe = 24 + nombre de bits

Toujours dans notre exemple, on a 8 réseaux de 32 hôtes par réseau.

$8 = 2$  puissance 3, donc 3 bits sont utilisés par le réseau. Ce qui nous donne le suffixe 27 (24 + 3).

Vous pouvez également vous référer au tableau suivant :

Bits*	1	2	3	4	5	6	7	8
<b>Masque</b>	128	192	224	240	248	252	254	255
<b>Suffixe</b>	/25	/26	/27	/28	/29	/30	/31	/32

\*Nombre de bits utilisés par le réseau.

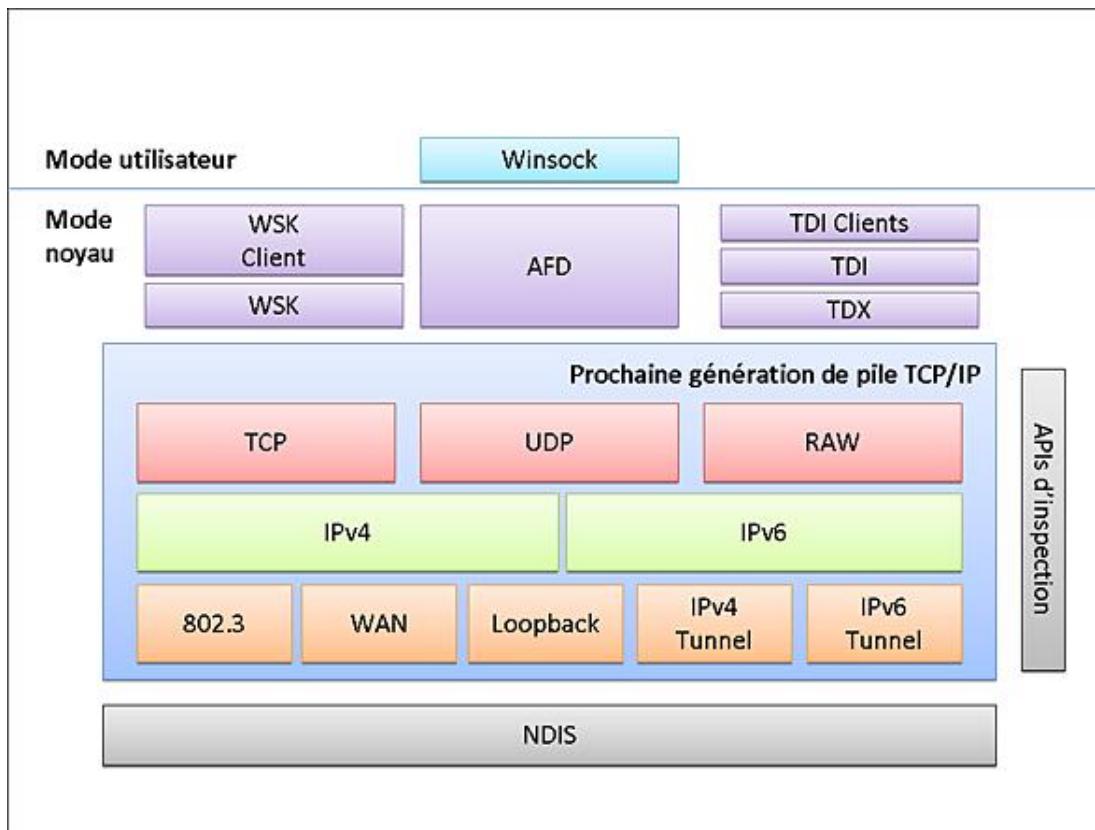
Finalement, nous choisissons la plage **172.30.1.160/27** pour notre réseau.

# Présentation de l'architecture réseau Windows Server 2008

Microsoft a redéfini et réécrit entièrement l'architecture de la pile réseau dans Windows Vista et Windows Server 2008 afin d'améliorer les performances pour augmenter la productivité dans les sites distants. La bande passante est utilisée de manière plus efficiente pour augmenter le débit.

Supportant nativement les protocoles IPv4 et IPv6, la nouvelle pile réseau introduit également la notion de carte réseau virtuelle et physique comme nous le verrons dans une prochaine section.

La figure suivante montre la nouvelle architecture de la pile réseau :



Les nouveautés introduites sont :

## Réglage automatique de la fenêtre de réception



La fenêtre de réception est une mémoire tampon utilisée pour recevoir les paquets. La nouvelle implémentation permet de modifier dynamiquement la taille de cette fenêtre en fonction du débit des paquets pour utiliser le maximum de bande passante disponible, ce qui a un impact non négligeable sur la vitesse de transmission des données. Il est nécessaire que tous les appareils entre le client et le serveur soient compatibles avec la RFC 1323. Il faut peut-être pour cela mettre à jour les BIOS des appareils réseau.

La taille de la fenêtre de réception est déterminée et modifiée automatiquement pour chaque connexion à une fréquence régulière en mesurant le produit bande passante par délai (bande passante multipliée par la latence de connexion) et le taux de récupération des applications.

La commande suivante gère ce paramètre :

```
netsh interface tcp set global autotuninglevel= disabled | enabled
```

## Protocole Compound TCP (CTCP)



Le protocole Compound TCP (CTCP) optimise le débit côté émission et agit de concert avec la fenêtre de réception. Le protocole CTCP est considéré comme agressif car il tente toujours de réduire le temps de transmission de l'information.

La commande suivante gère ce paramètre :

```
netsh interface tcp set global congestionprovider=ctcp | none
```

### **Amélioration dans des environnements à forte perte de paquets**

Prise en charge des RFC suivantes pour optimiser les débits lorsque la qualité de connexion est mauvaise.

#### **RFC 2582**

Modification NewReno de l'algorithme de récupération rapide de TCP.

#### **RFC 2883**

Extension de l'option d'accusé de réception sélectif (SACK, Selective Acknowledgment) pour TCP.

#### **RFC 3517**

Algorithme conservatif de récupération de perte basé sur SACK pour TCP.

#### **RFC 4538**

Récupération F-RTO (*Forward RTO-Recovery*) : algorithme pour la détection des fausses expirations de retransmission avec TCP et le protocole SCTP (*Schema Control Transmission Protocol*).

### **Détection des voisins non atteignables pour IPv4**

Caractéristique venant d'IPv6, elle permet de rechercher l'état d'accessibilité des nœuds IPv4 dans le cache des routes IPv4.

La détection d'inaccessibilité peut s'effectuer en utilisant des requêtes ARP en monodiffusion ou en utilisant des protocoles des couches supérieures tel que TCP.

### **Modification dans la détection de passerelle par défaut inactive**

Bien que Windows Server 2003 et Windows XP aient pu déjà basculer vers une autre passerelle définie (*failover*), Windows Server 2008 tente de revenir vers la passerelle inactive (*fallback*) en testant régulièrement son état.

### **Modifications de la détection des routeurs de type trou noir (Black Hole) PMTU**

Le PMTU (*Path Maximum Transmission Unit*) défini dans la RFC 1191 permet de fragmenter un paquet dont la taille est trop importante pour un segment de réseau. Pour des raisons de sécurité, certains routeurs détruisent les paquets fragmentés sans en avertir l'émetteur. Ils sont appelés routeurs de type Black Hole.

La détection de ce type de routeurs se fait par modification de la taille du segment TCP lors d'une tentative de retransmission.

Cette fonctionnalité est activée par défaut alors qu'elle était désactivée dans Windows Server 2003 et Windows XP. Pour changer l'état du PMTU, il faut modifier dans la base de registre la valeur de type DWORD enablePMTUBHDetect dans HKLM\SYSTEM\CurrentControlSet\Services\TCPPIPC\Parameters de 0 (désactivé) à 1 (activé).

### **Compartiments de routage**

Le compartimentage du routage permet de créer des routes rattachées à la session et non plus à l'ordinateur. Cela permet par exemple d'utiliser une connexion VPN disposant de ses propres adresses et de sa table de routage à côté d'une connexion Internet avec ses propres adresses et sa table de routage.

Le compartimentage agit comme un système de virtualisation des connexions Internet en les isolant.

La commande pour afficher les compartiments est la suivante :

```
Ipconfig /allcompartments /all
```

Cette fonctionnalité n'est pas actuellement implémentée. Vous pouvez seulement visualiser le compartiment actif. Il semble que cette fonctionnalité s'appellera le routage split-tunnel dans Windows 7 et Windows Server 2008 R2.

### **Infrastructure de diagnostics réseau**

Elle permet de disposer d'une architecture extensible qui aide à dépanner les problèmes réseau.

Elle permet de diagnostiquer principalement les problèmes suivants :

- adresse IP incorrecte ;
- passerelle par défaut indisponible ;
- mauvaise passerelle par défaut ;
- problèmes de résolution de noms NetBIOS sur TCP/IP (NetBT) ;
- mauvaise configuration des paramètres DNS ;
- port local déjà utilisé ;
- service client DHCP non démarré ;
- aucun écouteur distant ;
- média déconnecté ;
- port local bloqué ;
- mémoire disponible insuffisante ;
- support de statistiques TCP étendues (ESTATS) qui permet de localiser les goulets d'étranglement (émetteurs, réseau, destinataire).

### **Plate-forme de filtrage Windows (WPF)**

Au fil des années, se sont développées trois méthodes de filtrage qui rendaient la configuration et le dépannage problématiques. Microsoft les a remplacées par la plate-forme de filtrage Windows WPF qui est une architecture ouverte disposant d'APIs à l'attention de sociétés fournissant des pare-feu, anti-virus et autres logiciels de protection.

### **Notification explicite des congestions ECN**

Basée sur la RFC 3168, la congestion est gérée au niveau des segments TCP. Afin de diminuer la perte de paquets à cause d'une congestion se situant au niveau du routeur, les routeurs peuvent marquer les paquets et indiquer qu'il faut diminuer le flux afin d'éviter une congestion.

La commande suivante gère ce paramètre :

```
netsh interface tcp set global encapability = enabled / disabled
```

### **Adaptation de la charge à travers plusieurs processeurs**

Dans les versions précédentes, un seul processeur pouvait être utilisé pour gérer la pile réseau. Depuis Windows Vista, il est possible de répartir la charge réseau entre plusieurs processeurs.

### **Amélioration du protocole IPv6**

Les améliorations sont décrites dans la section correspondante.

### **Qualité de services (QoS)**

À partir de Windows Vista, il est possible de définir les stratégies QoS dans des stratégies de groupe.

Une stratégie QoS permet de :

- définir des priorités ;
- gérer la fréquence d'envoi de trafic réseau sortant ;
- limiter des applications à des adresses IP sources, des adresses IP destinations ainsi que des ports TCP ou UDP sources ou de destinations.

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre plusieurs objectifs décrits dans la section **Configuration des services et de l'adressage IP**.

### Configurer l'adressage IPv4 et IPv6

Cela inclut, sans s'y limiter :

- configurer les options IP ;
- utiliser l'adressage IP en fonction du nombre d'hôtes.

### Configurer le routage

Cela inclut, sans s'y limiter :

- routage statique ;
- routage persistant ;
- RIP (*Routing Internet Protocol*) ;
- OSPF (*Open Shortest Path First*).

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



## 3. Objectifs

La communication tient une place primordiale dans la vie de l'entreprise, celle-ci repose de plus en plus sur des moyens informatiques, que ce soient des périphériques réseau ou des ordinateurs.

Il est donc important de connaître et maîtriser les enjeux afin de supporter et faciliter la communication de l'entreprise qui devient de plus en plus gourmande en ressources et est polluée par des communications non voulues, que ce soient des pourriels, des virus, des spywares, etc.

Ce chapitre commence par décrire la nouvelle architecture réseau apparue avec Windows Vista, continue par une introduction concernant les adressages IPv4 et IPv6 puis aborde la configuration de l'adressage d'une carte réseau. Il se termine par l'étude du routage.

Enfin une procédure de dépannage réseau jusqu'à la couche réseau 3 du modèle OSI est présentée.

Après la lecture de ce chapitre, vous pourrez indiquer les nouveautés introduites par la nouvelle architecture réseau. Vous saurez également configurer une carte réseau aussi bien avec le protocole IPv4 qu'avec IPv6, transformer votre serveur en routeur. Enfin, vous pourrez dépanner un réseau jusqu'à la couche 3 du modèle OSI.

## Résumé du chapitre

Dans ce chapitre, vous avez découvert les nouveautés introduites dans Windows Server 2008 y compris une présentation succincte du NAP (*Network Access Protection*).

Vous savez maintenant reconnaître une adresse IPv4 et une adresse IPv6 et la configurer pour le serveur.

Vous savez comment activer et configurer le routage.

Enfin vous pouvez dépanner un réseau jusqu'au niveau de la couche 3 du modèle OSI.

# Intégration avec l'Active Directory

Comme il a été cité plusieurs fois, le stockage de la base de données DNS dans l'Active Directory appelée **zone intégrée Active Directory** est une méthode conseillée. Pour cela, il faut installer le rôle Serveur DNS sur le contrôleur de domaine, soit en même temps que l'installation de l'Active Directory pour le premier contrôleur de domaine, soit plus tard.

## 1. Quelques mots sur la réPLICATION

Ensuite la réPLICATION est entièrement gérée par l'Active Directory. Il faut noter qu'en fonction de l'emplacement de stockage spécifié pour la zone, la réPLICATION concerne :

- tous les contrôleurs de domaine DNS de la forêt ;
- tous les contrôleurs de domaine DNS du domaine ;
- seulement les contrôleurs de domaine du domaine ;
- plus spécifiquement les contrôleurs de domaine de la forêt qui hébergent une partition applicative.

Bien entendu, il est également possible de créer une réPLICATION mixte avec des serveurs hébergeant des zones secondaires, néanmoins ce n'est pas une solution sécurisée, ni efficace.

## 2. Chargement de zone en arrière-plan

À partir de Windows Server 2008, les zones intégrées Active Directory peuvent se charger en arrière-plan et le serveur DNS peut résoudre les requêtes sans attendre le chargement complet, il est donc *multithread*. Si une requête concerne une zone en chargement, le serveur DNS retrouve l'enregistrement directement en interrogeant l'Active Directory.

La mise à jour d'enregistrements nécessite toujours un chargement complet de la zone. C'est une nouveauté avantageuse pour les entreprises qui disposent de plusieurs milliers d'enregistrements et dont le chargement peut être long.

## 3. Enregistrements manquants pour l'Active Directory

Il arrive parfois que des enregistrements propres à l'Active Directory ou un sous-domaine manquent. Pour recréer les enregistrements manquants, vous pouvez :

- les ajouter manuellement dans le contrôleur de domaine, ce qui est ni évident ni facile ;
- redémarrer le serveur afin que les enregistrements manquants s'inscrivent, cette solution n'est pas très efficace non plus ;
- utiliser la commande **net** pour redémarrer uniquement les services de l'Active Directory, c'est la méthode préférée, comme le montre les commandes suivantes :
  - net stop netlogin
  - net start netlogin

## 4. Zone principale en lecture uniquement

Il s'agit également d'une nouveauté de Windows Server 2008 qui permet d'utiliser des zones en lecture uniquement sur des contrôleurs de domaine. Pour cela, il faut que le serveur DNS soit sur le même serveur qu'un contrôleur de domaine en lecture seule (RODC). Cette solution permet de placer des serveurs DNS dans des zones sensibles tout

en limitant les risques de sécurité.

Il faut noter que seules les zones DNS incluses dans les partitions applicatives **partition de domaine**, **ForestDnsZones** et **DomainDNSZones** sont répliquées.

# Utilitaires en ligne de commande

## 1. L'utilitaire nslookup



L'utilitaire **nslookup** est utilisé pour isoler des problèmes provenant de la résolution de noms en adresses IP.

Prenons par exemple un utilisateur désirant se rendre sur le site Web [www.eni.fr](http://www.eni.fr). Pour rappel, une fois qu'il a tapé l'URL dans son navigateur, et si l'adresse IP correspondante ne se trouve pas dans le cache de l'ordinateur ou dans le fichier Hosts, alors l'ordinateur fait appel au serveur DNS pour la résolution ; celui-ci peut rechercher directement ou faire appel à un serveur de cache distant pour retrouver l'adresse IP. En résumé, les endroits où une erreur peut surgir sont nombreux. Il n'est pas évident de déterminer où se situe le problème, est-ce :

- un problème réseau entre l'ordinateur et le site Web ?
- un problème réseau entre l'ordinateur et le serveur DNS ?
- un problème d'inscription dans le serveur DNS ?
- un problème de cache DNS ?

L'utilitaire nslookup permet d'isoler les problèmes réseau entre l'ordinateur et le serveur DNS qui fait autorité, et un problème de cache DNS sur un serveur DNS servant de cache ou sur l'ordinateur local.

Avant d'utiliser nslookup, vous devez vous assurer qu'une connexion IP est possible entre l'adresse IP de l'ordinateur et l'adresse IP du serveur DNS.

Pour rechercher un hôte en utilisant un serveur DNS particulier

- Connectez-vous en tant qu'administrateur.
- Ouvrez une invite de commande avec les privilèges d'administration.
- Saisissez `nslookup www.eni.fr MonServeur DNS` puis [Entrée].

Pour démarrer nslookup en mode interactif

- Connectez-vous en tant qu'administrateur.
- Ouvrez une invite de commande avec les privilèges d'administration.
- Saisissez `nslookup` puis [Entrée]. Vous pouvez également indiquer le nom d'un serveur DNS.

Pour afficher l'aide

- Saisissez `help` puis [Entrée].

Pour résoudre un nom

- Saisissez `www.eni.fr` par exemple puis [Entrée].

Pour rechercher un serveur de messagerie

- Saisissez `set type=mx` puis [Entrée].

- Saisissez eni.fr par exemple puis [Entrée].

Pour afficher un maximum d'informations

- Saisissez set debug = true puis [Entrée].

## 2. L'utilitaire dnscmd



L'utilitaire **dnscmd** permet de gérer complètement un serveur DNS à l'aide d'une invite de commandes ou de scripts. Il est fortement recommandé de l'utiliser.

La syntaxe est la suivante :

```
Administrator : invite de commandes
C:\>dnscmd

Utilisation : DnsCmd <NonServeur> <Commande> [<Paramètres de commande>]

<NonServeur> :
  adresse IP ou nom d'hôte  -- serveur DNS distant ou local
  .                               -- serveur DNS sur ordinateur local

<Commande> :
  /Info                           -- Obtenir des informations du serveur
  /Config                         -- Réinitialiser la configuration du serveur ou de la zone
  /EnumZones                      -- Enumérer les zones
  /Statistics                      -- Interroger/effacer les données de statistiques du serveur
  /ClearCache                      -- Effacer le cache du serveur DNS
  /WriteBackFiles                 -- Réécrire tous les fichiers de données de zone ou d'indications de racine
  /StartScavenging                 -- Initie le nettoyage du serveur
  /IpValidate                      -- Valider les serveurs DNS distants
  /ResetListenAddresses           -- Définir la ou les adresses IP des serveurs en vue de traiter les demandes DNS
  /ResetForwarders                -- Définir les serveurs DNS en vue de transférer les requêtes récursives vers
  /ZoneAdd                         -- Afficher les informations de zone
  /ZoneDelete                      -- Supprimer une zone du serveur DNS ou du DS
  /ZoneAdd                         -- Créer une nouvelle zone sur le serveur DNS
  /ZonePause                        -- Suspender une zone
  /ZoneResume                       -- Reprendre une zone
  /ZoneReload                       -- Recharger la zone à partir de sa base de données (fichier ou DS)
  /ZoneWriteBack                   -- Réécrire la zone dans le fichier
  /ZoneRefresh                      -- Forcer l'actualisation de la zone secondaire à partir du serveur maître
  /ZoneUpdateFromDs               -- Mettre à jour une zone DS intégrée à l'aide de données issues de DS
  /ZonePrint                        -- Afficher tous les enregistrements de la zone
  /ZoneResetType                   -- Réinitialiser les informations secondaires ou de notification d'une zone
  /ZoneResetSecondaries            -- Réinitialiser les serveurs de nettoyage d'une zone
  /ZoneResetScavengingServers      -- Réinitialiser les serveurs maîtres de la zone secondaire
  /ZoneResetMasters                -- Réinitialiser les serveurs maîtres de la zone secondaire
  /ZoneExport                       -- Exporter une zone dans un fichier
  /ZoneChangeDirectoryPartition    -- Déplacer une zone vers une autre partition d'annuaire
  /EnumRecords                     -- Enumérer les enregistrements au niveau d'un nom
  /RecordAdd                        -- Créer un enregistrement dans la zone ou les indications de racine
  /RecordDelete                     -- Supprimer un enregistrement de la zone, des indications de racine ou du cache
  /ModeDelete                        -- Supprimer tous les enregistrements au niveau d'un nom
  /AgefullRecords                  -- Forcer le vieillissement sur le ou les nœuds de la zone
  /EnumDirectoryPartitions         -- Enumérer les partitions d'annuaire
  /DirectoryPartitionInfo          -- Obtenir des informations sur une partition d'annuaire
  /CreateDirectoryPartition        -- Créer une partition d'annuaire
  /DeleteDirectoryPartition        -- Supprimer une partition d'annuaire
  /EnlistDirectoryPartition       -- Ajouter un serveur DNS à l'étendue de réplication de la partition
  /UnenlistDirectoryPartition     -- Supprimer un serveur DNS de l'étendue de réplication
  /CreateBuiltInDirectoryPartitions -- Créer des partitions intégrées
  /ExportSettings                  -- Diriger les paramètres vers le fichier DnsSettings.txt dans le répertoire de base de données du serveur DNS

<Paramètres de commande> :
  DnsCmd <NonCommande> /? -- Pour des informations d'aide sur une commande spécifique
```

Voici quelques exemples d'utilisation de l'utilitaire dnscmd.

- Pour afficher les informations concernant le serveur DNS, saisissez dnscmd localhost /info par exemple puis [Entrée].
- Pour afficher les zones stockées sur le serveur DNS, saisissez dnscmd localhost /enumzones puis [Entrée].
- Pour ajouter une zone, saisissez dnscmd localhost /addzone MaZone.com /Primary /File mazone.dns par exemple puis [Entrée].
- Pour recharger une zone, saisissez dnscmd localhost /zonereload MaZone.com par exemple puis [Entrée].

## 3. Utilitaire dnslint



L'utilitaire **dnslint** est à télécharger à partir du site Web de Microsoft. Il peut créer des rapports au format HTML. Il peut être utilisé pour résoudre des problèmes liés à l'Active Directory comme la réPLICATION, mais également à un domaine particulier.

Il s'utilise aussi bien pour une entreprise que sur Internet.

La figure suivante montre le rapport d'interrogation d'une zone à l'aide de la commande `dnslint /ad 172.30.1.180 /s 172.30.1.180`.

## ***DNSLint Report***

System Date: Wed May 21 17:27:03 2008

Command run:

**`dnslint /ad 172.30.1.180 /s 172.30.1.180`**

Root of Active Directory Forest:

[artvinum.com](http://artvinum.com)

### **Active Directory Forest Replication GUIDs Found:**

DC: AD1

GUID: b56f650b-e239-4f89-913a-5ccf5ab96e1c

### **Total GUIDs found: 1**

The following 1 DNS servers were checked for records related to AD forest replication:

#### **DNS server: ad1.artvinum.com**

IP Address: 172.30.1.180

UDP port 53 responding to queries: YES

TCP port 53 responding to queries: Not tested

Answering authoritatively for domain: YES

#### **SOA record data from server:**

Authoritative name server: ad1.artvinum.com

Hostmaster: hostmaster.artvinum.com

Zone serial number: 12

Zone expires in: 1.00 day(s)

Refresh period: 900 seconds

Retry delay: 600 seconds

Default (minimum) TTL: 3600 seconds

#### **Additional authoritative (NS) records from server:**

ad1.artvinum.com 172.30.1.180

#### **Alias (CNAME) and glue (A) records for forest GUIDs from server:**

CNAME: b56f650b-e239-4f89-913a-5ccf5ab96e1c. msdcs.artvinum.com



# Rôle Serveur DNS sur un Server Core

## 1. Installer le rôle Serveur DNS



- Dans l'invite de commande, saisissez `start /w ocsetup DNS-Server-Core-Role` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que le serveur DHCP est bien installé puis appuyez sur [Entrée].

## 2. Désinstaller le rôle Serveur DNS



- Dans l'invite de commande, saisissez `start /w ocsetup DNS-Server-Core-Role /uninstall` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que le serveur DHCP est bien désinstallé puis appuyez sur [Entrée].

## 3. Gestion du serveur

Pour la gestion du serveur DNS, vous pouvez soit utiliser les commandes **dnscmd** en ayant pris soin de créer vos commandes à l'avance dans des scripts, soit le gérer à distance par l'intermédiaire de la console DNS.

# Gestion d'une zone

## 1. Création d'une zone de recherche directe



La création d'une zone de recherche directe permet de résoudre des noms en adresses IP. Une zone directe est requise à la création d'Active Directory. Elle peut être créée automatiquement en même temps que l'Active Directory.

- Microsoft recommande de créer une zone pour l'Active Directory qui utilise un nom interne différent du nom externe visible sur Internet. Vous verrez l'explication de cette recommandation plus loin dans ce chapitre.

La procédure manuelle est la suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur **Zones de recherche directes** puis cliquez sur **Nouvelle zone**.
- Sur la page **Bienvenue ! de l'Assistant Nouvelle zone**, cliquez sur **Suivant**.
- Sur la page **Type de zone**, sélectionnez l'option **Zone principale**. Si le serveur DNS est également un contrôleur de domaine, vous pouvez enregistrer la zone dans l'Active Directory en sélectionnant la case à cocher correspondante.

**Zone principale** permet de créer une zone DNS en lecture et écriture. La zone peut être stockée dans un fichier ou dans l'Active Directory.

**Zone secondaire** permet de créer une copie de la zone en lecture uniquement sur le serveur DNS. Il faut également configurer le transfert de zone correctement. La zone ne peut être stockée que dans un fichier.

**Zone de stub** permet de créer une zone en lecture qui ne contient que les enregistrements SOA, NS et les enregistrements A correspondant aux enregistrements des serveurs DNS hébergeurs de la zone (appelés aussi "glue A records"). Elle peut être stockée dans un fichier ou l'Active Directory.

La case à cocher **Enregistrer la zone dans Active Directory** permet de stocker la zone dans l'Active Directory au lieu d'un fichier. On parle alors de zone intégrée Active Directory.

- Si vous ajoutez une zone secondaire, il faut connaître l'adresse IP d'au moins un serveur maître à utiliser et les serveurs doivent autoriser les transferts de zone vers votre serveur. Une zone secondaire est toujours stockée dans un fichier et ne peut donc être intégrée dans l'Active Directory.

Cliquez sur **Suivant**.

- Si la page **Étendue de la zone de réPLICATION de Active Directory** apparaît, il faut indiquer la façon de stocker les informations dans l'Active Directory.

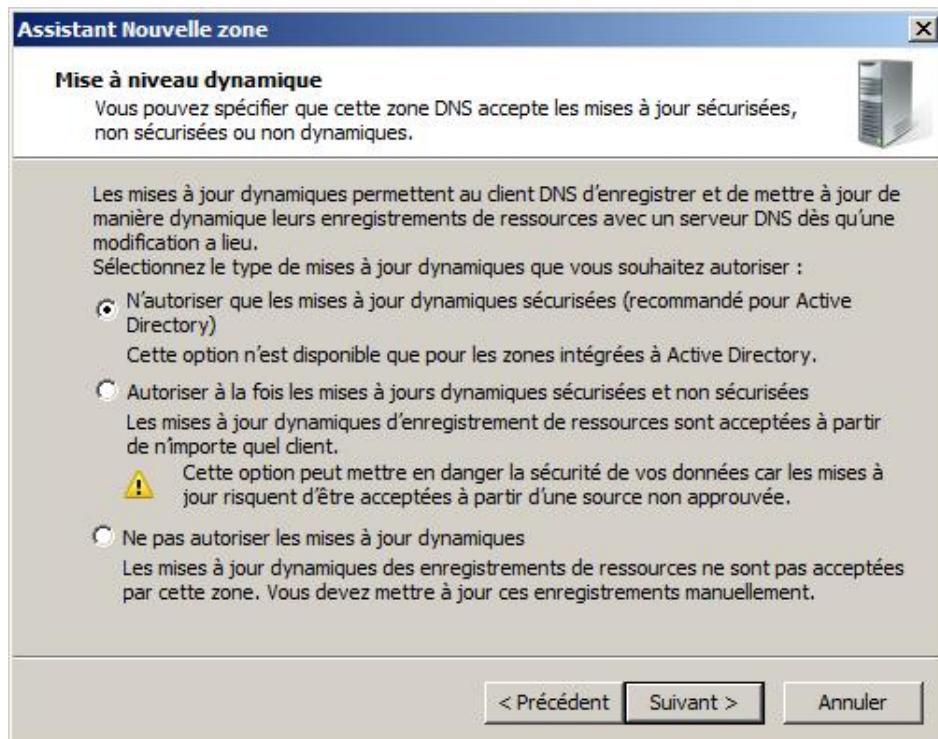
Les options proposées sont :

- **Vers tous les serveurs DNS de cette forêt** réplique la zone sur tous les serveurs contrôleurs de domaine étant également serveurs DNS de la forêt.
- **Vers tous les serveurs DNS de ce domaine** réplique la zone sur tous les serveurs contrôleurs de domaine étant également serveurs DNS du domaine. Il s'agit du paramètre par défaut.

- **Vers tous les contrôleurs de ce domaine** réplique la zone sur tous les contrôleurs de domaine du domaine. Ce paramètre doit être utilisé si vous disposez de contrôleurs de domaine Windows Server 2000 agissant en tant que serveurs DNS.
- **Dans la partition de domaine applicative** réplique la zone uniquement vers les serveurs qui font partie de l'étendue de réPLICATION de la zone applicative. Il faut au préalable créer une partition d'application.

Vous pouvez cliquer sur **Suivant**.

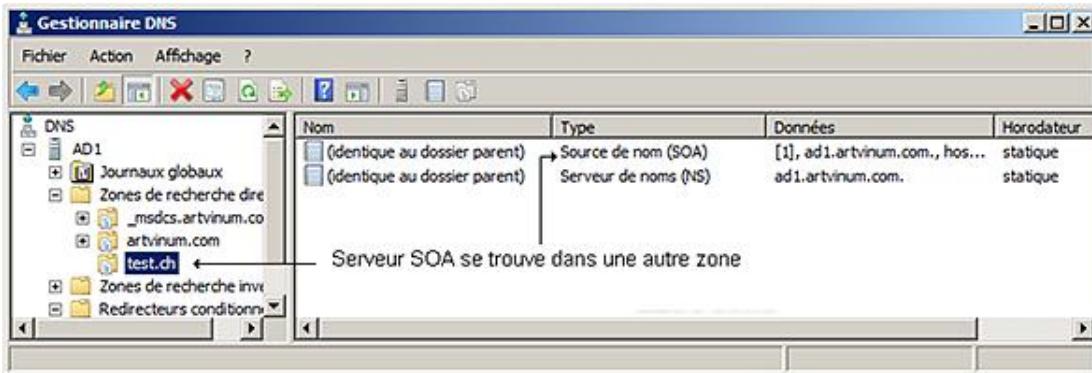
- Sur la page **Nom de la zone**, saisissez le nom DNS de la zone à créer, puis cliquez sur **Suivant**.
- Sur la page **Mise à niveau dynamique**, choisissez soit d'accepter les mises à jour dynamiques des enregistrements DNS, soit de les interdire. Les mises à jour dynamiques sécurisées ne sont disponibles qu'avec des zones intégrées à Active Directory.



Si votre serveur DNS héberge une zone utilisée par Active Directory, il est conseillé d'autoriser les mises à jour dynamiques. Il est même conseillé que le serveur DNS soit également un serveur contrôleur de domaine afin de bénéficier de la sécurité induite par l'Active Directory. L'option **Ne pas autoriser les mises à jour dynamiques** est à utiliser dans une zone périphérique (DMZ) ou directement sur Internet.

- Sur la page **Fin de l'Assistant Nouvelle zone**, vérifiez vos informations puis cliquez sur **Terminer**. La nouvelle zone apparaît dans le volet gauche.

L'écran suivant montre le résultat d'une création de zone ; remarquez que seuls les enregistrements SOA et NS ont été créés et que le serveur DNS se trouve dans une autre zone.



## 2. Création d'une zone de recherche inversée



La création d'une zone de recherche inversée permet de résoudre des adresses IP en noms. Une zone de recherche inversée n'est pas requise pour créer une Active Directory mais elle est conseillée. Elle n'est pas créée automatiquement lors de la création de l'Active Directory. Il vous faut créer autant de zones de recherche inversée que vous avez de sous-réseaux (un octet égale un domaine). La procédure est la suivante :

- Sur Internet, prévoyez au moins une zone de recherche inversée pour vos serveurs de messagerie SMTP.
  
- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur **Zones de recherche inversée** puis cliquez sur **Nouvelle zone**.
- Sur la page **Bienvenue !** de l'**Assistant Nouvelle zone**, cliquez sur **Suivant**.
- Sur la page **Type de zone**, sélectionnez l'option **Zone principale**. Si le serveur DNS est également un contrôleur de domaine, vous pouvez enregistrer la zone dans l'Active Directory en sélectionnant la case à cocher correspondante. Cliquez sur **Suivant**.
- Si la page **Étendue de la zone de réPLICATION de Active Directory** apparaît, il faut indiquer la façon de stocker les informations dans l'Active Directory, puis vous pouvez cliquer sur **Suivant**.
- Sur la page **Nom de la zone de recherche inversée**, sélectionnez le type d'adressage IPv4 ou IPv6, puis cliquez sur **Suivant**. La nouvelle page porte le même nom dans les deux cas mais vous devez saisir l'**ID réseau** ou le **Nom de la zone de recherche inversée** en IPv4, alors qu'en IPv6 vous saisissez uniquement le préfixe d'adresse du réseau (il est possible d'associer jusqu'à 8 zones par préfixe). L'écran suivant montre un **ID réseau IPv4**, remarquez que le nom de la zone est renseigné automatiquement et est grisé.

Pour identifier la zone de recherche inversée, entrez l'ID réseau ou le nom de la zone.

ID réseau :  
172 .30 .1 .

L'ID réseau est la partie des adresses IP qui appartient à cette zone. Entrez l'ID réseau dans son ordre normal (non inversé).

Si vous utilisez un zéro dans l'ID réseau, il va apparaître dans le nom de la zone. Par exemple, l'ID réseau 10 crée la zone 10.in-addr.arpa, l'ID réseau 10.0 crée la zone 0.10.in-addr.arpa.

Nom de la zone de recherche inversée :  
1.30.172.in-addr.arpa

- Sur la page **Mise à niveau dynamique**, choisissez d'accepter les mises à jour dynamiques des enregistrements DNS ou de les interdire. Les mises à jour dynamiques sécurisées ne sont disponibles qu'avec des zones intégrées Active Directory.
- Sur la page **Fin** de l'**Assistant Nouvelle zone**, vérifiez vos informations puis cliquez sur **Terminer**. La nouvelle zone apparaît dans le volet gauche.

### 3. Gestion de la source de noms SOA

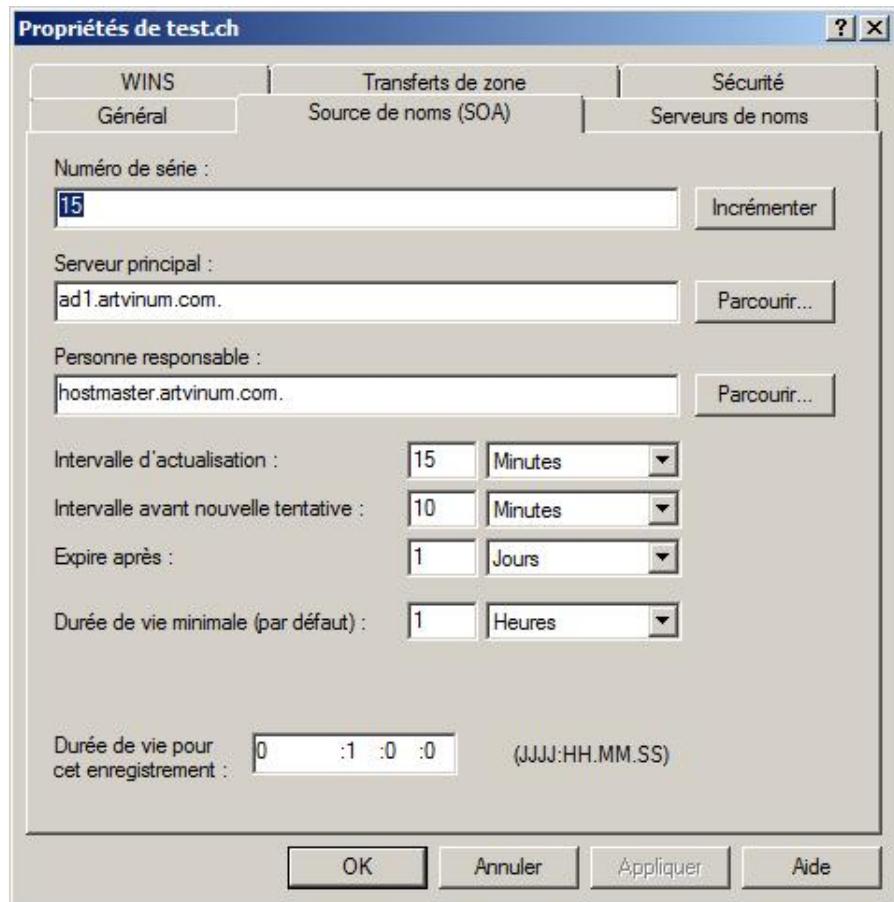


Win2

La source de noms permet de configurer plusieurs paramètres importants pour la zone. Microsoft définit ces paramètres par défaut mais il peut être utile de les modifier pour qu'ils correspondent à vos besoins.

La procédure est la suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** ou **Zones de recherche inversée** pour faire apparaître la zone considérée.
- Cliquez sur la zone pour développer le nœud.
- Cliquez avec le bouton droit de la souris sur la zone puis sur **Propriétés**.
- Cliquez sur l'onglet **Source de noms (SOA)** de la boîte de dialogue **Propriétés**.



Le **Numéro de série** correspond aux nombres de modifications qui ont été effectuées sur le serveur DNS ; ce numéro de série est utilisé pour le transfert de zone afin de transférer les enregistrements de manière incrémentielle. En cas de conflit, c'est-à-dire si deux serveurs ont le même numéro de série mais pas les mêmes informations, vous pouvez cliquer sur **Incrémenter** afin de forcer le processus de réPLICATION.

Le **Serveur principal** affiche le premier serveur de la zone, c'est lui qui fait autorité. En cliquant sur **Parcourir**, vous pouvez modifier le serveur.

L'option **Personne responsable** correspond à une adresse e-mail pour l'administrateur de la zone. Ce paramètre est malheureusement rarement correctement renseigné. Remarquez que l'arobase (@) est remplacé par un point (.). @ est un caractère spécial, il faut utiliser un enregistrement de type RNAME (cf. RFC 2142).

Les paramètres suivants sont utilisés comme valeurs d'expiration pour les zones secondaires :

- L'**Intervalle d'actualisation** est l'intervalle de temps pendant lequel un serveur d'une zone secondaire attend avant de contacter sa source pour remettre à jour sa zone si nécessaire.
- L'**Intervalle avant nouvelle tentative** correspond au temps d'attente avant de recontacter le serveur source s'il n'a pu être contacté lors de l'intervalle de réactualisation. Le serveur retentera de contacter le serveur source jusqu'à l'expiration.

L'option **Exire après** définit la durée maximum pendant laquelle le serveur peut répondre aux requêtes sans avoir pu contacter le serveur source.

La **Durée de vie minimale** correspond à la valeur TTL de tout enregistrement de la zone. En d'autres termes, les serveurs de cache utiliseront la valeur du TTL pour stocker temporairement l'enregistrement. Il est également possible de gérer le TTL pour chaque enregistrement en modifiant les propriétés de ce dernier.

Si vous prévoyez de modifier l'adresse IP d'un serveur, que ce soit sur Internet ou dans votre entreprise, afin d'éviter que des clients ne reçoivent une adresse IP incorrecte, diminuez temporairement la valeur du TTL à quelques secondes et ne modifiez les adresses qu'au moment où l'ancien TTL a expiré.

La **Durée de vie pour cet enregistrement** correspond au TTL de l'enregistrement du SOA.

- Cliquez sur **OK** pour mettre fin à la procédure.

## 4. Création d'un sous-domaine



Afin d'organiser les enregistrements au sein d'une zone, il est possible de créer une structure hiérarchique en créant des sous-domaines qui sont des sortes de dossiers si l'on fait une analogie avec le système de fichiers. Chaque sous-domaine peut contenir des enregistrements ou d'autres sous-domaines.

La procédure pour créer un sous-domaine est la suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** pour faire apparaître les zones. Recommencez l'opération jusqu'au niveau du domaine/sous-domaine considéré.
- Cliquez avec le bouton droit de la souris sur le domaine/sous-domaine puis sur **Nouveau domaine**.
- Dans la boîte de dialogue **Nouveau domaine DNS**, saisissez uniquement le nom du domaine et pas son FQDN, puis cliquez sur **OK**. Le sous-domaine apparaît sous le domaine principal.

## 5. Création d'une zone déléguée



On utilise la délégation de zone afin de scinder une zone sur laquelle on a autorité en parties plus petites afin d'améliorer les performances, voire diminuer le trafic de réPLICATION. Pour cela, il faut utiliser la délégation de l'autorité pour ce domaine vers un autre serveur DNS.

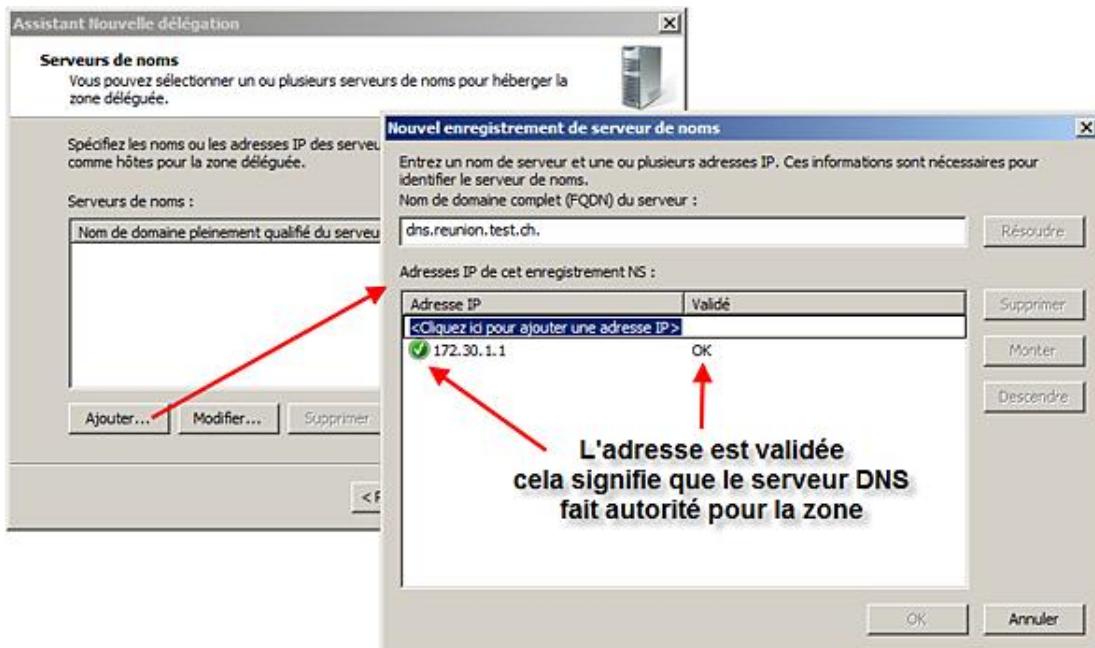
Par exemple, la société PFFC dispose d'une branche située à La Réunion. Le nom de domaine choisi est pffc.ch et pour diminuer les problèmes de transfert dus à la réPLICATION DNS de la zone pffc.ch, il a été décidé de créer un domaine appelé reunion dont le FQDN est test.ch et de déléguer l'autorité de ce domaine à un serveur DNS situé à La Réunion. Il n'y a donc pas de réPLICATION de zone DNS entre les deux serveurs DNS. De cette façon, les clients situés des deux côtés peuvent effectuer des interrogations en limitant le trafic.

La procédure pour créer une zone déléguée est la suivante.

Afin de bien comprendre la procédure, il faut avoir créé une zone ( primaire ou intégrée à AD) sur le serveur délégué qui est Core1 puis effectuer la procédure ci-dessous sur Win2 appelé également serveur local.

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** pour faire apparaître les zones. Recommencez l'opération jusqu'au niveau supérieur du domaine/sous-domaine considéré.
- Cliquez avec le bouton droit de la souris sur le niveau parent du domaine/sous-domaine puis cliquez sur **Nouvelle délégation**. Le domaine délégué n'a pas besoin d'être créé au préalable sur le serveur DNS local mais il est nécessaire que la zone existe sur le serveur DNS délégué.
- Sur la page **Bienvenue !** de l'assistant, cliquez sur **Suivant**.
- Sur la page **Nom du domaine délégué**, entrez le nom du domaine dont vous voulez déléguer l'autorité, puis cliquez sur **Suivant**.

- Sur la page **Serveurs de noms**, cliquez sur **Ajouter** afin d'ajouter le serveur DNS qui fera autorité pour la zone comme le montre l'image suivante, puis cliquez sur **Suivant**.



- Le serveur DNS distant doit déjà contenir la zone déléguée.

- Sur la page **L'Assistant Nouvelle délégation est terminé**, cliquez sur **Terminer**. La zone est déléguée et elle apparaît comme un domaine mais la couleur de l'icône correspondante dans l'arborescence est grise. La zone déléguée ne contient que l'adresse du serveur DNS faisant autorité.

## 6. Gestion des enregistrements

Un enregistrement représente un hôte ou un service d'un hôte se situant dans la zone. Les ordinateurs peuvent s'inscrire dynamiquement, par l'intermédiaire d'un serveur DHCP, ou manuellement grâce à un administrateur.

- Utilisez la commande **ipconfig /registerdns** pour réinscrire un enregistrement dans le serveur DNS s'il accepte les mises à jour dynamiques.

Les enregistrements principaux sont :

- A** ou hôte, pour résoudre un nom d'hôte en adresse IPv4.
- AAAA** ou hôte, pour résoudre un nom d'hôte en adresse IPv6.
- CNAME** ou alias permet d'associer un nom supplémentaire à un nom d'hôte.
- MX** ou serveur de messagerie, pour afficher le(s) serveur(s) SMTP d'un nom de domaine.
- NS** ou serveur de nom définit un serveur DNS.
- PTR** ou pointeur, pour résoudre une adresse IP en nom d'hôte.
- SOA** ou Start of Authority définit le serveur DNS maître pour la zone.
- SRV** ou emplacement de service, permet d'associer un service spécifique à un hôte. Il faut également une

application cliente réseau prévue spécialement pour tirer parti des enregistrements de services. Le client Active Directory représente le meilleur exemple possible.



La procédure pour créer un enregistrement est la suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** ou **Zones de recherche inversée** pour faire apparaître les zones. Recommencez l'opération jusqu'au niveau du domaine/sous-domaine considéré.
- Cliquez avec le bouton droit de la souris sur le domaine/sous-domaine puis cliquez sur **Nouvel hôte (A ou AAAA)** ou **Nouvel alias (CNAME)** ou **Nouveau serveur de messagerie (MX)** ou **Nouveau pointeur (PTR)** ou **Nouveaux enregistrements**.

Les pages suivantes montrent comment configurer les enregistrements les plus importants.

#### a. Enregistrement d'hôte A ou AAAA et pointeur PTR

Saisissez au minimum le **Nom** et l'**Adresse IP**. Laissez la sélection pour la création du pointeur PTR.

La case à cocher **Autoriser tout utilisateur identifié à mettre à jour les enregistrements DNS avec le même nom propriétaire** ne s'affiche que lorsque la zone est intégrée à l'Active Directory et permet à un administrateur d'enregistrer un nom hôte dans le serveur DNS au nom de ce dernier même si l'hôte est hors ligne.

Pour l'enregistrement pointeur ou PTR, les champs **Adresse IP** et **Nom** sont inversés.

#### b. Enregistrement d'alias ou CNAME

Il faut saisir le **Nom de l'alias** et le nom de l'hôte qui doit être associé. Vous pouvez utiliser le bouton **Parcourir** pour le rechercher.

#### c. Nouveau serveur de messagerie MX

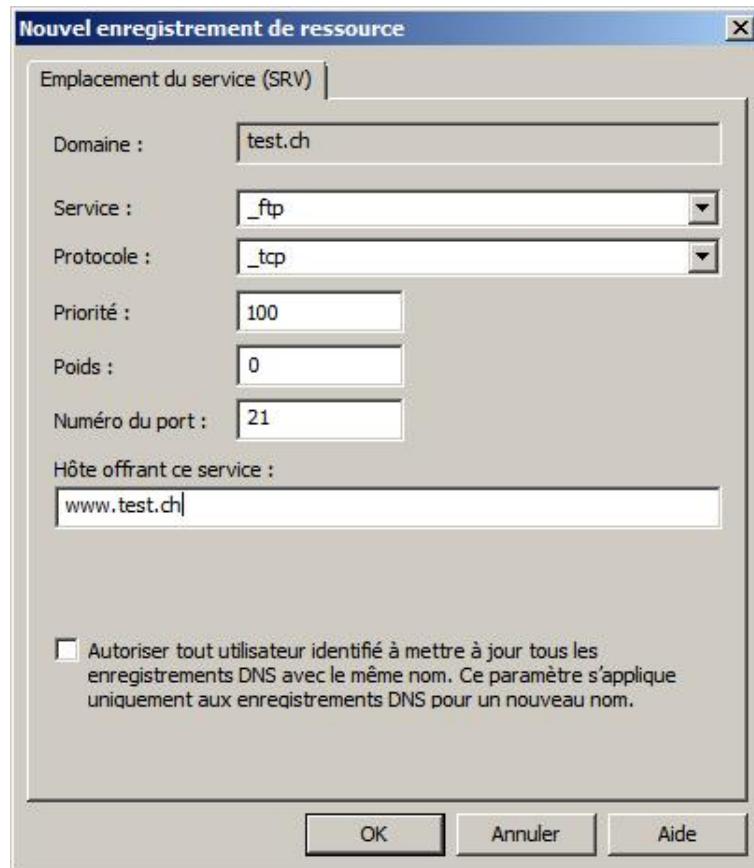
A screenshot of a Windows dialog box titled "Serveur de messagerie (MX)".

- Hôte ou domaine enfant :** An empty text input field.
- Par défaut, DNS utilise le nom de domaine parent lors de la création d'un enregistrement de courrier Exchange. Vous pouvez spécifier un nom d'hôte ou d'enfant mais dans la plupart des déploiements, le champ ci-dessus est conservé vide.** A descriptive text note.
- Nom de domaine pleinement qualifié (FQDN) :** A text input field containing "test.ch."
- Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie :** A text input field containing "a.test.ch" with a "Parcourir..." button to its right.
- Priorité du serveur de messagerie :** A text input field containing "10".

Généralement, il faut laisser vide le champ **Hôte ou domaine enfant**. Ajoutez simplement le nom du serveur de messagerie dans le champ **Nom de domaine pleinement qualifié (FQDN) pour le serveur de messagerie** ainsi qu'une valeur pour la **Priorité du serveur de messagerie**.

Cette priorité est utile lorsqu'il existe plusieurs serveurs de messagerie afin de définir l'ordre de priorité pour tenter de remettre le courrier. Si un serveur SMTP distant ne peut joindre et remettre le message au serveur ayant la priorité la plus faible, il tentera de contacter le suivant dans la liste. En cas d'égalité de priorité, le choix est aléatoire. Les valeurs acceptables vont de 0 à 65535.

#### d. Emplacement de services SRV



Le **Service** peut être un service existant ou un nom que vous ajoutez.

Il faut indiquer le **Protocole** supporté par le service, UDP ou TCP, mais également un protocole personnalisé.

Les services de l'Active Directory utilisent les enregistrements de service pour trouver par exemple les serveurs catalogue globaux ou les serveurs LDP dans une zone.

Concernant la **Priorité**, vous pouvez y placer une valeur allant de 0 à 65535, la valeur la plus élevée correspondant à la priorité la plus forte. Cette valeur est utilisée pour donner un avantage à un serveur plutôt qu'à un autre si le service existe sur plusieurs serveurs.

Le **Poids**, dont la valeur peut aller de 1 à 65535, met en place un mécanisme d'équilibrage de la charge. Sauf dans certaines implémentations, il est conseillé de laisser la valeur à 0 qui signifie ne pas utiliser un mécanisme d'équilibrage de la charge.

Le **Numéro de port** correspond au numéro de port utilisé pour le service.

Enfin, indiquez l'hôte, soit le serveur qui offre le service.

- 
- Vous trouvez les enregistrements SRV d'un DC dans le répertoire %systemroot%\system32\config\NetLogon.dns. Ces enregistrements sont automatiquement créés au démarrage de Netlogon.
- 

#### e. Enregistrement d'alias de domaine DNAME

L'enregistrement DNAME est une nouveauté dans Windows 2008, basée sur la RFC2672. Bien que similaire à un enregistrement CNAME qui permet de créer des alias pour un nœud dans l'espace de nom, DNAME permet de mapper une arborescence d'un espace de nom DNS sous un autre domaine. Vous pouvez l'utiliser pour une migration en douceur d'un espace de nom comme peut l'illustrer l'exemple suivant :

Avec l'invite de commande, vous allez créer deux domaines et un enregistrement dans le domaine qui doit avoir un alias. Puis vous allez créer l'alias et voir le résultat avec l'utilitaire **nslookup**.

Création du domaine à migrer :

```
dnscmd /zoneadd MonVieuxDomaine.local /primary
```

Création d'un enregistrement dans ce domaine :

```
dnscmd /recordadd MonvieuxDomaine.local www A 192.168.6.1
```

Création du nouveau nom pour le domaine :

```
dnscmd /zoneadd MonNouveauDomaine.local /primary
```

Création d'un enregistrement DNAME :

```
dnscmd /recordadd MonNouveauDomaine.local @ DNAME MonVieuxDomaine
```

Test avec nslookup :

```
nslookup www.MonNouveauDomaine.local  
nslookup www.MonVieuxDomaine.local
```

➤ L'enregistrement DNAME n'est configurable que via l'invite de commande **dnscmd**. Il faut noter que le domaine d'alias doit être créé sur le serveur DNS et ne peut contenir d'enregistrements lors de la création de l'enregistrement DNAME.

## 7. Déplacement du stockage



Le serveur DNS peut stocker les enregistrements DNS soit dans un fichier placé dans %systemroot%\system32\dns, soit dans l'Active Directory.

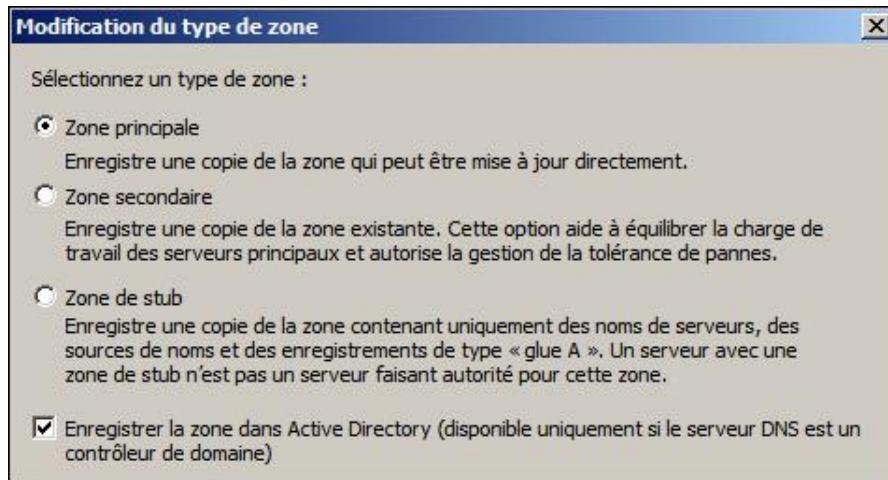
Pour des raisons de sécurité, que ce soit au niveau du stockage, du transfert de zone ou de la mise à jour dynamique des enregistrements, il est préférable de stocker les zones dans l'Active Directory.

➤ Windows Server 2008 répond aux demandes des requêtes DNS pendant le chargement de la zone si l'enregistrement est déjà chargé.

Vous pouvez à tout moment modifier le type de stockage ou l'emplacement en utilisant la procédure suivante :

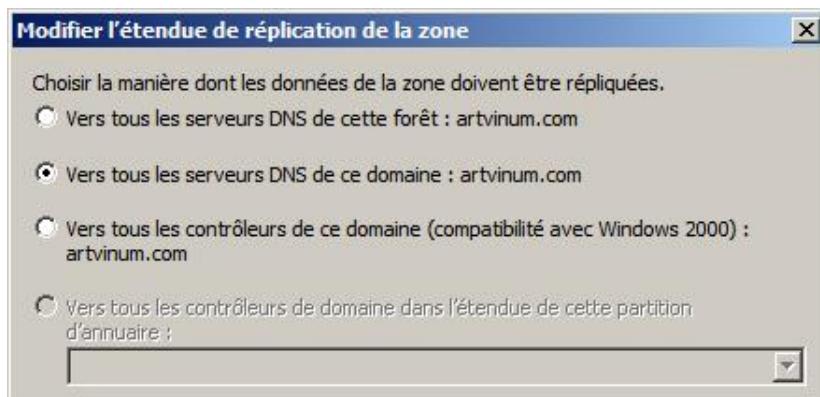
- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** ou **Zones de recherche inversée** pour faire apparaître la zone considérée.
- Cliquez sur la zone pour développer le nœud.
- Cliquez avec le bouton droit de la souris sur la zone puis sur **Propriétés**.
- Cliquez sur l'onglet **Général** de la boîte de dialogue **Propriétés**.

La zone **Type** indique s'il s'agit d'une zone intégrée à Active Directory. Vous pouvez modifier le type de zone à tout moment en cliquant sur le bouton correspondant comme le montre l'image suivante :



Ces options sont expliquées dans la section Gestion d'une zone - Crédation d'une zone de recherche directe de ce chapitre.

Le bouton **RéPLICATION** n'est activé que pour une zone intégrée Active Directory. Il permet de définir la manière dont la zone est répliquée vers les autres contrôleurs de domaine.



Reportez-vous à la section Gestion d'une zone - Crédation d'une zone de recherche directe de ce chapitre pour plus d'informations sur ces options.

La liste déroulante **Mises à jour dynamiques** permet de définir si la zone accepte les mises à jour des enregistrements de manière dynamique, voire sécurisée, c'est-à-dire qu'un contrôle des ACLs (Access Control List) de l'Active Directory est effectué pour savoir si la mise à jour est permise.

## 8. RéPLICATION des zones du serveur DNS



Selon que la zone est intégrée à l'Active Directory ou non, le transfert de zone ne fonctionne pas de la même manière.

Le transfert d'une zone intégrée à l'Active Directory utilise la réPLICATION de l'Active Directory et requiert que chaque serveur DNS soit également un contrôleur de domaine. Les contrôleurs de domaine qui reçoivent une copie de la zone sont définis dans la modification de l'étendue de réPLICATION comme étudié dans la section précédente.

La latence est basée sur l'intervalle de réPLICATION de l'Active Directory. C'est la méthode la plus sécurisée pour transférer des enregistrements entre serveurs DNS.

Si le stockage de la zone se fait dans un fichier, alors il faut configurer le transfert de zone ; plusieurs cas peuvent se présenter mais ils utilisent tous la notion de zone secondaire et de serveur maître.

Dès qu'un serveur héberge une zone secondaire, il doit se synchroniser auprès d'un serveur maître, celui-ci pouvant héberger la zone en tant que zone principale, zone intégrée Active Directory ou même zone secondaire. Sur le serveur Maître, il est donc requis d'autoriser le transfert de zone.

Il est nécessaire de planifier correctement le transfert de zone et de choisir judicieusement les serveurs maîtres afin

de diminuer le temps de convergence des zones.

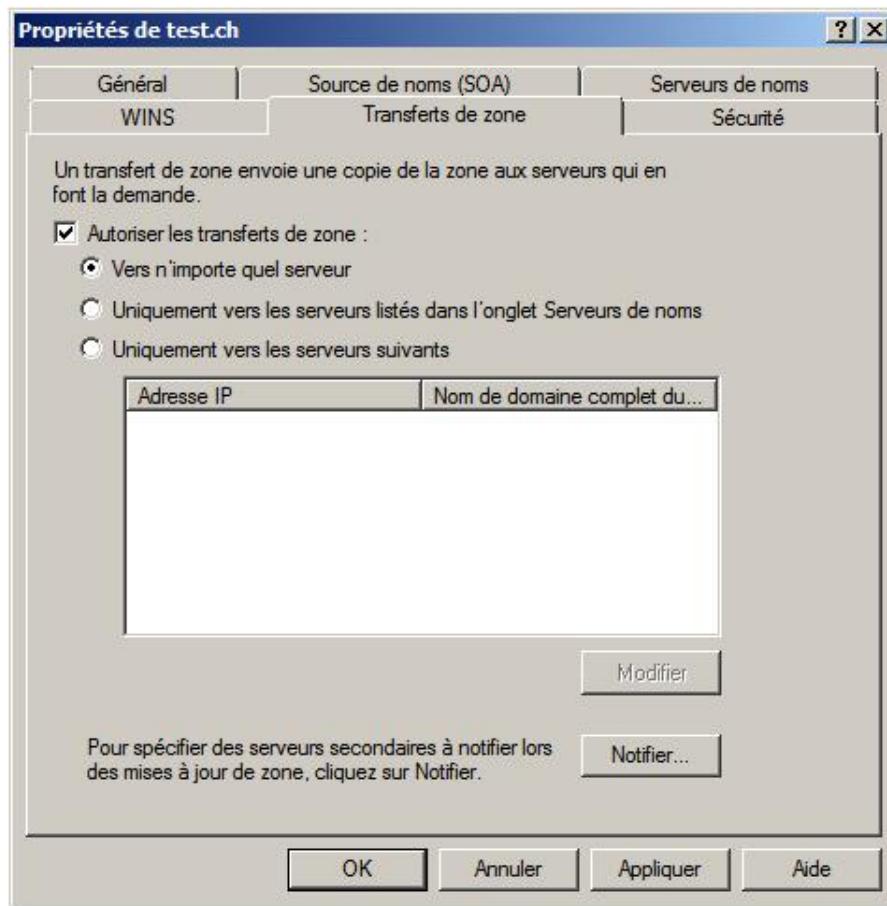
- 
- Il est préférable d'utiliser uniquement des zones intégrées à Active Directory et d'éviter autant que possible l'utilisation de zones secondaires.
- 

Au préalable, il faut autoriser le transfert de zone en suivant cette procédure. Pour effectuer un exercice complet, vous allez créer une zone secondaire sur le serveur Win2 dont le nom correspond au domaine et utiliser le Server Core1 en tant que maître.

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** ou **Zones de recherche inversée** pour faire apparaître la zone considérée.
- Cliquez sur la zone pour développer le nœud.
- Cliquez avec le bouton droit de la souris sur la zone puis sur **Propriétés**.
- Cliquez sur l'onglet **Transferts de zone** de la boîte de dialogue **Propriétés**.

La case à cocher **Autoriser les transferts de zone** doit être cochée. Ensuite vous devez déterminer la méthode :

- **Vers n'importe quel serveur** est la méthode la moins sécurisée car toutes les demandes de synchronisation sont acceptées, cette méthode est déconseillée.
- **Uniquement vers les serveurs suivants**, soit ceux définis dans la liste ci-dessous. Cette option est plus restrictive que la suivante.
- **Uniquement vers les serveurs listés dans l'onglet Serveurs de noms** est une méthode plus sécurisée car le transfert ne sera permis que vers les serveurs de noms définis pour la zone comme le montre l'image suivante.



Le bouton **Modifier** permet de gérer les adresses IP des serveurs qui peuvent demander une synchronisation avec la zone.

Le bouton **Notifier** permet d'avertir les serveurs de noms des mises à jour de la zone. Vous pouvez avertir tous les serveurs listés dans l'onglet **Serveurs de noms** ou dans une liste de serveurs que vous entrez manuellement.

Vous pouvez ajouter des serveurs de noms pour la zone, que ce soient des serveurs DNS Microsoft ou autres.

Sur le serveur qui héberge la zone secondaire contrôlez que la réPLICATION s'effectue correctement.

- 
- La commande **Transfert à partir du maître** signifie que le serveur DNS contacte le serveur maître pour se synchroniser. Le transfert est incrémentiel et utilise le protocole IXFR et non un transfert complet AXFR. La commande **Rechargement à partir du maître** est identique à la précédente exceptée que la zone est d'abord vidée avant le transfert. La commande **Changer à Nouveau** change la zone à partir de la copie fichier ou de l'Active Directory.
- 

## 9. WINS

L'autre méthode pour résoudre des noms en adresses IP se base sur le protocole NetBIOS qui utilise un serveur WINS à la place d'un serveur DNS. Bien que ce protocole ne soit plus nécessaire avec Windows Server 2008, il est encore largement répandu dans les entreprises.

Les deux protocoles peuvent coexister, néanmoins si le nom ne peut être résolu, le client fait appel dans ce cas à la résolution basée sur NetBIOS et cela prend du temps. Si un serveur WINS existe, il peut être intéressant de l'associer à une zone de recherche directe ou inversée. Dans ce cas, si le serveur DNS ne peut résoudre le nom dans la zone considérée, il fait appel aux serveurs WINS définis pour tenter de résoudre le nom.

- 
- Le scénario le plus commun est de désactiver la résolution de noms NetBIOS pour les ordinateurs fonctionnant sous Windows Vista, voire Windows XP et de permettre une recherche via un serveur WINS par l'intermédiaire du serveur DNS.
- 

Un problème récurrent dans la résolution de noms vient du fait que les enregistrements de type WINS ne comportent que le nom de l'ordinateur et pas un FQDN complet. Si un utilisateur tente de se connecter sur un ordinateur en tapant `http://zeus` sans rajouter le suffixe, le client ajoute automatiquement son suffixe principal puis passe la

requête auprès du serveur DNS qui recherche dans la zone en question. S'il ne trouve pas l'enregistrement et qu'une recherche auprès d'un serveur WINS est configurée, le serveur DNS interroge le serveur WINS. En cas de non réponse, d'autres suffixes peuvent être utilisés s'ils ont été configurés pour être utilisés dans la résolution.

Cette méthode est inefficace et peut demander un délai relativement long pour obtenir une réponse. Windows Server 2008 introduit la notion de zone globale DNS. Cette zone permet de définir des enregistrements statiques sans extension. Ensuite, ils sont mappés en utilisant un alias (CNAME) vers un enregistrement d'hôte ou d'alias dans une des zones sur laquelle on a autorité.

Bien entendu, à chaque demande non résolue dans la zone, le serveur DNS recherche dans la zone globale si un enregistrement correspondant existe.

En plus de réduire le temps de recherche et de simplifier la configuration, la zone globale permet de rendre inutile l'utilisation d'un serveur WINS et de ne pas modifier la façon de travailler des ordinateurs clients. Les ordinateurs fonctionnant uniquement sous IPv6 peuvent également résoudre des noms sans suffixe.

- Bien que Microsoft propose la zone globale comme une alternative au serveur WINS, elle peut être envisagée comme un emplacement pour y placer des noms communs pour des serveurs dont le nom réel serait complexe, que ce soit dans une Active Directory mono ou multidomaines, voire multiforêts.

## a. Désactiver la résolution NetBIOS



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer** puis saisissez **control ncpa.cpl** dans la zone de saisie **Rechercher** et appuyez sur [Entrée].
- Cliquez avec le bouton droit de la souris sur l'interface désirée puis cliquez sur **Propriétés**.
- Double cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
- Dans la boîte de dialogue **Propriétés de protocole Internet version 4 (TCP/IPv4)**, cliquez sur **Avancé**.
- Dans la boîte de dialogue **Paramètres TCP/IP avancés**, cliquez sur l'onglet **WINS**.
- Dans l'onglet **WINS**, désactivez la case à cocher **Activer la recherche LMHOSTS** et cliquez sur l'option **Désactiver NetBIOS sur TCP/IP**.
- Cliquez trois fois sur **OK**.

- Vous pouvez également utiliser les stratégies de groupe pour désactiver la résolution NetBIOS, c'est même la méthode préférée.

- La commande **nbtstat** permet de gérer les enregistrements dans le cache NetBIOS.

## b. Configurer un serveur DNS pour utiliser la résolution WINS



Si vous devez installer un serveur WINS, il est placé en tant que fonctionnalité et non en tant que rôle.

- Connectez-vous en tant qu'administrateur.

- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez sur le nœud **Zones de recherche directes** ou **Zones de recherche inversée** pour faire apparaître la zone considérée.
- Cliquez sur la zone pour développer le nœud.
- Cliquez avec le bouton droit de la souris sur la zone puis sur **Propriétés**.
- Cliquez sur l'onglet **WINS** ou **WINS-R** de la boîte de dialogue **Propriétés**.

 Cet onglet n'est pas disponible pour des zones de Stub.

Pour activer la recherche également vers un serveur DNS, cochez la case **Utiliser la recherche directe WINS**.

Si d'autres serveurs DNS gérant la zone ne reconnaissent pas les enregistrements de type WINS, comme certains serveurs DNS non Microsoft et en particulier les serveurs BIND/Unix, il peut y avoir des problèmes lors du transfert de zone ; pour éviter ces problèmes, il est conseillé de cocher la case **Ne pas répliquer cet enregistrement**.

Sous **Adresse IP**, ajoutez les adresses des serveurs WINS.

En cliquant sur le bouton **Avancé**, vous configurez le **Délai d'expiration du cache**, c'est-à-dire le TTL de l'enregistrement retourné par le serveur WINS et le **Délai d'expiration de la recherche**, c'est-à-dire le délai avant que le serveur ne retourne une réponse de type "Nom introuvable".

 Un serveur WINS n'est utilisable que pour des adresses IPv4.

### c. Créer et configurer une zone globale DNS



Cette procédure montre comment créer la zone, la configurer avec un enregistrement et ce qu'il se passe lorsque le client effectue une demande de résolution du nom.

- Connectez-vous en tant qu'administrateur.
- Ouvrez une invite de commande avec les priviléges d'administration.
- Saisissez la commande suivante : `dnscmd NomDuServeur /config /enableglobalnamessupport 1` puis appuyez sur [Entrée].

**NomDuServeur** est un serveur DNS Windows Server 2008 qui est contrôleur de domaine.

- Pour créer la zone, vous pouvez passer par l'interface graphique mais également saisir la commande suivante : `dnscmd NomDuServeur /ZoneAdd GlobalNames /DsPrimary /DP /forest` puis appuyer sur [Entrée]. La zone **GlobalNames** est créée sur le serveur.

 La zone créée est intégrée à l'Active Directory, elle n'accepte pas les mises à jour dynamiques et est répliquée sur tous les serveurs DNS de la forêt.

- Ajoutez un enregistrement de type CNAME dans la zone globale. Pour le test, vous allez ajouter l'enregistrement Web comme le montre la figure suivante. À partir de l'invite de commande, saisissez `dnscmd /RecordAdd GlobalNames web CNAME www.test.ch` puis appuyez sur [Entrée].



L'enregistrement associé est stocké dans une zone sur laquelle on a autorité. Chaque enregistrement doit être enregistré manuellement.



L'ordinateur client n'a pas besoin d'être configuré. Il lui suffit de faire partie du domaine considéré. Car si vous saisissez ping web sur l'ordinateur client, il va automatiquement rajouter un suffixe pour l'enregistrement.

Dans notre cas, c'est la requête web.artvinum.com qui est passée au serveur DNS. Le serveur DNS ne trouve pas l'enregistrement dans la zone artvinum.com mais comme il existe une zone appelée **GlobalDNS**, il regarde dans cette zone avant d'essayer éventuellement d'autres suffixes. Dans la zone **GlobalDNS**, l'enregistrement est trouvé, donc le serveur DNS répond à la requête en indiquant le nom réel du serveur, ici ordi.test.ch et son adresse IP. Les figures suivantes montrent la capture des paquets réseau pour la requête DNS.

Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description
9	3.114478		222.73.27.23	172.30.1.104	UDP	UDP: SrcPort = 4512, DstPort = 2035, Length = 71
10	3.164950		172.30.1.170	172.30.1.180	ARP	ARP: Request, 172.30.1.170 asks for 172.30.1.180
11	3.174564		172.30.1.180	172.30.1.170	ARP	ARP: Response, 172.30.1.180 at 00-03-FF-CE-6ACF
12	3.193933		172.30.1.170	172.30.1.180	CIFS	DNS: QueryId = 0x15EA, QUERY (Standard query), Query for web.artvinum.com of type Host Addr on class Internet
13	3.254680		172.30.1.180	172.30.1.170	ARP	ARP: Request, 172.30.1.180 asks for 172.30.1.170
14	3.264694		172.30.1.170	172.30.1.180	ARP	ARP: Response, 172.30.1.170 at 00-03-FF-C56ACF
15	3.264694		172.30.1.180	172.30.1.180	DNS	DNS: QueryId = 0x15EA, QUERY (Standard query), Response - Success
16	3.274708		172.30.1.170	172.30.1.180	CIFS	DNS: QueryId = 0x83F0, QUERY (Standard query), Query for web.artvinum.com of type AAAA on class Internet
17	3.304752		172.30.1.180	172.30.1.170	DNS	DNS: QueryId = 0x83F0, QUERY (Standard query), Response - Success
18	3.605184		172.30.1.170	ordi.test.ch	ARP	ARP: Request, 172.30.1.170 asks for 172.30.1.59

Frame Details

- + DestinationAddress: Microsoft Corporation C56ACF
- + SourceAddress: Microsoft Corporation CE6ACF
- EthernetType: Internet IP (IPv4), 2048(0x800)
- + Ipv4: Next Protocol = UDP, Packet ID = 21767, Total IP Length = 129
- + Udp: SrcPort = DNS(53), DstPort = 53534, Length = 109
- + Dns: QueryId = 0x15EA, QUERY (Standard query), Response - Success
  - QueryIdentifier: 5610 (0x15EA)
  - + Flags: Response, Opcode - QUERY (Standard query), AA, RD, RA, Rcode
    - QuestionCount: 1 (0x1)
    - AnswerCount: 3 (0x3)
    - NameServerCount: 0 (0x0)
    - AdditionalCount: 0 (0x0)
  - QRecord: web.artvinum.com of type Host Addr on class Internet
    - QuestionName: web.artvinum.com
    - QuestionType: A, IPv4 address, 1(0x1)
    - QuestionClass: Internet, 1(0x1)
  - + ARecord: web.artvinum.com of type CNAME on class Internet
  - + ARecord: www.test.ch of type CNAME on class Internet
  - + ARecord: ordi.test.ch of type Host Addr on class Internet

# Configuration d'un serveur DNS

## 1. Configurer le serveur DNS



L'utilisation de l'assistant **Configuration d'un serveur DNS** permet de :

- Créer une zone de recherche directe.
- Éventuellement créer une zone de recherche inversée.
- Configurer les mises à jour dynamiques.
- Configurer les racines ou les redirecteurs.

Il n'est pas recommandé d'effectuer la création de zone par cette méthode, elle est plutôt réservée à un administrateur peu expérimenté. Elle est totalement inutile si le serveur DNS est un contrôleur de domaine.

La procédure suivante montre comment l'utiliser.

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, cliquez avec le bouton droit de la souris sur le serveur DNS puis choisissez **Configurer un serveur DNS**.
- Sur la page **Bienvenue dans l'assistant Configuration d'un serveur DNS**, cliquez sur **Suivant**.
- Sur la page **Sélectionnez une action de configuration**, sélectionnez **Configurer les indications de racine uniquement**, puis cliquez sur **Suivant**. Vous pouvez choisir une autre option si vous voulez créer une zone.
- Sur la page **Fin de l'assistant Configuration d'un serveur DNS**, cliquez sur **Terminer**.

## 2. Définir le vieillissement et le nettoyage



Il est recommandé de mettre à jour régulièrement le contenu de la base de données du serveur DNS afin que des enregistrements devenus obsolètes ne polluent pas la base.

Pour que le nettoyage s'effectue, il faut configurer correctement les éléments suivants :

- Il faut garantir que chaque enregistrement puisse être supprimé.
- Il faut garantir que la zone DNS puisse être nettoyée.
- Il faut garantir qu'au moins un serveur DNS puisse nettoyer les enregistrements.

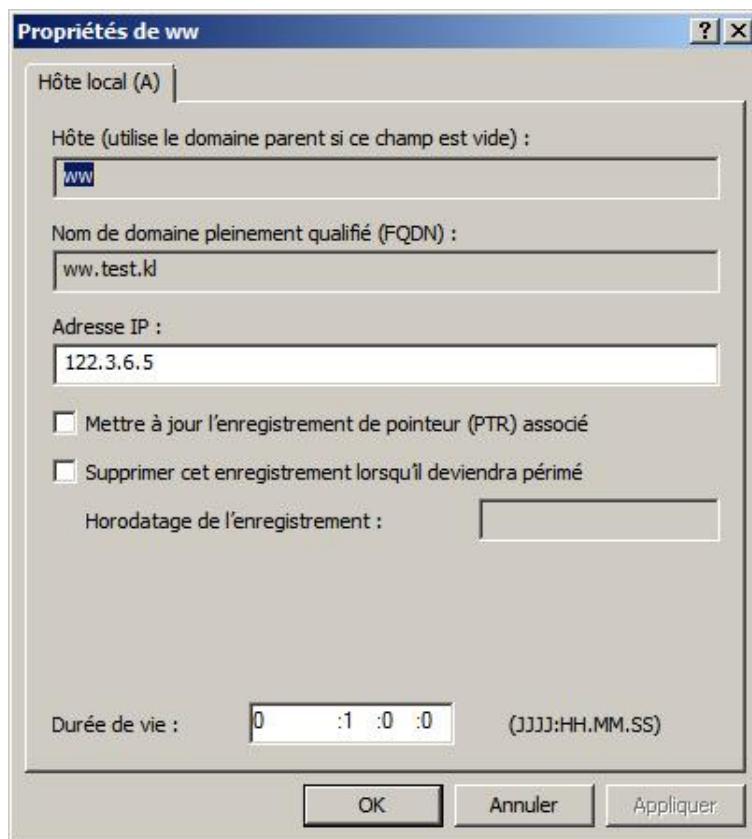
Comme vous pouvez le constater, il faut activer le nettoyage au niveau de l'enregistrement, de la zone et d'au moins un serveur qui gère la zone.

Les procédures suivantes devraient toujours être effectuées.

### a. Permettre la suppression d'un enregistrement

Il faut distinguer entre des enregistrements statiques et des enregistrements dynamiques. Par défaut un enregistrement statique ne permet pas la suppression automatique de l'enregistrement. Si vous voulez l'effacer automatiquement suivez la procédure ci-dessous.

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, développez l'arborescence pour faire apparaître dans la fenêtre principale l'enregistrement statique concerné.
- Cliquez avec le bouton droit de la souris sur l'enregistrement puis sur **Propriétés** dans le menu contextuel.



 Si la case à cocher **Supprimer cet enregistrement lorsqu'il deviendra périmé** n'est pas visible, fermez la boîte de dialogue **Propriétés** puis cliquez sur **Affichage détaillé** dans le menu **Affichage** et ouvrez à nouveau la boîte de dialogue **Propriétés**.

- Cochez la case **Supprimer cet enregistrement lorsqu'il deviendra périmé** puis cliquez sur **Appliquer** pour faire apparaître la valeur de l'horodatage.
- Cliquez sur **OK** pour fermer la boîte de dialogue.

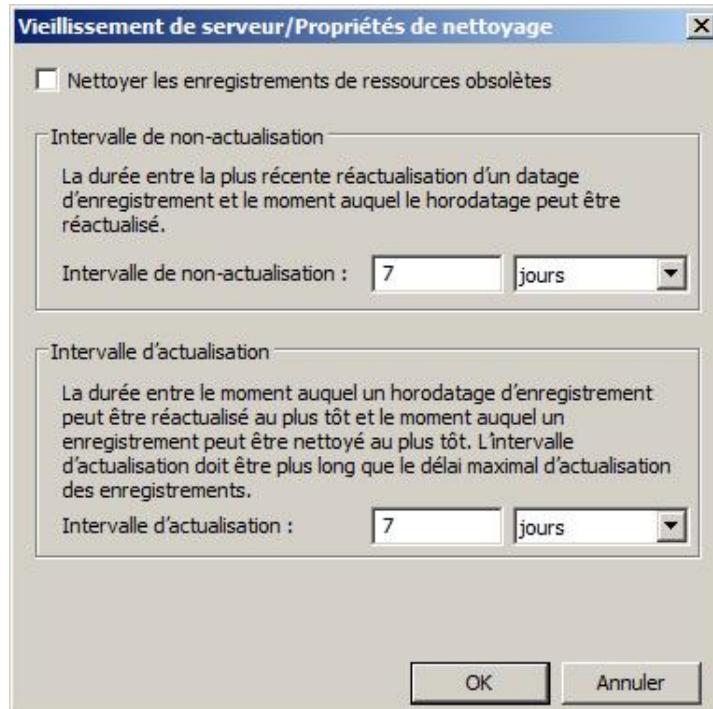
Pour les enregistrements dynamiques (DDNS) les hôtes Microsoft tentent de mettre à jour l'enregistrement toutes les 24 heures. Un horodatage est associé à l'enregistrement et il est mis à jour si la zone permet le nettoyage des enregistrements. La valeur de l'horodateur est à 0 pour les enregistrements statiques sans que la case à cocher soit activée et elle correspond à la date de création de l'enregistrement pour les autres ou à la date de la mise à jour si la zone permet la suppression.



Les enregistrements NS (*Name Server*) et SOA (*Start Of Authority*) utilisent les valeurs de la zone.

## b. Définir le vieillissement/nettoyage pour toutes les zones

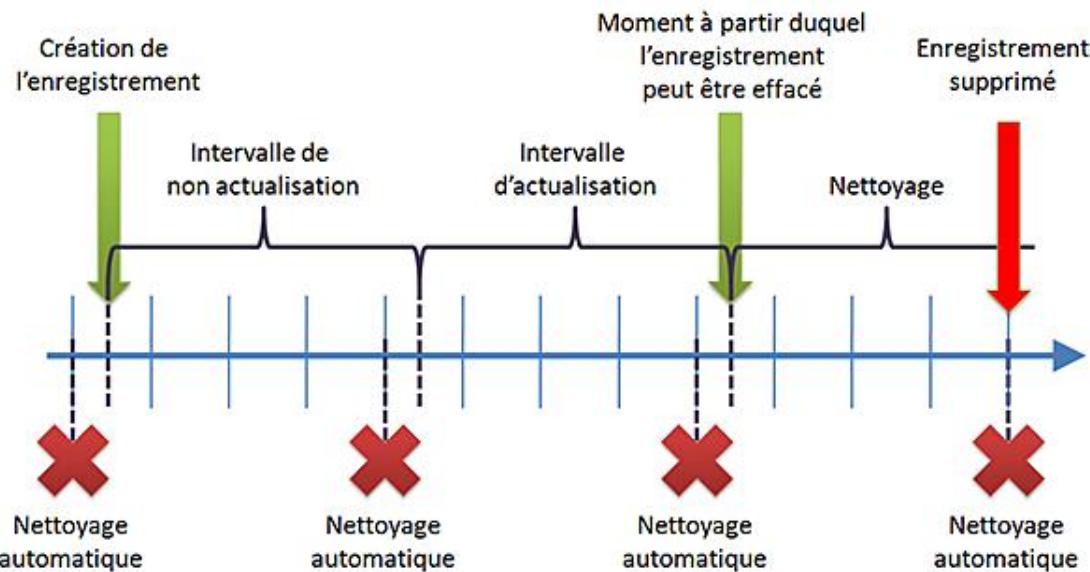
- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, cliquez avec le bouton droit de la souris sur le serveur DNS puis sur **Définir le vieillissement/nettoyage pour toutes les zones**.



La case à cocher **Nettoyer les enregistrements de ressources obsolètes** devrait être toujours sélectionnée afin que le système efface automatiquement ces enregistrements.

L'**Intervalle de non-actualisation** indique un intervalle durant lequel il n'est pas possible de réactualiser cet enregistrement. L'adresse IP peut être modifiée.

L'**Intervalle d'actualisation** indique l'intervalle durant lequel les enregistrements doivent rester dans le serveur DNS après la fin de l'intervalle de non-actualisation. Cet intervalle devrait correspondre à la durée de bail du serveur DHCP.



➤ Vous pouvez également définir le vieillissement/nettoyage pour chaque zone à partir de l'onglet **Général** de la boîte de dialogue **Propriétés de la zone**, en cliquant sur **Vieillissement**.

### 3. Nettoyer les enregistrements de ressources obsolètes

Vous pouvez lancer manuellement ou automatiquement le nettoyage des zones sur lesquelles le serveur a autorité.

#### a. Activer le nettoyage automatique



- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, cliquez avec le bouton droit de la souris sur le serveur DNS puis sur **Propriétés**.
- Cliquez sur l'onglet **Avancé**, sélectionnez la case à cocher **Activer le nettoyage automatique des enregistrements obsolètes**, modifiez éventuellement le **Délai de nettoyage** puis cliquez sur **OK**.



#### b. Lancer le nettoyage manuellement



- Connectez-vous en tant qu'administrateur.

- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, cliquez avec le bouton droit de la souris sur le serveur DNS puis sur **Nettoyer les enregistrements de ressources obsolètes**.
- Dans la boîte de dialogue DNS qui vous demande si vous voulez nettoyer tous les enregistrements périmés du serveur, cliquez sur **Oui**.

➤ Vous pouvez déterminer le moment où un enregistrement sera supprimé en recherchant les derniers événements 2501 et 2502 dans le journal puis en lui ajoutant la valeur du délai de nettoyage.

## 4. Journaux globaux



Avec la nouvelle console DNS, les événements dus au serveur DNS sont placés sous **Journaux globaux** dans le volet de gauche.

La procédure est la suivante.

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, cliquez sur **Journaux globaux** pour développer l'arborescence.
- Cliquez sur **Événements DNS** pour faire apparaître les événements dans la fenêtre principale.

➤ Vous pouvez définir quels événements seront enregistrés dans le journal des événements dans l'onglet **Enregistrement des événements** de la boîte de dialogue **Propriétés du serveur**.

## 5. Désactiver l'écoute de requêtes DNS sur une adresse IP



Si le serveur DNS est configuré avec plusieurs adresses IP, que ce soient des adresses IPv4 ou IPv6, il est possible de désactiver l'écoute de requêtes. La procédure est la suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche du Gestionnaire DNS, cliquez avec le bouton droit de la souris sur le serveur DNS puis cliquez sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Interfaces** puis cochez les cases des adresses IP sur lesquelles le serveur doit écouter et cliquez sur **OK**.

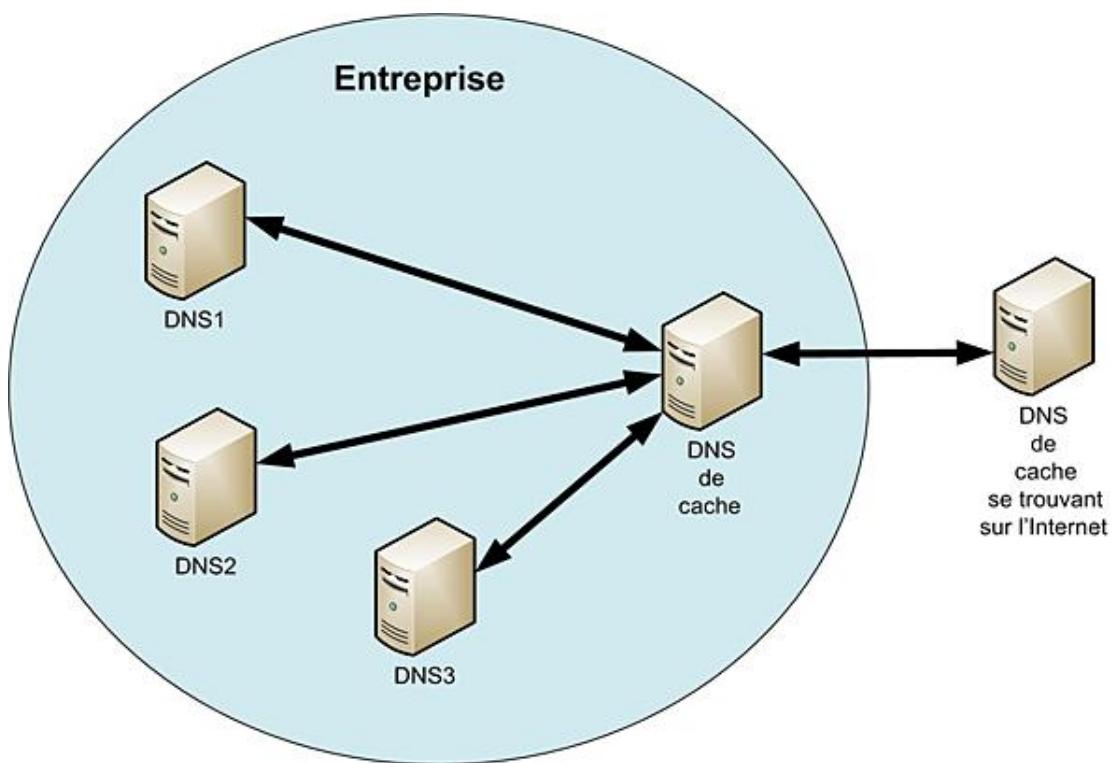
Remarquez qu'il est possible de sélectionner une adresse IP et non la carte réseau.

## 6. Serveur de cache DNS

Le serveur DNS peut être un serveur de cache, c'est-à-dire qu'il s'occupe de la résolution des noms en adresses IP pour les zones sur lesquelles il n'a pas autorité. Lorsqu'il a accès à Internet, il faut ouvrir le port UDP 53 dans le pare-feu. Il conserve dans un cache local toutes les résolutions effectuées selon le TTL qui les accompagne.

Aucune configuration n'est nécessaire, par défaut le serveur DNS est conçu pour fonctionner en tant que serveur de cache en utilisant les serveurs racine configurés. Il est possible de contrôler le trafic du serveur de cache en recourant à un serveur de cache externe.

- Afin de réduire les menaces dues aux serveurs DNS, il est recommandé de rediriger les requêtes vers un serveur de cache interne qui sera redirigé vers un serveur de cache externe, comme le montre l'image suivante :



- Dans un environnement virtualisé, il faut également tenir compte de la portée de la carte réseau virtuelle, soit locale à l'ordinateur, soit qui permet également d'être visible sur le réseau physique.

- En production, il est possible de placer des serveurs DNS de cache à la place d'un serveur DNS de zone dans un bureau distant afin de ne pas pénaliser la bande passante disponible par des transferts de zone fréquents.

### a. Afficher ou masquer la zone de cache



- Connectez-vous en tant qu'administrateur.
- Pour afficher la zone de cache, lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.

- Dans le volet de gauche, cliquez sur le nom du serveur puis sur l'option **Affichage détaillé** du menu **Affichage**. La zone **Recherches mises en cache** apparaît dans le volet de gauche.



Pour masquer la zone de cache, effectuez la même opération.

## b. Effacer le cache DNS



La zone de cache du serveur DNS est vidée avec la procédure suivante.

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur le nom du serveur puis cliquez sur **Effacer le cache**.



Cette opération ne vide pas le cache DNS du serveur mais uniquement la zone de cache du serveur DNS. Pour vider le cache DNS d'un ordinateur, saisissez la commande **ipconfig /flushdns** dans une invite de commande en disposant des privilèges élevés. Pour visualiser le cache DNS, saisissez la commande **ipconfig /displaydns**.

## 7. Serveurs racine

Chaque serveur DNS dispose d'une liste des serveurs racine. L'organisme IANA (*Internet Assigned Numbers Authority*) gère la liste de ces serveurs. Actuellement, ils sont au nombre de 13, disséminés un peu partout dans le monde. Leur nom est de type **lettre.root-servers.net** où lettre peut avoir une valeur allant de a à m. L'URL suivante vous donne la liste actuelle de ces serveurs : <http://www.iana.org/domains/root/db/arpa.html>



La liste fournie par Microsoft à la sortie de la version RTM utilise les noms actuels mais certaines adresses sont encore basées sur les anciens serveurs racine d'Internet.

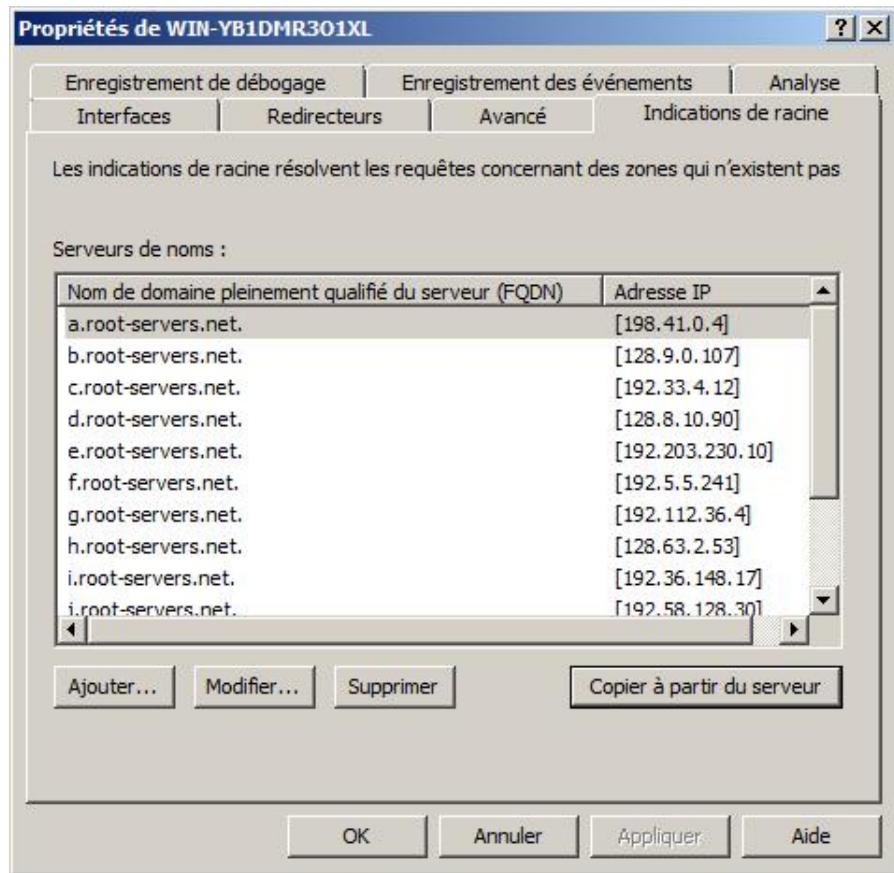


Pour consulter la liste des serveurs, modifier ou supprimer un serveur, utilisez la procédure suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur le nom du serveur puis choisissez **Propriétés**.
- Cliquez sur l'onglet **Indications de racine**.



Il n'est pas conseillé de modifier ces serveurs.



**Ajouter** permet d'ajouter de nouveaux serveurs racine.

**Modifier** permet de modifier un serveur existant ou d'ajouter une nouvelle adresse IP pour un nom existant.

**Supprimer** permet de supprimer un serveur racine.

**Copier à partir du serveur** permet de copier la liste à partir d'un serveur qui fait référence. Cette liste peut être également récupérée sur le site [www.internic.net/zones/named.root](http://www.internic.net/zones/named.root) ou dans le répertoire %systemroot%\system32\dns\samples\cache.dns.

## 8. Redirecteurs

Il existe plusieurs types de redirecteurs, à savoir :

- le redirecteur par défaut,
- le redirecteur conditionnel,
- la zone de stub.

Lorsque le serveur DNS reçoit une requête, il tente de résoudre le nom en adresse IP en utilisant les ressources dans l'ordre suivant :

- 1. Une zone DNS locale au serveur en utilisant les priorités suivantes :
  - zone DNS faisant autorité ou non ;
  - redirection de la zone déléguée ou de la zone de stub.
- 2. La redirection conditionnelle.
- 3. La redirection par défaut.

- 4. Les serveurs DNS racine.

Le redirecteur par défaut redirige les requêtes DNS qui n'ont pu être résolues sur le serveur DNS vers le premier serveur de la liste. En cas de non réponse, il tente de contacter les autres serveurs de la liste selon l'ordre défini.

Les redirecteurs conditionnels permettent de rediriger les requêtes non résolues localement pour un domaine spécifique vers un serveur DNS particulier.

Cette méthode est très utile lorsque votre entreprise collabore avec des entreprises partenaires et vous donne accès à un extranet. Il vous suffit simplement d'ajouter les adresses des serveurs DNS pour cette zone.

Néanmoins, si les adresses des serveurs DNS changent, vous devez être averti et les modifier. Pour pallier ce problème, vous pouvez créer une zone de stub c'est-à-dire créer une zone qui ne contient que les noms des serveurs DNS de la zone considérée et leur adresse IP. La mise à jour des données de la zone se fait par transfert de zone. Il faut donc que les serveurs source acceptent d'effectuer un transfert de zone vers vos serveurs DNS.

-  La zone de stub est une amélioration du redirecteur conditionnel mais ne peut s'utiliser que s'il est possible d'effectuer un transfert de zone.

### a. Ajout d'un redirecteur par défaut



- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur le nom du serveur puis choisissez **Propriétés**.
- Cliquez sur l'onglet **Redirecteurs**.

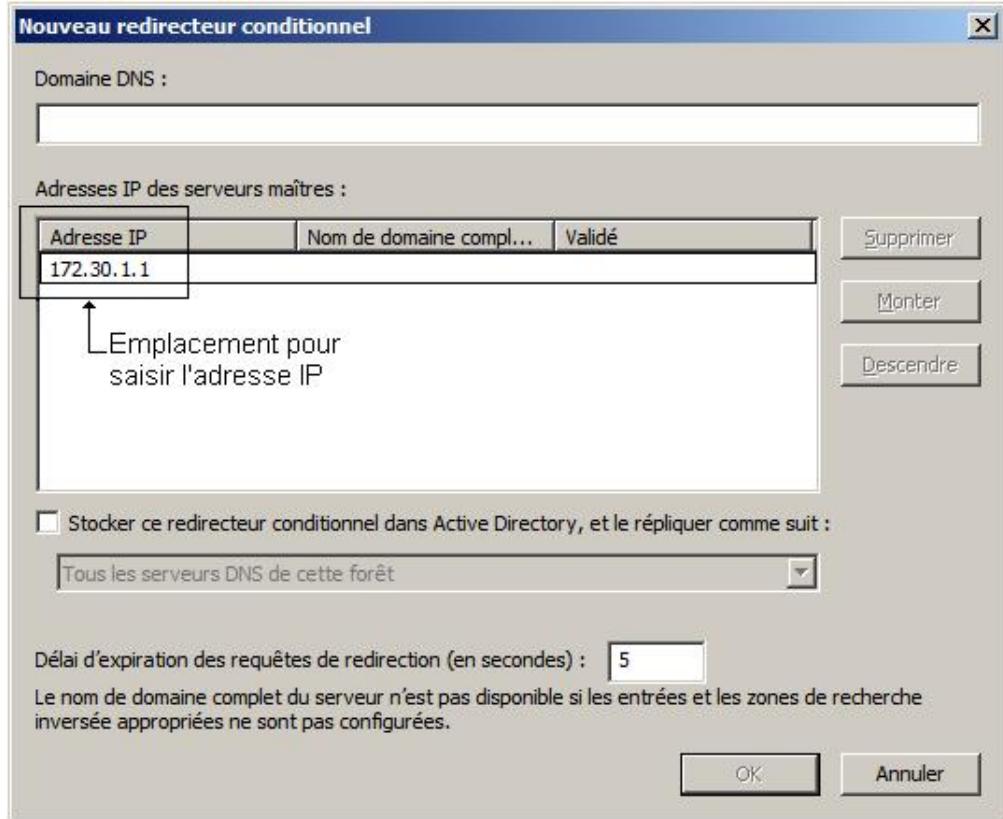
Le bouton **Modifier** permet d'ajouter, de modifier ou de supprimer l'adresse IP d'un serveur DNS. Dès que l'on ajoute une adresse IP, le serveur DNS va essayer de retrouver son nom si une zone inverse existe. Vous pouvez modifier la valeur du délai d'expiration pour recevoir une réponse, par défaut elle est de 3 secondes.

La sélection de la case à cocher **Utiliser les indications de racine si aucun redirecteur n'est disponible** permet d'utiliser les serveurs DNS racine, lorsqu'aucun redirecteur ne répond.

### b. Ajout d'un redirecteur conditionnel



- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur la zone **Redirecteurs conditionnels** puis cliquez sur **Nouveau redirecteur conditionnel**.
- Saisissez le nom du domaine qui doit être redirigé puis associez-lui une ou plusieurs adresses IP qui correspondent aux serveurs DNS qui gèrent ce domaine en tapant l'adresse IP de chaque serveur dans la zone **Adresses IP des serveurs maîtres** comme le montre l'image suivante. Si le serveur DNS est également un serveur contrôleur de domaine (DC), vous pouvez stocker ces informations dans l'Active Directory et les répliquer selon les valeurs de la liste déroulante. Vous pouvez modifier la valeur du délai d'expiration pour recevoir une réponse, par défaut elle est de 5 secondes. Cliquez ensuite sur **OK**.



### c. Ajout d'une zone de stub



- Connectez-vous en tant qu'administrateur.
- Lancez le Gestionnaire DNS en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **DNS**.
- Dans le volet de gauche, cliquez avec le bouton droit de la souris sur **Zones de recherche directes** puis cliquez sur **Nouvelle zone**.
- Sur la page **Bienvenue !** de l'**Assistant Nouvelle zone**, cliquez sur **Suivant**.
- Sur la page **Type de zone**, sélectionnez l'option **Zone de stub**. Si le serveur DNS est également un contrôleur de domaine, vous pouvez enregistrer la zone dans l'Active Directory en sélectionnant la case à cocher correspondante. Enfin cliquez sur **Suivant**.
- La page **Étendue de la zone de réPLICATION de Active Directory** apparaît seulement si vous avez sélectionné la case à cocher correspondante dans la page précédente. Sélectionnez l'option désirée puis cliquez sur **Suivant**.
- Sur la page **Nom de la zone**, saisissez le nom de domaine DNS qui doit être redirigé puis cliquez sur **Suivant**.
- La page **Fichier de zone** apparaît si vous n'avez pas sélectionné la case à cocher **Enregistrer la zone dans Active Directory** sur la page **Type de zone**. Vous pouvez soit créer un nouveau fichier nommé (recommandé), soit utiliser un fichier existant. Par défaut, ces fichiers sont stockés dans le répertoire %systemroot%\system32\dns. Cliquez sur **Suivant**.
- Sur la page **Serveurs DNS maîtres**, ajoutez les serveurs DNS servant de références pour la zone considérée. Si

vous stockez la zone dans l'Active Directory, la case à cocher **Utiliser les serveurs suivants pour créer une liste locale des serveurs maîtres** apparaît. Vous pourrez alors utiliser les serveurs de la liste en tant que maître pour la zone et non les serveurs maîtres stockés dans l'Active Directory. Cliquez ensuite sur **Suivant**.

- Sur la page **Fin** de l'**Assistant Nouvelle zone**, vérifiez vos informations puis cliquez sur **Terminer**.

# Installation du rôle Serveur DNS

Pour installer le rôle Serveur DNS, il existe deux méthodes. La première consiste à installer le rôle Serveur DNS en même temps que l'Active Directory. La seconde méthode, décrite ici, effectue l'installation du rôle par l'intermédiaire du Gestionnaire de serveur.

 La méthode conseillée par Microsoft consiste à installer le rôle Serveur DNS en même temps que l'Active Directory. En d'autres termes, il faut installer le serveur DNS sur un contrôleur de domaine.

## 1. Pré-requis

Le pré-requis pour l'installation du rôle DNS est que le serveur dispose d'une adresse IP. Cette adresse devrait être statique (méthode conseillée), il faut empêcher qu'elle soit modifiée en effectuant une réservation auprès de son serveur DHCP (méthode possible). En effet, si l'adresse IP du serveur DNS change, les clients DNS ne peuvent le contacter.

Il est possible de contrôler l'adresse IP du serveur avec la commande **ipconfig /all**.

## 2. Installation



Win2

L'assistant d'ajout de rôles installe le service DNS et permet également de configurer le serveur DNS avec les options les plus courantes.

- Connectez-vous en tant qu'administrateur.
- Pour démarrer l'installation, lancez le Gestionnaire de serveur en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur **Rôles**.
- Dans **Rôles**, cliquez sur **Ajouter des rôles**.
- Dans l'**Assistant Ajout de rôles**, si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez le rôle **Serveur DNS** puis cliquez sur **Suivant**.
- Sur la page **Serveur DNS**, cliquez sur **Suivant**.
- Sur la page **Confirmation**, cliquez sur **Installer**.
- Consultez la page **Résultats** pour voir si l'installation a réussi puis cliquez sur **Fermer**.

 Il n'est pas possible d'utiliser l'assistant Ajout de rôles pour installer un serveur DNS sur un ordinateur disposant des services Active Directory. Il faut installer le service Serveur DNS pendant l'exécution de la commande **dcpromo**.

# Introduction

Le système DNS (*Domain Name System*) utilise un espace de noms. Il se compose d'une arborescence de domaines dont le niveau le plus bas correspond à un enregistrement de ressources. Les nœuds de niveaux supérieurs permettent d'organiser ces enregistrements de manière hiérarchique, on les appelle **domaines**.

La racine d'un espace de noms peut être une racine Internet ou une racine d'entreprise. Dans la suite du chapitre, il sera toujours fait référence à la racine Internet.

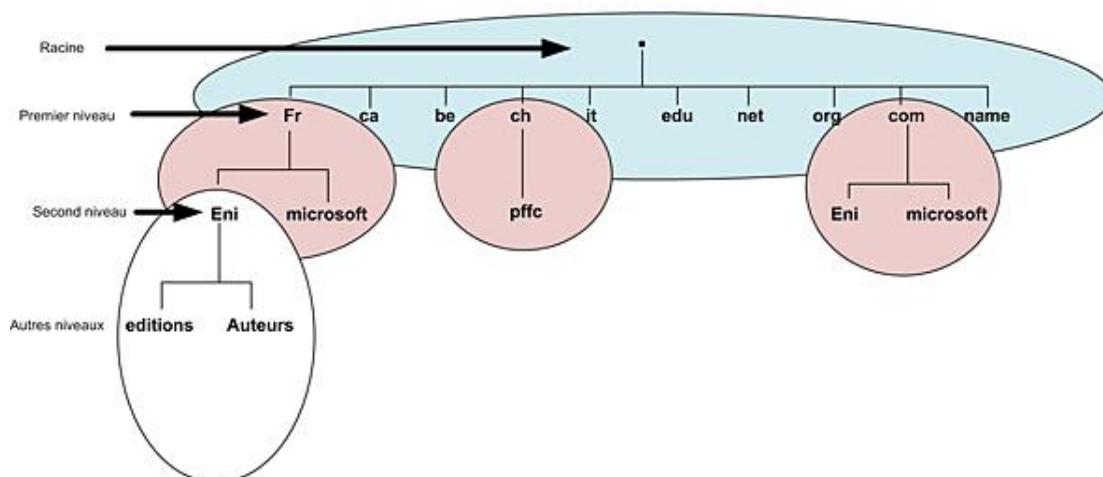
La racine est représentée par un point sous lequel on trouve les domaines de premier niveau comme les pays, les organisations ; fr, ch, com, gov, edu, net, name, museum sont quelques exemples de noms de domaine de premier niveau. L'IANA (*Internet Assigned Numbers Authority*) gère la racine et coordonne la délégation des noms de domaine de premier niveau auprès d'organismes. Par exemple, l'AFNIC gère le domaine fr, Switch gère le domaine ch, etc.

Les entreprises ou les particuliers peuvent acheter, ou plus exactement louer, un nom de domaine à partir du second niveau selon des règles édictées par les organismes qui gèrent le premier niveau.

L'organisme de premier niveau vous délègue l'autorité pour le domaine que vous avez acheté, ce qui vous permet d'ajouter des sous-domaines ou des enregistrements en fonction de vos besoins.

La délégation signifie que vous avez autorité sur le domaine. En fait, on ne parle plus d'espace de noms mais de zone, ce qui signifie que l'IANA n'a autorité que sur les domaines de premier niveau et que les organismes se situant au premier niveau ont autorité jusqu'au second niveau. Au-delà, la responsabilité devient celle de l'entreprise ou du particulier. Ce sont donc des serveurs DNS différents qui gèrent les différents niveaux.

La figure suivante montre l'organisation hiérarchique de l'espace de noms Internet et la gestion des zones à l'aide des serveurs DNS. Notez qu'il n'est pas possible d'avoir deux noms identiques sous le même niveau dépendant du même parent mais que deux noms identiques dépendant de parents différents peuvent appartenir à deux entités différentes (règle d'unicité de niveau).



Pour les entreprises et les particuliers, il est possible de créer d'autres niveaux ou de déléguer une partie de leur domaine.

**💡** Bien qu'il soit en théorie possible de créer jusqu'à 127 niveaux de 63 caractères, le nom du domaine est limité à un maximum de 255 caractères, voire moins sur Internet. De même, les caractères accentués ne sont pas permis pour la plupart des noms de domaine. Windows est moins restrictif. Attention aux caractères réservés surtout le "point".

On appelle FQDN (*Fully Qualified Domain Name*) un nom complet identifiant la ressource depuis ses parents jusqu'à la racine. Chaque point étant un séparateur de niveau hiérarchique. Par exemple, www.eni.fr. est un FQDN où :

- . (point) représente la racine.
- **fr** représente le nom de domaine de premier niveau.
- **eni** représente le nom de domaine de second niveau.
- **www** représente un enregistrement dans la zone, ici un enregistrement de type hôte.

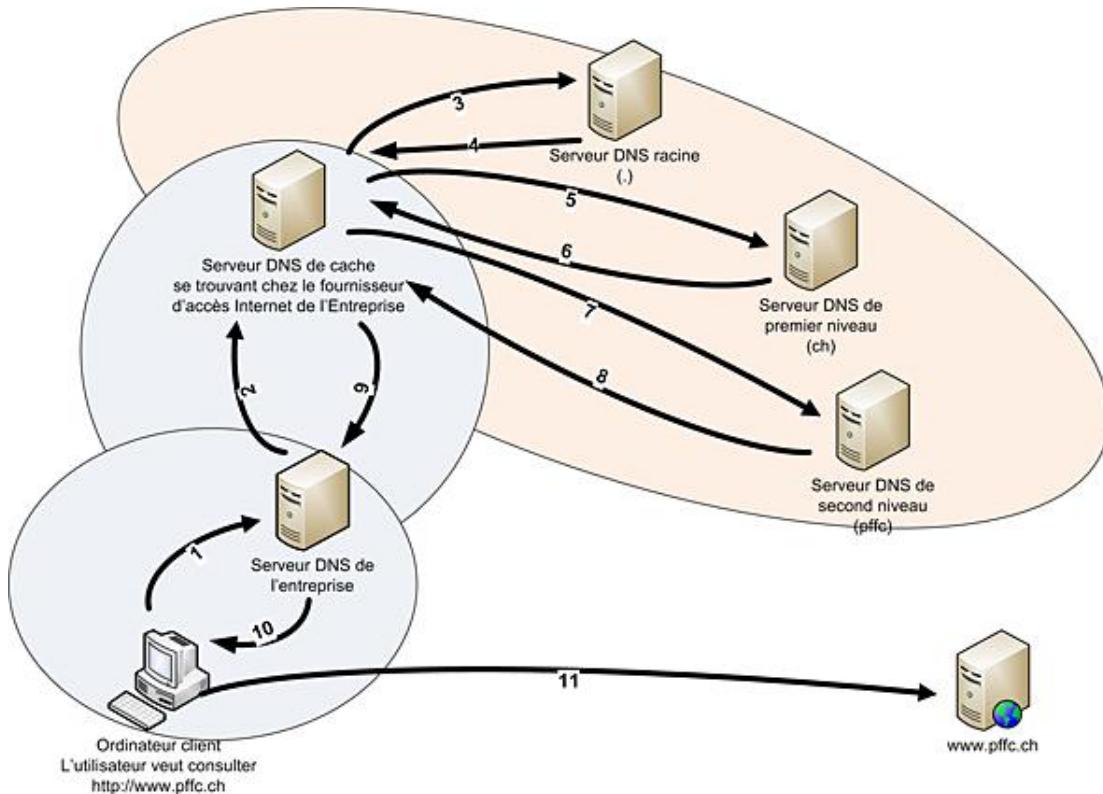


Dans un navigateur Internet, le . (point) symbolisant la racine est ajouté automatiquement à la fin de l'URL.

Pour résoudre un nom en adresse IP, il faut utiliser un résolveur ; celui-ci peut travailler soit de manière récursive, soit de manière itérative.

Le mode récursif est surtout utilisé par les ordinateurs clients qui font une requête et attendent une réponse de type résolu ou non résolu. Le mode itératif est utilisé par les serveurs DNS qui ont la charge de localiser un hébergeur potentiel de la zone recherchée en commençant par la racine.

La figure suivante illustre la procédure suivie pour qu'un ordinateur client reçoive l'adresse IP pour le nom considéré.



L'ordinateur client veut afficher le site [www.pffc.ch](http://www.pffc.ch) dans son navigateur. Comme l'adresse IP ne se trouve pas dans le cache local, il effectue une requête récursive auprès du serveur DNS (1).

Le serveur DNS de l'entreprise reçoit la requête du client ; comme il ne fait pas autorité pour la zone, et que l'adresse ne se trouve pas dans le cache DNS, il effectue une demande récursive auprès du serveur DNS de cache de son fournisseur d'accès Internet (2).

Le serveur DNS du fournisseur d'accès Internet ne trouve pas l'adresse dans son cache, il effectue alors une requête itérative auprès des serveurs racine (3).

Un serveur racine répond en disant de contacter le serveur gérant le premier niveau du domaine ch, il lui fournit l'adresse IP du serveur (4).

Le serveur DNS de cache contacte alors le serveur DNS de premier niveau avec une requête itérative (5).

Le serveur DNS de premier niveau répond en disant de contacter le serveur gérant le second niveau du domaine pffc.ch, il lui fournit l'adresse IP du serveur (6).

Le serveur DNS de cache contacte alors le serveur DNS de second niveau avec une demande itérative (7).

Le serveur DNS de second niveau répond en fournissant l'adresse IP pour le nom [www.pffc.ch](http://www.pffc.ch) (8). L'adresse est maintenant résolue.

Le serveur DNS de cache du fournisseur Internet renvoie la réponse auprès du serveur de cache de l'entreprise (9) après l'avoir stockée dans son cache. Elle sera utilisée pour les demandes ultérieures et restera dans le cache pendant la durée de vie (TTL) de l'enregistrement.

Le serveur DNS de cache de l'entreprise renvoie la réponse auprès du client (10) après l'avoir stockée dans son cache. Elle sera utilisée pour les demandes ultérieures et restera dans le cache pendant la durée de vie (TTL) de l'enregistrement.

Enfin, l'ordinateur client reçoit la réponse et la stocke dans son cache local afin d'être réutilisée ultérieurement tant que le TTL est plus grand que 0. Il peut maintenant contacter le site Web [www.pffc.ch](http://www.pffc.ch) dont il connaît l'adresse IP.

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre les objectifs suivants décrits dans les sections suivantes :

### Configurer un serveur DNS (Domain Name System)

Cela inclut, sans s'y limiter :

- installation et gestion du serveur DNS ;
- mise en œuvre du serveur de cache ;
- mise en œuvre de redirecteur externe et conditionnel ;
- mise en œuvre de serveur racine ;
- intégration entre WINS et DNS ;

### Configurer les zones DNS

Cela inclut, sans s'y limiter :

- création et gestion de zones primaires et secondaires ;
- gestion de zones intégrées Active Directory ;
- gestion des zones dynamiques (DDNS), intervalle de réactualisation et mise à jour du serveur DNS ;
- intégration de serveurs Wins ;
- création et gestion de GlobalNames ;
- outils de gestion nslookup, dnsclient, dnslint.

### Configurer les enregistrements DNS

Cela inclut, sans s'y limiter :

- types d'enregistrement ;
- gestion des enregistrements SOA (*Start Of Authority*) ;
- gestion des enregistrements A (hôte) ;
- gestion des enregistrements P (Pointeur) ;
- gestion des enregistrements MX (Messagerie) ;
- gestion des enregistrements SRV (Service) ;
- gestion des enregistrements NS (Serveur de noms) ;
- mises à jour dynamiques ;
- gestion du TTL (*Time To Live*) d'un enregistrement.

## **Configurer la réPLICATION DNS**

Cela inclut, sans s'y limiter :

- réPLICATION vers une zone DNS secondaire ;
- réPLICATION vers une zone de stub DNS ;
- nettoyage des enregistrements DNS ;
- portée de la réPLICATION.

## **Configurer la résOLUTION de noms pour des ordinateurs clients**

Cela inclut, sans s'y limiter :

- gestion des fichiers HOSTS ;
- gestion des fichiers LMHOSTS ;
- mise en œuvre des types de noeud NetBIOS ;
- mise en œuvre de LLMNR (*Link-Local Multicast Name Resolution*) ;
- résolution de noms en utilisant des messages de diffusion ;
- mise en œuvre du cache de resolver ;
- gestion de la liste des serveurs DNS ;
- mise en œuvre de l'ordre de recherche des suffixes DNS ;
- gestion des paramètres du client via une stratégie de groupe.

## **2. Pré-requis matériels**

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



## **3. Objectifs**

Depuis l'apparition de l'Active Directory, le serveur DNS est devenu un élément incontournable de l'infrastructure d'un réseau Windows. Il est utilisé pour rechercher les serveurs Active Directory afin de permettre une connexion des utilisateurs mais également pour l'accès à Internet.

Ce chapitre vous présente tout d'abord d'une façon théorique les espaces de noms et les zones DNS et les méthodes utilisées pour la résolution d'un nom en adresse IP. Vous apprendrez ensuite à installer le service DNS pour une version complète ou un Server Core et à utiliser la console MMC pour configurer et gérer le service DNS. Pour en terminer avec les serveurs DNS, vous verrez comment utiliser les outils de type ligne de commandes pour dépanner ou gérer un serveur DNS.

Le chapitre se terminera par l'étude de la résolution de noms pour un client. Les différentes méthodes y seront présentées afin de bien comprendre les mécanismes mis en œuvre.

# Validation des acquis

## 1. Questions

### Questions triviales

- 1** Quelle commande saisir pour activer l'**autotunning** ?
- 2** Quel est le nom du protocole permettant d'optimiser le débit du côté de l'émission ?
- 3** Que signifie le terme **Black Hole** ?
- 4** Citez au moins trois problèmes pouvant être diagnostiqués à l'aide de l'infrastructure de diagnostics réseau.
- 5** Citez les plages d'adresses provenant de la RFC1918.
- 6** Qu'est-ce qu'une adresse APIPA ?
- 7** Citez une adresse de loopback en **IPv4** et en **IPv6**.
- 8** Citez les types d'adresses que vous pouvez trouver en **IPv6**.
- 9** Citez une adresse de liaison locale.
- 10** Quel est le préfixe d'une adresse Teredo ?
- 11** Sur un Server Core, comment configurez-vous une adresse IP ?
- 12** Citez un avantage du routage dynamique.
- 13** Citez au moins un avantage du protocole OSPF sur RIP.
- 14** Quel algorithme utilise protocole RIP ?
- 15** Citez au moins une méthode pour afficher la table de routage locale d'un ordinateur.

### Questions de compréhension

- 16** Indiquez si l'adresse IP 172.255.255.0/23 est valide.
- 17** Quel est le type de l'adresse IP 224.0.0.5 ?
- 18** Quel est le type de l'adresse IP 192.168.1.255/24 ?
- 19** Votre collègue ne comprend pas pourquoi votre serveur Windows 2008 est configuré avec des adresses IPv6. Vous lui répondez ?
- 20** Votre collègue vient de désactiver le protocole IPv6 à l'aide des propriétés de la carte réseau. Néanmoins il semble que le protocole soit toujours là. Que lui répondez-vous ?
- 21** Vous migrez le protocole IPv4 vers le protocole IPv6. Les segments 1 et 3 sont déjà migrés, néanmoins le segment 2 se situant entre les segments 1 et 3 est encore sous IPv4. Quelle serait la plage d'adresses IPv6 pour ce scénario ?
- 22** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Le routeur 2 permet également d'avoir accès à Internet. Votre collègue utilise un moniteur réseau et remarque un trafic double sur le segment 2 lorsque la destination est le segment 3 ou Internet. Quelle peut en être la cause ?
- 23** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Le routeur 2 permet également d'avoir accès à Internet. Des utilisateurs du segment 1 se plaignent qu'ils ne peuvent atteindre un serveur se trouvant sur le segment 3. Depuis votre station de travail du segment 2, vous parvenez à atteindre ledit serveur. Quelle peut en être la cause probable ?
- 24** Votre collègue doit effectuer un test qui demande de créer un réseau séparé mais accessible depuis votre poste de travail. Il propose d'utiliser un serveur 2008 et de configurer le protocole de routage RIP mais il n'est pas sûr que l'implémentation de RIP du serveur Microsoft soit compatible avec vos routeurs Cisco. Que lui répondez-vous ?
- 25** En dépannant un serveur, votre collègue a détecté une mauvaise configuration de l'adressage IP, soit l'adresse 169.254.56.34/16. Il veut la modifier, qu'en pensez-vous ?

### Questions d'implémentation

- 26** Votre fournisseur d'accès Internet vous attribue la plage d'adresses 82.54.255.64/30, quelles sont la première

et la dernière adresse utilisables ainsi que le masque de sous-réseau ?

- 27** Vous devez segmenter la plage d'adresses IP 192.168.8.0/23 de manière à créer un réseau ayant 200 adresses, un réseau ayant 66 adresses et un réseau ayant 32 adresses, comment faites-vous ?
- 28** Vous aimeriez permettre à vos ordinateurs, en cas de panne du serveur DHCP, de pouvoir au moins communiquer avec le serveur de fichiers et d'impression distant, comment feriez-vous ?
- 29** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Le routeur 2 permet également d'avoir accès à Internet. Votre collègue décide d'implémenter le protocole RIP sans succès. Vous vérifiez la configuration et elle vous semble correcte mais aucun message RIP ne transite sur le segment 2. Quelle peut en être la cause ?
- 30** Votre collègue aimerait implémenter le protocole de routage RIP sur un Server Core, mais il ne sait pas comment procéder, comment pouvez-vous l'aider ?
- 31** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Sur le segment 2, vous disposez d'un serveur 2008 qui permet l'accès à Internet. Les utilisateurs du segment 2 peuvent accéder à Internet mais pas ceux des segments 1 et 3, quelle peut en être la cause ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /31

Pour ce chapitre, votre score minimum doit être de 23 sur 31.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

## 3. Réponses

### Questions triviales

- 1** Quelle commande saisir pour activer l'**Auto-Tuning** ?

*Netsh interface tcp set global autotuninglevel=enabled*

- 2** Quel est le nom du protocole permettant d'optimiser le débit du côté de l'émission ?

*Compound TCP.*

- 3** Que signifie le terme **Black Hole** ?

*Pour des raisons de sécurité, certains routeurs détruisent les paquets fragmentés sans en avertir l'émetteur. Ils sont appelés routeurs Black Hole.*

- 4** Citez au moins trois problèmes pouvant être diagnostiqués à l'aide de l'infrastructure de diagnostics réseau.

*Vous pouvez citer :*

*Adresse IP incorrecte*

*Passerelle par défaut indisponible*

*Mauvaise passerelle par défaut*

*Problèmes de résolution de noms NetBIOS sur TCP/IP*

*Mauvaise configuration DNS*

*Port local déjà utilisé*

*Service client DHCP désactivé*

*Aucun écouteur distant*

*Média déconnecté*

*Port local bloqué*

*Peu de mémoire disponible*

*Support de statistiques TCP étendus (ESTATS)*

- 5** Citez les plages d'adresses provenant de la RFC1918.

*Vous pouvez citer :*

*10.0.0.0 à 10.255.255.255*

*172.16.0..0 à 172.31.255.255*

192.168.0.0 à 192.168.255.255

**6** Qu'est-ce qu'une adresse APIPA ?

*Il s'agit d'une adresse autoattribuée provenant de la plage **169.254.0.0/16** lorsque l'ordinateur n'arrive pas à contacter un serveur DHCP.*

**7** Citez une adresse de loopback en **IPv4** et en **IPv6**.

*Vous pouvez citer **127.0.0.1** et **::1**.*

8 Citez les types d'adresses que vous pouvez trouver en IPv6.

*Vous pouvez citer :*

**Adresse non spécifiée**

*Absence d'adresse IPv6 comme par exemple lorsque le nœud arrive sur le réseau et qu'il attend pour recevoir une adresse. Sa notation est **::/128**.*

**Adresse de bouclage**

*L'adresse de bouclage est **::1/128**.*

**Adresse multicast**

*Cette adresse commence toujours par **FF00 ::/8**.*

**Adresse de liaison locale unicast**

*Cette adresse commence toujours par **FE80 ::/10**.*

**Adresse globale unicast**

*Toutes les autres adresses.*

**Adresse anycast**

*Est prise dans l'espace d'adressage Unicast et ne peut syntaxiquement être distinguée par rapport à une adresse Unicast.*

**9** Citez une adresse de liaison locale.

*Vous pouvez citer toute adresse dont le préfixe commence par **FE80::/10**.*

**10** Quel est le préfixe d'une adresse Teredo ?

*Le préfixe commence par **200 ::/32**.*

**11** Sur un Server Core, comment configurez-vous une adresse IP ?

*En utilisant la commande **netsh**. Vous pouvez également créer des scripts en VBS.*

**12** Citez un avantage du routage dynamique.

*Si la topologie change, comme par exemple lorsqu'un routeur devient inaccessible, les routes s'adaptent automatiquement.*

**13** Citez au moins un avantage du protocole OSPF sur RIP.

*Il est plus adapté dans des grands environnements ou des environnements WAN.*

**14** Quel algorithme utilise protocole RIP ?

*RIP utilise un algorithme dit à vecteur de distance pour choisir la meilleure route.*

**15** Citez au moins une méthode pour afficher la table de routage locale d'un ordinateur.

*Vous pouvez citer la commande **route print** ou utiliser la console MMC routage et accès distant.*

### **Questions de compréhension**

**16** Indiquez si l'adresse IP 172.255.255.0/23 est valide.

*Oui.*

**17** Quel est le type de l'adresse IP 224.0.0.5 ?

*Il s'agit d'une adresse IPv4 de multidiffusion.*

**18** Quel est le type de l'adresse IP 192.168.1.255/24 ?

*Il s'agit d'une adresse IPv4 de diffusion locale. Soit la dernière adresse de la plage considérée.*

**19** Votre collègue ne comprend pas pourquoi votre serveur Windows 2008 est configuré avec des adresses IPv6. Vous lui répondez ?

*Par défaut les deux protocoles sont configurés.*

**20** Votre collègue vient de désactiver le protocole IPv6 à l'aide des propriétés de la carte réseau. Néanmoins il semble que le protocole soit toujours là. Que lui répondez-vous ?

*Pour désactiver le protocole IPv6, il faut modifier des clés dans le registre et non pas décocher la case **IPv6** dans les Propriétés de la carte.*

**21** Vous migrez le protocole IPv4 vers le protocole IPv6. Les segments 1 et 3 sont déjà migrés, néanmoins le

segment 2 se situant entre les segments 1 et 3 est encore sous IPv4. Quelle serait la plage d'adresses IPv6 pour ce scénario ?

*Vous pouvez utiliser des adresses 6to4 ou mieux les encapsuler avec Teredo.*

- 22** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Le routeur 2 permet également d'avoir accès à Internet. Votre collègue utilise un moniteur réseau et remarque un trafic double sur le segment 2 lorsque la destination est le segment 3 ou Internet. Quelle peut en être la cause ?

*L'adresse de la passerelle par défaut pour les ordinateurs du segment 2 est le routeur 1 qui ensuite doit rediriger les paquets vers le routeur 2.*

- 23** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Le routeur 2 permet également d'avoir accès à Internet. Des utilisateurs du segment 1 se plaignent qu'ils ne peuvent atteindre un serveur se trouvant sur le segment 3. Depuis votre station de travail du segment 2, vous parvenez à atteindre ledit serveur. Quelle peut en être la cause probable ?

*Le routeur 1 ne connaît pas la route pour aller vers le segment 3 ou le retour 2 ne connaît pas la route pour aller vers le segment 1. Il se peut aussi que la configuration de la passerelle par défaut de l'ordinateur du segment 1 soit incorrecte.*

- 24** Votre collègue doit effectuer un test qui demande de créer un réseau séparé mais accessible depuis votre poste de travail. Il propose d'utiliser un serveur 2008 et de configurer le protocole de routage RIP mais il n'est pas sûr que l'implémentation de RIP du serveur Microsoft soit compatible avec vos routeurs Cisco. Que lui répondez-vous ?

*Oui le protocole RIP est multivendeur. Cette configuration est possible.*

- 25** En dépannant un serveur, votre collègue a détecté une mauvaise configuration de l'adressage IP, soit l'adresse 169.254.56.34/16. Il veut la modifier, qu'en pensez-vous ?

*Le serveur DHCP n'est pas atteignable, c'est la raison pour laquelle le serveur a une adresse APIPA. Il vaut mieux comprendre pourquoi le serveur n'a pas reçu d'adresse provenant du serveur DHCP. Cela peut aller d'une indisponibilité du serveur DHCP au manque d'adresses pour la plage considérée en passant par un serveur DHCP non autorisé dans l'Active Directory, mais peut également indiquer un problème réseau ou de routage.*

### **Questions d'implémentation**

- 26** Votre fournisseur d'accès Internet vous attribue la plage d'adresses 82.54.255.64/30, quelles sont la première et la dernière adresse utilisables ainsi que le masque de sous-réseau ?

*Le masque de sous-réseau est 255.255.255.252 soit 4 adresses possibles dont 2 seulement sont utilisables, elles sont 80.54.255.65 et 80.54.255.66.*

- 27** Vous devez segmenter la plage d'adresses IP 192.168.8.0/23 de manière à créer un réseau ayant 200 adresses, un réseau ayant 66 adresses et un réseau ayant 32 adresses, comment faites-vous ?

*Une solution serait de définir les plages suivantes :*

*Plage 1, au minimum 200 adresses donc 254 adresses soit 192.168.8.0/24*

*Plage 2, au minimum 66 adresses donc 126 adresses soit 192.168.9.0/25*

*Plage 3, au minimum 32 adresses donc 62 adresses soit 192.168.9.128/26.*

- 28** Vous aimeriez permettre à vos ordinateurs, en cas de panne du serveur DHCP, de pouvoir au moins communiquer avec le serveur de fichiers et d'impression distant, comment feriez-vous ?

*Comme ils sont clients du serveur DHCP, vous remplissez les champs de la configuration alternative.*

- 29** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Le routeur 2 permet également d'avoir accès à Internet. Votre collègue décide d'implémenter le protocole RIP sans succès. Vous vérifiez la configuration et elle vous semble correcte mais aucun message RIP ne transite sur le segment 2. Quelle peut en être la cause ?

*Une cause fréquente de cette panne est l'activation du protocole RIP sur la mauvaise interface réseau.*

- 30** Votre collègue aimerait implémenter le protocole de routage RIP sur un Server Core, mais il ne sait pas comment procéder, comment pouvez-vous l'aider ?

*Ce n'est pas possible, il faut utiliser une installation complète.*

- 31** Votre réseau se compose de 3 segments et 2 routeurs. Les segments 1 et 2 sont reliés au routeur 1. Les segments 2 et 3 sont reliés au routeur 2. Sur le segment 2, vous disposez d'un serveur 2008 qui permet l'accès à Internet. Les utilisateurs du segment 2 peuvent accéder à Internet mais pas ceux des segments 1 et 3, quelle peut en être la cause ?

*Le serveur 2008 ne connaît pas les routes pour accéder aux segments 1 et 3.*

## Meilleures pratiques

Les recommandations suivantes devraient être prises en compte lors du déploiement d'un serveur DNS :

- Les serveurs DNS devraient être déployés sur des Server Core.
- Le rôle Serveur DNS devrait être installé sur un contrôleur de domaine afin de créer et d'utiliser des zones intégrées Active Directory.
- Protégez les zones DNS dans des emplacements peu sécurisés en utilisant des contrôleurs de domaine en lecture seule (RODC).
- Configurez les zones pour utiliser uniquement les mises à jour dynamiques sécurisées.
- Restreignez le transfert de zone en spécifiant le nom des serveurs DNS vers lesquels le transfert est autorisé, ou modifiez le type de zone afin d'utiliser des zones Intégrées Active Directory.
- Pour Internet utilisez un serveur DNS externe et pour un intranet utilisez un serveur DNS interne. Si le nom de domaine est identique entre intranet et Internet, ajoutez manuellement les quelques enregistrements définis dans le serveur externe sur le serveur interne. N'utilisez jamais le transfert de zone.
- Configurez le pare-feu afin de protéger les espaces de noms internes et les serveurs DNS internes.
- Activez la récursivité uniquement vers les serveurs DNS appropriés
- Assurez-vous que l'option avancée du serveur **Sécuriser le cache contre la pollution** est bien activée. Il utilise alors un mécanisme qui sécurise les caches des serveurs DNS contre des données malveillantes ou de réponses ne faisant pas autorité.
- Si vous utilisez un espace de noms privé, vérifiez que cet espace de noms est le domaine racine.

# **Validation des acquis : questions/réponses**

## **1. Questions**

### **Questions triviales**

- 1** Quelle est la taille maximale d'une partition NTFS supportée par Windows Server 2008 ?
- 2** Quel est le nouveau format de fichier introduit dans Windows Server 2008 ?
- 3** Qu'entend-on par NTFS transactionnel ?
- 4** Vous formatez un volume de 500 Go en NTFS, quelle est la taille du cluster disque ?
- 5** Quel est le nom générique pour permission NTFS ?
- 6** Quelle est la différence entre une ACE et une ACL ?
- 7** Que veut dire refus implicite ?
- 8** Existe-t-il une autorisation NTFS appelée Suppression ?
- 9** Est-il possible d'appliquer une autorisation aux sous-dossiers et fichiers seulement ?
- 10** Quel est le nom de l'utilitaire de type ligne de commandes pour gérer les autorisations NTFS ?
- 11** Que signifie audit pour le système de fichiers ?
- 12** Qu'est-ce qu'un chemin UNC ?
- 13** Comment peut-on cacher un partage ?
- 14** Existe-t-il une permission de partage appelé Ecriture ?
- 15** Pour des dossiers compressés, dans quels cas, les permissions NTFS de la source sont conservées ?
- 16** Combien de clichés instantanés peuvent être créés au maximum ?
- 17** Quel est le numéro de l'erreur rencontrée dans le journal indiquant qu'une tâche planifiée n'a pas pu s'exécuter ?
- 18** Comment un utilisateur peut-il voir un fichier stocké hors connexion ?
- 19** Est-il possible de permettre à plusieurs utilisateurs de consulter le même fichier chiffré ?
- 20** Que se passe-t-il lorsque vous copiez un dossier chiffré appelé A vers un dossier non chiffré dans le même volume ?
- 21** Quel est le nom de l'utilitaire de sauvegarde en ligne de commande ?
- 22** Quelle est la granularité pour la sauvegarde et la restauration avec l'utilitaire de sauvegarde fourni avec Windows ?
- 23** Citez au moins trois composantes faisant partie du rôle de services de fichiers.
- 24** Citez au moins deux différences entre les quotas NTFS et les quotas du rôle de services de fichiers.
- 25** Quelle est la différence entre les quotas et le filtrage des fichiers ?
- 26** À quoi servent les services pour NFS ?

### **Questions de compréhension**

- 27** Votre collègue met à jour un serveur Windows NT4 dont le système de fichiers est FAT vers NTFS, quelle commande pouvez-vous lui proposer pour effectuer la conversion ?
- 28** Un utilisateur vient de recevoir une clé USB d'une capacité de 64 Go. Il se plaint qu'il ne peut pas créer un volume supérieur à 32 Go. Il doit rester compatible avec des systèmes fonctionnant sous Linux. Comment pouvez-vous l'aider ?
- 29** Votre collègue ne comprend pas l'intérêt de défragmenter et d'utiliser des clusters disques adéquats. Que lui répondez-vous ?
- 30** Votre collègue ne comprend pas pourquoi les fichiers du dossier A ne peuvent être modifiés bien que les permissions NTFS soient correctes. Quelle pourrait en être la cause ?
- 31** Votre collègue effectue de la maintenance sur le serveur de fichiers. Pour cela il ajoute un nouveau disque qu'il formate en NTFS, ce disque est reconnu comme étant le volume E:. Ensuite, il déplace le contenu du volume D:

vers le volume E:. Maintenant les utilisateurs se plaignent qu'ils n'ont plus accès à certains fichiers.

- 32** Quelle est la permission résultante sur le document fichier.doc pour l'utilisateur Jean si les autorisations suivantes sont définies ?

<b>Utilisateur Jean fait partie de</b>	<b>Autres groupes</b>	<b>Autorisations sur le fichier</b>	
		<b>Autoriser</b>	<b>Refuser</b>
Jean			
Marketing		Modification	
Recherche et développement		Lecture	
	Support informatique		Écriture
	Développeurs	Modification	Lecture et exécution

- 33** Quelle est la permission résultante sur le document fichier.doc pour l'utilisatrice Tara si les autorisations suivantes sont définies ?

<b>Utilisatrice Tara fait partie de</b>	<b>Autres groupes</b>	<b>Autorisations sur le fichier</b>		<b>Autorisations héritées sur le fichier</b>	
		<b>Autoriser</b>	<b>Refuser</b>	<b>Autoriser</b>	<b>Refuser</b>
Tara		Modification			
Marketing					Lecture
Recherche et développement		Lecture			
	Support informatique		Ecriture		
ventes				Modification	

- 34** Quelle est la permission résultante sur le document fichier.doc pour l'utilisateur Richard si les autorisations suivantes sont définies ?

<b>Utilisateur Richard fait partie de</b>	<b>Autres groupes</b>	<b>Autorisations sur le fichier</b>		<b>Autorisations héritées sur le fichier</b>	
		<b>Autoriser</b>	<b>Refuser</b>	<b>Autoriser</b>	<b>Refuser</b>
Richard		Modification			
Marketing					Lecture
Recherche et développement		Lecture			
Support informatique				Ecriture	
ventes			Contrôle total		
	Direction	Contrôle total			

- 35** Quelle est la permission résultante sur le point de partage pour l'utilisateur Alain si les autorisations suivantes

sont définies ?

Utilisateur Alain fait partie de	Autres groupes	Autorisations NTFS sur le dossier		Autorisations NTFS héritées sur le dossier		Autorisations de partage	
		Autoriser	Refuser	Autoriser	Refuser	Autoriser	Refuser
Alain		Modification					
Marketing					Contrôle Total		
Recherche		Contrôle total					
Support informatique				Ecriture			
ventes			Contrôle total				
	Direction	Contrôle total					
Utilisateurs authentifiés						Modifier	

**36** Votre collègue aimerait activer les audits uniquement pour la base de registre et vous demande votre aide. Quelle serait votre proposition ?

**37** Votre collègue reçoit une demande d'un utilisateur qui aimerait comprendre pourquoi quand il déplace sur le même volume, certains fichiers compressés ils restent compressés et parfois pas. Que lui répondez-vous ?

#### **Questions de mise en œuvre**

- 38** Un administrateur junior a installé un serveur Windows Server 2008. Ensuite il a déplacé sur le stockage local les images du département Marketing. Des utilisateurs se plaignent que l'espace disque est manquant sur leur volume de travail. Après investigation, un de vos collègues a constaté que le format utilisé pour le volume des données est FAT. L'administrateur junior a alors supprimé le volume puis la recréé et l'a formaté en NTFS. Maintenant les utilisateurs se plaignent de ne pas trouver leurs images. Pourquoi ? Et quelle aurait dû être la bonne procédure ?
- 39** On vous demande de créer un dossier pour les utilisateurs de l'entreprise de manière à ce que tous les collaborateurs puissent créer et lire des documents mais que seul le collaborateur qui a créé le fichier puisse le modifier. Comment faites-vous ?

## **2. Résultats**

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /39

Pour ce chapitre, votre score minimum doit être de 29 sur 39.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

## **3. Réponses**

#### **Questions triviales**

- 1** Quelle est la taille maximale d'une partition NTFS supportée par Windows Server 2008 ?  
*4 To pour une partition MBR et 256 To pour une partition GPT.*

**2** Quel est le nouveau format de fichier introduit dans Windows Server 2008 ?

*ExFat.*

**3** Qu'entend-on par NTFS transactionnel ?

*Le NTFS transactionnel est une nouvelle fonctionnalité qui permet aux programmeurs de créer des transactions pour des opérations de copie ou déplacement de plusieurs fichiers et d'annuler ou d'approuver l'ensemble.*

**4** Vous formatez un volume de 500 Go en NTFS, quelle est la taille du cluster disque ?

*4 Ko.*

**5** Quel est le nom générique pour permission NTFS ?

*Une permission DACL (Discretionary Control List).*

**6** Quelle est la différence entre une ACE et une ACL ?

*Une ACE est un descripteur de sécurité qui définit une autorisation unitaire pour un utilisateur. Une ACL est un ensemble d'ACE.*

**7** Que veut dire refus implicite ?

*Un refus implicite signifie que l'utilisateur sans une autorisation explicite est refusé.*

**8** Existe-t-il une autorisation NTFS appelée Suppression ?

*Non, c'est une autorisation spéciale.*

**9** Est-il possible d'appliquer une autorisation aux sous-dossiers et fichiers seulement ?

*Oui avec les autorisations spéciales.*

**10** Quel est le nom de l'utilitaire de type ligne de commandes pour gérer les autorisations NTFS ?

*icalcs*

**11** Que signifie audit pour le système de fichiers ?

*L'audit enregistre les événements de tentatives d'accès en lecture, écriture, etc. dans le journal des événements. Les événements peuvent être limités en succès ou en échec.*

**12** Qu'est-ce qu'un chemin UNC ?

*UNC signifie Universal Naming Convention. Il s'agit d'un chemin basé sur la syntaxe suivante utilisé pour se connecter à un point de partage ou un serveur distant.*

*\NomServeur\NomDuPartage*

**13** Comment peut-on cacher un partage ?

*En ajoutant le caractère \$ à la fin du nom.*

**14** Existe-t-il une permission de partage appelé Ecriture ?

*Non, il faut utiliser la permission de modification pour disposer du droit d'écriture.*

**15** Pour des dossiers compressés, dans quels cas, les permissions NTFS de la source sont conservées ?

*Lors du déplacement au sein du même volume.*

**16** Combien de clichés instantanés peuvent être créés au maximum ?

*Un maximum de 64.*

**17** Quel est le numéro de l'erreur rencontré dans le journal indiquant qu'une tâche planifiée n'a pas pu s'exécuter ?

*L'erreur 7001.*

**18** Comment un utilisateur peut-il voir un fichier stocké hors connexion ?

*Une méthode consiste à ouvrir **Fichiers hors connexion** du panneau de configuration puis à cliquer sur **Afficher vos fichiers hors connexion**.*

**19** Est-il possible de permettre à plusieurs utilisateurs de consulter le même fichier chiffré ?

*Oui, seulement si le propriétaire du fichier vous a ajouté à la liste des utilisateurs pouvant accéder de manière transparente à ce fichier.*

**20** Que se passe-t-il lorsque vous copiez un dossier chiffré appelé A vers un dossier non chiffré dans le même volume ?

*Il reste chiffré.*

**21** Quel est le nom de l'utilitaire de sauvegarde en ligne de commande ?

*Wbadmin.*

**22** Quelle est la granularité pour la sauvegarde et la restauration avec l'utilitaire de sauvegarde fourni avec Windows ?

*Pour la sauvegarde, il s'agit du volume.*

*Pour la restauration, il s'agit du fichier.*

**23** Citez au moins trois composantes faisant partie du rôle de services de fichiers.

*Vous pouvez citer :*

- *Gestion du partage et du stockage.*
- *Système de fichiers distribués (DFS).*
- *Gestionnaire de ressources du serveur de fichiers (FSRM).*
- *Services pour NFS.*
- *Service de recherche Windows*
- *Service de fichiers Windows Server 2003.*

**24** Citez au moins deux différences entre les quotas NTFS et les quotas du rôle de services de fichiers.

*Vous pouvez citer :*

- *La granularité n'est plus un volume mais peut être un répertoire.*
- *Utilisation de modèles de quota.*
- *Différentes méthodes pour la notification.*
- *Differentes seuils d'avertissements.*

**25** Quelle est la différence entre les quotas et le filtrage des fichiers ?

*Le filtrage de fichiers ne sert pas à limiter l'espace disque utilisé comme les quotas mais il contrôle que seuls les types de fichiers autorisés sont placés sur le stockage.*

**26** À quoi servent les services pour NFS ?

*Ils permettent d'échanger des fichiers en utilisant le protocole NFS, principalement avec des ordinateurs sous Linux/Unix.*

### **Questions de compréhension**

**27** Votre collègue met à jour un serveur Windows NT4 dont le système de fichiers est FAT vers NTFS, quelle commande pouvez-vous lui proposer pour effectuer la conversion ?

*La commande convert <Lecteur :> /fs:ntfs.*

**28** Un utilisateur vient de recevoir une clé USB d'une capacité de 64 Go. Il se plaint qu'il ne peut pas créer un volume supérieur à 32 Go. Il doit rester compatible avec des systèmes fonctionnant sous Linux. Comment pouvez-vous l'aider ?

*NTFS n'est pas forcément un bon choix, il faudrait plutôt utiliser ExFat.*

**29** Votre collègue ne comprend pas l'intérêt de défragmenter et d'utiliser des clusters disques adéquats. Que lui répondez-vous ?

*Un fichier est stocké dans des clusters. Ces derniers ne sont pas forcément contigus sur le disque. Il est donc nécessaire de régulièrement modifier leur emplacement afin qu'ils soient si possible contigus pour diminuer le temps de lecture ou d'écriture du fichier.*

*Concernant les clusters, leur taille dépend des documents ou des applications. Si l'on a beaucoup de petits fichiers, plus petits que 4 Ko, il est nécessaire de disposer de clusters de petite taille afin de diminuer l'espace perdu inutilement. Dans d'autres cas, comme par exemple avec SQL Server, une taille de cluster de 8 Ko semble plus judicieuse.*

**30** Votre collègue ne comprend pas pourquoi les documents situés dans le dossier A ne peuvent être modifiés bien que les permissions NTFS soient correctes. Quelle pourrait en être la cause ?

*L'attribut en lecture seule est appliquée. Il ne dépend pas des permissions NTFS mais des propriétés du fichier.*

**31** Votre collègue effectue de la maintenance sur le serveur de fichiers. Pour cela il ajoute un nouveau disque qu'il formate en NTFS, ce disque est reconnu comme étant le volume E:. Ensuite, il déplace le contenu du volume D: vers le volume E:. Maintenant les utilisateurs se plaignent qu'ils n'ont plus accès à certains fichiers.

*Les permissions NTFS ont été perdues car on hérite des permissions du dossier de destination parce que les volumes source et cible sont différents.*

**32** Quelle est la permission résultante sur le document fichier.doc pour l'utilisateur Jean si les autorisations suivantes sont définies ?

<b>Utilisateur Jean fait partie de</b>	<b>Autres groupes</b>	<b>Autorisations sur le fichier</b>	
		<b>Autoriser</b>	<b>Refuser</b>
Jean			
Marketing		Modification	
Recherche et développement		Lecture	
	Support informatique		Écriture
	Développeurs	Modification	Lecture et exécution

*Jean a les autorisations en modification et lecture donc la résultante est Modification.*

**33** Quelle est la permission résultante sur le document fichier.doc pour l'utilisatrice Tara si les autorisations suivantes sont définies ?

<b>Utilisatrice Tara fait partie de</b>	<b>Autres groupes</b>	<b>Autorisations sur le fichier</b>		<b>Autorisations héritées sur le fichier</b>	
		<b>Autoriser</b>	<b>Refuser</b>	<b>Autoriser</b>	<b>Refuser</b>
Tara		Modification			
Marketing					Lecture
Recherche et développement		Lecture			
	Support informatique		Ecriture		
ventes				Modification	

*Tara a :*

- *Les autorisations NTFS en modification et lecture donc la résultante est Modification.*
- *Les autorisations héritées échec en Lecture et autorisation en Modification donc la résultante est Ecriture.*
- *La résultante NTFS pour le fichier est donc Modification.*

**34** Quelle est la permission résultante sur le document fichier.doc pour l'utilisateur Richard si les autorisations suivantes sont définies ?

<b>Utilisateur Richard fait partie de</b>	<b>Autres groupes</b>	<b>Autorisations sur le fichier</b>		<b>Autorisations héritées sur le fichier</b>	
		<b>Autoriser</b>	<b>Refuser</b>	<b>Autoriser</b>	<b>Refuser</b>
Richard		Modification			
Marketing					Lecture
Recherche et développement		Lecture			

Support informatique				Ecriture	
ventes			Contrôle total		
	Direction	Contrôle total			

Richard a :

- Les autorisations NTFS en Modification et Lecture, et en échec Contrôle total, donc la résultante est Refuser Contrôle total.
- Les autorisations héritées en échec Lecture, et autorisation Ecriture donc la résultante est Ecriture en autorisation et Refuser en lecture.
- La résultante NTFS pour le fichier est donc Refuser en Contrôle total.

**35** Quelle est la permission résultante sur le point de partage pour l'utilisateur Alain si les autorisations suivantes sont définies ?

Utilisateur Alain fait partie de	Autres groupes	Autorisations NTFS sur le dossier		Autorisations NTFS héritées sur le dossier		Autorisations de partage	
		Autoriser	Refuser	Autoriser	Refuser	Autoriser	Refuser
Alain		Modification					
Marketing					Contrôle Total		
Recherche		Contrôle total					
Support informatique				Ecriture			
Ventes			Contrôle total				
	Direction	Contrôle total					
Utilisateurs authentifiés						Modifier	

Alain dispose des permissions suivantes :

Étape 1 : affichez les groupes et les utilisateurs qui reçoivent pour la ressource et donné dans par le tableau de la question.

Étape 2 : déterminez de quels groupes l'utilisateur est membre et notez leurs autorisations en différenciant les autorisations explicites et les autorisations héritées :

- **Autorisation explicite**

Groupe Recherche Autoriser en contrôle total.

Groupe Ventes Refuser en contrôle total.

- **Autorisation héritée**

Groupe Marketing Refuser en contrôle total

Groupe Support informatique Autoriser en écriture

*Étape 3 : notez les autorisations affectées directement pour l'utilisateur. Pour Alain, Autoriser en modification.*

*Étape 4 : en utilisant le résultat des étapes 2 et 3, déterminez la résultante des autorisations héritées. La résultante pour les autorisations héritées est Refuser en contrôle total.*

*Étape 5 : en utilisant le résultat des étapes 2 et 3, déterminez la résultante des autorisations explicites. La résultante des autorisations explicites est Autoriser en Lecture et exécution et Lecture et Refusé en Ecriture.*

*Étape 6 : il faut commencer par déterminer la résultante des permissions NTFS qui correspond à la résultante des permissions explicites et des permissions héritées soit dans notre cas Autoriser en Lecture et exécution. Concernant le partage, la permission résultante du partage est Autoriser pour le groupe Utilisateurs authentifiés. Enfin la résultante du point du partage est donc uniquement Autoriser en Lecture et exécution et Lecture et Refusé en Ecriture (c'est la résultante la plus restrictive qui l'emporte entre la résultante NTFS et la résultante du partage).*

- 36** Votre collègue aimerait activer les audits uniquement pour la base de registre et vous demande votre aide. Quelle serait votre proposition ?

*Pour obtenir une granularité plus fine qu'avec les stratégies de groupes et de l'accès aux objets, il faut utiliser la commande auditpol.*

- 37** Votre collègue reçoit une demande d'un utilisateur qui aimerait comprendre pourquoi quand il déplace sur le même volume, certains fichiers compressés ils restent compressés et parfois pas. Que lui répondez-vous ?

*Certains fichiers sont compressés en utilisant la compression NTFS et d'autres doivent l'être en utilisant la compression zip. La compression ZIP est indépendante des attributs de compression du système de fichiers.*

### **Questions de mise en œuvre**

- 38** Un administrateur junior a installé un serveur Windows Server 2008. Ensuite il a déplacé sur le stockage local les images du département Marketing. Des utilisateurs se plaignent que l'espace disque est manquant sur leur volume de travail. Après investigation, un de vos collègues a constaté que le format utilisé pour le volume des données est FAT. L'administrateur junior a alors supprimé le volume puis la recréé et l'a formaté en NTFS. Maintenant les utilisateurs se plaignent de ne pas trouver leurs images. Pourquoi ? Et quelle aurait dû être la bonne procédure ?

*Les données ont été supprimées lorsque le volume a été détruit.*

*Il aurait fallu effectuer une conversion en NTFS puis étendre le volume.*

- 39** On vous demande de créer un dossier pour les utilisateurs de l'entreprise de manière à ce que tous les collaborateurs puissent créer et lire des documents mais que seul le collaborateur qui a créé le fichier puisse le modifier. Comment faites-vous ?

*Il faut utiliser les groupes spéciaux de la manière suivante :*

*Utilisateurs authentifiés autorisés en lecture et Ecriture.*

*Créateur propriétaire en modification.*

## Résumé du chapitre

Dans ce chapitre, vous avez vu la mise en œuvre d'un système de fichiers d'abord en examinant les concepts et les outils traditionnels pour gérer les permissions NTFS, les points et permissions de partage, la compression, les quotas, les fichiers hors connexion et le chiffrage EFS.

Le nouvel outil de sauvegarde a été présenté et ses avantages ont été mis en avant.

Enfin, le rôle de serveur de fichiers et ses outils modulaires et centralisés ont été présentés.

## Travaux pratiques

Dans les travaux pratiques pour l'exercice 12, vous devrez effectuer les opérations suivantes :

- Configurations d'autorisations NTFS et de partage.
- Mise en œuvre des clichés instantanés.
- Mise en œuvre des fichiers hors connexion.
- Mise en œuvre d'EFS.
- Mise en œuvre de la sauvegarde.
- Mise en œuvre du serveur de fichiers.
- Mise en œuvre de DFS.
- Mise en œuvre des quotas.

# Rôle de serveur de fichiers

## 1. Introduction

Le serveur de fichiers est un emplacement central sur votre réseau où les utilisateurs peuvent stocker des documents. La gestion par des administrateurs peut s'effectuer à distance grâce à des outils spécialement adaptés et la granularité des services qui peuvent être proposés dépend des besoins des utilisateurs. Ces services sont réunis dans les consoles suivantes :

- **Gestion du partage et du stockage.** Cet utilitaire permet la gestion centralisée des partages, des autorisations de partages, des permissions NTFS des points de partage et la gestion du stockage. Enfin, il est possible de gérer les utilisateurs connectés et les fichiers ouverts.
- **Système de fichiers distribués** ou **DFS** pour *Distributed File System*. Elle offre la possibilité de créer une arborescence logique dont les partages peuvent se trouver physiquement sur différents serveurs.
- **Gestionnaire de ressources du serveur de fichiers** ou **FSRM** pour *File System Resources Manager* regroupe un ensemble d'utilitaires pour contrôler et gérer la quantité et le type de données sur un serveur.
- **Services pour NFS** installe le client et le serveur pour le protocole NFS (*Network File System*).
- **Service de recherche Windows** est une nouvelle solution de création d'index plus efficace et évolutive que le service d'indexation de Windows 2003.
- **Service de fichiers Windows Server 2003** permet une compatibilité descendante avec les serveurs 2003.

Les outils complémentaires sont les suivants :

- **Sauvegarde de Windows Server**, le nouvel outil de sauvegarde présenté dans la section précédente.
- **Gestionnaire de stockage pour réseau SAN**, outil permettant de gérer des sous-systèmes de stockage Fibre Channel ou iSCSI dans un réseau SAN.
- **Clustering avec basculement**, fonctionnalité qui permet d'installer et de configurer des systèmes hautement disponibles.
- **MPIO (Multipath I/O)**, permettant la prise en charge de plusieurs chemins d'accès entre le serveur et les périphériques de stockage.

## 2. Installation du rôle de serveur de fichiers



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans le volet gauche du **Gestionnaire de serveur**, cliquez sur **Rôles**.
- Dans la fenêtre centrale, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** apparaît dans l'assistant **Ajout de rôles**, cliquez sur **Suivant**.

- Sur la page **Rôles de serveurs de l'assistant**, sélectionnez **Services de fichiers** puis cliquez sur **Suivant**.
- Sur la page **Services de fichiers**, consultez les informations avant de cliquer sur **Suivant**.
- Sur la page **Services de rôles**, sélectionnez éventuellement d'autres services de rôles puis cliquez sur **Suivant**.
- Sur la page **Confirmation**, contrôlez vos paramètres avant de cliquer sur **Installer**.
- Sur la page **Résultats**, vérifiez que l'installation est réussie avant de cliquer sur **Fermer**.

 L'utilitaire Gestionnaire de ressources du serveur de fichiers ne peut gérer que des ordinateurs exécutant Windows Server 2008 ou ultérieur ayant le rôle installé.

### 3. Utilitaire Gestion du partage et du stockage



Avec cet outil, vous pouvez gérer les partages, les permissions NTFS et le stockage sur l'ordinateur local ou un ordinateur distant. Il remplace avantageusement les outils présentés précédemment dans le chapitre.

 Sur un serveur contrôleur de domaine, l'utilitaire **Gestion du partage et du stockage** est installé bien que le rôle ne le soit pas !

Ce sous-rôle n'existe pas sur un Server Core.

Pour l'ouvrir, utilisez la procédure suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestion du partage et du stockage**.

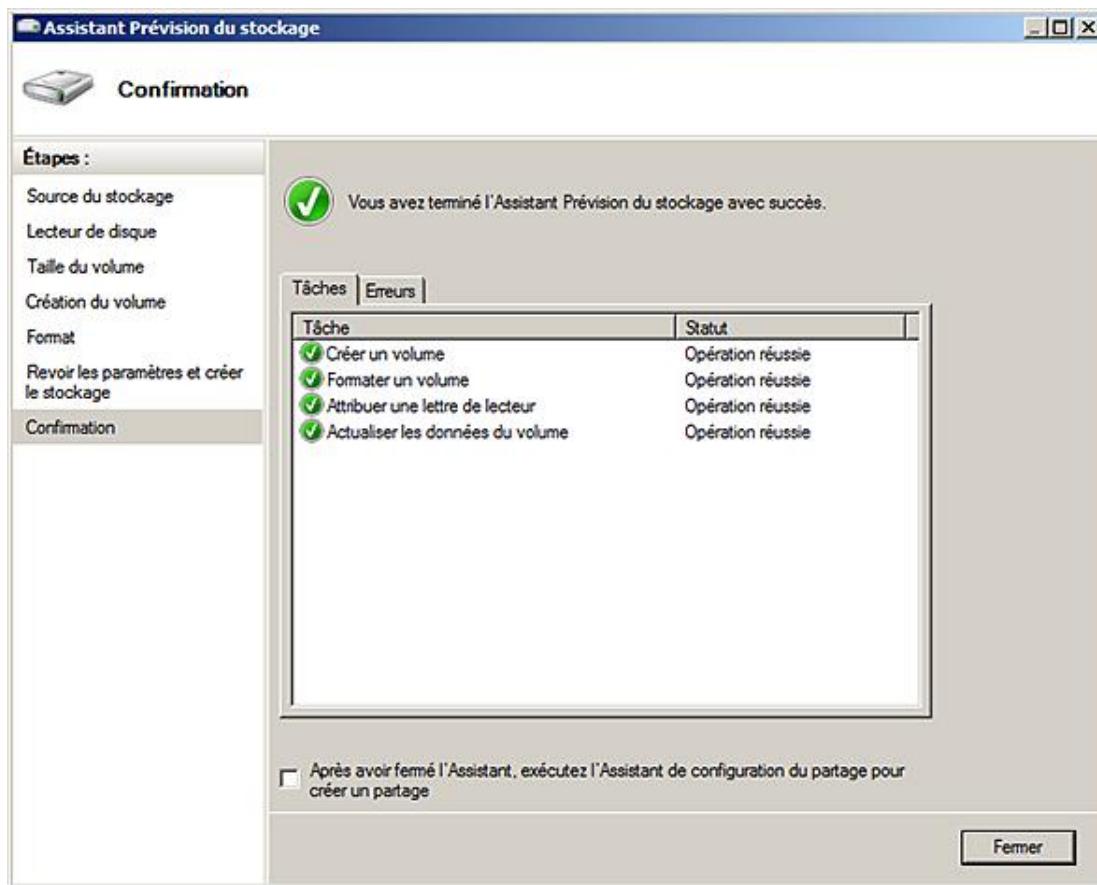
#### a. Prévoir le stockage

- Ouvrez la console **Gestion du partage et du stockage**.
- Dans le volet de droite, cliquez sur l'action **Prévoir le stockage**.
- Sur la page **Source du stockage** de l'assistant, sélectionnez une des options proposées avant de cliquer sur **Suivant**. L'option **Sur un ou plusieurs disques disponibles sur ce serveur** fait référence à un espace non alloué local alors que la seconde option fait référence à un numéro d'unité logique rattachée au serveur, pour autant qu'il dispose d'un espace non alloué et qu'un fournisseur de matériel **VDS** (*Virtual Disk Service*) est installé. VDS, introduit avec Windows Server 2003, est un protocole de type DCOM qui permet une gestion de la configuration uniformisée et simplifiée des disques NAS (*Network Attached System*), des SAN, des systèmes iSCSI, et des systèmes de stockage direct.

 Lorsque vous ajoutez un nouveau disque à votre serveur, Il faut l'initialiser avant de pouvoir utiliser l'assistant !

- Sur la page **Lecteur de disque**, sélectionnez le disque désiré puis cliquez sur **Suivant**.
- Sur la page **Taille du volume**, sélectionnez la taille désirée pour le nouveau volume puis cliquez sur **Suivant**.

- Sur la page **Création du volume**, spécifiez la lettre du lecteur ou un point de montage avant de cliquer sur **Suivant**.
- Sur la page **Format**, désélectionnez la case à cocher correspondante si vous ne voulez pas formater le volume sinon indiquez le nom du volume ; vous pouvez éventuellement modifier la taille d'unité d'allocation et demander un formatage rapide avant de cliquer sur **Suivant**. Notez que vous ne pouvez formater qu'en NTFS.
- Sur la page **Revoir les paramètres et créer le stockage**, contrôlez que les paramètres sont corrects avant de cliquer sur **Créer**.
- Enfin sur la page **Confirmation**, vérifiez que toutes les tâches se sont terminées avec succès, sinon consultez l'onglet **Erreurs**. Vous pouvez lancer directement l'**Assistant de configuration du partage** en sélectionnant la case à cocher avant de cliquer sur **Fermer**.



## b. Prévoir le partage

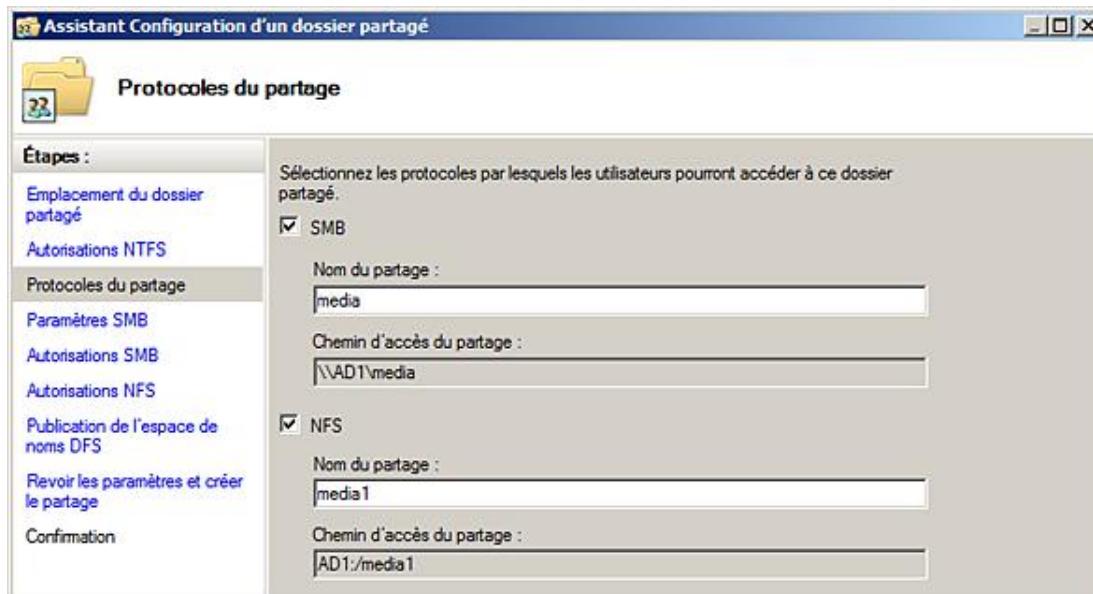
- Ouvrez la console **Gestion du partage et du stockage**.
- Dans le volet de droite, cliquez sur l'action **Prévoir le partage**. La fenêtre **Assistant Configuration d'un dossier partagé** s'ouvre.

Notez que la section **Détails** affiche des informations pratiques sur le disque sélectionné.

Vous pouvez également lancer l'assistant **Prévoir le stockage** à partir de cette fenêtre.

- Sur la page **Emplacement du dossier partagé**, cliquez sur **Parcourir** pour sélectionner un dossier à partager, puis cliquez sur **OK**.
- Sur la page **Autorisations NTFS**, vous pouvez éventuellement modifier les autorisations NTFS avant de cliquer sur **Suivant**.

- Sur la page **Protocoles du partage**, vous pouvez décider quels seront les protocoles utilisés par les ordinateurs clients pour accéder à ce partage : SMB (*Server Message Block*) pour les ordinateurs clients Windows ou SAMBA, une implémentation SMB Open Source, soit NFS (*Network File System*) pour les ordinateurs clients Unix si le rôle de services NFS est installé sur le serveur. Cliquez ensuite sur **Suivant**. L'écran suivant montre la page de l'assistant pour un serveur dont le service NFS est installé. Notez que le nom de partage des deux protocoles doit être différent.



- Sur la page **Paramètres SMB**, vous pouvez saisir une description pour le partage. La section **Paramètres avancés** affiche les valeurs des paramètres suivants que vous pouvez modifier en cliquant sur le bouton **Avancé** :
  - Le **nombre maximal d'utilisateurs** pouvant se connecter simultanément.
  - L'**activation de l'énumération basée sur l'accès**, c'est-à-dire l'application d'un filtre cachant le partage si l'utilisateur n'a pas une permission de partage en lecture.
  - La méthode spécifiée pour la **mise en cache**.

Ensuite, cliquez sur **Suivant**.

- Sur la page **Autorisations SMB**, vous pouvez spécifier les permissions du point de partage, comme montré dans les sections précédentes. Ensuite, cliquez sur **Suivant**.
- Si vous avez activé le protocole NFS pour le partage, une page spécifique permet de gérer les **Autorisations NFS**. Cliquez sur **Suivant**.
- Sur la page **Publication de l'espace de noms DFS**, vous pouvez ajouter ce partage à un espace de noms DFS existant localement ou sur le réseau (défaut) en tapant le chemin UNC du dossier parent et le nom du dossier de partage ou désélectionner l'option. Cliquez sur **Suivant**.
- Sur la page **Revoir les paramètres et créer le partage**, contrôlez que les paramètres sont corrects avant de cliquer sur **Créer**.
- Enfin sur la page **Confirmation**, vérifiez que toutes les tâches se sont terminées avec succès, sinon consultez l'onglet **Erreurs**. Vous pouvez lancer directement l'**Assistant de configuration du partage** en sélectionnant la case à cocher avant de cliquer sur **Fermer**.

### c. Gérer les sessions

- Ouvrez la console **Gestion du partage et du stockage**.

- Dans le volet droit, cliquez sur l'action **Gérer les sessions**.

Il vous est possible de sélectionner un ou plusieurs utilisateurs afin de fermer leur session, de fermer toutes les sessions et d'actualiser la liste des utilisateurs connectés.

- Lorsque vous fermez une session, le message d'avertissement suivant apparaît. Prenez le temps de le lire avant d'éventuellement poursuivre votre action.



#### d. Gérer les fichiers ouverts

- Ouvrez la console **Gestion du partage et du stockage**.
- Dans le volet droit, cliquez sur l'action **Gérer les fichiers ouverts**.

Il est possible de sélectionner un ou plusieurs utilisateurs afin de fermer certains de leurs fichiers ouverts, de fermer tous les fichiers ouverts et d'actualiser la liste des fichiers ouverts.

Le même message d'avertissement que pour la fermeture de session apparaît.

- Il est à regretter que l'on visualise le nom des dossiers contenant des fichiers ouverts et non celui des fichiers, ce qui peut rendre le travail difficile pour un administrateur lorsqu'un utilisateur a plusieurs fichiers ouverts dans le même dossier.

#### e. Gérer les partages

En utilisant la fenêtre principale, les **actions** suivantes sont disponibles si vous sélectionnez un partage existant :

- **Cesser de partager** supprime le ou les partages sélectionnés.
- **Propriétés** affiche une boîte de dialogue pour gérer les **Propriétés** du protocole SMB comme décrit dans la section sur l'assistant **Prévoir le partage**.
- **Modifier la configuration NFS**. Bien que cette action soit globale du fait qu'elle apparaît dès que le service NFS est installé et configuré, elle est placée ici car elle permet de gérer la configuration NFS sans utiliser l'utilitaire Services NFS.

#### f. Gérer les volumes

En utilisant la fenêtre principale, les **actions** suivantes sont disponibles si vous sélectionnez un volume existant :

- **Étendre** permet d'étendre un volume sur le même disque. Pour étendre un volume sur des disques différents, utilisez le Gestionnaire de disques.
- **Formater** affiche la boîte de dialogue de formatage de l'Explorateur.

- **Propriétés** affiche la boîte de dialogue **Propriétés** de l'Explorateur.

## 4. Service DFS

Le service DFS permet de créer et de gérer un espace de noms dont l'arborescence logique est rattachée à sur un serveur ou un domaine alors que l'arborescence physique, soit les dossiers de partage appelés cibles, peut se trouver sur différents serveurs de l'entreprise.

Un des grands intérêts d'un système DFS est la possibilité de gérer dynamiquement à l'aide de scripts les dossiers et les cibles pour créer l'arborescence logique la plus adaptée aux besoins de l'entreprise.

Un autre intérêt est l'utilisation d'un espace de noms de domaine afin de pouvoir stocker les mêmes données sur plusieurs serveurs, offrir un système hautement disponible et équilibrer la charge en fonction des besoins de partage de l'information.

L'ordinateur client reçoit une copie de l'arborescence logique qu'il conserve en cache pendant une durée définie ; de cette manière, il sait exactement où se trouve le dossier partagé recherché.

- 
- Il est possible d'installer le service du rôle DFS sur un Server Core.
- 

### a. Installation du service de rôle DFS



Procédez comme suit :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans le volet gauche du Gestionnaire de serveur, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de fichiers** pour faire apparaître les informations correspondantes dans la fenêtre centrale.
- Dans la fenêtre centrale, cliquez sur **Ajouter des services de rôles**.
- Sur la page **Sélectionner les services de rôle** de l'assistant, sélectionnez **Système de fichiers distribués (DFS)** puis cliquez sur **Suivant**.
- Sur la page **Espace de noms DFS**, vous pouvez choisir de construire un espace de noms ou de le créer ultérieurement. Dans le second cas, vous passez directement à la page de **Confirmation**. Cliquez sur **Suivant**.
- Sur la page **Type d'espace de noms**, vous pouvez créer soit un espace de noms de domaine, soit un espace de noms autonome. Il faut être dans un domaine pour pouvoir créer un espace de noms de domaine. Pour l'espace de noms de domaine, vous pouvez également activer le mode Windows Server 2008 qui prend en charge l'ennumération basée sur l'accès si vous disposez d'un niveau fonctionnel de domaine Windows Server 2008 et que tous les serveurs d'espaces de noms exécutent Windows Server 2008. Cliquez sur **Suivant**.

- 
- Il ne peut y avoir qu'un espace de noms de domaine par domaine alors que le nombre d'espaces de noms de serveur n'est pas limité.
- 

- Sur la page **Configurer l'espace de noms**, vous pouvez ajouter des dossiers et des cibles de dossier à votre arborescence. Cliquez ensuite sur **Suivant**.
- Sur la page **Confirmation**, contrôlez vos paramètres avant de cliquer sur **Installer**.

- Sur la page **Résultats**, vérifiez que l'installation est réussie avant de cliquer sur **Fermer**.

## b. Ouverture de la console Gestion du système de fichiers distribués DFS

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire du système de fichiers distribués DFS**.

Vous pouvez gérer les espaces de noms et la réPLICATION.

## c. Ajout d'un dossier

- Dans le volet de gauche de la console **Gestion du système de fichiers distribués DFS**, déplacez-vous vers le niveau considéré d'un espace de noms sous lequel vous voulez ajouter un dossier.
- Dans le volet de droite, cliquez sur **Nouveau dossier**.
- Dans la boîte de dialogue **Nouveau dossier**, saisissez le nom du dossier tel qu'il apparaîtra à l'utilisateur puis ajoutez le chemin UNC de la cible et enfin cliquez sur **OK**.

## d. La réPLICATION

La réPLICATION utilise actuellement la réPLICATION DFS au lieu de la réPLICATION FRS. La réPLICATION DFS se base sur l'algorithme de compression RDC qui détecte les modifications des données à la volée et réplique des blocs et non des fichiers entiers.



Vous pouvez gérer le système DFS à l'aide des commandes DfsUtil, DfsCmd, DfsrAdmin et DfsrDiag.

## 5. Gestionnaire de ressources du serveur de fichiers



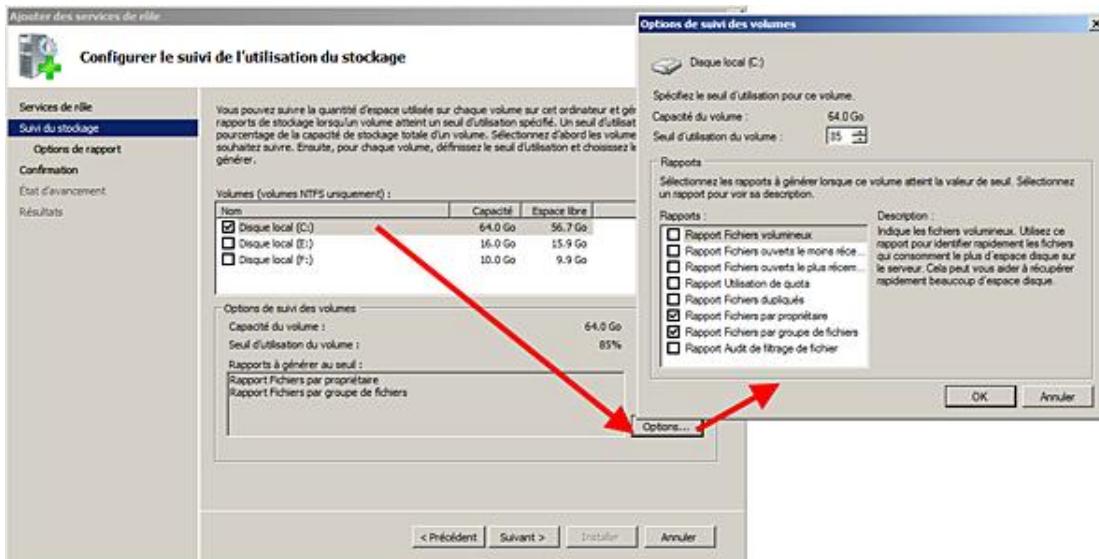
Win

Ce service de rôle regroupe un ensemble d'outils, comme la notification par e-mail lorsqu'un seuil d'utilisation de l'espace de stockage est atteint, qu'il faut déjà configurer à l'installation du service de rôle. Ce service de rôle n'est pas disponible sur un Server Core.

### a. Installation du service de rôle Gestionnaire de ressources du serveur de fichiers

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans le volet gauche du Gestionnaire de serveur, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de fichiers** pour faire apparaître les informations correspondantes dans la fenêtre centrale.
- Dans la fenêtre centrale, cliquez sur **Ajouter des services de rôles**.
- Sur la page **Sélectionner les services de rôle** de l'assistant, sélectionnez **Gestion de ressources du serveur de fichiers** puis cliquez sur **Suivant**.

- Sur la page **Configurer le suivi et l'utilisation du stockage**, pour chaque disque dont vous voulez contrôler l'utilisation, sélectionnez les informations de stockage en cliquant sur **Options** puis en indiquant un **Seuil d'utilisation du volume** (85 % défaut), c'est-à-dire le niveau d'avertissement pour la gestion des quotas et la création des rapports. Cliquez sur **Suivant**.



- Sur la page **Options de rapport**, indiquez l'emplacement où vous voulez stocker les rapports et, si vous voulez les recevoir par courrier électronique, saisissez les adresses des destinataires et l'adresse du serveur SMTP à utiliser. Notez que le serveur doit pouvoir être atteint lors de la configuration. D'autre part, il faut utiliser un compte d'utilisateur disposant des droits pour envoyer les messages avec SMTP. Enfin, cliquez sur **Suivant**.
- Sur la page **Confirmation**, contrôlez que les paramètres sont corrects avant de cliquer sur **Installer**.
- Attendez que la page **Résultats** s'affiche pour savoir si l'installation a réussi puis cliquez sur **Fermer**.

## b. Configuration du Gestionnaire de ressources du serveur de fichiers

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de ressources du serveur de fichiers**.



Vous pouvez vous connecter à un autre ordinateur à partir de cette console.

- Dans le volet de droite, cliquez sur **Configurer les options**.

Une boîte de dialogue comprenant cinq onglets apparaît :

- L'onglet **Notifications par courrier électronique** vous permet de définir le serveur de messagerie SMTP, les destinataires pour la notification par messagerie électronique et l'adresse de messagerie de l'expéditeur.
- L'onglet **Limites de notification** indique l'intervalle minimal avant de renvoyer une notification en cas de dépassement répété d'un quota ou de détection d'un fichier non autorisé. Ceci afin de diminuer le nombre de notifications émises.

Vous pouvez définir ces limites de notifications pour les envois par courrier électronique, le journal des événements, les commandes et les rapports. Par défaut, la même limite est appliquée à tous les types et elle est de 60 mn.

- L'onglet **Rapports de stockage** permet de configurer les paramètres par défaut pour chaque type de

rapport.

- L'onglet **Emplacement des rapports** permet de définir l'emplacement de stockage des rapports d'incidents (%systemdrive%\StorageReports\Incident), des rapports planifiés (%systemdrive%\StorageReports\Scheduled) et des rapports à la demande (%systemdrive%\StorageReports\Interactive).
- L'onglet **Vérification du filtrage de fichiers** permet d'enregistrer ou non l'activité du filtrage dans une base de données qui pourra être consultée avec un rapport de vérification du filtrage des fichiers.



L'utilitaire **starept admin** permet de configurer le Gestionnaire de ressources du serveur de fichiers.

## 6. Gestion des quotas

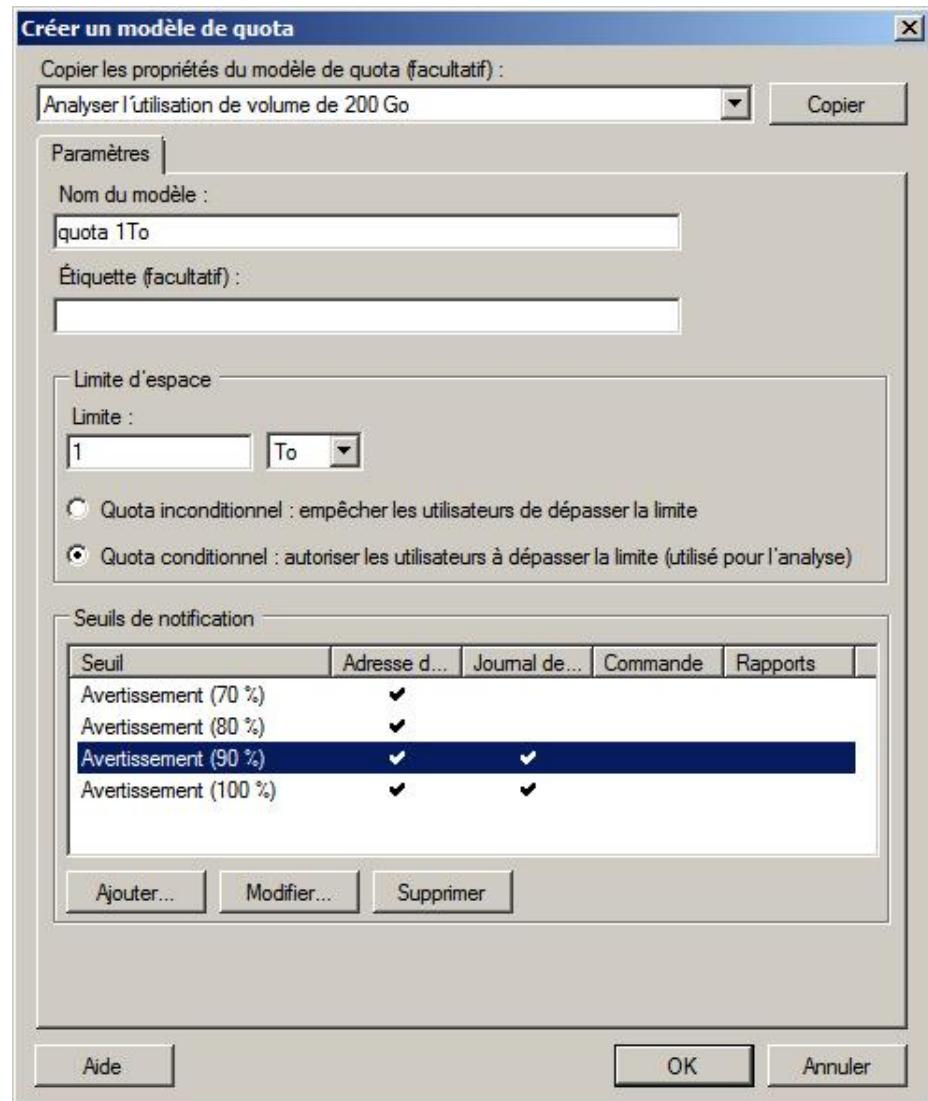


La gestion des quotas fonctionne un peu différemment des quotas NTFS car ici la granularité est le chemin d'accès, soit le dossier ou le volume.

Il faut commencer par définir des modèles de quota que l'on appliquera aux quotas.

La procédure suivante montre comment créer un modèle de quota.

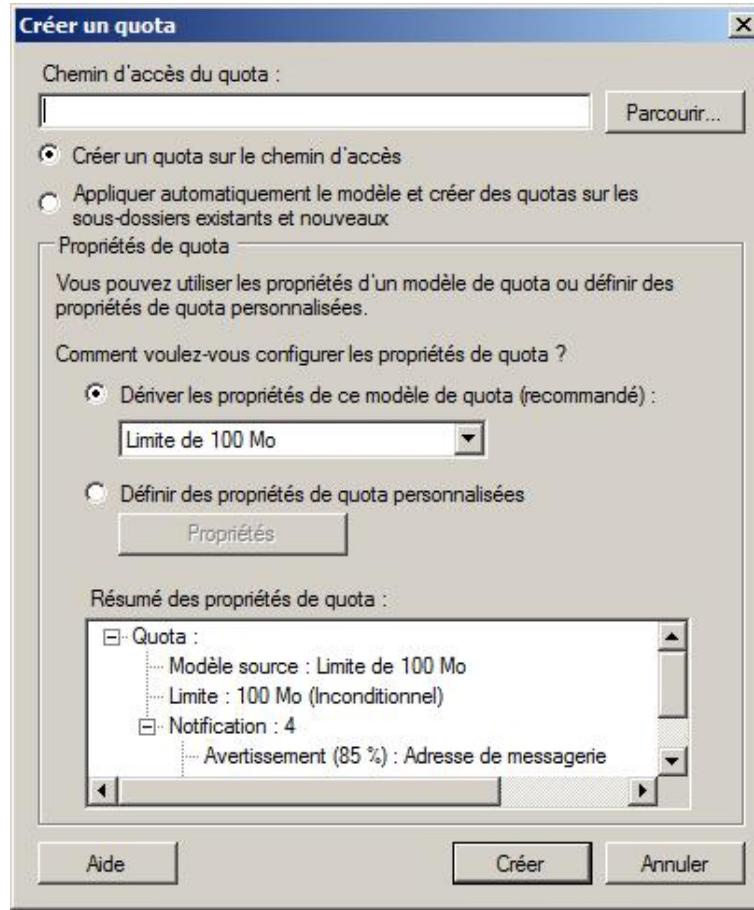
- Ouvrez le **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur **Modèles de quotas**.
- Dans le volet de droite, cliquez sur **Créer un modèle de quota**.



- Dans la boîte de dialogue **Créer un modèle de quota**, saisissez les informations du quota en vous aidant éventuellement d'un modèle de quota existant. Le quota est soit **inconditionnel**, c'est-à-dire qu'il empêche les utilisateurs de dépasser la limite, soit **conditionnel**, l'intérêt de ce type de quota étant de créer des rapports dans le but d'analyser le comportement des utilisateurs.
- Vous pouvez définir plusieurs seuils d'avertissement, disposant chacun d'une ou de plusieurs méthodes de notifications, en cliquant sur les boutons **Ajouter** ou **Modifier**.
- Enfin, cliquez sur **OK**.

Ensuite, vous pouvez créer le quota en suivant cette procédure :

- Ouvrez le **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur **Quotas**.
- Dans le volet de droite, cliquez sur **Créer un quota**.



- Indiquez le chemin d'accès au quota, soit un dossier, soit un volume, indiquez la portée du quota et ses propriétés soit en utilisant un modèle prédéfini (recommandé), soit en le personnalisaient. Cliquez ensuite sur **Créer**.



Pour une gestion via la ligne de commande, il faut utiliser l'utilitaire **dir quota**.

## 7. Gestion du filtrage de fichiers (*file screening*)



Win

Comme les quotas, le filtrage des fichiers permet de définir quels types de fichiers il est possible de stocker sur un dossier ou un volume. Le fonctionnement est identique à la gestion des quotas. Soit vous utilisez le filtrage pour l'analyse, soit vous l'utilisez pour bloquer des types de fichiers ou des fichiers non autorisés.

Ce sous-rôle n'est pas disponible sur un Server Core.

Le filtrage se fait sur les extensions des fichiers en constituant des groupes de fichiers comme le montre la procédure suivante :

- Ouvrez le **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur le nœud **Gestion du filtrage de fichiers**.
- Cliquez sur **Groupes de fichiers**. Les groupes déjà définis apparaissent dans la fenêtre centrale.
- Dans le volet de droite, cliquez sur **Créer un groupe de fichiers**.
- Saisissez le **Nom du groupe de fichiers** et les extensions ou les noms à inclure et/ou à exclure puis cliquez sur **OK**.

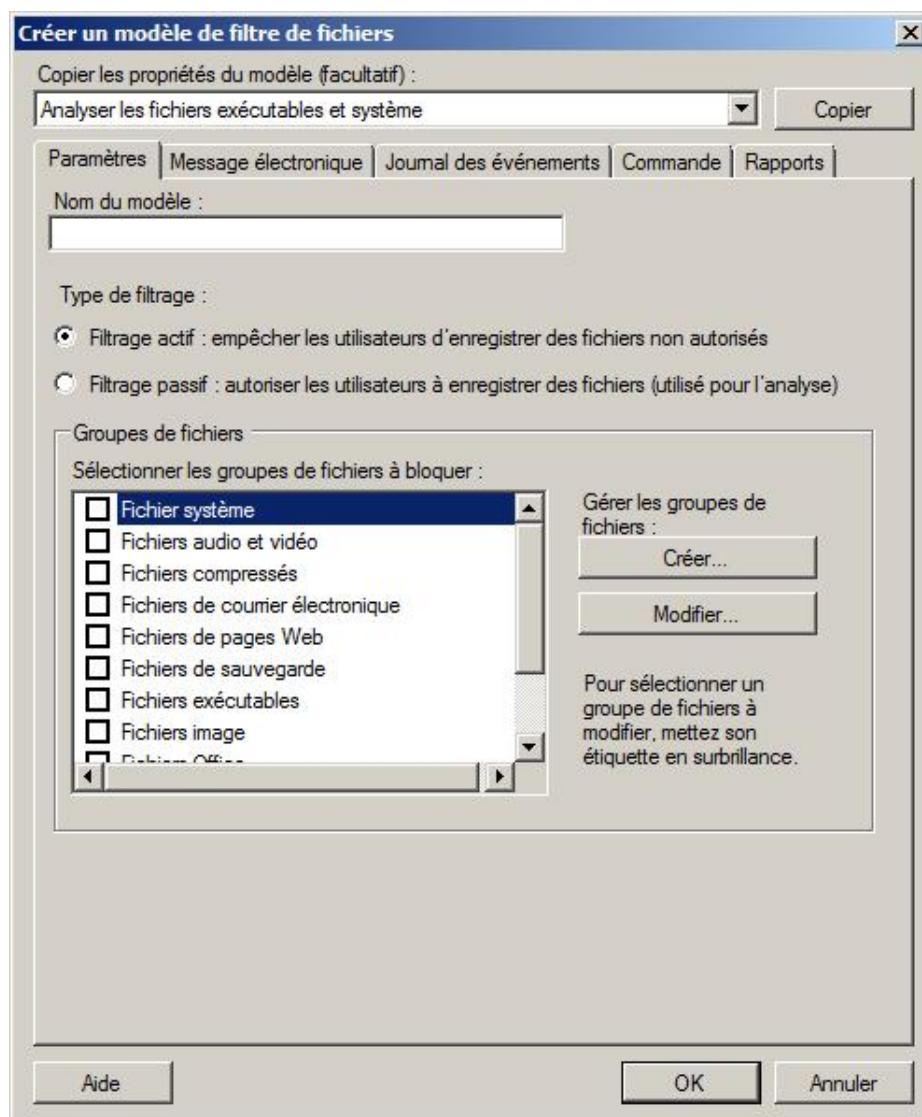


Il est conseillé de regrouper les extensions par type de fichiers.

À ce niveau, vous regroupez les éléments dont vous avez besoin. Ensuite, il faut définir un filtre de fichiers qui permet de mettre en place soit une analyse, soit un blocage des fichiers.

La procédure suivante montre la création d'un modèle de filtre de fichiers.

- Ouvrez le **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur le nœud **Gestion du filtrage de fichiers**.
- Cliquez sur **Modèles de filtres de fichiers**. Les modèles déjà définis apparaissent dans la fenêtre centrale.
- Dans le volet de droite, cliquez sur **Créer un modèle de filtre de fichiers**.



- Vous pouvez copier les paramètres provenant d'un modèle existant ou créer un modèle. Commencez par saisir un nom explicite pour le modèle puis sélectionnez le type de filtrage : **actif** pour bloquer, **passif** pour l'analyse. Ensuite, sélectionnez au moins un groupe de fichiers. N'oubliez pas d'indiquer les méthodes de notification à utiliser pour le filtre, soit par message électronique, journal des événements, commande ou rapport. Cliquez sur **OK**.

Enfin, c'est au tour du filtre d'être créé en utilisant la procédure suivante.

- Ouvrez le **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur le nœud **Filtres de fichiers**.

- Cliquez sur **Filtres de fichiers**. Les filtres déjà définis apparaissent dans la fenêtre centrale.
- Dans le volet de droite, cliquez sur **Créer un filtre de fichiers**.
- Saisissez le chemin d'accès du filtre qui peut être un dossier ou un volume, puis sélectionnez un modèle de filtre de fichiers avant de cliquer sur **OK**.

Vous pouvez éventuellement définir une exception pour votre filtre en utilisant la commande **Créer une exception de filtre de fichiers**.

Pour gérer les filtres de fichiers via l'invite de commande, il faut utiliser l'utilitaire **filescrn** qui s'installe avec le sous-rôle.

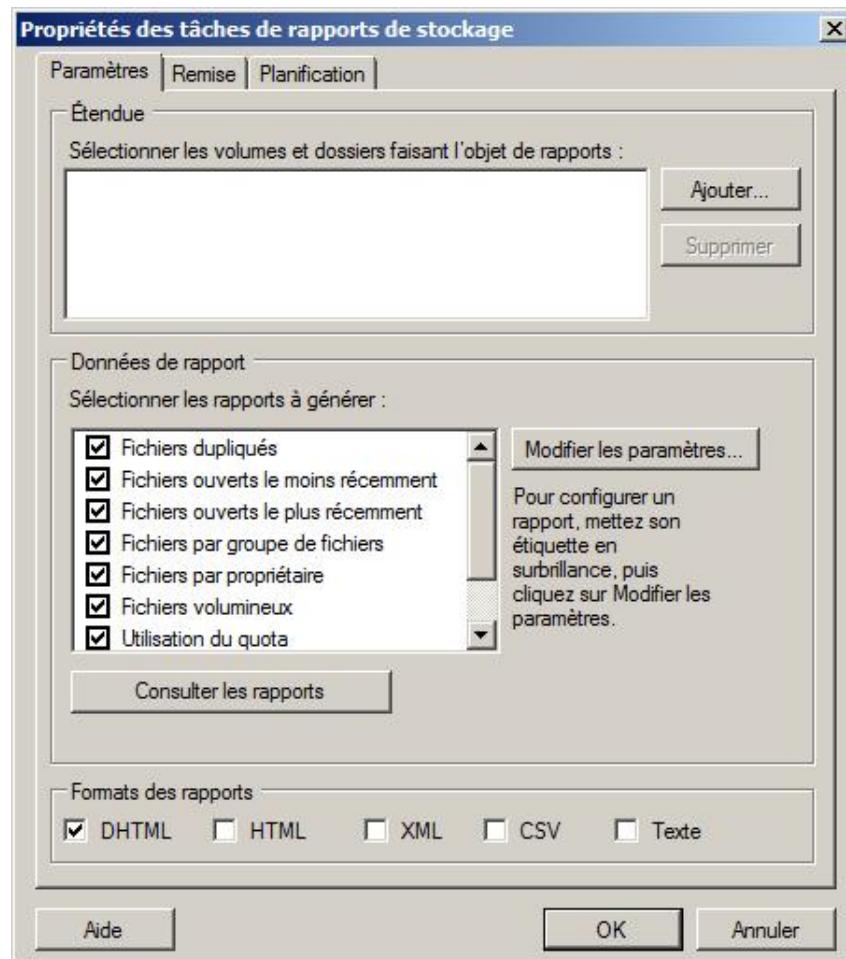
## 8. Gestion des rapports de stockage



La dernière partie de cet utilitaire concerne la gestion des rapports qui peuvent être planifiés ou générés à la demande.

La procédure suivante montre comment planifier des rapports :

- Ouvrez le **Gestionnaire de ressources du serveur de fichiers** puis cliquez sur **Gestion des rapports de stockage**.
- Dans le volet droit, cliquez sur **Planifier une nouvelle tâche de rapport**.



- Sélectionnez les volumes et les dossiers pour lesquels vous voulez planifier les rapports puis les rapports qu'il faut générer. Pour chaque rapport, vous pouvez modifier les paramètres standards. Enfin, spécifiez le format dans lequel les rapports doivent être créés puis cliquez sur l'onglet **Remise**.
- Dans l'onglet **Remise**, spécifiez les adresses e-mail qui doivent recevoir les rapports générés puis cliquez sur l'onglet **Planification**.
- Dans l'onglet **Planification**, cliquez sur **Créer une planification**.
- Dans la boîte de dialogue **Planifier**, créez une planification puis cliquez sur **OK**.
- Cliquez sur **OK**.

Les rapports générés en DHTML ressemblent à celui présenté dans l'image suivante.

The screenshot shows a DHTML-based report window. At the top, there's a warning message: "Le nombre de fichiers correspondant aux critères du rapport est supérieur au nombre maximal défini. Seules les 1000 premières correspondances sont affichées." Below this, the title is "Rapport Fichiers ouverts le moins récemment Table des matières". There are four links: "Totaux des rapports", "Taille par propriétaire", "Taille par groupe de fichiers", and "Statistiques de rapport". A table titled "Totaux des rapports" is displayed:

Fichiers affichés dans le rapport		Tous les fichiers correspondant aux critères du rapport	
Fichiers	Taille totale sur le disque	Fichiers	Taille totale sur le disque
1000	286 Mo	38429	5'986 Mo

Below the table is a link "Haut du rapport actif". The next section is titled "Taille par propriétaire" and contains a pie chart. The legend indicates the following distribution:

- AUTORITE NT\SYSTEM: 3'570 Mo; (59.64 %)
- NT SERVICE\TrustedInstaller: 1'927 Mo; (32.19 %)
- BUILTIN\Administrateurs: 478 Mo; (7.98 %)
- Autres: 11.2 Mo; (0.19 %)

- Pour une gestion via l'invite de commande, il faut utiliser l'utilitaire **storrept**.

## 9. Services pour NFS

Les services pour NFS (*Network File System*) permettent de transférer des fichiers entre votre serveur et un serveur UNIX à l'aide du protocole NFS. Il s'agit d'un service de rôle optionnel. Il regroupe la partie cliente NFS ainsi que la partie serveur.

Il est également supporté sur un Server Core.

Les fonctionnalités suivantes ont été supprimées dans Windows Server 2008 :

- Passerelle pour NFS.

- Serveur pour PCNFS.
- Tous les composants PCNFS du service Client pour NFS.
- Le mappage de noms d'utilisateurs.

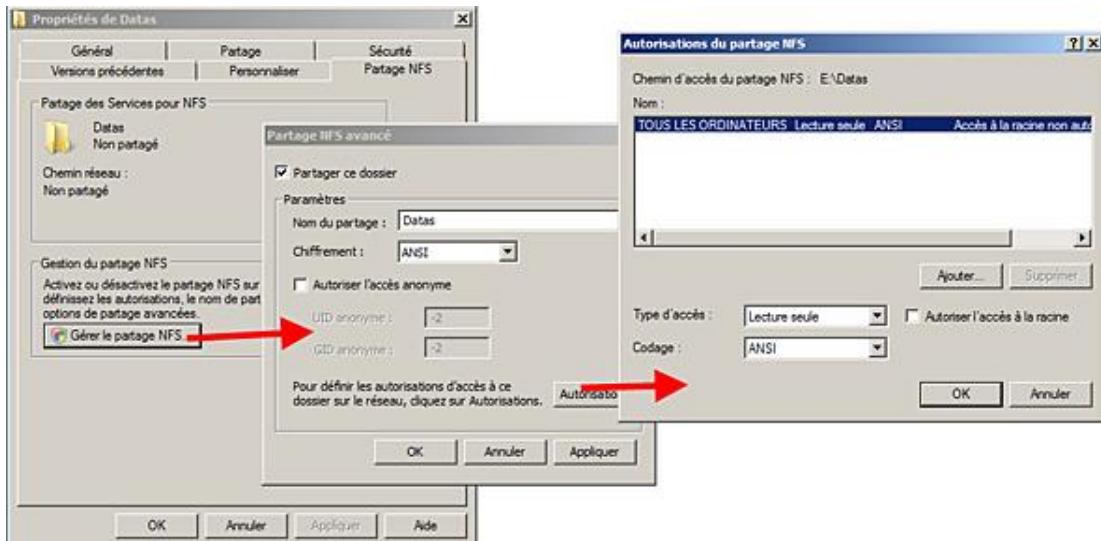
Les fonctionnalités suivantes ont été ajoutées ou améliorées dans Windows Server 2008 :

- **Recherche Active Directory.** Le schéma Active Directory est modifié pour inclure des champs d'identificateurs d'utilisateur (UID) et d'identificateurs de groupe UNIX (GID) lorsque le composant **Gestion des identités pour Unix** est installé. Cela permet aux clients et aux serveurs NFS de rechercher des mappages de comptes d'utilisateurs Windows vers Unix directement à partir de l'Active Directory.
- **Prise en charge des éditions 64 bits de Windows 2008.**
- **Performances serveurs améliorées** par l'utilisation d'un pilote de filtre de fichiers pour réduire les temps d'accès aux fichiers.
- **Prise en charge de périphériques spéciaux UNIX**, appelée **mkmod**.
- **Prise en charge UNIX améliorée** de Sun Solaris V9, Red Hat V9, IBM AIX V5L 5.2 et HP-UX.

Le service installe la partie cliente qui permet l'accès à des serveurs NFS, et la partie serveur qui permet de répondre à des clients NFS.

Avant de pouvoir utiliser ce service, il faut :

- Au niveau du client :
  - **Configurer le mappage des identités utilisateurs**, c'est-à-dire la méthode avec laquelle le service Client NFS obtient des informations sur les utilisateurs et les groupes Windows.
  - **Configurer les paramètres des services pour NFS**, c'est-à-dire la configuration des différents paramètres permettant la gestion correcte du service NFS.
  - **Monter les partages NFS** comme des chemins UNC.
- Au niveau du serveur ;
  - **Installer et configurer le mappage des identités utilisateurs**, c'est-à-dire la méthode avec laquelle le service Serveur NFS obtient des informations sur les utilisateurs et les groupes Windows.
  - **Configurer les paramètres des services pour NFS**, c'est-à-dire la configuration des différents paramètres permettant la gestion correcte du service NFS.
  - **Exporter des partages NFS**, un onglet supplémentaire apparaît dans la boîte de dialogue **Propriétés** du dossier, permettant la gestion des partages NFS à l'aide des outils de partage présentés précédemment ainsi qu'avec l'outil **Gestion du partage et du stockage**, comme le montre la figure suivante.



- Les commandes `nfsadmin`, `nfsshare`, `nfsstat` et `mapadmin` permettent la gestion des services NFS à l'aide de l'invite de commande.

## 10. Service de recherche Windows

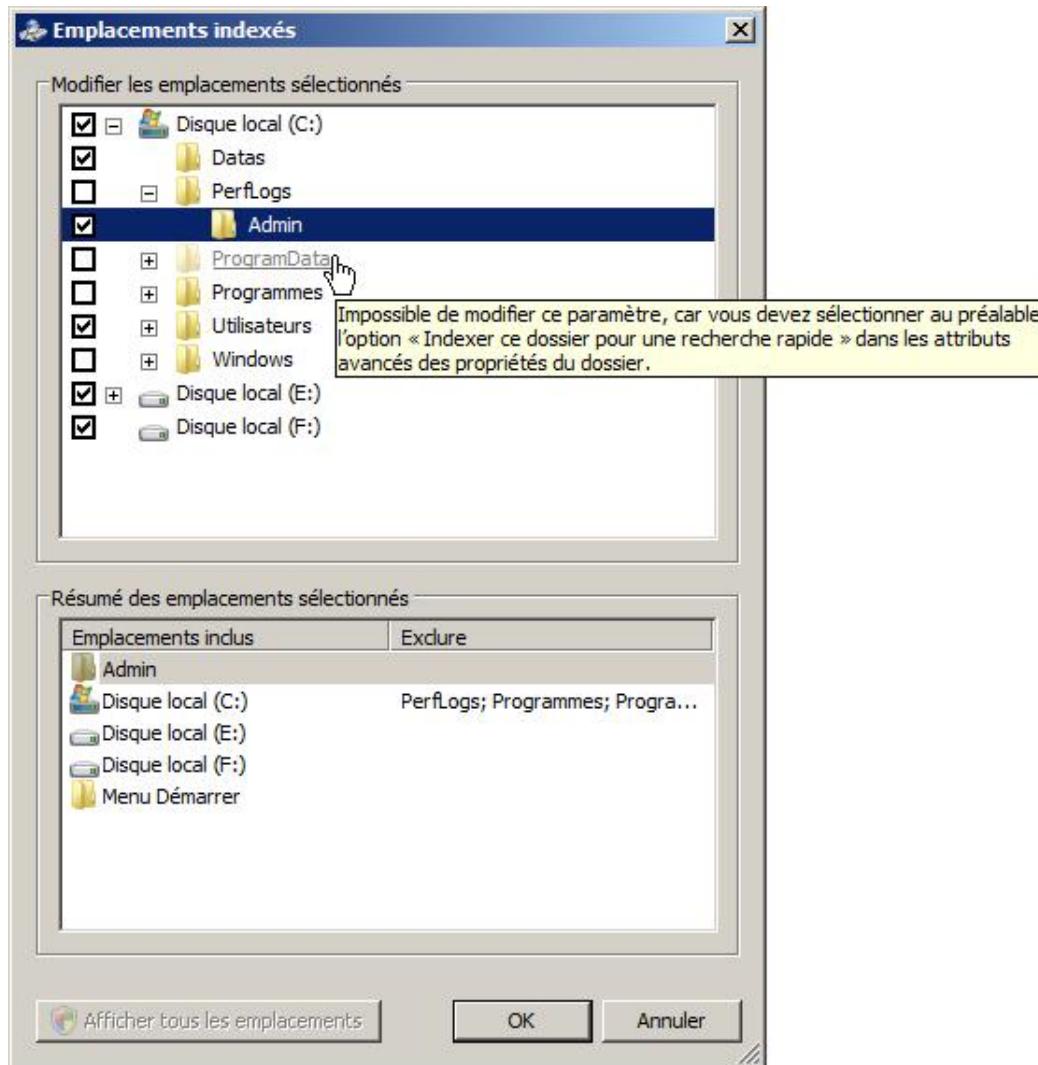
Une fois le service de rôle installé, le service **Recherche Windows** est activé. Il permet de rechercher efficacement des documents en utilisant des informations basées sur les propriétés ou le contenu des documents.

Pour gérer le service, il faut passer par le paramètre **Options d'indexation** du **Panneau de configuration**.

- Vous ne pouvez pas installer en même temps le service de recherche Windows et le service d'indexation des Services de fichiers Windows Server 2003.

### a. Modification des emplacements de recherche

- Ouvrez le paramètre **Options d'indexation**.
- Dans la boîte de dialogue **Options d'indexation**, cliquez sur **Modifier**.
- Dans la boîte de dialogue **Emplacements indexés**, sélectionnez les emplacements que vous voulez indexer. Certains dossiers ne peuvent pas être indexés si leur propriétés avancées ne le permettent pas. Pour les indexer, utilisez l'explorateur pour afficher les propriétés avancées.



## b. Paramètres avancés

- Ouvrez le paramètre **Options d'indexation**.
- Dans la boîte de dialogue **Options d'indexation**, cliquez sur **Avancé**.

La boîte de dialogue **Options avancées** contient deux onglets, l'onglet **Paramètres d'indexation** et l'onglet **Types de fichiers**.

L'onglet **Paramètres d'indexation** permet d'inclure dans l'indexation les fichiers chiffrés et de traiter les accents et les signes diacritiques comme des mots différents, ce qui relance l'indexation complète des emplacements pour inclure ce dernier paramètre.

En cas de problèmes, vous pouvez reconstruire l'indexation, c'est-à-dire redéfinir les emplacements ou restaurer les paramètres par défaut.

Enfin, vous pouvez définir l'emplacement de la base de données d'indexation qui par défaut se trouve dans le dossier c:\ProgramData\Microsoft\Search.

L'onglet **Types de fichiers** permet de définir, pour chaque extension de fichier, s'il faut l'indexer et dans ce cas s'il faut se contenter de l'indexation des propriétés du fichier ou également inclure son contenu. Vous pouvez également ajouter vos propres extensions.

## 11. Services de fichiers Windows Server 2003

Les services de fichiers Windows Server 2003 comprennent les services de rôle suivants :

- le **Service de réPLICATION de fichiers FRS** (*File Replication Service*) gère la synchronisation de dossiers en utilisant le protocole FRS au lieu du protocole de réPLICATION DFS. À n'utiliser qu'avec des serveurs ne prenant pas en charge la réPLICATION DFS pour la gestion du système DFS.
- le **Service d'indexATION** correspond à l'ancien service d'indexATION qui est remplacé par le **Service de recherche Windows**.

# Sauvegarde de Windows Server

## 1. Introduction

Un fichier corrompu ou un disque qui tombe en panne sont des exemples de problèmes courants, et pour se prémunir contre ce type de risque il est nécessaire de créer une copie des données sur un autre emplacement. Le moyen le plus simple et efficace est l'utilisation d'un utilitaire de sauvegarde. L'utilitaire de sauvegarde de Windows 2008 est entièrement nouveau, son nom est **wbadmin**. Plus simple à utiliser, il a été conçu pour limiter les manipulations, donc les risques d'erreur. Dans Windows Server 2008, la granularité de la sauvegarde est le volume et non plus le fichier ! Pour la récupération, la granularité est le fichier. Pour stocker les sauvegardes, Windows requiert un disque dédié à la sauvegarde. Ce disque peut être :

- un disque dur (externe) USB,
- un disque dur (externe) Firewire,
- un volume du disque,
- un média amovible ; attention les bandes ne sont plus supportées.

 Pour effectuer une sauvegarde sur bande, il vous faut utiliser un logiciel tiers.

 Il n'est pas possible de lire les sauvegardes réalisées avec l'utilitaire Windows Backup des versions antérieures. Si malgré tout vous devez utiliser l'ancienne version appelée **ntbackup**, vous pouvez toujours télécharger la version fonctionnant avec Windows Server 2008 à partir du site Web de Microsoft.

## 2. Installation de la fonctionnalité de sauvegarde



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans le volet gauche du **Gestionnaire de serveur**, cliquez sur **Fonctionnalités**.
- Dans la fenêtre centrale, cliquez sur **Ajouter des fonctionnalités**.
- Sur la page **Fonctionnalités** de l'Assistant **Ajout de fonctionnalités**, sélectionnez **Fonctionnalités de la sauvegarde de Windows Server**, puis cliquez sur **Suivant**. Attention, par défaut l'outil en ligne de commande n'est pas installé. Développez le nœud pour sélectionner l'outil en ligne de commande, il requiert l'installation de **PowerShell**.
- Sur la page **Confirmation**, vérifiez vos informations avant de cliquer sur **Installer**.
- Consultez le résultat de l'installation sur la page **Résultats**, puis cliquez sur **Fermer**.

 En cliquant sur **Action** puis sur **Se connecter à un autre ordinateur**, vous pouvez effectuer des sauvegardes distantes.

### 3. Installation sur un Server Core



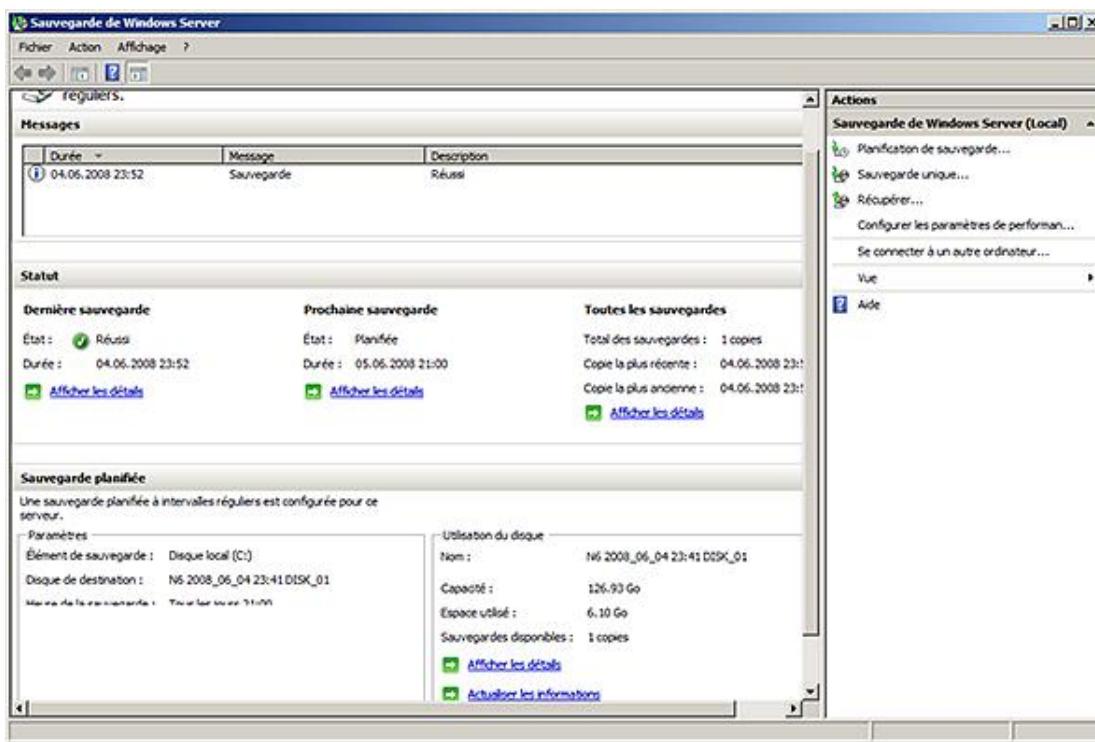
Bien que l'installation soit possible, vous ne pouvez pas gérer la sauvegarde en mode graphique localement, mais seulement à partir d'un autre ordinateur. D'autre part, comme il n'est pas possible d'installer PowerShell, certaines cmdlets ne sont pas disponibles.

- Dans l'invite de commandes, saisissez `start /w ocsetup WindowsServerBackup` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que l'utilitaire de sauvegarde est bien installé puis appuyez sur [Entrée].

### 4. Lancement de la sauvegarde de Windows Server



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Sauvegarde de Windows Server**.



La fenêtre centrale affiche des informations dans trois sections :

- **Messages** : informations qui concernent les sauvegardes.
- **Statut** : informations résumées sur la dernière sauvegarde, la prochaine et toutes les sauvegardes. Pour plus de détails, il faut cliquer sur les liens correspondants.
- **Sauvegarde planifiée** : informations sur la sauvegarde planifiée ainsi que sur l'utilisation des disques de

stockage.

Les seules opérations possibles sont :

- la planification de la sauvegarde,
- la sauvegarde unique,
- la configuration des paramètres de performance,
- la récupération.

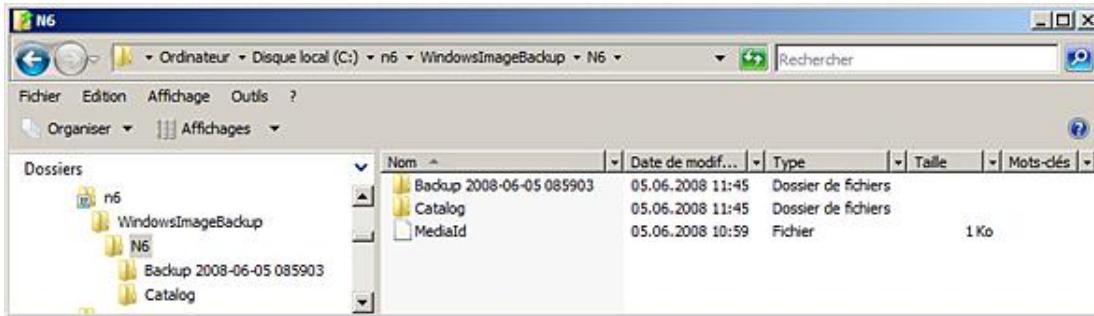
## 5. Création d'une sauvegarde



### a. Création d'une sauvegarde manuelle unique

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Sauvegarde de Windows Server**.
- Dans le volet de droite, cliquez sur **Sauvegarde unique**.
- Sur la page **Options de sauvegarde**, sélectionnez soit l'option **Les mêmes options que pour les sauvegardes planifiées dans l'assistant Planification de sauvegarde**, soit l'option **D'autres options**. Puis cliquez sur **Suivant**. Dans le premier cas, la page suivante correspond à la page de Confirmation.
- Sur la page **Sélectionner la configuration de la sauvegarde**, sélectionnez soit l'option **Serveur entier**, soit l'option **Personnalisé**, puis cliquez sur **Suivant**. L'option **Personnalisé** vous permet de sélectionner les volumes que vous voulez sauvegarder et prévoit à cet effet une étape dans l'assistant pour sélectionner ces volumes.
- Sur la page **Spécifier le type de destination**, sélectionnez l'option **Lecteurs locaux** ou l'option **Dossier partagé distant**, puis cliquez sur **Suivant**.
- Si vous avez choisi l'option pour la sauvegarde sur un dossier partagé, la page **Spécifiez un dossier distant** apparaît. Sélectionnez un dossier partagé sur un serveur en utilisant un chemin UNC sur lequel vous avez un droit en écriture, puis sélectionnez une des options pour gérer les autorisations sur le répertoire qui sera créé et qui contiendra la sauvegarde : soit l'option **Ne pas hériter**, soit l'option **Hériter des autorisations provenant du répertoire partagé**, avant de cliquer sur **Suivant**.
- Sur la page **Spécifier une option avancée**, sélectionnez soit l'option **Sauvegarde de copie VSS** si vous utilisez déjà un autre utilitaire de sauvegarde pour les volumes, soit **Sauvegarde complète VSS**, puis cliquez sur **Suivant**.
- Sur la page **Confirmation**, relisez attentivement les informations puis cliquez sur **Sauvegarde**. L'assistant lance la sauvegarde.
- Sur la page **Sauvegarde en cours**, dès que la sauvegarde est terminée, cliquez sur **Fermer**.

Sur le serveur distant, la structure créée dans le répertoire est la suivante :



Sur l'image précédente, vous pouvez remarquer qu'un catalogue est créé ainsi qu'un dossier par sauvegarde.

### b. Planification de la sauvegarde

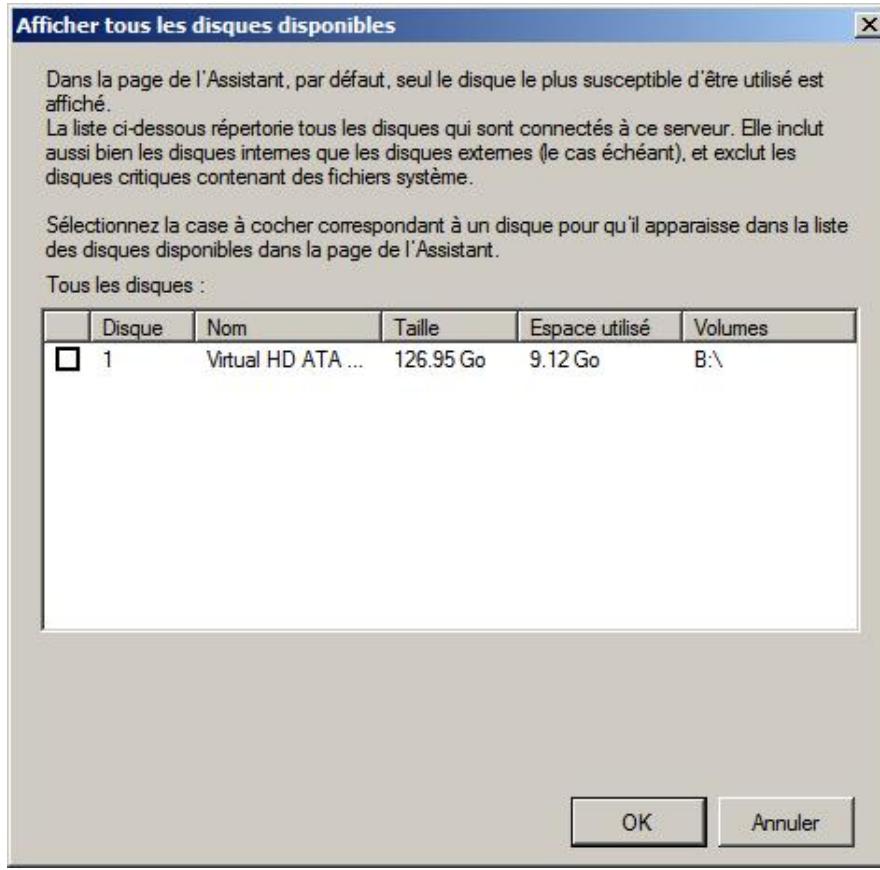
Il ne peut exister qu'une planification par serveur. La procédure pour la créer est la suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Sauvegarde de Windows Server**.
- Dans le volet de droite, cliquez sur **Planification de sauvegarde**.
- Sur la page **Démarrer** de l'**Assistant de planification de sauvegarde**, cliquez sur **Suivant**.
- Sur la page **Sélectionner la configuration de la sauvegarde**, sélectionnez soit l'option **Serveur entier**, soit l'option **Personnalisé**, puis cliquez sur **Suivant**. L'option **Personnalisé** vous permet de sélectionner les volumes que vous voulez sauvegarder et prévoit à cet effet une étape dans l'assistant pour sélectionner ces volumes. Vous pouvez également désélectionner la récupération système.
- Sur la page **Spécifiez l'heure de la sauvegarde**, sélectionnez soit l'option **Tous les jours**, soit l'option **Plusieurs fois par jour** en fonction de vos besoins, puis spécifiez la planification horaire dont la granularité est la demi-heure, enfin cliquez sur **Suivant**. Si votre serveur ne dispose pas de disque dédié pour la sauvegarde, l'assistant vous empêche de poursuivre.
- Sur la page **Sélectionner le disque de destination**, cliquez sur le bouton **Afficher tous les disques disponibles** pour sélectionner le disque sur lequel les sauvegardes seront stockées, comme le montre l'image suivante.

---

 Il est conseillé d'utiliser un disque amovible, un disque externe ou un support de média bande ou DVD. Si vous utilisez un disque dur interne, celui-ci sera dédié à la sauvegarde.

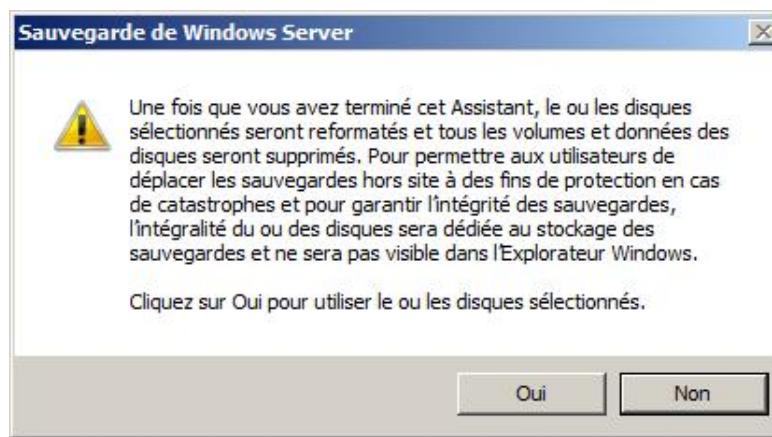
---



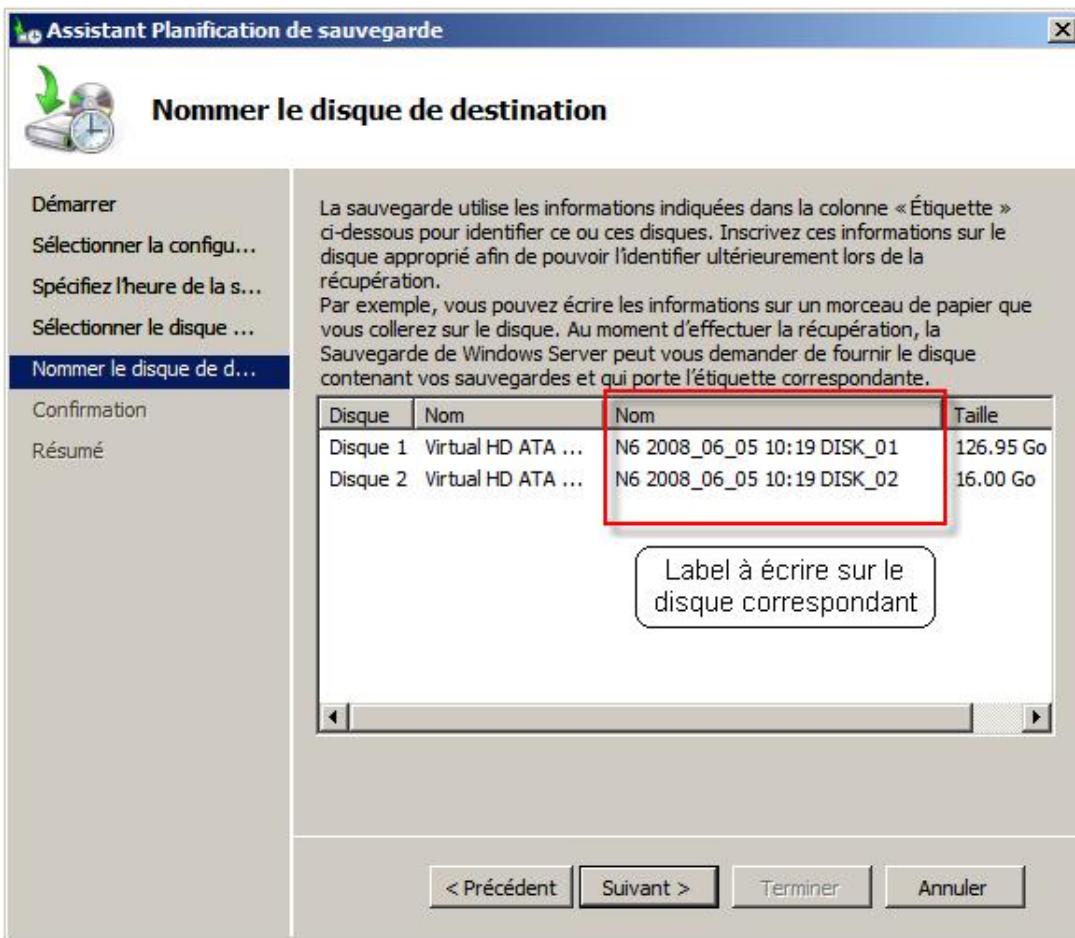
- Les disques qui contiennent le système d'exploitation et des applications ne peuvent pas contenir la sauvegarde.

- Dans la boîte de dialogue **Afficher tous les disques disponibles**, sélectionnez le disque qui contiendra la sauvegarde puis cliquez sur **OK**. Il est possible de sélectionner plusieurs disques pour la sauvegarde.

La boîte de dialogue suivante apparaît, lisez attentivement le contenu puis cliquez sur **Oui** pour continuer.



- Sur la page **Nommer le disque de destination**, relevez les noms attribués par Windows et inscrivez-les sur les disques afin de les identifier par la suite. Cliquez sur **Suivant**.



- Sur la page **Confirmation**, relisez attentivement les informations puis cliquez sur **Terminer**. L'assistant formate les disques et crée la planification.
- Sur la page **Résumé**, lisez le statut puis cliquez sur **Fermer**.

 En relançant l'assistant, vous pouvez soit modifier la planification de la sauvegarde, soit supprimer la planification.

## 6. Configuration des paramètres de performance



Cette action permet de définir le type de sauvegarde que vous voulez effectuer. Vous avez le choix entre une sauvegarde complète et une sauvegarde incrémentielle. Par défaut, Windows Server 2008 effectue chaque fois des sauvegardes complètes.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Sauvegarde de Windows Server**.
- Dans le volet de droite, cliquez sur **Configurer les paramètres de performance**.

Par défaut, l'option **Toujours effectuer une sauvegarde complète** est sélectionnée, vous pouvez décider d'effectuer des sauvegardes incrémentielles afin de réduire le temps de la sauvegarde.

- Sélectionnez l'option désirée puis cliquez sur **OK**.

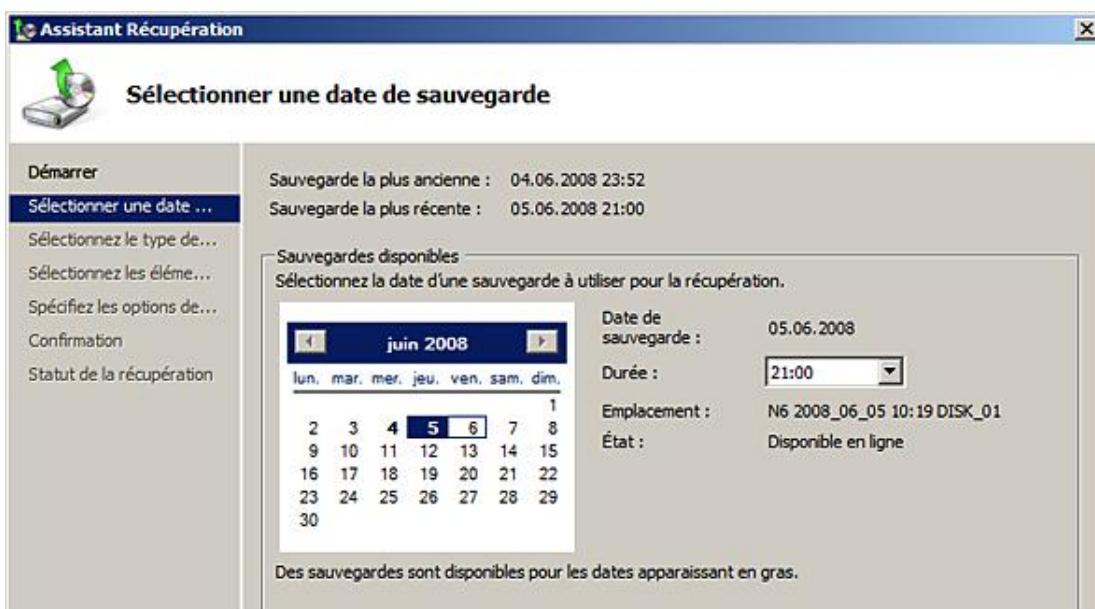
## 7. Récupération de fichiers, d'applications et de volumes



Win

La procédure est la suivante.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Sauvegarde de Windows Server**.
- Dans le volet de droite, cliquez sur **Récupérer**.
- Sur la page **Démarrer** de l'**Assistant Récupération**, sélectionnez l'emplacement de la sauvegarde puis cliquez sur **Suivant**.
- Sur la page **Sélectionner une date de sauvegarde**, indiquez la date et l'heure de la sauvegarde à utiliser. L'assistant indique quel est le nom du volume et s'il est disponible, comme le montre la figure suivante. Cliquez ensuite sur **Suivant**.



- Sur la page **Sélectionnez le type de récupération**, sélectionnez **Fichiers et dossiers**, **Applications** ou **Volumes**, puis cliquez sur **Suivant**.

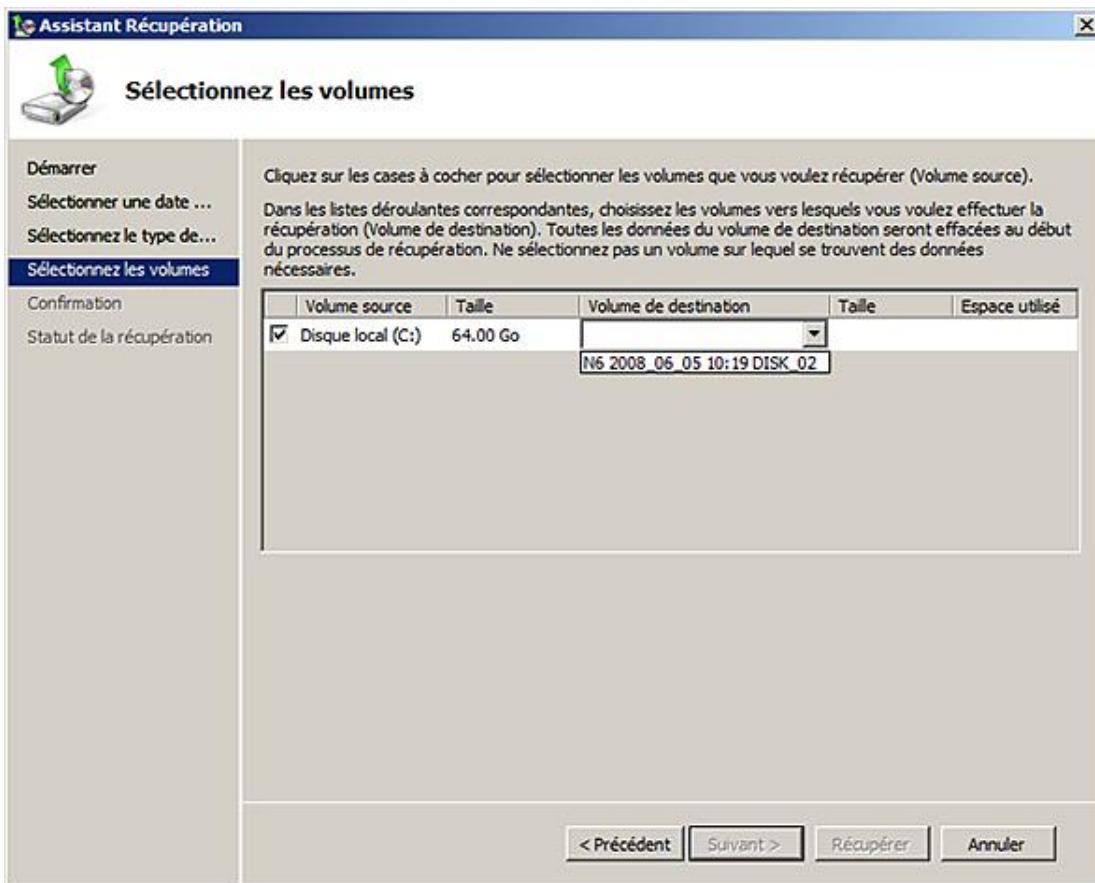
### a. Récupérer des fichiers et dossiers

- Sur la page **Sélectionnez les éléments à récupérer**, sélectionnez les fichiers ou dossiers à récupérer, sachant que la granularité est le fichier et qu'il n'est pas possible de sélectionner plus d'un élément de la liste de gauche, puis cliquez sur **Suivant**.
- Sur la page **Spécifiez les options de récupération**, indiquez si l'emplacement de destination est l'emplacement d'origine, la méthode de résolution à utiliser pour les conflits avec les fichiers et dossiers existants, et précisez s'il faut restaurer les paramètres de sécurité avant de cliquer sur **Suivant**.
- Sur la page **Confirmation**, contrôlez les éléments à récupérer puis cliquez sur **Récupérer**.

- Sur la page **Statut de la récupération**, vérifiez que les éléments ont bien été récupérés avant de cliquer sur **Fermer**.

## b. Récupérer des volumes

- Sur la page **Sélectionnez les volumes**, sélectionnez le ou les volumes à récupérer et indiquez le volume de destination avant de cliquer sur **Suivant**.
- Sur la page **Confirmation**, contrôlez les éléments à récupérer puis cliquez sur **Récupérer**.



- Sur la page **Statut de la récupération**, vérifiez que les volumes ont bien été récupérés avant de cliquer sur **Fermer**.

## 8. Récupération du système d'exploitation



Vous pouvez récupérer le système d'exploitation sur le même ordinateur ou un ordinateur similaire, ce qui suppose que la taille des disques est importante et qu'elle doit être au moins égale à la taille des disques de l'ancien système.

- Démarrez votre serveur à l'aide du DVD d'installation de Windows Server 2008.
- Spécifiez les paramètres de langue puis cliquez sur **Suivant**.
- Cliquez sur **Réparer votre ordinateur**.

- Sur la page **Options de récupération système**, sélectionnez le système d'exploitation puis cliquez sur **Suivant**. Si vous avez changé de disque, cliquez sur **Suivant**.
- Sur la page **Choisir un outil de récupération**, cliquez sur **Restauration de l'ordinateur Windows**.
- Sur la page **Restauration de l'ordinateur Windows**, sélectionnez la sauvegarde à utiliser puis cliquez sur **Suivant**.

 La sauvegarde peut se trouver sur un partage réseau.

- Sur la page **Choisissez comment restaurer la sauvegarde**, choisissez éventuellement de formater et de repartitionner les disques, ou d'installer des pilotes pour les disques. Vous pouvez aussi sélectionner les options avancées, comme rechercher et mettre à jour automatiquement des informations relatives aux disques ou redémarrer l'ordinateur automatiquement à la fin de la restauration, en cliquant sur le bouton **Avancé**. Cliquez ensuite sur **Suivant**.
- Sur la page **Restauration de l'ordinateur**, contrôlez vos paramètres avant de cliquer sur **Terminer**.
- Dans la boîte de dialogue **Restauration de l'ordinateur Windows**, sélectionnez la case à cocher **Je confirme que je souhaite effacer toutes les données existantes et restaurer la sauvegarde** avant de cliquer sur **OK**.

La restauration commence et lorsqu'elle est terminée, l'ordinateur redémarre.

## 9. Utilisation de l'invite de commande



Certaines opérations comme la sauvegarde et la restauration de l'état système sont uniquement possibles en mode ligne de commande en utilisant `wbadmin`.

La syntaxe est la suivante :

```
C:\>wbadmin /help
wbadmin 1.0 - Outil de ligne de commande de sauvegarde
<C> Copyright 2004 Microsoft Corp.

---- Commandes prises en charge ----

ENABLE BACKUP          -- Active ou modifie une sauvegarde quotidienne
                       -- planifiée.
DISABLE BACKUP         -- Désactive l'exécution des sauvegardes
                       -- quotidiennes planifiées.
START BACKUP           -- Exécute une sauvegarde.
STOP JOB               -- Arrête la sauvegarde ou la récupération
                       -- en cours d'exécution.
GET VERSIONS          -- Affiche la liste détaillée des sauvegardes
                       -- récupérables à partir d'un emplacement spécifique.
GET ITEMS              -- Liste les éléments contenus dans la sauvegarde.
START RECOVERY         -- Exécute une récupération.
GET STATUS             -- Affiche l'état de la tâche en cours d'exécution.
GET DISKS              -- Affiche les disques actuellement en ligne.
START SYSTEMSTATERECOVERY -- Exécute une récupération de l'état du système.
START SYSTEMSTATEBACKUP  -- Exécute une sauvegarde de l'état du système.
DELETE SYSTEMSTATEBACKUP -- Supprime la ou les sauvegardes de l'état
                           -- du système.

C:\>
```

Cet utilitaire ne fonctionne qu'en mode local.

### a. Sauvegarde de l'état système

- Ouvrez une invite de commande avec les privilèges élevés.
- Saisissez `wbadmin start systemstatebackup -backupTarget:<disque>` où `<disque>` représente l'emplacement du stockage de la sauvegarde comme **d:**.

### **b. Restauration de l'état système**

- Ouvrez une invite de commande avec les privilèges élevés.
- Saisissez `wbadmin start systemstaterecovery-version:<IdentificateurVersion> -showsummary [-backupTarget:{<disque> | <CheminPartageRéseau>}]` où `<disque>` représente l'emplacement du stockage de la sauvegarde comme **d:**.

### **c. Sauvegarde manuelle**

- Ouvrez une invite de commande avec les privilèges élevés.
- Saisissez `wbadmin start backup -backuptarget \\serveur\bk -include d:.`

# Mise en œuvre du chiffrage EFS

## 1. Introduction

Dans le but d'améliorer la confidentialité des documents, le chiffrage **EFS** (*Encrypted File System*), associé au système de fichiers NTFS depuis Windows 2000, est un outil indispensable au sein de l'entreprise.

Conceptuellement, le fichier est chiffré sur le serveur à l'aide d'une clé symétrique appelée FEK (*File Encryption Key*) en utilisant un algorithme AES (*Advanced Encryption Standard*).

La FEK va être chiffrée à l'aide de la clé EFS publique de l'utilisateur, chiffrement qui utilise un algorithme RSA, le résultat est stocké dans la zone **DDF** (*Data Decryption Field*) du fichier. La zone DDF est conçue pour accueillir des clés d'autres utilisateurs. Il y est également ajouté l'agent de récupération dans la zone **DRF** (*Data Recovery Field*). Le schéma suivant montre la structure d'un document chiffré avec EFS.



Par défaut, les certificats utilisent des clés RSA d'une longueur de 2048 bits.

Depuis Windows Vista, il est possible de stocker les clés privées RSA sur des smartcards.

- 
- Pour pouvoir déchiffrer le document, il faut pouvoir déchiffrer la clé FEK.

L'agent de récupération permet de déchiffrer les documents qui ont été chiffrés par les utilisateurs. Comme son nom l'indique, il doit être utilisé pour récupérer des documents dont l'utilisateur n'existe plus ou lorsque la clé EFS de l'utilisateur est corrompue, etc. L'administrateur de domaine ou local est l'agent de récupération par défaut. Il peut déchiffrer les documents à l'aide de l'Explorateur ou de la commande **cipher**. Une procédure stricte doit être mise en place dans l'entreprise pour le déchiffrement de documents à l'aide de l'agent de récupération.

Il est possible de désactiver le chiffrement EFS via :

- La base de registre pour un ordinateur hors domaine :

**HKLM\Software\Microsoft\Windows NT\CurrentVersion\EFS**

Valeur : **EfsConfiguration**

Type valeur : **DWORD**

Donnée de la valeur : **0x1**

Base : **Hexadécimale**

- Une stratégie de groupe pour un ordinateur faisant partie du domaine :

■ Dans l'éditeur de gestion des stratégies de groupe, développez sur le volet de gauche les nœuds suivants : **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de clé publique - Système de fichiers EFS**

■ Cliquez avec le bouton droit de la souris sur **Système de fichiers EFS** puis sur **Propriétés**.

■ Sélectionnez l'option **Ne pas autoriser**.

## 2. Chiffrer un fichier ou un dossier

Cette procédure peut s'effectuer sur tout ordinateur à partir de Windows 2000.

- Connectez-vous en tant qu'utilisateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier ou fichier que vous voulez chiffrer.
- Cliquez avec le bouton droit de la souris sur le dossier ou le fichier, puis sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés**, cliquez sur **Avancé**.

Le bouton **Détails** permet au propriétaire de l'objet d'autoriser d'autres utilisateurs à consulter son fichier.

- Sélectionnez la case à cocher **Chiffrer le contenu pour sécuriser les données** puis cliquez sur deux fois **OK**.
- Si vous chiffrer un dossier, une boîte de dialogue peut apparaître vous demandant si vous voulez appliquer le chiffrement au dossier uniquement ou au dossier et aux sous-dossiers et aux fichiers. Dans ce cas, sélectionnez l'option désirée puis cliquez sur **OK**.

---

 Le dossier ou le fichier chiffré apparaît en vert.

---

## 3. Autoriser d'autres utilisateurs

Cette procédure peut s'effectuer sur tout ordinateur à partir de Windows XP.

Le propriétaire des documents peut autoriser d'autres utilisateurs à consulter les documents. Pour cela, il faut utiliser la procédure suivante.

- Connectez-vous en tant qu'utilisateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au fichier chiffré pour lequel vous voulez autoriser l'accès à d'autres utilisateurs.
- Cliquez avec le bouton droit de la souris sur le fichier puis cliquez sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés**, cliquez sur **Avancé**.
- Dans la boîte de dialogue **Attributs avancés**, cliquez sur **Détails**.

Le bouton **Ajouter** permet d'autoriser un autre utilisateur à accéder au fichier pour autant qu'il dispose d'un certificat EFS.

Le bouton **Supprimer** annule une autorisation pour un utilisateur de la liste.

Le bouton **Sauvegarder les clés** permet la sauvegarde des clés de l'utilisateur.

La seconde liste affiche les certificats des agents de récupération.

- Cliquez sur **Ajouter**.

Si l'utilisateur ne se trouve pas dans la liste, vous pouvez le chercher avec le bouton **Chercher un utilisateur**. Avec le bouton **Afficher le certificat**, vous pouvez afficher les informations du certificat d'un utilisateur.

- Sélectionnez les utilisateurs puis cliquez quatre fois sur **OK**.

## 4. Gérer l'agent de récupération



Win

Par défaut, l'agent de récupération est l'administrateur qui a été créé lors de l'installation. C'est une bonne méthode que de choisir un autre utilisateur pour cette tâche. Il est même recommandé de créer un utilisateur dont la seule tâche est d'agir en tant qu'agent de récupération. Seul un administrateur spécialement formé s'acquittera de cette tâche.

Pour cela, il faut planifier une politique de chiffrage au niveau du domaine puis mettre en place une infrastructure de clé publique.

Il est indispensable de sauvegarder les clés de l'agent de récupération et de les stocker dans un lieu sécurisé hors du site.

La procédure suivante montre comment gérer un agent de récupération à l'aide des stratégies de groupe.

- Connectez-vous en tant qu'administrateur sur un contrôleur de domaine.
- Cliquez sur **Démarrer - Outils d'administration** puis **Stratégie de groupe**.
- Développez la structure arborescente du domaine pour sélectionner la stratégie **Default Domain Policy**.
- Cliquez avec le bouton droit de la souris sur la stratégie puis cliquez sur **Modifier**.
- Dans l'éditeur de gestion des stratégies de groupe, développez sur le volet de gauche les nœuds suivants : **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégie de clé publique - Système de fichiers EFS**.

Les actions que vous pouvez effectuer à ce niveau vous permettent de gérer correctement la création et la gestion de l'agent de récupération.

## 5. Copier et déplacer des fichiers chiffrés

Il faut distinguer les opérations de déplacement et de copie s'effectuant sur le même serveur de celles s'effectuant sur des serveurs différents :

	Même volume		Sur un serveur distant	
	Dossier chiffré	Dossier non chiffré	Supportant le chiffrement EFS	Ne supportant pas le chiffrement EFS
<b>Déplacement d'un dossier source A vers un dossier de destination B</b>	Chiffré	Conserve son état	Chiffré	Avertissement et possibilité d'annulation
<b>Copie d'un dossier source A vers un dossier de destination B</b>	Chiffré	Chiffré	Chiffré	Avertissement et possibilité d'annulation

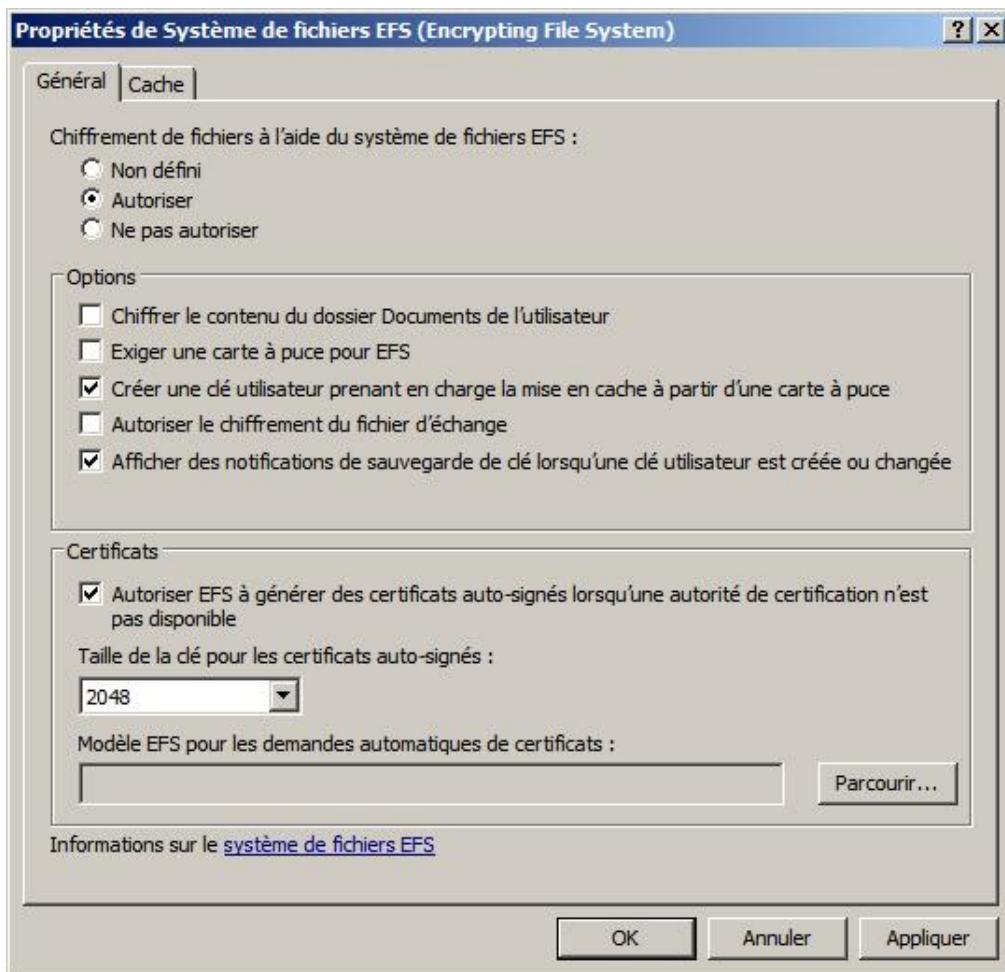
► Le fichier n'est chiffré que sur le serveur où il est stocké. Il est déchiffré avant d'être envoyé en clair sur le réseau. Une stratégie IPsec est à prévoir.

## 6. Gestion d'EFS à l'aide des stratégies de groupe

À l'aide de la console GPMC ou de l'éditeur de stratégie de groupe local (secpol.msc), vous pouvez configurer plusieurs paramètres EFS, à savoir :

Modèle et paramètre	Chemin et description	Valeur par défaut
<b>GroupPolicy.admx</b> - Traitement de la stratégie de récupération EFS	<b>Configuration ordinateur\Modèles d'administration\Système\Stratégie de groupe</b> - Détermine quand les stratégies de chiffrement sont mises à jour.	Non configuré
<b>EncryptFilesonMove.admx</b> - Ne pas chiffrer automatiquement les fichiers déplacés vers des dossiers chiffrés	<b>Configuration ordinateur\Modèles d'administration\Système\</b> - Empêche l'Explorateur Windows de chiffrer les fichiers qui sont déplacés vers un dossier chiffré.	Non configuré
<b>OfflineFiles.admx</b> - Chiffrer le cache des fichiers hors connexion	<b>Configuration ordinateur\Modèles d'administration\Réseau\Fichiers hors connexion\</b> - Ce paramètre détermine si les fichiers hors connexion sont chiffrés ou non avec la clé de l'utilisateur, alors que pour les versions précédentes cela s'effectuait avec la clé système.	Non configuré
<b>Search.admx</b> - Autoriser l'indexation des fichiers chiffrés	<b>Configuration ordinateur\Modèles d'administration\Composants Windows\Recherche\</b> - Ce paramètre permet aux éléments chiffrés d'être indexés par le service Recherche Windows.	Non configuré

De même en cliquant sur le nœud **Système de fichiers EFS (Encrypted File System)** du chemin **Configuration ordinateur - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de clé publique** pour faire apparaître la boîte de dialogue suivante :



**Chiffrement de fichiers à l'aide du système de fichiers EFS** permet d'autoriser l'utilisation d'EFS.

**Chiffrer le contenu du dossier Documents de l'utilisateur** active le chiffrement dudit dossier.

**Exiger une carte à puce pour EFS**, option apparue avec Windows Vista, permet de sauvegarder la clé privée EFS sur une smartcard afin d'augmenter la sécurité.

**Créer une clé utilisateur prenant en charge la mise en cache à partir d'une carte à puce**. La mise en cache améliore les performances car lorsqu'un certificat est utilisé il est mis en cache. Pour la carte à puce, ce n'est pas directement la clé privée qui est mise en cache mais un descripteur de clés.

**Autorise le chiffrement du fichier d'échange (swapfile).**

**Afficher des notifications de sauvegarde de clé lorsqu'une clé utilisateur est créée ou changée** indique qu'il est nécessaire d'effectuer une sauvegarde des clés.

**Autoriser EFS à générer ces certificats auto-signés lorsqu'une autorité de certification n'est pas disponible** est l'option par défaut. Cette option permet d'utiliser EFS sans mettre en œuvre une autorité de certification.

**Taille de la clé pour les certificats auto-signés** définit la longueur de la clé utilisée par le chiffrement.

**Modèle EFS pour les demandes automatiques de certificats** permet de définir le modèle de certificat à utiliser pour gérer les certificats. S'utilise pour définir des certificats personnalisés.

## 7. Utiliser EFS via l'invite de commandes



Vous pouvez utiliser la commande `cipher` pour :

- chiffrer ou déchiffrer des fichiers, des dossiers ;

- lister et localiser les fichiers chiffrés ;
- obtenir un nouveau certificat EFS ;
- sauvegarder les clés.

La syntaxe est la suivante :

```
C:\>cipher /?
Affiche ou modifie le chiffrement de répertoires [fichiers] sur
partitions NTFS.

CIPHER [/E | /D | /C]
    [/S:rép] [/B] [/H] [chemin [...]]]

CIPHER /K

CIPHER /R:nomfich [/SMARTCARD]

CIPHER /U [/N]

CIPHER /W:rép

CIPHER /X[:fichEFS] [nomfich]

CIPHER /Y

CIPHER /ADDUSER [/CERTHASH:hach | /CERTFILE:nomfich]
    [/S:rép] [/B] [/H] [chemin [...]]]

CIPHER /REMOVEUSER /CERTHASH:hach
    [/S:rép] [/B] [/H] [chemin [...]]]

CIPHER /REKEY [Chemin [...]]

/B      Abandon sur erreur. Par défaut, CIPHER continue
       l'exéc. même sur erreur.
/C      Affiche des infos sur le fichier chiffré.
/D      Déchiffre fichiers ou rép. spéciés.
/E      Chiffre fichiers ou rép. Les rép.
       sont marqués pour que les fichiers ajoutés + tard soient
       chiffrés. Le fichier chiffré peut devenir déchiffré lors
       de modifs si son rép parent n'est pas chiffré. Le
       chiffrement du fichier et du rép. parent est conseillé.
/H      Affiche les fichiers avec les attrib. Caché ou Système. Ces
       fichiers sont omis par défaut.
/K      Crée certif. et clé à utiliser avec EFS. Si
       cette option est choisie, ttes les autres sont ignorées.
/N      Cette option fonctionne uniqt avec /U. Elle empêche la
       MÀJ des clés. Elle permet de rechercher ts les
       fichiers chiffrés sur les lecteurs locaux.
/R      Crée une clé et un certif. d'agent de récup. EFS et les
       écrit ds un fichier .PFX <contenant certificat et clé
       privée> et un fichier .CER <contenant uniqt le certif>.
       Un Administrateur peut ajouter le contenu du fichier .CER à la
       stratégie de récup. EFS pour créer l'agent de récup.
       pr les utilisateurs et importer le fichier .PFX pour récupérer
       des fichiers individuels. Si SMARTCARD est spécié, écrit
       la clé de récupération et le certificat sur une carte à puce.
       Un fichier .CER est généré <if il ne contient que le certificat>.
       Aucun fichier .PFX n'est généré.
/S      Effectue l'opération spéciée sur les rép. d'un
       rép. donné et ts ses ss-rép.
/U      Essaie d'atteindre ts les fichiers chiffrés sur les lecteurs
       locaux. Cette option MÀJ la clé de chiffrement de fichier
       de l'utilisateur ou la clé de l'agent de récup. avec les
       clés en cours si elles ont été modifiées. Elle ne fonctionne
       avec aucune autre option sauf /N.
```

/W	Supprime les données de l'espace disque inutilisé sur l'intégralité d'un volume. Si cette option est choisie, ttes les autres options st ignorées. Le répertoire spécifié peut être n'importe où sur un volume local. S'il s'agit d'un ou plusieurs pts de montage vers un rép. d'un autre vol., les données de ce vol. sont supprimées.
/X	Sauvegarde certif. et clés EFS dans nomfichier. Si fichEFS est fourni, le ou les certif. de l'utilisateur actif servant à chiffrer le fichier sont sauvegardés. Sinon, certif. et clés EFS en cours de l'utilisateur sont sauvegardés.
/Y	Affiche l'empreinte numérique du certificat EFS actif sur l'ordinateur local.
/ADDUSER	Ajoute un utilisateur aux fichiers chiffrés spécifiés. Si CERTHASH est fourni., le chiffrement recherche un certif. comportant ce hachage SHA1. Si CERTFILE est fourni, le chiffrement extrait le certif. du fichier.
/REKEY	MàJ les fichiers chiffrés pour qu'ils utilisent la clé EFS configurée active.
/REMOVEUSER	Supprime un utilisateur des fichiers spécifiés. CERTHASH doit être le hachage SHA1 du certif. à supprimer.

rép Chemin d'accès à un rép.

nomfich Nom de fichier sans son extension.

chemin Spécifie un modèle, un fichier ou un rép.

fichESF Chemin d'accès à un fichier chiffré.

Utilisé sans paramètres, CIPHER affiche l'état de chiffrement du rép. actif et de ts ses fichiers. Vous pouvez utiliser plusieurs noms de rép. et des caract. génériques. Vous devez placer des espaces entre les param.

Cet utilitaire fonctionne en mode local.

#### **a. Chiffrer le répertoire c:\toto : mais pas son contenu**

```
cipher /E c:\toto
```

#### **b. Chiffrer le dossier et son contenu**

```
cipher /E /S: c:\toto
```

# Mise en œuvre des fichiers hors connexion

## 1. Introduction

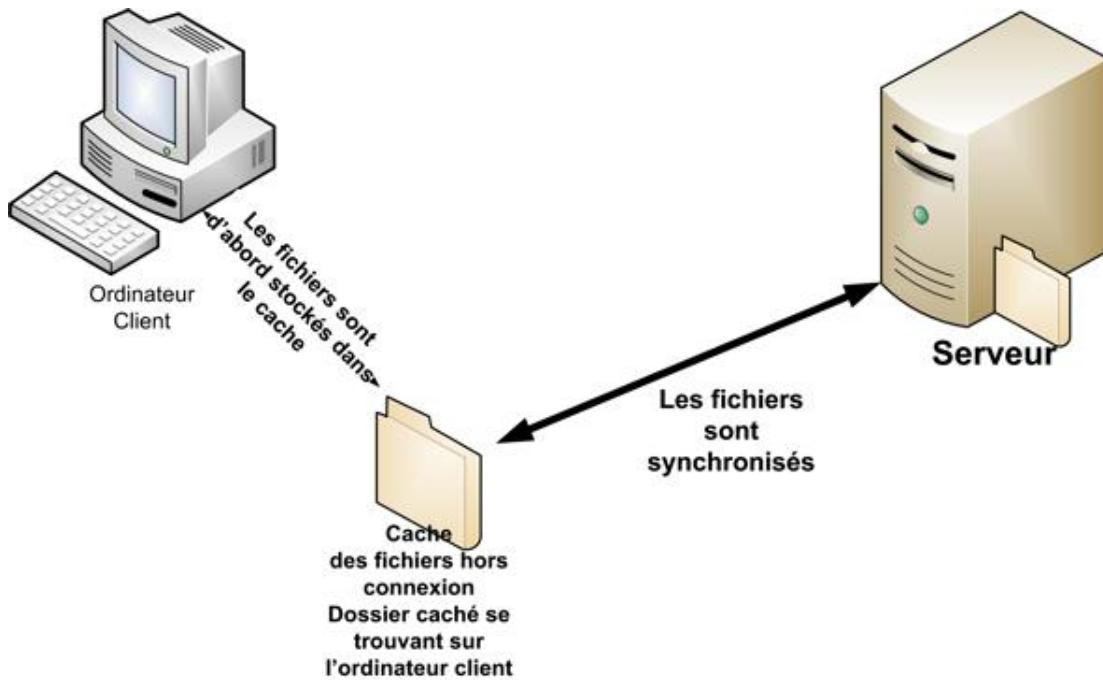
Les fichiers hors connexion peuvent être utilisés dans plusieurs scénarios comme par exemple la publication quotidienne des documents en lecture pour des voyageurs de commerce qui se connectent à l'entreprise chaque matin, ou pour stocker le profil itinérant de l'utilisateur d'ordinateur portable afin qu'il soit disponible à tout moment et que le profil puisse être sauvegardé de temps à autre. Cette fonctionnalité, introduite avec Windows 2000, est facile à mettre en œuvre car il faut un logiciel client et éventuellement, un logiciel serveur.

La partie cliente permet de synchroniser les documents et de préparer un espace disque pour accueillir les fichiers.

La partie serveur indique au client comment gérer les documents hors connexion.

Pour un serveur exécutant Terminal Server, il n'est pas possible d'être client pour des fichiers hors connexion. L'onglet correspondant n'est pas disponible.

La figure suivante montre le principe de fonctionnement : lorsqu'un fichier d'un serveur est configuré pour utiliser les fichiers hors connexion, il est stocké dans un cache de l'ordinateur client et de ce fait, devient disponible à tout moment. L'utilisateur peut le lire, le modifier et sauvegarder les modifications. Celles-ci sont enregistrées dans le fichier en cache avant que le système client des fichiers hors connexion tente de synchroniser la version se trouvant sur le serveur. Si ce dernier n'est pas disponible, la synchronisation aura lieu dès que le serveur devient disponible. La procédure est transparente et seule la résolution d'un conflit comme par exemple la modification du fichier des deux côtés (client et serveur) entraîne une intervention de l'utilisateur pour choisir comment résoudre ce conflit.



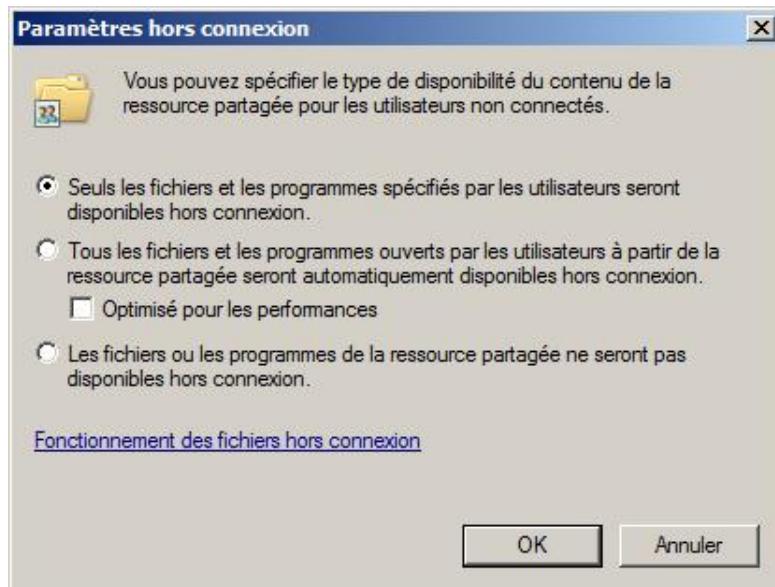
## 2. Mise en œuvre de la partie serveur



En fait, il n'y a rien à faire car par défaut les fichiers et dossiers peuvent être mis en cache. Néanmoins, vous pouvez contrôler comment la mise en cache peut s'effectuer en utilisant la procédure suivante :

- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier concerné.

- Cliquez avec le bouton droit de la souris sur le dossier puis cliquez sur **Propriétés**.
- Dans l'onglet **Partage**, cliquez sur le bouton **Avancé**.
- Cliquez sur le bouton **Mise en cache**.



Les fichiers peuvent être mis en cache par les utilisateurs :

- S'ils sont spécifiés par l'utilisateur, correspond à l'option **Seuls les fichiers et les programmes spécifiés par les utilisateurs seront disponibles hors connexion**.
- Automatiquement mais seulement pour les fichiers correspond à l'option **Tous les fichiers et les programmes ouverts par les utilisateurs à partir de la ressource partagée seront automatiquement disponibles hors connexion**.
- Automatiquement pour les fichiers et les programmes correspond à l'option **Tous les fichiers et les programmes ouverts par les utilisateurs à partir de la ressource partagée seront automatiquement disponibles hors connexion** avec la case à cocher **Optimisé pour les performances**.
- Jamais correspond à l'option **Les fichiers ou les programmes de la ressource partagée ne seront pas disponibles hors connexion**.



Il est possible d'utiliser la commande suivante `net share NomDuPartage /cache:manual | documents | programs | none`.

### 3. Mise en œuvre de la partie cliente



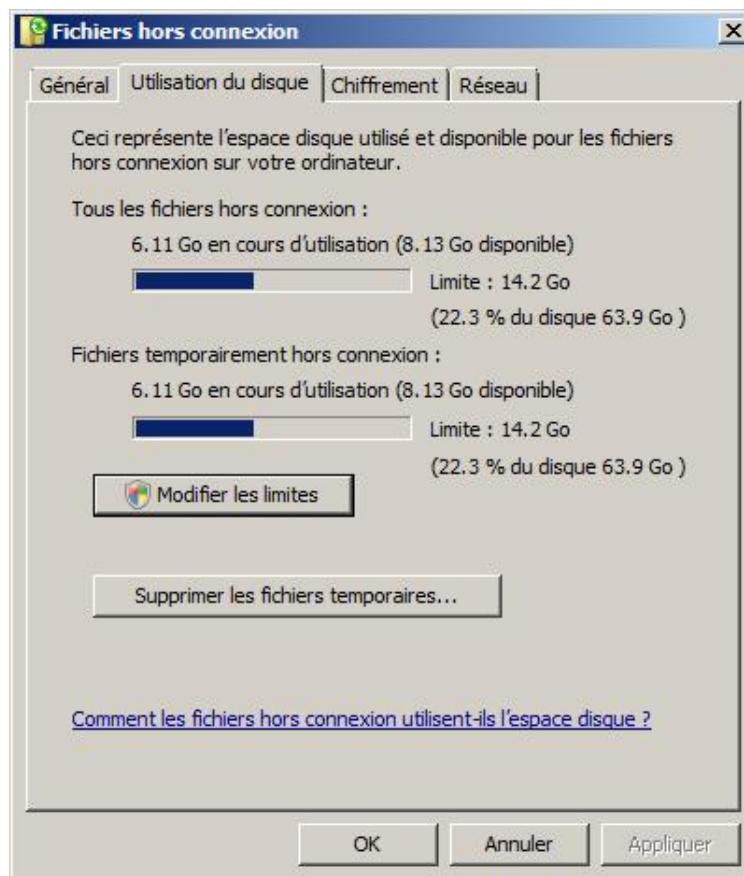
#### a. Activer les fichiers hors connexion

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer** puis **Panneau de configuration**.

- Si l'affichage n'est pas en mode classique, cliquez sur **Affichage classique** et cliquez sur l'icône **Fichiers hors connexion**.
- Cliquez sur le bouton **Autoriser l'utilisation des fichiers hors connexion** si cette fonctionnalité n'est pas déjà activée puis cliquez sur **OK**. Vous devez redémarrer l'ordinateur pour que les modifications soient prises en compte.

### b. Configurer les fichiers hors connexion

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer** puis **Panneau de configuration**.
- En mode **Affichage classique**, cliquez sur l'icône **Fichiers hors connexion**.
- Cliquez sur l'onglet **Utilisation du disque**.



L'onglet affiche l'utilisation de l'espace disque pour les fichiers hors connexion que ce soit pour des fichiers temporaires (par exemple utilisés par la sauvegarde) ou pour tous les fichiers. L'espace réservé par défaut est de 22,3 % du volume. Vous pouvez modifier ces valeurs en cliquant sur le bouton **Modifier les limites**. Vous pouvez récupérer l'espace occupé par les fichiers mis temporairement hors connexion en cliquant sur le bouton **Supprimer les fichiers temporaires**.

- Cliquez sur l'onglet **Chiffrement**, puis cliquez sur **Chiffrer** si vous voulez améliorer la confidentialité des données hors connexion. Par défaut, les données ne sont pas chiffrées.

### c. Rendre toujours disponible hors connexion

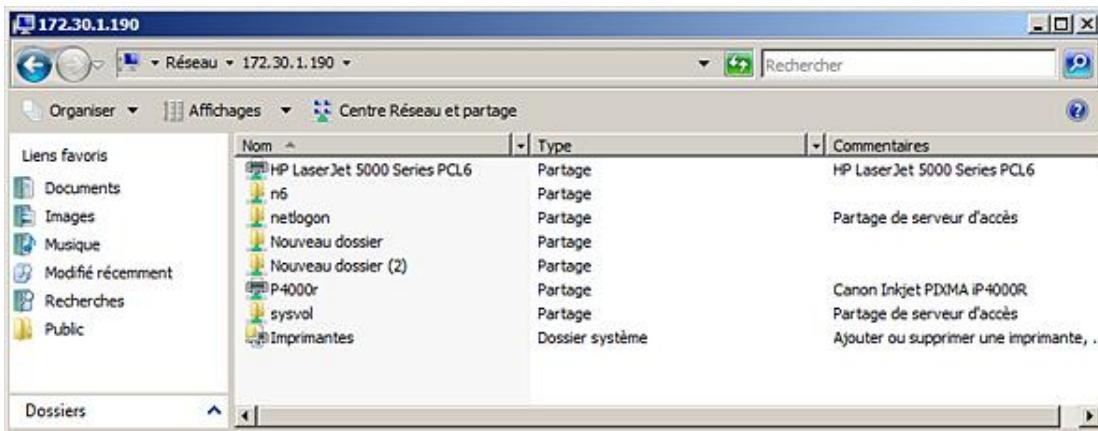


Win

Il est possible de rendre disponibles hors connexion des fichiers et des dossiers en utilisant la procédure suivante.

C'est à l'utilisateur de décider s'il doit rendre disponible hors connexion un dossier complet ou seulement des fichiers.

- Connectez-vous sur votre ordinateur.
- Ouvrez un dossier partagé sur un autre serveur en utilisant un chemin UNC tel que \\serveur. Une fenêtre montre les partages disponibles :



- Cliquez avec le bouton droit de la souris sur le dossier dont vous voulez rendre disponibles hors connexion les objets puis cliquez sur **Propriétés**.
- Cliquez sur l'onglet **Fichiers hors connexion**.
- Sélectionnez la case à cocher **Toujours disponible hors connexion**.
- Pour synchroniser le dossier, vous pouvez cliquer sur le bouton **Synchroniser maintenant**.
- Cliquez sur **OK**.



Vous pouvez également ouvrir le **Centre de synchronisation** à partir du paramètre **Fichiers hors connexion** du **Panneau de configuration**.

#### d. Afficher les fichiers hors connexion



Win

Une des méthodes pour afficher les fichiers hors connexion est la suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer** puis **Panneau de configuration**.
- En mode **Affichage classique**, cliquez sur l'icône **Fichiers hors connexion**.



Une autre méthode consiste à utiliser le chemin UNC.

---

# Mise en œuvre des quotas

## 1. Introduction

Certaines entreprises veulent limiter la quantité de données que les utilisateurs peuvent stocker, et pour éviter que quelques utilisateurs occupent tout l'espace disponible il est possible de restreindre l'espace par utilisateur à l'aide des quotas.

Windows Server permet, depuis la version 2000, de gérer les quotas sur des volumes utilisant le système de fichiers NTFS, la granularité étant le volume.

En activant les quotas, l'administrateur peut limiter l'espace disque alloué aux utilisateurs.

Il est conseillé de ne pas activer les quotas sur les disques contenant les profils de l'utilisateur.

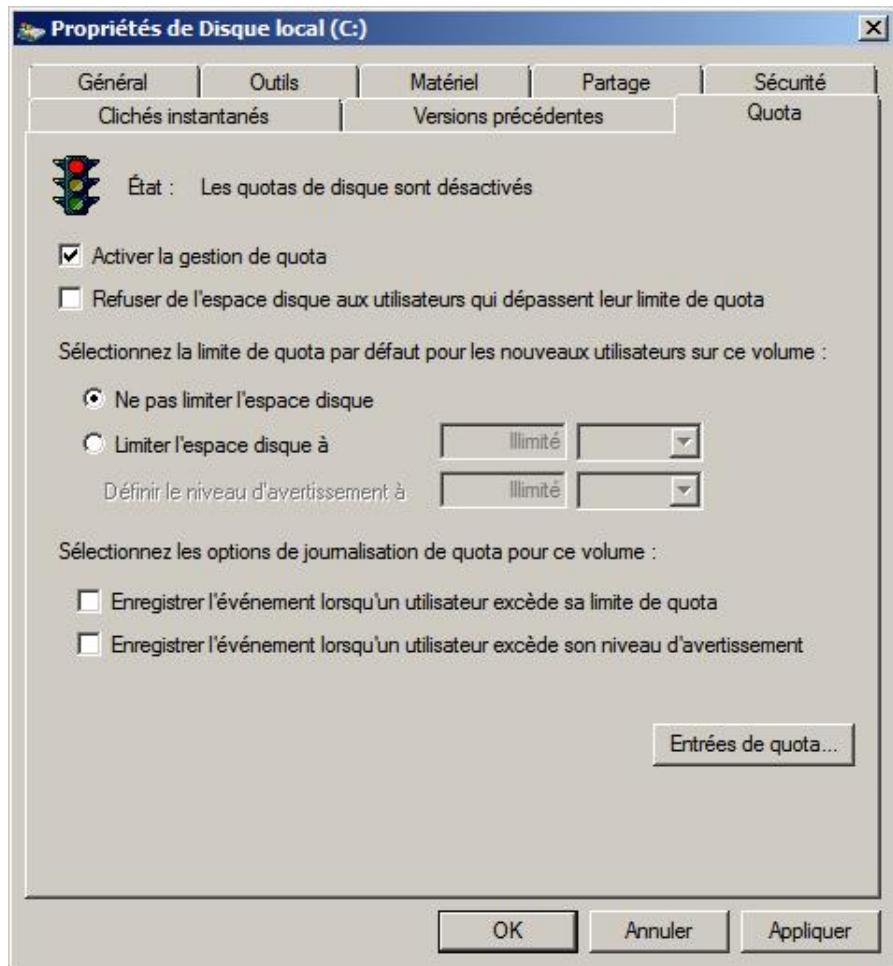
## 2. Activation des quotas



- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou le **Poste de travail**.
- Sélectionnez le lecteur disque sur lequel vous voulez activer les quotas, puis cliquez avec le bouton droit de la souris sur le lecteur et enfin cliquez sur **Propriétés**.
- Dans l'onglet **Quota**, cliquez sur la case à cocher **Activer la gestion de quota**.



L'activation des quotas s'applique à tous les fichiers déjà créés de tous les utilisateurs. En conséquence, il faut être prudent lorsque vous activez les quotas.



La case à cocher **Activer la gestion de quota** active ou désactive les quotas ; attention, une fois que les quotas sont activés, leur désactivation n'efface pas les entrées que vous avez placées. Les quotas ne sont plus contrôlés.

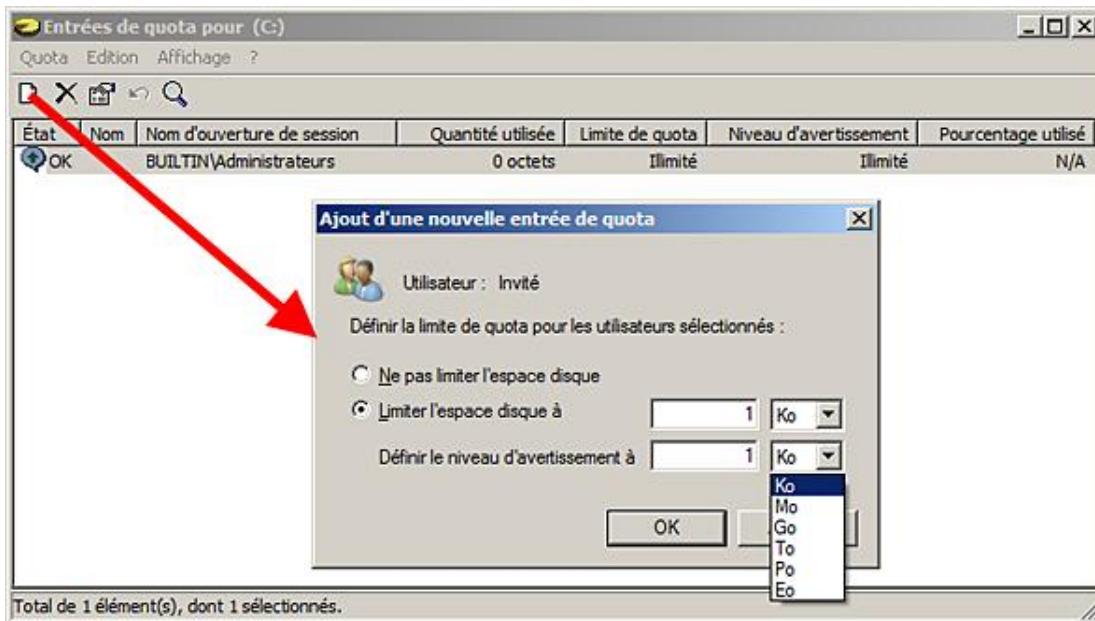
La case à cocher **Refuser de l'espace disque aux utilisateurs qui dépassent leur limite de quota** garantit que l'utilisateur ne peut pas dépasser l'espace qui lui est alloué.

L'option de limite du quota par défaut définit un quota pour tous les utilisateurs de l'une des manières suivantes :

- **Ne pas limiter l'espace disque** (défaut), une exception est possible en cliquant sur le bouton **Entrées de quota**.
- **Limiter l'espace disque à** vous permet de spécifier un niveau d'alerte et un niveau maximal. Les valeurs peuvent être exprimées en (Ko, Mo, Go, To, Po et Eo).

La case à cocher **Enregistrer l'événement lorsqu'un utilisateur excède sa limite de quota** et la case à cocher **Enregistrer l'événement lorsqu'un utilisateur excède son niveau d'avertissement** permettent d'ajouter un événement dans le journal des événements.

Le bouton **Entrées de quota** permet de définir un quota pour un utilisateur, comme le montre la boîte de dialogue suivante.



Chaque ligne correspond à une entrée de quota pour un utilisateur. Il est possible de lui affecter une règle de quota différente par rapport à la règle par défaut pour tous les utilisateurs. Vous ne pouvez pas supprimer une règle de quota tant que l'utilisateur est propriétaire d'au moins un des fichiers.

- Un administrateur local n'est pas affecté par les règles des quotas.
- Lorsqu'un fichier est comprimé, le système se base sur sa taille non compressée pour calculer les quotas.

### 3. Ligne de commande



Vous pouvez également utiliser la commande `fsutil quota` pour gérer les quotas sur des volumes NTFS.

Pour afficher les quotas sur un volume : `fsutil quota query`

Plus loin, vous apprendrez à gérer les quotas à l'aide du **Gestionnaire de ressources du serveur de fichiers**.

# Les clichés instantanés (Shadow copy)

## 1. Introduction

Apparus dans Windows Server 2003, les clichés instantanés permettent de créer des copies ponctuelles de tous les dossiers partagés d'un volume.

Il ne s'agit pas d'un nouveau type de sauvegarde mais d'une possibilité pour l'utilisateur de récupérer un fichier à un moment particulier sans aide.

Par défaut, l'utilisateur accède toujours à la version la plus récente. Néanmoins, il arrive qu'un fichier soit effacé par erreur, et dans ce cas l'utilisateur a des chances de retrouver son fichier en partie ou en totalité. L'activation des clichés instantanés ne garantit pas une récupération à 100 %.

Le fonctionnement des clichés instantanés est simple. Après avoir défini le volume, la zone de stockage et la planification, le système crée un cliché instantané pour tous les dossiers partagés du volume, puis selon la planification, seules les modifications sont enregistrées.

Pour des raisons d'efficacité et de rapidité, les clichés instantanés travaillent au niveau des secteurs de disque et non des fichiers.

## 2. Meilleures pratiques

- Choisissez un volume distinct pour stocker les clichés instantanés.
- Concevez une vraie stratégie pour vos clichés instantanés en ce qui concerne les dossiers candidats pour les réunir sur un volume spécifique, la fréquence de création afin de correspondre aux besoins de vos utilisateurs, et l'espace disque supplémentaire nécessaire.

---

 Les lecteurs associés à un point de montage ne sont pas pris en charge par les clichés instantanés.

---

- Sauvegardez les données du volume normalement, y compris les dossiers partagés.
- Ne définissez aucune planification ayant une fréquence inférieure à une heure.
- Formatez le volume où vous activez les clichés instantanés avec une taille de cluster disque égale ou supérieure à 16 Ko.
- Formez les utilisateurs à l'utilisation de cette fonctionnalité.

## 3. Mise en œuvre des clichés instantanés sur le serveur



Il existe au moins trois méthodes pour lancer l'utilitaire de configuration des clichés instantanés.

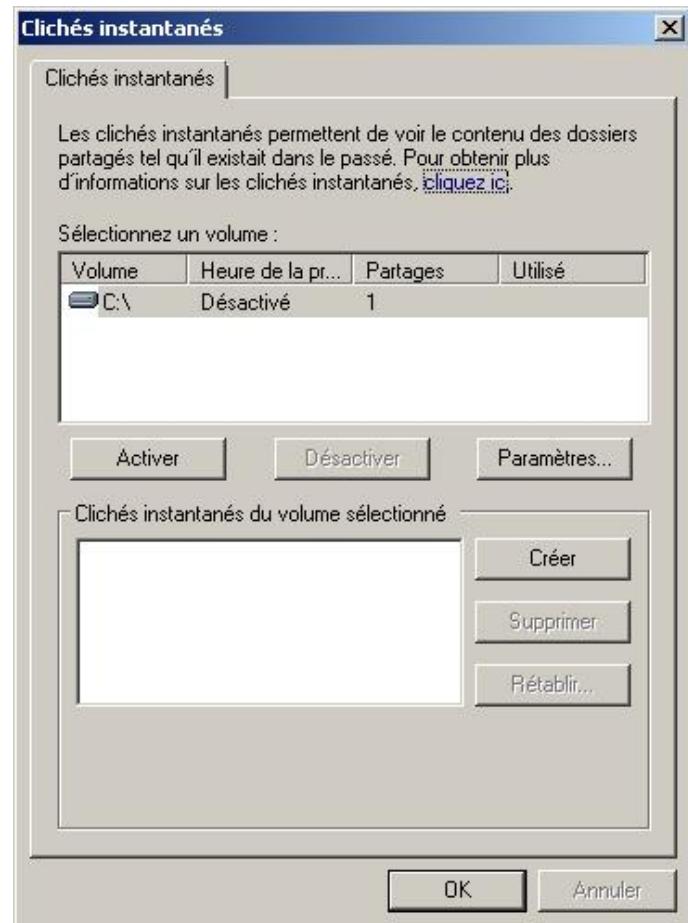
- Sur le serveur, cliquez sur **Démarrer** puis sur **Ordinateur**.
- Dans **Ordinateur**, sélectionnez le lecteur de disque dur où vous voulez activer les clichés instantanés puis cliquez avec le bouton droit de la souris et cliquez sur **Configurer les clichés instantanés**.

---

 Le système de fichiers doit être formaté en NTFS.

---

- Dans la boîte de dialogue **Clichés instantanés**, cliquez sur **Paramètres**.



La granularité la plus fine est le volume et tous les partages du volume bénéficient de la fonctionnalité de clichés instantanés.

- Sélectionnez une **Zone de stockage**.



Il n'est pas possible de sélectionner un espace de stockage sur le réseau.

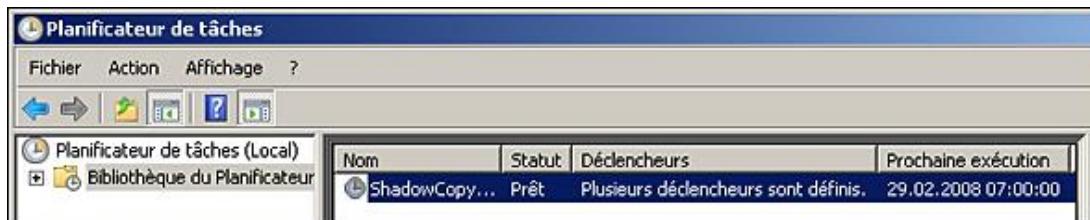
Par défaut, le système utilise 300 Mo jusqu'à concurrence de 10 % de l'espace disque disponible. Il est possible de modifier cette limite selon les besoins planifiés ou de limiter la taille jusqu'à concurrence de l'espace disque disponible.

Les clichés instantanés sont stockés dans le dossier système caché appelé **System Volume Information**.

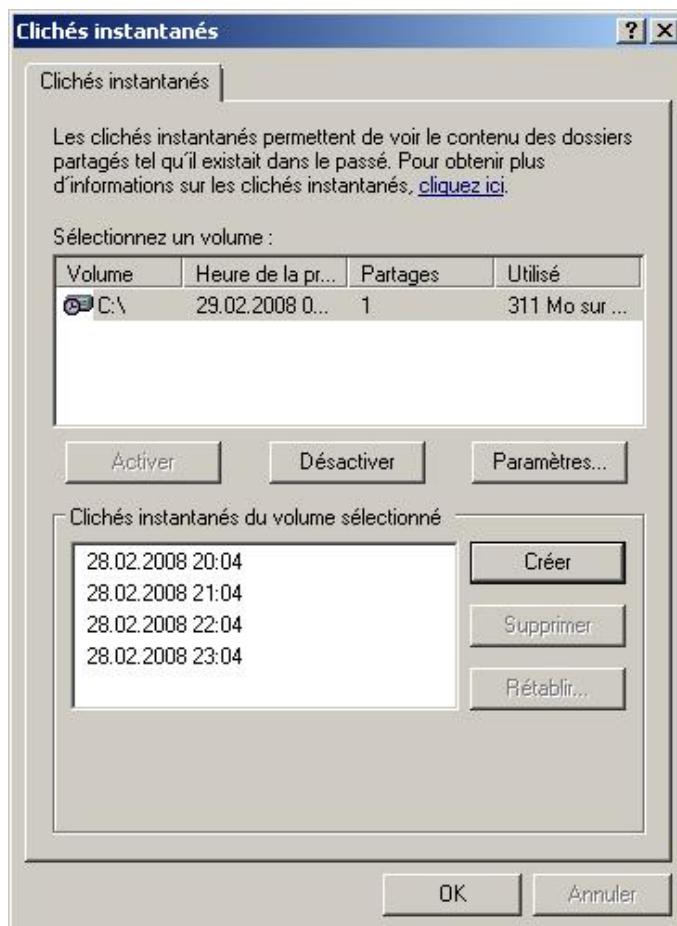
Si le système n'a plus assez d'espace sur le volume de stockage, il écrase automatiquement les clichés instantanés les plus anciens. D'autre part, le nombre total de clichés instantanés pouvant être stockés est de 64 par volume.

Le bouton **Détails** affiche l'espace disponible et l'espace utilisé par les clichés instantanés sur le volume. Le bouton **Planifier** permet de définir les horaires pour la création des clichés instantanés. Il active également les clichés instantanés. Par défaut, le système effectue deux clichés instantanés par jour du lundi au vendredi, soit un à 7h00 et un autre à midi. Il est possible d'ajouter de nouvelles planifications pour augmenter la fréquence ou de modifier les planifications existantes, voire de les supprimer.

Il est recommandé de ne pas créer plus d'un cliché instantané par heure. L'image suivante montre la planification créée :



Contrôlez que les clichés instantanés ont été activés, sinon cliquez sur le bouton **Activer**. C'est une bonne pratique de créer un cliché instantané initial. Si le volume de données est très important, il est recommandé de planifier la création du cliché instantané initial à un moment où le serveur sera peu chargé.



Le bouton **Créer** sert surtout pour effectuer des tests et des dépannages.

Le bouton **Supprimer** permet de détruire un cliché instantané spécifique.

Le bouton **Rétablir** permet de revenir pour un volume particulier à une version spécifique du cliché instantané. Toutes les modifications faites depuis la date de la version du cliché instantané sont perdues et l'opération ne peut être annulée. Il faut en user avec précaution.

Le bouton **Désactiver** supprime tous les clichés instantanés créés ainsi que la planification associée.

Les problèmes susceptibles d'être rencontrés sont :

- Erreur 7001 dans le journal des événements qui signifie qu'une tâche planifiée n'a pas pu être exécutée. Cette erreur surgit lorsque le volume contenant un cliché instantané est supprimé mais pas la tâche planifiée. Il suffit simplement de supprimer la tâche planifiée.
- Si des clichés instantanés sont supprimés alors qu'il reste de la place sur le disque, il suffit de contrôler si le nombre de 64 clichés instantanés a été atteint et si oui, de modifier la planification.

## 4. Mise en œuvre via l'invite de commandes



Il est possible d'utiliser la commande vssadmin pour gérer les clichés instantanés.

L'image suivante montre la commande à utiliser pour activer les clichés instantanés pour le volume C:\.

Une capture d'écran d'une invite de commandes sous Windows. La fenêtre a le titre "Administrator : Invite de commandes". Le prompt est "C:\>". La commande entrée est "vssadmin create shadow /For=c:". La réponse de la ligne de commande indique : "vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume", "Copyright 2001-2005 Microsoft Corp.", "Le cliché instantané de 'c:' a été créé.", "ID du cliché instantané : {132a077b-4263-4d17-b30c-8e6099712c35}", "Nom du volume de cliché instantané : \GLOBALROOT\Device\HarddiskVolumeShadowCopy8".

Il faut encore créer une planification soit en utilisant le Planificateur de tâches, soit en utilisant la commande schtasks.

## 5. Installation de la partie cliente

Par défaut, les systèmes d'exploitation Windows Vista, Windows Server 2003 et Windows Server 2008 disposent déjà du client **Restaurer les versions précédentes**.

Pour les systèmes d'exploitation antérieurs, il faut au préalable installer le client **ShadowCopyClient.msi** en le téléchargeant depuis le site de Microsoft.

Une version de ce client est également disponible pour Windows XP sur un serveur Windows 2003 dans le dossier **%systemroot%\system32\clients\twclient\x86** sous le nom de **twcli32.msi**.

## 6. Récupération d'un fichier, d'un dossier ou d'un volume

Pour récupérer un fichier, la procédure est simple :

- Connectez-vous au serveur en utilisant un chemin UNC : **\nom du Serveur\NomduPartage**.
- Sélectionnez le fichier puis cliquez avec le bouton droit de la souris et sélectionnez **Restaurer les versions précédentes**.
- Dans l'onglet **Versions précédentes**, sélectionnez la version en fonction de l'heure puis appuyez sur un des boutons (**Ouvrir, Copier ou Restaurer**).



Il existe en tout trois versions du document *Nouvelle image Bitmap.bmp*, la version actuelle plus une version datée du 28/02/08 à 23h41 et une autre à 23h34.

Le bouton **Ouvrir** permet de visualiser le document de la version du cliché instantané sélectionnée. Le bouton **Copier** permet de créer une nouvelle copie du document, par exemple pour le comparer à la toute dernière version. Le bouton **Restaurer** remplace la version actuelle par la version sélectionnée. La restauration est définitive et ne peut être annulée.

- 
- Il est également possible de restaurer un dossier complet si le chemin UNC se limite au serveur, soit \\serveur.
-

# Mise en œuvre de la compression

## 1. Introduction

Depuis plusieurs années, le besoin en espace disque n'a cessé d'augmenter dans les entreprises alors que le coût de stockage par mégaoctet n'a cessé de baisser. Lorsque le prix d'un disque dur était très élevé, plusieurs entreprises ont développé des logiciels de compression de données afin de limiter la taille des fichiers.

Le scénario actuel pour utiliser efficacement la compression concerne les données qui sont peu ou pas modifiées et dont la taille du fichier dépasse la taille du cluster disque.

Il ne faut pas oublier que si la taille du fichier est inférieure à la taille du cluster disque, le fichier occupe un cluster disque. Il n'y a pas d'intérêt à compresser des fichiers de petite taille.

En terme de performance, il est admis que le temps de calcul pour la compression ou la décompression est compensé par le fait que moins de clusters disques sont lus ou écrits.

Microsoft Windows permet d'utiliser la compression de manière transparente pour le système de fichiers NTFS ainsi que pour l'utilisation des fichiers zip compressés.

## 2. La compression NTFS



Windows Server 2008 permet de compresser des fichiers, des dossiers ou des volumes qui utilisent le système de fichiers NTFS.

La granularité est le fichier, mais il est préférable de compresser un volume ou un dossier.

La compression est totalement transparente pour l'utilisateur.

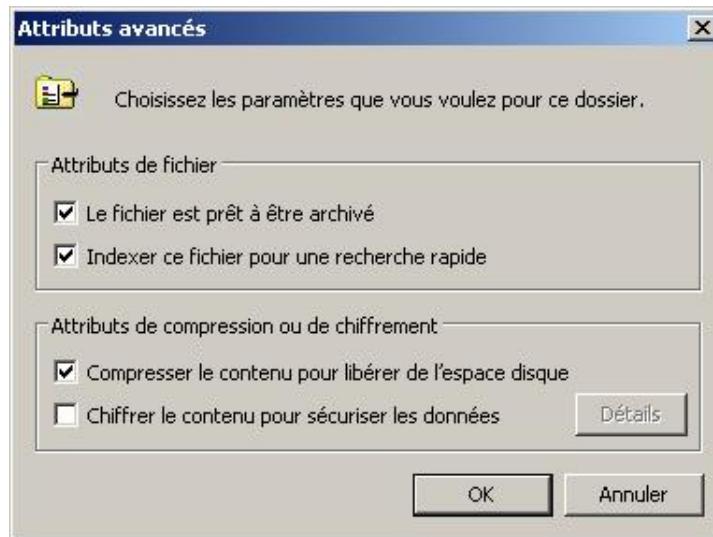
Il est possible de compresser le disque de boot, mais ce n'est pas recommandé pour des questions de performance.

Concernant la copie ou le déplacement de fichiers, les règles suivantes s'appliquent :

	<b>Sur le même volume</b>	<b>Sur des volumes différents</b>
<b>Déplacement d'un dossier source A vers un dossier de destination B</b>	Conserve les attributs de compression du dossier source*	Hérite des attributs de compression du dossier de destination
<b>Copie d'un dossier source A vers un dossier de destination B</b>	Hérite des attributs de compression du dossier de destination	Hérite des attributs de compression du dossier de destination

\* Si le fichier existe déjà mais que les attributs de compression sont différents, seul le contenu est déplacé.

- Pour activer la compression au niveau d'un fichier, d'un dossier ou d'un volume, ouvrez la fenêtre **Ordinateur**, déplacez-vous vers le type d'objet à compresser puis sélectionnez-le.
- Cliquez avec le bouton droit de la souris puis cliquez sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés de**, cliquez sur **Avancé**.
- Dans la boîte de dialogue **Attributs avancés**, sélectionnez **Compresser le contenu pour libérer de l'espace disque** puis cliquez sur **OK**.



- Il n'est pas possible de compresser et de chiffrer le contenu en même temps.

Un message vous demandant de confirmer la portée (soit dossier actuel, soit dossier actuel et tous les sous-dossiers et fichiers) des modifications que vous allez apporter peut apparaître, sélectionnez l'option qui convient puis cliquez sur **OK**.

- Les fichiers compressés apparaissent par défaut en bleu. Il est possible de supprimer la couleur en passant par la boîte de dialogue **Options des dossiers** puis l'onglet **Affichage**.

Il est possible d'utiliser la commande compact avec l'invite de commande.

La commande suivante décomprime le volume **C:**, y compris les sous-dossiers et les fichiers système ou cachés. En cas d'erreur, la commande continue sans s'arrêter.

```
C:\>compact /u /s:c: /f /I /A
Paramétrage du répertoire C:\ pour ne pas compresser les nouveaux fichiers [OK]

Décompression des fichiers dans C:\

$Recycle.Bin [OK]
autoexec.bat [OK]
Boot [OK]
C:\bootmgr: Accès refusé.
BOOTSECT.BAK [OK]
config.sys [OK]
C:\Documents and Settings: Accès refusé.
media [OK]
Nouveau dossier [ERR]
C:\pagefile.sys: Le processus ne peut pas accéder au fichier car ce fichier est
utilisé par un autre processus.
PerfLogs [OK]
```

### 3. La compression ZIP



Win

Le format ZIP est un format populaire de fichiers compressés. Son grand avantage vient du fait qu'il s'affranchit du système d'exploitation, du système de fichiers utilisé et que les données peuvent rester compressées lorsqu'elles transitent sur le réseau.

Largement utilisée à l'âge d'or des disquettes, la compression ZIP est apparue en tant qu'extension depuis Windows XP. Cette extension permet à l'utilisateur de compresser rapidement un ou plusieurs fichiers en les envoyant vers un dossier compressé au format ZIP. L'utilisateur dispose alors de deux versions du fichier, une compressée et une normale.

La lecture, la copie et le déplacement sont transparents pour l'utilisateur.

- Pour compresser un fichier ou un dossier au format zip, ouvrez la fenêtre **Ordinateur**, déplacez-vous vers le type d'objet à compresser puis sélectionnez-le.
- Cliquez avec le bouton droit de la souris puis cliquez sur **Envoyer vers - Dossier compressé**.
- Pour extraire le contenu d'un dossier au format zip, ouvrez la fenêtre Ordinateur, déplacez-vous vers une archive ZIP puis sélectionnez-la.
- Cliquez avec le bouton droit de la souris puis cliquez sur **Extraire tout**.
- Dans la boîte de dialogue **Extraire les dossiers compressés**, saisissez l'emplacement du dossier de destination (le dossier sera créé si nécessaire) ou sélectionnez-en un en cliquant sur **Parcourir**.

Le document ZIP original n'est pas supprimé ou altéré par cette opération.

---

 Pour les extractions, une autre méthode consiste à ouvrir la fenêtre **Ordinateur** et se déplacer dans le dossier compressé puis à copier ou déplacer les fichiers.

---

## 4. Utilitaire en ligne de commande

Vous pouvez utiliser la commande **compact**.

La commande suivante compresse le répertoire actuel, ses sous-répertoires ainsi que les fichiers existants :

```
compact /c /s
```

Afficher l'état de compression des fichiers du répertoire actuel : **compact**.

## Les partages

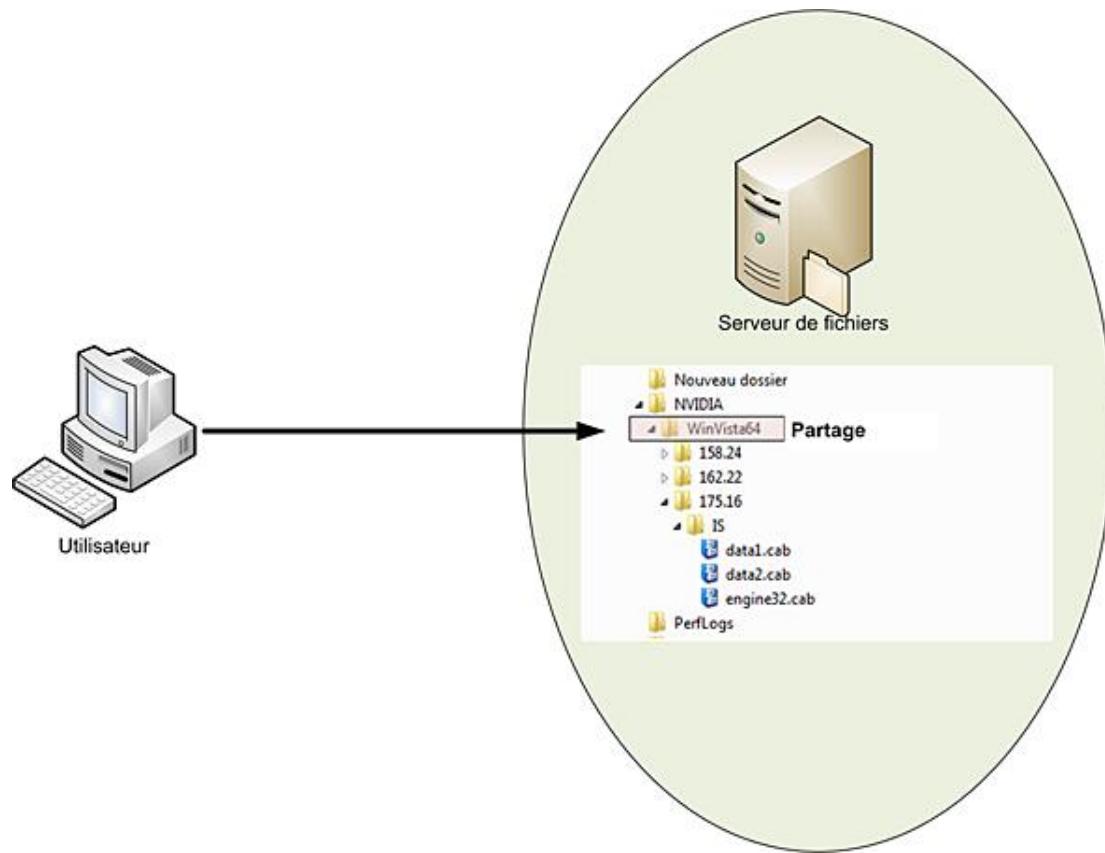
Un partage est un point d'entrée réseau pour accéder à des ressources de type fichier sur un serveur. Il est possible de créer plusieurs points de partage sur un serveur, de même qu'un unique dossier peut correspondre à plusieurs points de partage nommés différemment et disposant de permissions différentes.

À partir d'un point de partage, l'utilisateur a accès à toute l'arborescence de fichiers se trouvant au-dessous. Bien entendu, si le volume qui contient l'arborescence est formaté avec le système de fichiers NTFS, les permissions NTFS peuvent empêcher l'utilisateur d'avoir accès aux objets.

L'accès au dossier partagé utilise un chemin **UNC** (*Universal Convention Name*) qui utilise la syntaxe suivante **\NomDuServeur\NomDuPartage**.

Vous pouvez ajouter le caractère dollar à la fin du partage pour qu'il soit caché, c'est-à-dire qu'il n'apparaîsse pas dans la liste des partages.

La figure suivante montre un partage appelé **WinVista64** où l'utilisateur aura, une fois connecté, accès à tous les dossiers et fichiers situés en dessous.



Il est conseillé de :

- créer les points de partage le plus haut possible dans la hiérarchie selon les besoins de l'entreprise.
- créer autant de points de partage que nécessaire.

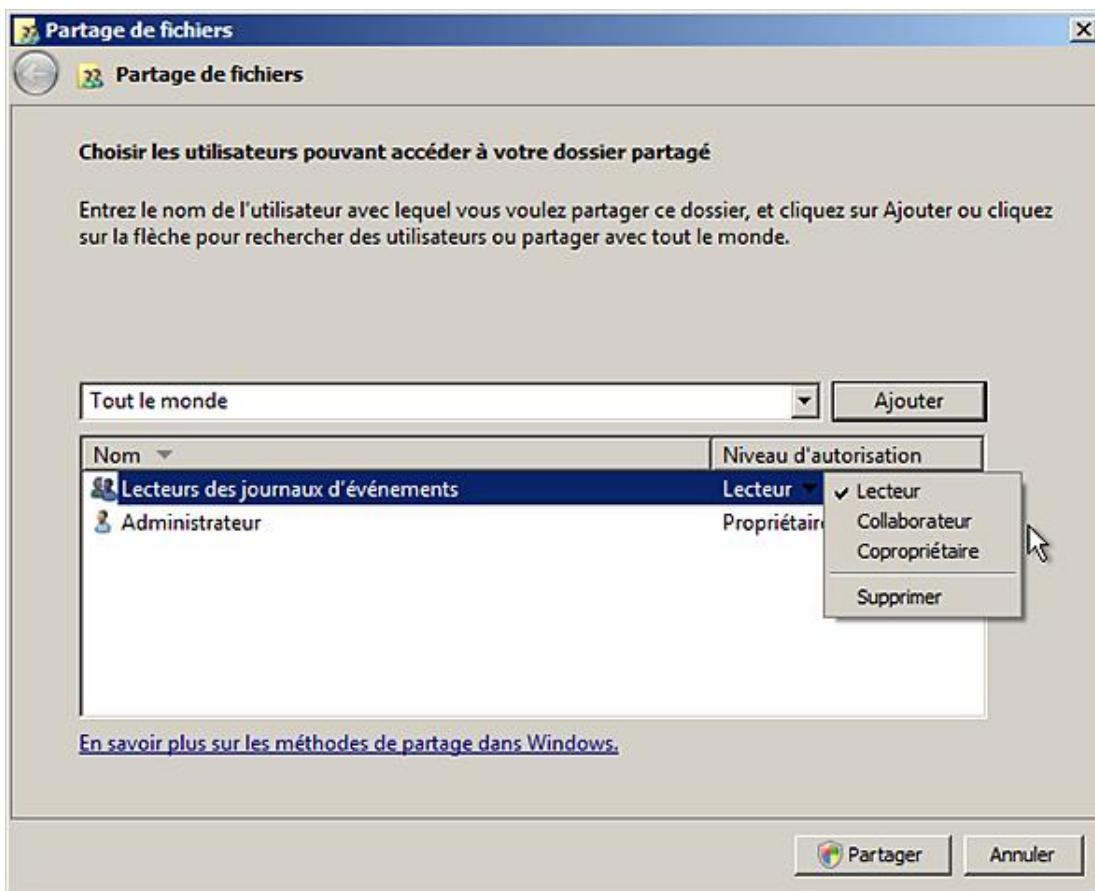
**►** Le déplacement d'un dossier partagé supprime le partage. Dans Windows Server 2008, Microsoft a ajouté de nouveaux outils pour la création et la gestion des partages, ce qui multiplie les procédures et rend confus le choix de la bonne procédure.

### 1. Création d'un partage en utilisant l'assistant



Win

- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier que vous voulez partager.
- Cliquez avec le bouton droit de la souris sur le dossier puis sur **Partager**.



La liste déroulante permet de sélectionner un utilisateur ou un groupe à ajouter. La liste contient le nom des utilisateurs ou des groupes pouvant accéder au partage ainsi que leur niveau d'autorisation qui est décrit plus loin dans ce chapitre.

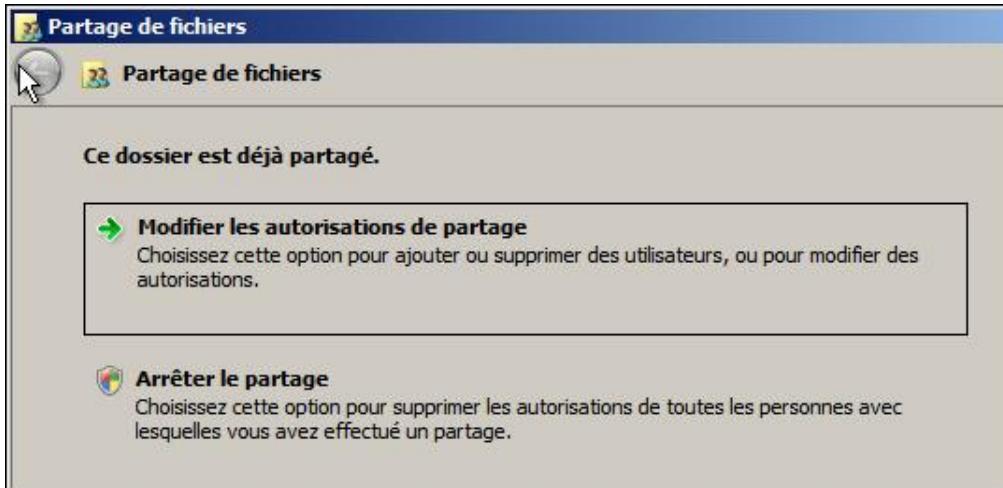
- Cliquez sur la liste déroulante afin d'ajouter des utilisateurs ou des groupes. Si vous ne connaissez pas le nom du groupe, cliquez sur l'option **Rechercher**. Une fois l'utilisateur ou le groupe sélectionné, cliquez sur **Ajouter** pour le faire apparaître dans la liste.
- Modifiez ensuite son niveau d'autorisation (par défaut, **Lecteur**) si nécessaire sinon, ajoutez un autre utilisateur ou groupe ou cliquez sur **Partager**.
- Une nouvelle boîte de dialogue vous informe du nom du partage. Avant de cliquer sur **Terminé**, vous avez la possibilité de cliquer sur le lien **envoyer** afin d'informer les utilisateurs du nouveau partage par courrier électronique ou sur **copier** pour placer un lien vers le partage dans le Presse-papiers.

## 2. Modification d'un partage en utilisant l'assistant



Win

- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier dont vous voulez modifier le partage.



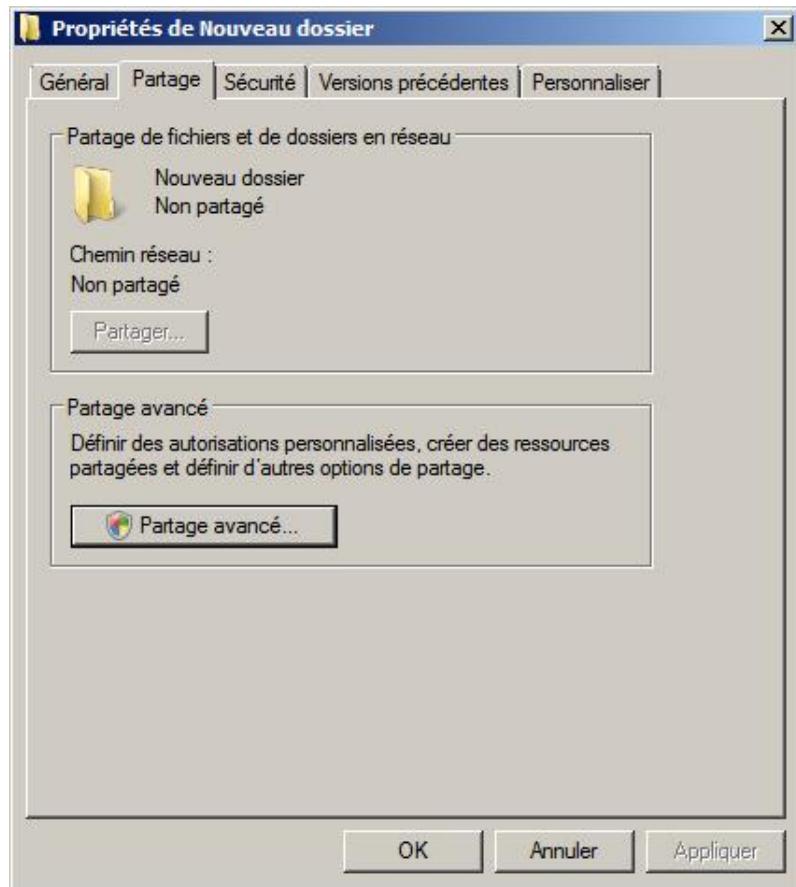
- Cliquez avec le bouton droit de la souris sur le dossier puis sur **Partager**.
- Vous pouvez cliquer sur **Modifier les autorisations de partage** afin de faire apparaître l'assistant **Partage de fichiers** ou sur **Arrêter le partage** si vous désirez ne plus partager le dossier.

### 3. Création ou modification d'un partage sans l'assistant



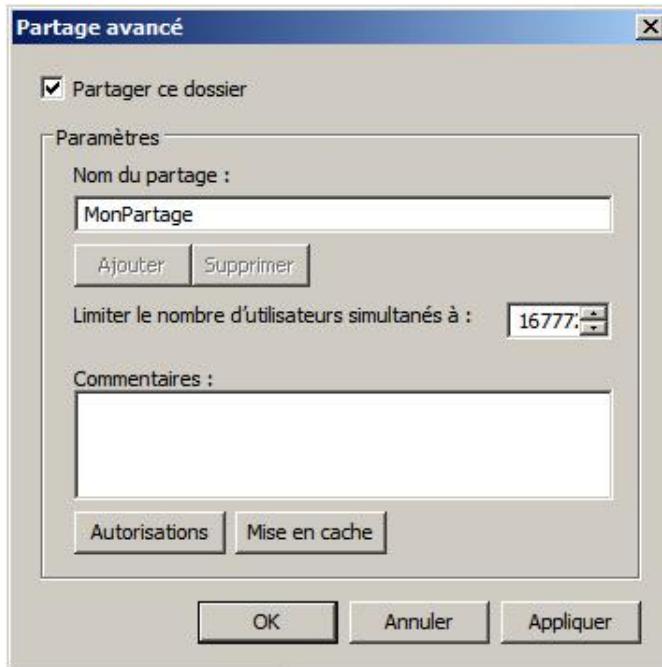
Win

- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier que vous voulez partager.
- Cliquez avec le bouton droit de la souris sur le dossier puis cliquez sur **Propriétés**.
- Cliquez sur l'onglet **Partage**.



Le bouton **Partager** est activé seulement si le partage a été créé avec l'assistant. Il permet d'afficher la boîte de dialogue **Partage de fichiers** pour gérer le partage existant (cf. section Crédit d'un partage).

Le bouton **Partage avancé** permet de créer ou de gérer les partages en mode avancé.



La case à cocher **Partager ce dossier** permet de créer ou supprimer le premier partage appliqué au dossier.

Le **Nom du partage** est le nom du partage courant dont les informations sont affichées en dessous.

- 
- Pour rendre un partage invisible dans l'explorateur, ajoutez le caractère \$ à la fin du nom.
-

Le bouton **Ajouter** permet de créer un autre point de partage pour le dossier.

Le bouton **Supprimer** permet de supprimer un point de partage.

Vous pouvez **Limiter le nombre d'utilisateurs simultanés** à et saisir des **Commentaires** pour le point de partage.

Le bouton **Autorisations** permet d'affecter des permissions au point de partage.

Le bouton **Mise en cache** permet d'indiquer à l'ordinateur client comment mettre en cache les objets si cette fonctionnalité est activée.

## 4. Création d'un partage via l'outil Gestion de l'ordinateur



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** et **Gestion de l'ordinateur**.
- Dans le volet de gauche de la console, cliquez sur le nœud **Dossiers partagés** pour développer l'arborescence.

Nom du p...	Chemin du dossier	Type	Nb. de connexions client	Description
ADMIN\$	C:\Windows	Windows	0	Administration à distance
C\$	C:\	Windows	0	Partage par défaut
home\$	C:\home	Windows	1	
IPC\$		Windows	0	IPC distant
NETLOGON	C:\Windows\SYSVOL...	Windows	0	Partage de serveur d'accès
Nouveau dos...	C:\Nouveau dossier	Windows	0	
Nouveau dos...	C:\Nouveau dossier...	Windows	0	
print\$	C:\Windows\system...	Windows	0	Pilotes d'imprimantes
prnproc\$	C:\Windows\system...	Windows	0	Pilotes d'imprimantes
profil\$	C:\profil	Windows	0	
SYSVOL	C:\Windows\SYSVOL...	Windows	0	Partage de serveur d'accès

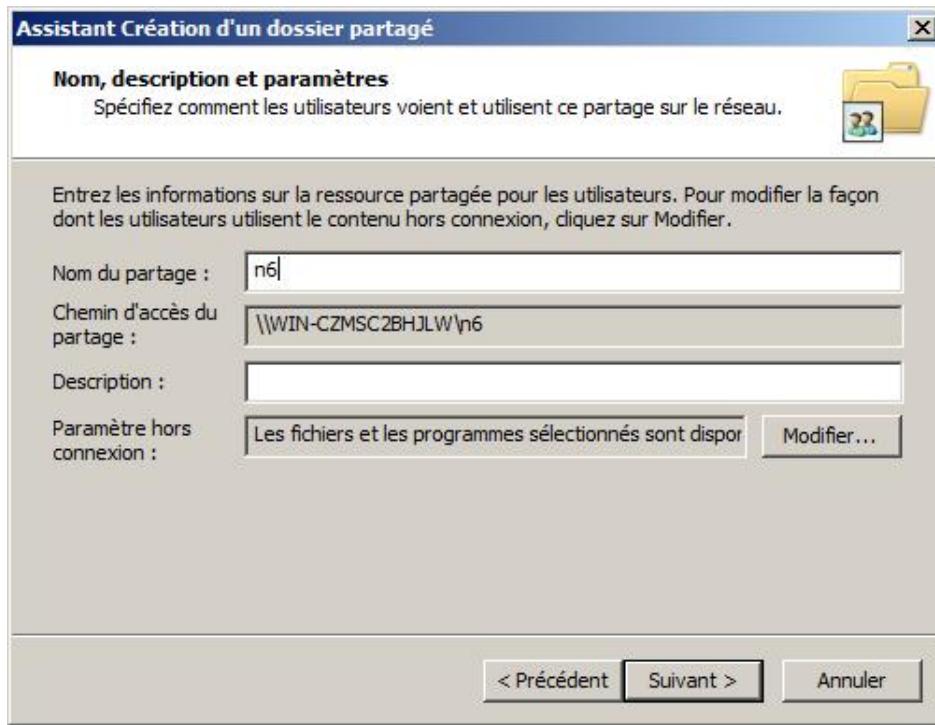
► Dans la figure précédente, les partages ADMIN\$, FAX\$, IPC\$, NETLOGON, PRINT\$, PUBLIC, SYSVOL et les partages de lecteur Lettre\$ sont des partages spéciaux créés par Windows. Si vous les supprimez, ils seront automatiquement recréés lors du prochain démarrage sauf si vous mettez 0 pour les valeurs de la base de registre AutoShowServer et AutoShareWho se situant dans HKLM\SYSTEM\Current Control Set\Services\Lanmanserver\parameters.

Le nœud **Partages** affiche tous les partages de l'ordinateur. L'administrateur peut créer de nouveaux partages, gérer le point de partage et supprimer le partage.

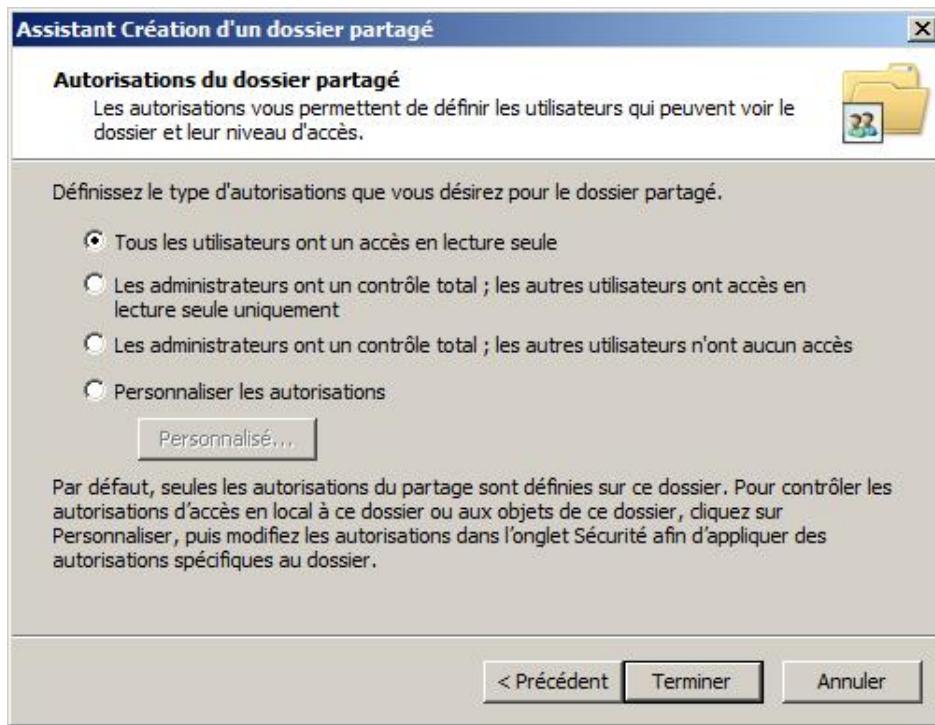
Le nœud **Sessions** affiche les utilisateurs actuellement connectés sur les dossiers partagés. L'administrateur peut déconnecter les utilisateurs.

Le nœud **Fichiers ouverts** affiche des informations sur les fichiers actuellement ouverts, comme leur emplacement, qui y accède, si le fichier est verrouillé et le mode d'ouverture. L'administrateur peut fermer les fichiers ouverts.

- Cliquez avec le bouton droit de la souris sur **Partages** puis cliquez sur **Nouveau partage**.
- Sur la page **Assistant Création d'un dossier partagé**, lisez attentivement les informations concernant le pare-feu puis cliquez sur **Suivant**.
- Sur la page **Chemin du dossier**, saisissez ou recherchez l'emplacement du dossier que vous voulez partager puis cliquez sur **Suivant**.



- Sur la page **Nom, description et paramètres**, modifiez éventuellement le **Nom** proposé pour le partage ou ajoutez-lui le caractère dollar pour en faire un partage caché. Saisissez éventuellement une **Description** ou modifiez le **Paramètre hors connexion** (cf. section Mise en œuvre des fichiers hors connexion) avant de cliquer sur **Suivant**. La dernière page de l'assistant apparaît.



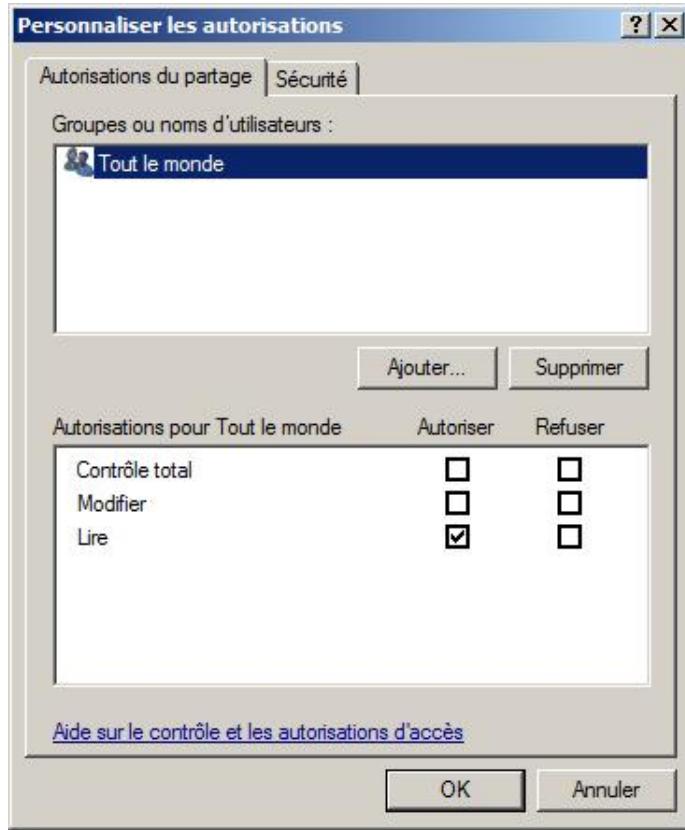
**Tous les utilisateurs ont un accès en lecture seule** équivaut à donner au groupe **Tout le monde** une autorisation en lecture.

**Les administrateurs ont un contrôle total ; les autres utilisateurs ont accès en lecture seule uniquement** équivaut à donner au groupe **Administrateurs** le contrôle total et au groupe **Tout le monde** une autorisation en lecture.

**Les administrateurs ont un contrôle total ; les autres utilisateurs n'ont aucun accès** équivaut à donner uniquement un accès en contrôle total aux **Administrateurs**.

**Personnaliser les autorisations** permet de définir les autorisations en utilisant la boîte de dialogue suivante. Les

utilisateurs ou les groupes sont choisis ainsi que les autorisations.



► L'onglet **Sécurité** permet de gérer les permissions NTFS du dossier du point de partage. Le groupe **Tout le monde** n'inclut plus le groupe **Anonyme**.

- Sélectionnez l'option qui convient pour les permissions puis cliquez sur **Terminer** pour créer le partage. Une dernière page vous indique si le partage a réussi et vous permet de recréer immédiatement un nouveau partage.

► Il s'agit de la méthode préférée pour créer des partages sur un serveur. La console peut gérer des partages locaux ou distants.

## 5. Gérer un partage via l'outil Gestion de l'ordinateur



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** et **Gestion de l'ordinateur**.
- Dans le volet de gauche de la console, cliquez sur le nœud **Dossiers partagés** pour développer l'arborescence, puis sur **Partages**.
- Cliquez avec le bouton droit de la souris sur le dossier partagé que vous voulez gérer puis cliquez sur **Propriétés**. La boîte de dialogue vous permet de gérer les permissions NTFS, les autorisations au niveau du partage ainsi que les autres propriétés du partage comme montré dans les sections précédentes. Notez juste que les **Paramètres hors connexion** correspondent à la mise en cache.

## 6. Supprimer un partage via l'outil Gestion de l'ordinateur



- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration et Gestion de l'ordinateur**.
- Dans le volet de gauche de la console, cliquez sur le nœud **Dossiers partagés** pour développer l'arborescence puis sur **Partages**.
- Cliquez avec le bouton droit de la souris sur le dossier partagé que vous voulez gérer puis cliquez sur **Arrêter le partage**.

## 7. Les permissions de partage

Les permissions de partage sont les permissions que l'on applique au point de partage. Elles permettent de protéger aussi bien un volume formaté en NTFS qu'un volume formaté en FAT.

Conceptuellement, une permission de partage fonctionne de la même manière qu'une permission NTFS. Les permissions de partage sont :

- **Contrôle total**
- **Modifier**
- **Lire**

Elles sont plus simples à gérer car il suffit d'indiquer la permission que l'on désire soit en autorisation, soit en refus. D'autre part, c'est une bonne pratique de simplifier au maximum les permissions de partage en utilisant les groupes les plus appropriés, c'est-à-dire en utilisant des groupes de sécurité intégrée.

La permission résultante au point de partage sur un volume NTFS correspond toujours à la permission la plus restrictive entre la permission résultante NTFS et la permission résultante du partage.



Les permissions NTFS doivent toujours être au moins aussi restrictives que les permissions de partage.

## 8. Gérer un partage via l'invite de commande

Vous pouvez créer, modifier et supprimer un partage à l'aide de la commande **net share** comme le montrent les exemples suivants :

Création d'un partage : `net share NomPartage = CheminDuDossierAPartager`

Suppression d'un partage sur un serveur distant : `net share NomPartage \\NomServeur /delete`

## Les permissions NTFS (New Technology File System)

Les permissions NTFS permettent de protéger les fichiers d'un système Windows contre des accès non autorisés. On parle également d'autorisation. Une autorisation est le second pilier d'un système triple **A**, soit : **A** pour l'authentification effectuée lors de la connexion, **A** pour l'autorisation donnée par les permissions NTFS et **A** pour Accounting, c'est-à-dire la journalisation (en français), effectuée par les audits.

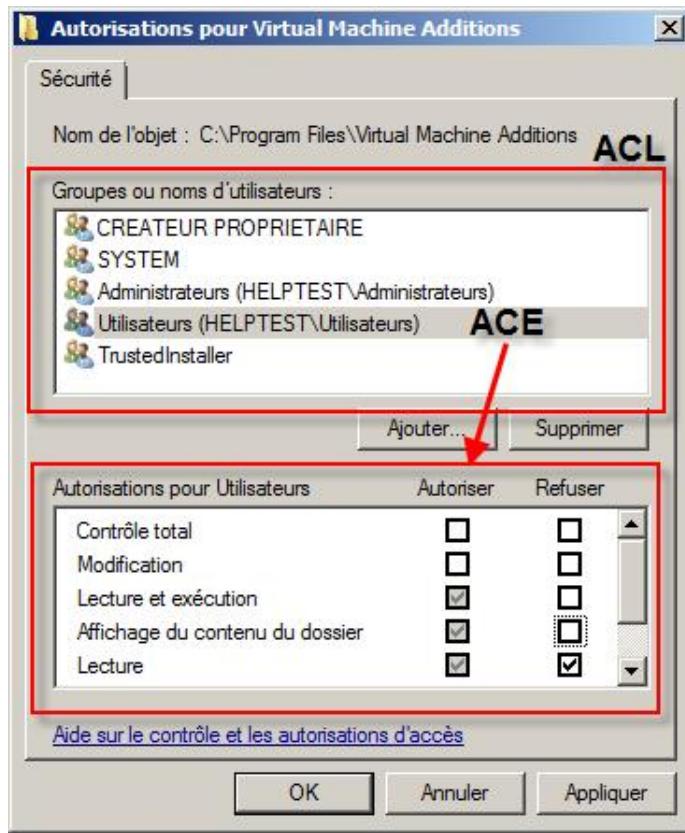
Le tableau suivant résume les méthodes pour sécuriser l'accès à un fichier en fonction du système de fichiers :

Méthode	Description	FAT	NTFS
Permission d'écriture/lecture	Il s'agit d'une case à cocher autorisant ou non l'écriture dans le dossier ou la modification d'un fichier. Cette opération peut être réalisée par tout utilisateur. Attention, il n'y a pas de sécurité contre l'accès non autorisé.	x	x
Permissions DACL	Chaque objet (fichier) ou dossier dispose d'une liste qui permet de définir qui peut y avoir accès et avec quelles autorisations. Généralement, ce sont les administrateurs qui définissent les accès aux objets. Exceptionnellement, il est possible de déléguer ce droit aux utilisateurs. Les administrateurs peuvent avoir accès aux documents en dehors des utilisateurs autorisés, ce qui peut poser des problèmes de confidentialité.		x
Chiffrage EFS	Chaque fichier ou dossier peut également être chiffré afin d'améliorer la confidentialité des documents. Le fichier n'est chiffré que sur le disque et non pendant son transport sur le réseau. L'utilisateur peut permettre à d'autres utilisateurs d'avoir accès au document. En dehors de l'utilisateur, seul l'agent de récupération peut avoir accès aux documents. Le chiffrage est transparent mais accorder les autorisations d'accès pour d'autres utilisateurs peut être difficile pour l'utilisateur. La gestion et l'utilisation des certificats sont transparentes et sécurisées.		x
Chiffrage type PGP	Ce type de chiffrage demande à l'utilisateur de chiffrer chaque document manuellement. L'utilisation des certificats peut vite devenir complexe pour l'utilisateur, ce qui rend ce type de chiffrage moins sécurisé que l'EFS. D'autre part, il faut transmettre la partie publique du certificat vers le destinataire en utilisant en autre canal de diffusion. Par contre, cette méthode est parfaite lorsque les utilisateurs concernés sont situés dans des entreprises différentes.	x	x

Microsoft Windows utilise les permissions NTFS basées sur les DACLs (*Discretionary Access Control List*) pour protéger les dossiers et les fichiers. À chaque demande d'accès à un objet fichier ou dossier, le système détermine la résultante des permissions pour autoriser ou non l'accès à l'objet.

À chaque objet est affectée une liste appelée **ACL** (*Access Control List*). L'ACL se compose de descripteurs de sécurité **ACE** (*Access Control Entry*). Chaque ACE définit une autorisation pour un utilisateur ou un groupe, comme le montre l'image suivante. L'ACE indique soit une autorisation, soit un refus.

- 
-  Par défaut, un utilisateur ou un groupe n'a pas d'autorisation sur l'objet ; en conséquence, il ne peut accéder à l'objet, on parle alors d'autorisation **Refus** implicite.
-



## 1. Les autorisations NTFS

Le tableau suivant présente les autorisations NTFS existant dans Windows Server 2008 :

Autorisation NTFS	Description	Fichier	Dossier
<b>Lecture</b>	Permet l'affichage du contenu d'un dossier et permet d'ouvrir un dossier ou un fichier.	x	x
<b>Écriture</b>	Permet l'ajout ou la modification d'un fichier ou d'un dossier.	x	x
<b>Lecture et exécution</b>	Reprend l'autorisation de lecture d'affichage du routeur de dossier et permet en plus l'exécution des programmes dans des dossiers.	x	x
<b>Affichage du contenu du dossier</b>	Reprend l'autorisation de lecture d'affichage du routeur de dossier et permet en plus l'exécution des programmes dans des dossiers.		x
<b>Modification</b>	Reprend l'autorisation de lecture, d'écriture, de lecture et exécution et d'affichage du contenu d'un dossier et permet en plus la suppression.	x	x
<b>Contrôle total</b>	Reprend l'autorisation de modification et permet en plus l'appropriation, la modification des autorisations et la suppression des sous-dossiers ou fichiers.	x	x

Les autorisations **Lecture** et **Écriture** sont complémentaires alors que les autres dépendent de celles du niveau précédent. Le tableau suivant présente ces dépendances.

	Lecture	Écriture	Affichage du contenu du dossier	Lecture et exécution	Modifier	Contrôle total

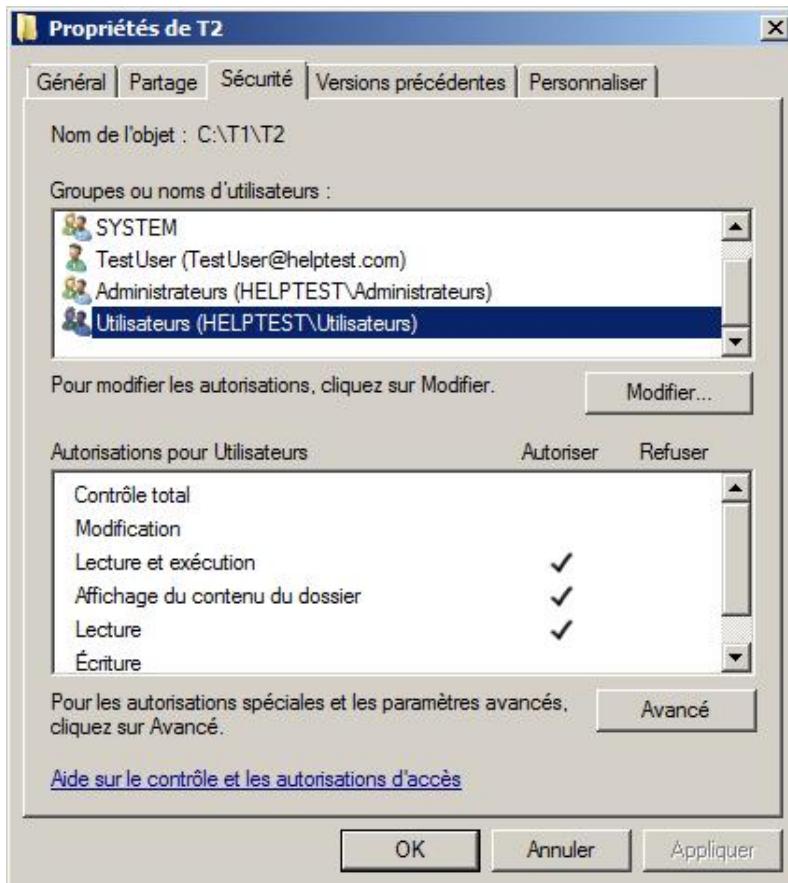
<b>Contrôle total</b>	x	x	x	x	x	x
<b>Modifier</b>	x	x	x	x	x	
<b>Lecture et exécution</b>	x			x		
<b>Affichage du contenu du dossier</b>	x		x			
<b>Écriture</b>		x				
<b>Lecture</b>	x					

Un refus de **Lecture** pour une autorisation **Contrôle total** accorde uniquement la permission d'**Écriture** car seule cette autorisation ne dépend pas de la lecture.

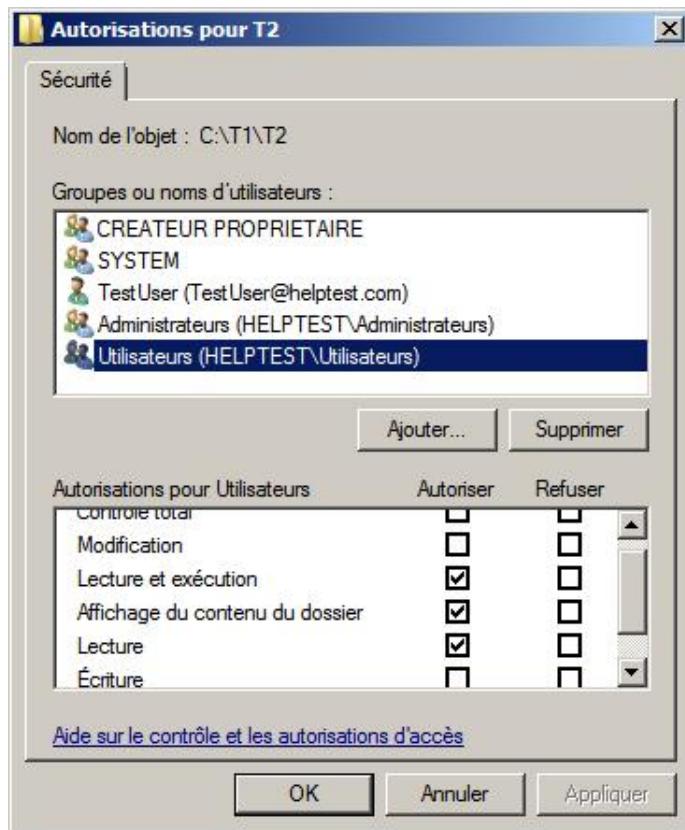


La procédure suivante permet d'afficher et modifier les permissions NTFS :

- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier ou sur le fichier dont vous voulez afficher les permissions NTFS qui y sont affectées.
- Cliquez avec le bouton droit de la souris sur le dossier ou le fichier puis cliquez sur **Propriétés**.
- Cliquez sur l'onglet **Sécurité**. Vous visualisez les permissions affectées aux utilisateurs ou aux groupes.



- Cliquez sur le bouton **Modifier**. La boîte de dialogue suivante vous permet de modifier les permissions actuelles ou d'ajouter de nouvelles permissions pour un groupe ou un utilisateur.



La liste **Groupes ou noms d'utilisateurs** affiche les objets pour lesquels des permissions ont été affectées. En cliquant sur un objet, la liste **Autorisations pour Utilisateurs** est modifiée pour refléter les autorisations de l'objet sélectionné. Il est possible de modifier les autorisations de l'objet courant en sélectionnant ou désélectionnant les cases à cocher **Autoriser** ou **Refuser**.

Il existe une différence fondamentale entre une autorisation **Refus** explicite et **Refus** implicite. Dès qu'un utilisateur ou un groupe est affecté avec un **Refus** explicite, celui-ci est prioritaire par rapport à des autorisations **Autoriser** qu'il pourrait recevoir, alors qu'un **Refus** implicite serait annulé. Il est conseillé de limiter au maximum les autorisations **Refus** explicite.

Le bouton **Ajouter** permet d'ajouter un groupe ou un utilisateur pour lui affecter une autorisation.

Le bouton **Supprimer** enlève l'objet sélectionné de la liste **Groupes ou noms d'utilisateurs**.

## 2. Les autorisations spéciales

En fait, chaque autorisation NTFS est basée sur les autorisations spéciales, comme le montre le tableau suivant :

Autorisations spéciales	Lecture	Écriture	Lecture et exécution*	Affichage du contenu d'un dossier*	Modification	Contrôle total
<b>Parcours du dossier/exécuter le fichier</b>			x	x	x	x
<b>Liste du dossier/lecture de données</b>	x		x	x	x	x
<b>Attributs de lecture</b>	x		x	x	x	x

<b>Lecture des attributs étendus</b>	x		x	x	x	x
<b>Création de fichier/écriture de données</b>		x			x	x
<b>Création de dossier/ajout de données</b>		x			x	x
<b>Attributs d'écriture</b>		x			x	x
<b>Écriture d'attributs étendus</b>		x			x	x
<b>Suppression de sous-dossier et fichier</b>						x
<b>Suppression</b>					x	x
<b>Autorisations de lecture</b>	x	x	x	x	x	x
<b>Modifier les autorisations</b>						x
<b>Appropriation</b>						x
<b>Synchroniser</b>	x	x	x	x	x	x

\* Bien qu'apparemment identiques, les autorisations s'appliquent à des types d'objets différents.

 L'autorisation **Suppression de sous-dossier et fichier** permet de détruire un dossier qui contient des fichiers sur lesquels on n'a aucun accès. Cette autorisation est conforme à la norme Posix. Dans la réalité, appliquée à un dossier sur lequel l'utilisateur a une autorisation de type **Contrôle total** et aucun accès sur au moins un document, elle permet la suppression du dossier et de tout ce qu'il contient. Normalement, l'utilisateur ne devrait pas pouvoir effacer ces fichiers.

Chaque autorisation spéciale a une portée, c'est-à-dire qu'elle s'applique à l'objet ou à d'autres objets, comme le montre le tableau suivant :

Appliquer les autorisations	Au dossier en cours	Aux sous-dossiers du dossier en cours	Aux fichiers du dossier en cours	À tous les sous-dossiers suivants	Aux fichiers dans tous les sous-dossiers suivants
<b>À ce dossier seulement</b>	x				
<b>À ce dossier, aux sous-dossiers et aux fichiers</b>	x	x	x	x*	x*
<b>À ce dossier et aux sous-dossiers</b>	x	x		x*	
<b>À ce dossier et aux fichiers</b>	x		x		x*
<b>Aux sous-dossiers et aux fichiers</b>		x	x	x*	x*

<b>seulement</b>					
<b>Aux sous-dossiers seulement</b>		x		x*	
<b>Aux fichiers seulement</b>			x		x*

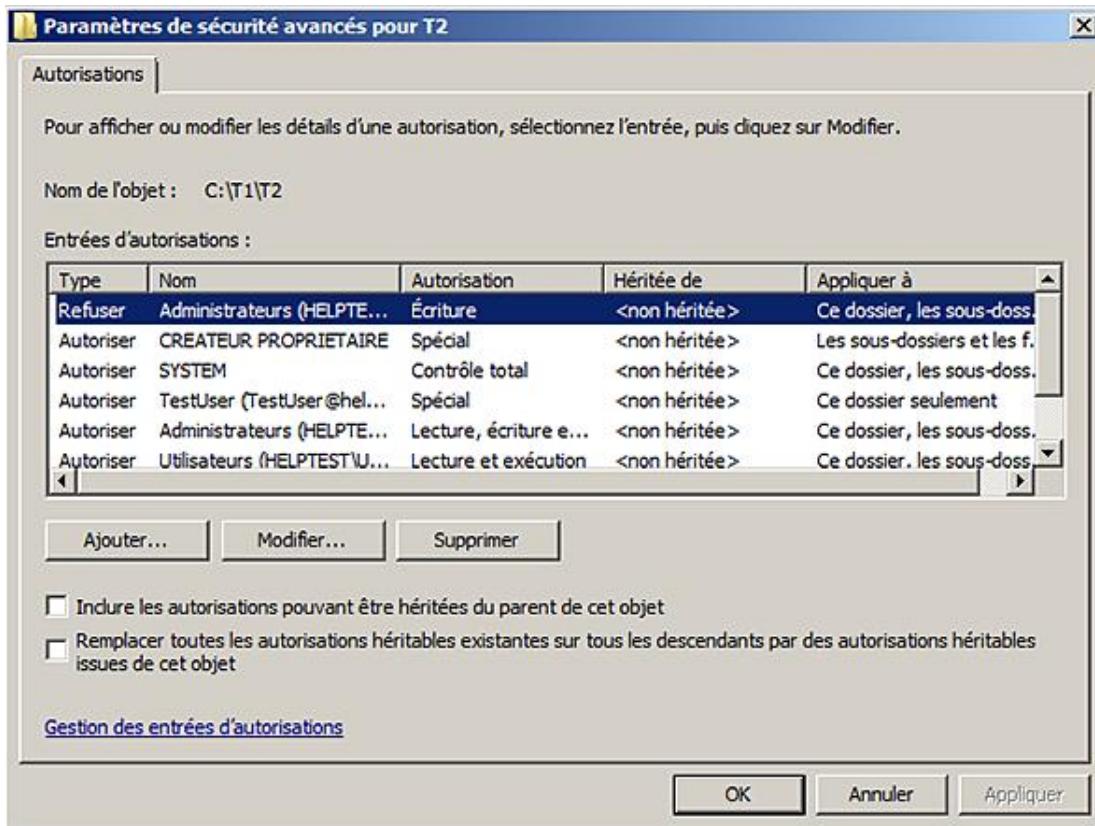
\*Ne s'applique que si la case à cocher **Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur** est désactivée dans la boîte de dialogue **Entrée d'autorisation**.

Les autorisations spéciales sont plus complexes à gérer, il est donc déconseillé de les utiliser, à moins qu'il ne soit pas possible d'utiliser les permissions NTFS.



La procédure pour visualiser et modifier une autorisation spéciale est la suivante :

- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier ou sur le fichier dont vous voulez afficher les permissions NTFS qui y sont affectées.
- Cliquez avec le bouton droit de la souris sur le dossier ou le fichier puis cliquez sur **Propriétés**.
- Dans l'onglet **Sécurité**, cliquez sur **Avancé**.
- Dans la boîte de dialogue **Paramètres de sécurité avancés pour**, cliquez sur **Modifier**.



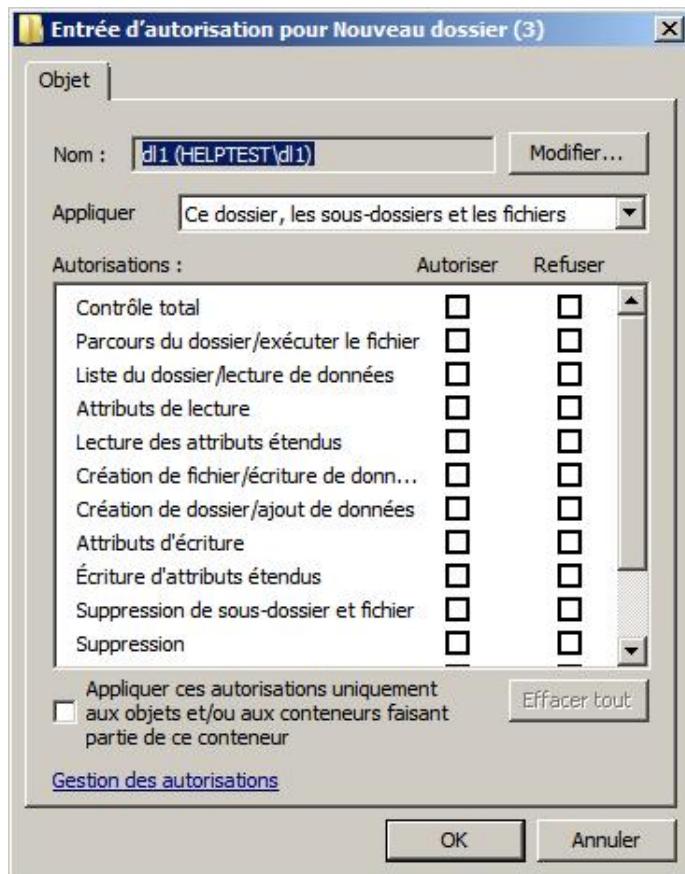
La liste **Entrées d'autorisations** affiche le nom de l'utilisateur ou du groupe auquel une autorisation est affectée, l'autorisation, son type, sa portée et si elle est héritée.

Le bouton **Ajouter** permet d'ajouter une autorisation pour un groupe ou un utilisateur.

Le bouton **Modifier** permet de modifier une autorisation pour un groupe ou un utilisateur.

Le bouton **Supprimer** permet de détruire une autorisation pour un groupe ou un utilisateur.

- Cliquez sur **Ajouter** pour sélectionner un objet puis sur **OK**.



Le **Nom** correspond à l'objet qui reçoit l'autorisation. Vous pouvez encore le modifier en cliquant sur **Modifier** et en sélectionnant un nouvel objet.

La liste déroulante **Appliquer** permet de définir la portée de l'autorisation.

La liste **Autorisations** correspond aux autorisations spéciales que vous pouvez affecter.

Le bouton **Effacer tout** permet d'effacer toutes les autorisations de la liste.

La case à cocher **Appliquer ces autorisations uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur** permet de définir également une portée.

- Sélectionnez les autorisations pour l'objet puis cliquez quatre fois sur **OK**.

### 3. Héritage des autorisations

#### a. Principe

Le système de fichiers est arborescent, il débute par le niveau du lecteur disque qui contient des dossiers et des fichiers, et continue à l'intérieur des dossiers qui peuvent eux-mêmes contenir des dossiers et des fichiers.

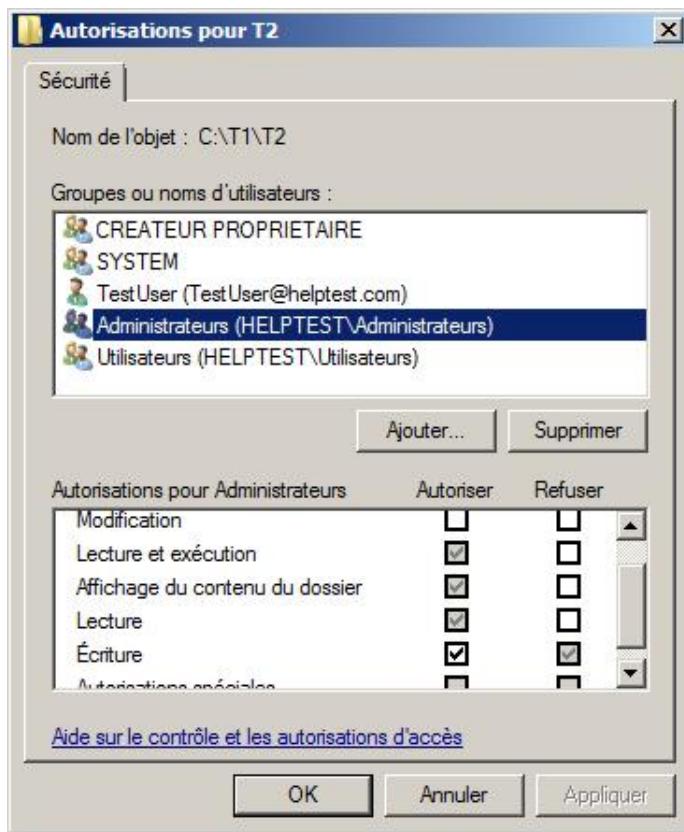
Une autorisation affectée à un niveau est automatiquement héritée par ses niveaux enfants.

Les permissions héritées apparaissent en grisé, alors que les permissions explicites apparaissent normalement. La procédure pour ajouter ou modifier une autorisation est identique à celle présentée dans la section précédente. Il n'est pas possible de modifier une permission héritée.

Il faut savoir qu'une permission héritée est annulée par une permission explicite, en d'autres termes, l'héritage peut

être utilisé pour définir des permissions restrictives au niveau de la racine puis des permissions explicites moins restrictives sont affectées au niveau d'un dossier enfant.

Prenons l'exemple illustré par l'image suivante : le groupe **Administrateurs** hérite de la permission refus d'écriture, ce qui empêcherait toute création de fichiers ou de dossiers pour les administrateurs dans le dossier T2, mais comme une autorisation explicite d'écriture à ce niveau annule la permission héritée, les administrateurs peuvent donc créer un fichier ou un dossier dans T2.



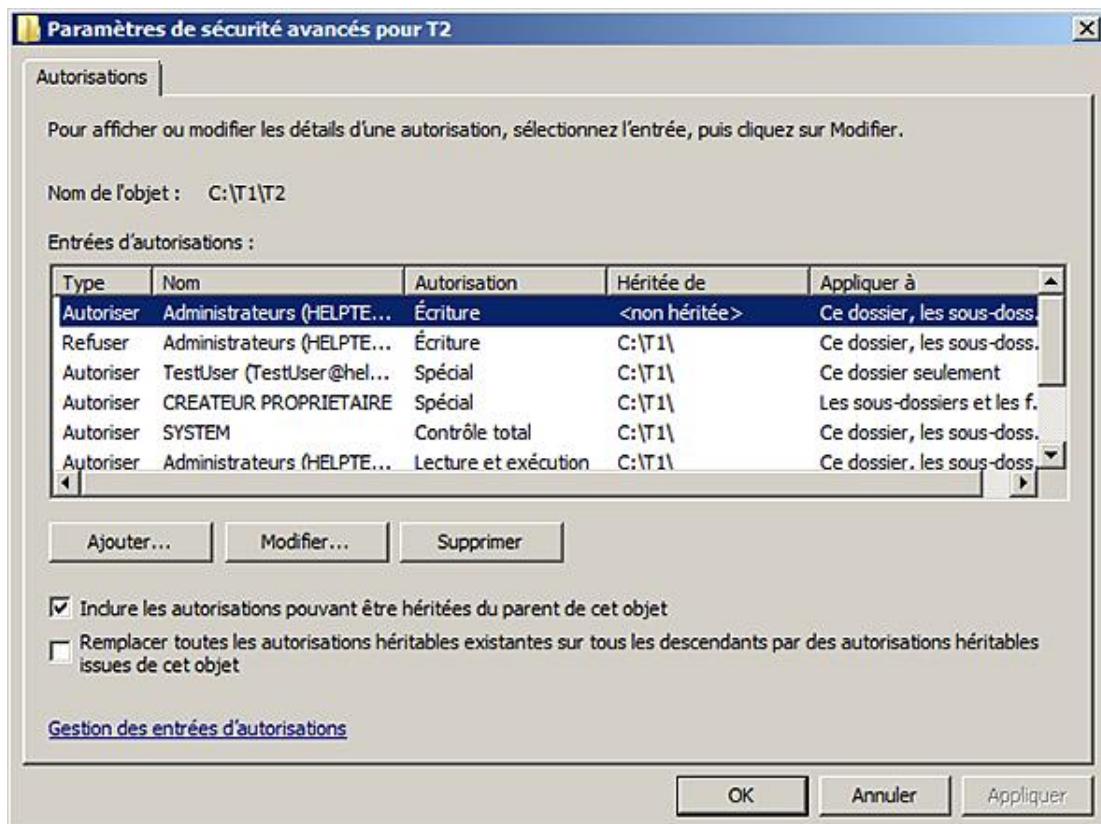
## b. Blocage de l'héritage

Une fonctionnalité intéressante est le blocage de l'héritage qui permet de créer une nouvelle racine pour les autorisations dont tous les objets enfants hériteront.

La procédure est la suivante :



- Affichez les autorisations du dossier concerné (cf. section Les autorisations spéciales).



La liste **Entrées d'autorisations** affiche les autorisations actuelles et indique entre autres si elles sont héritées et leur portée.

La case à cocher **Inclure les autorisations pouvant être héritées du parent de cet objet** permet d'indiquer si l'on conserve l'héritage des permissions ou non.

La case à cocher **Remplacer toutes les autorisations héritables existantes sur tous les descendants par des autorisations héritables issues de cet objet** permet de propager les autorisations sur les objets enfants.

- Cliquez sur la case à cocher **Inclure les autorisations pouvant être héritées du parent de cet objet** pour la désélectionner.

Une boîte de dialogue apparaît.

Le bouton **Copier** copie les permissions héritées afin qu'elles deviennent explicites puis supprime les permissions héritées. Le bouton **Supprimer** supprime les permissions héritées. Le bouton **Annuler** annule l'opération en cours.

- Lisez le message et cliquez sur **Supprimer**.
- Cliquez trois fois sur **OK**.

## 4. Utilitaire en ligne de commande icalcs



Vous pouvez gérer les permissions via **icalcs** apparu avec Windows Server 2003 SP2. Il remplace et étend les outils **cacls.exe** encore présents et **xcacs.vbs** téléchargeable depuis le site de Microsoft. Il permet de rechercher des permissions spécifiques, de remplacer, d'ajouter, de modifier ou de supprimer des permissions NTFS ou spéciales. Son cadre d'utilisation est principalement pour l'automatisation et le dépannage des automatismes.

## 5. La permission résultante NTFS

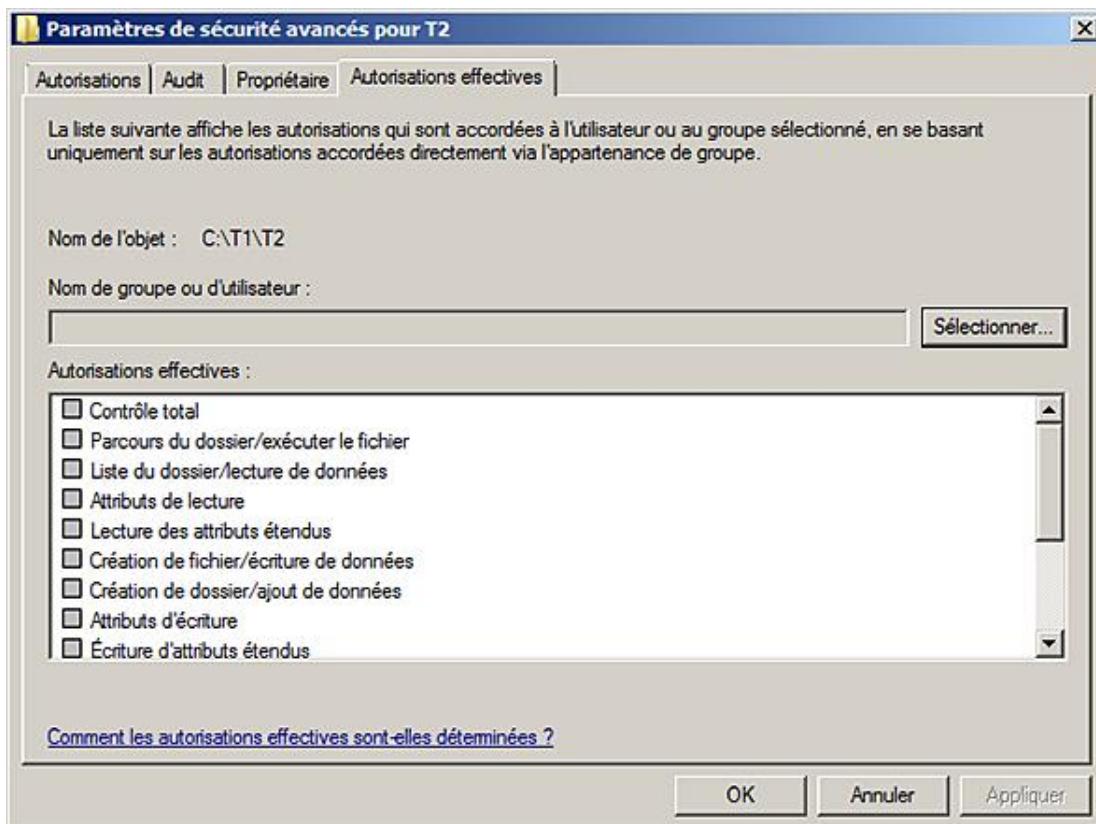
La permission résultante est la permission réelle de l'utilisateur lorsqu'il accède au dossier ou au fichier.

Pour déterminer cette permission, vous pouvez vous aider de l'outil Autorisations effectives, malheureusement il ne prend pas en compte les groupes entités de sécurité intégrée auxquels un utilisateur ou un groupe peut appartenir. Dès lors, le résultat peut être erroné.

La procédure est la suivante :



- Connectez-vous en tant qu'administrateur.
- Ouvrez l'**Explorateur Windows** ou l'**Ordinateur** et déplacez-vous jusqu'au dossier dont vous voulez connaître les autorisations effectives.
- Cliquez avec le bouton droit de la souris sur le dossier puis cliquez sur **Propriétés**.
- Cliquez sur l'onglet **Sécurité**. Vous visualisez les permissions héritées et les permissions explicites du dossier.
- Cliquez sur le bouton **Avancé**. La boîte de dialogue **Paramètres de sécurité avancés** apparaît.



- Cliquez sur l'onglet **Autorisations effectives**.
- Cliquez sur le bouton **Sélectionner** pour choisir un groupe ou un utilisateur et cliquez sur **OK**. Les autorisations effectives apparaissent.

Pour déterminer de manière manuelle la permission résultante pour des permissions NTFS, vous devez utiliser les règles suivantes :

- Un refus d'autorisation est prioritaire sur une autorisation accordée.

- Une autorisation explicite est prioritaire sur une autorisation héritée.
- Lorsqu'il existe des autorisations de même type (**Refus** ou **Autoriser**), elles se combinent en effectuant une union.

Ces règles permettent d'utiliser la procédure suivante :

- 1. Affichez les groupes et les utilisateurs qui reçoivent une autorisation pour la ressource.
- 2. Déterminez de quels groupes l'utilisateur est membre et notez leurs autorisations en différenciant les autorisations explicites des autorisations héritées.
- 3. Notez les autorisations affectées directement pour l'utilisateur.
- 4. En utilisant le résultat des étapes 2 et 3, déterminez la résultante des autorisations héritées de la manière suivante :
  - a. Trouvez la résultante des autorisations.
  - b. Trouvez la résultante des refus d'autorisations.
  - c. Trouvez la résultante des autorisations héritées basée sur les résultantes **Autoriser** et **Refuser**.
- 5. En utilisant le résultat des étapes 2 et 3, déterminez la résultante des autorisations explicites.
  - a. Trouvez la résultante des autorisations.
  - b. Trouvez la résultante des refus d'autorisations.
  - c. Trouvez la résultante des autorisations explicites basée sur les résultantes **Autoriser** et **Refuser**.
- 6. Déterminez la résultante des permissions NTFS.

Prenons un exemple concret : l'utilisateur U1 est membre des groupes GR1, GR2, GR3 et GR4 et tente d'accéder au fichier File1.txt qui se trouve sur le serveur ZEUS.

Le tableau suivant montre les permissions NTFS affectées au fichier :

Groupe ou utilisateur	Permission explicite	Permission héritée
SYSTEM		Contrôle total
RESAU		Refus d'écriture
GR1	Lecture et exécution	
GR2	Écriture	
GR3		Modification
Administrateurs		Contrôle total

L'étape 1 de la procédure correspond au tableau précédent.

Pour l'étape 2, l'utilisateur est membre des groupes GR1, GR2 et GR3. De plus, comme il se connecte via le réseau, il est membre du groupe RESAU.

Pour l'étape 3, l'utilisateur U1 ne reçoit pas directement d'autorisations.

Pour déterminer la résultante de l'étape 4, il faut déterminer la résultante des autorisations et des refus d'autorisation des permissions héritées puis déterminer la résultante de l'héritage ce qui nous donne :

- Autoriser : Modification.
- Refuser : Écriture.

La résultante des permissions héritées est :

- Autoriser : Lecture, Lecture et exécution, Affichage du contenu du dossier.
- Refuser : Écriture.

Pour déterminer la résultante de l'étape 5, il faut déterminer la résultante des permissions explicites puis déterminer la résultante de l'héritage ce qui nous donne :

- Autoriser : Lecture et exécution, Écriture.
- Refuser : Pas de refus.

La résultante des permissions explicites est :

- Autorisation : Lecture, Lecture et exécution, Affichage du contenu du dossier et Écriture.
- Refuser : Pas de refus.

Enfin pour l'étape 6, nous allons combiner les autorisations explicites et les autorisations héritées, ce qui nous donne :

- Autoriser : Modification.
- Refuser : Refus d'écriture hérité.

La résultante est Modification car le refus d'écriture hérité est moins prioritaire que l'écriture explicite. L'utilisateur a l'autorisation de modification.

## 6. Copier et déplacer des fichiers ou des dossiers

Lorsque vous déplacez ou copiez des fichiers ou des dossiers, des effets de bord indésirables peuvent survenir si vous ne prenez pas attention au tableau suivant qui montre les permissions NTFS affectées à l'objet après l'opération.

	<b>Sur le même volume NTFS</b>	<b>Sur des volumes NTFS différents</b>
<b>Déplacement d'un dossier source A vers un dossier de destination B</b>	Conserve les permissions NTFS du dossier source	Hérite des permissions NTFS du dossier de destination
<b>Copie d'un dossier source A vers un dossier de destination B</b>	Hérite des permissions NTFS du dossier de destination	Hérite des permissions NTFS du dossier de destination

Les permissions NTFS de l'objet sont conservées lorsque vous le déplacez d'un dossier vers un autre sur le même volume NTFS car c'est uniquement le chemin qui est modifié. Pour les autres cas, il y a création d'un nouvel objet.

Les permissions NTFS sont perdues si l'objet est copié ou déplacé vers un autre volume dont le format n'est pas NTFS.

## 7. Méthodes conseillées

- Organisez vos données selon le niveau de confidentialité (secret, confidentiel, interne et public).

- Utilisez des volumes dédiés au stockage de fichiers, voire des serveurs différents selon le niveau de confidentialité demandé.
- Créez des dossiers spécifiques selon les groupes de travail et le niveau de confidentialité.
- Le niveau du dossier le plus élevé est le dossier qui doit être le plus restrictif en terme de permissions.
- Utilisez de préférence les permissions NTFS par rapport aux permissions spéciales.
- Limitez les autorisations pour les utilisateurs, en leur donnant uniquement les permissions minimum nécessaires.
- Utilisez au maximum les groupes de sécurité intégrée pour affecter des autorisations.

## 8. Les audits

Le système de fichiers NTFS est également conçu pour enregistrer dans le journal de sécurité les événements de tentatives d'accès et d'accès.

### a. Activer l'audit des objets



Win

Pour activer l'audit, il faut utiliser les stratégies de groupe et plus particulièrement les stratégies de sécurité locale. La procédure suivante montre une méthode basée sur un serveur faisant partie d'un groupe de travail. Dans le cas d'un ordinateur faisant partie d'un domaine, utilisez la console Gestion des stratégies de groupe.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Stratégie de sécurité locale**.
- Dans le volet gauche de la console **Stratégie de sécurité locale**, développez l'arborescence selon les noeuds **Paramètres de sécurité - Stratégies locales - Stratégie d'audit**.
- Dans la fenêtre principale, double cliquez sur la stratégie **Auditer l'accès aux objets**.

La case à cocher **Réussite** permet d'activer les audits en succès.

La case à cocher **Échec** permet d'activer les audits en erreur.

- Sélectionnez les deux cases à cocher puis cliquez sur **OK**.
- Fermez la console.
- Ouvrez une invite de commandes et saisissez **gpupdate /force**. La stratégie est maintenant appliquée.

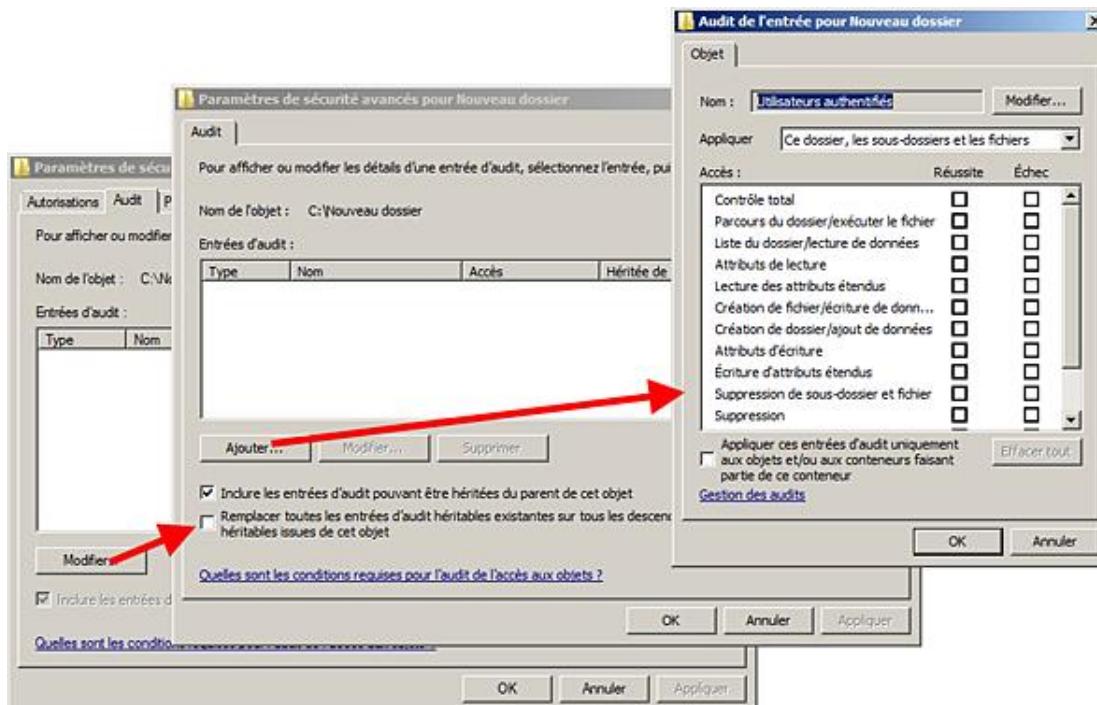
### b. Activer l'audit pour un dossier



Win

- Connectez-vous en tant qu'administrateur.

- Ouvrez l'**Explorateur Windows** ou le **Poste de travail** puis déplacez-vous jusqu'au dossier que vous voulez auditer.
- Cliquez avec le bouton droit de la souris sur le dossier puis cliquez sur **Propriétés**.
- Dans l'onglet **Sécurité**, cliquez sur le bouton **Avancé**.
- Dans la boîte de dialogue **Paramètres de sécurité avancés**, cliquez sur l'onglet **Audit**. La liste des entrées de l'audit devrait être vide.
- Cliquez sur le bouton **Modifier**.
- Remarquez que la boîte de dialogue ressemble à la boîte de dialogue des autorisations NTFS spéciales. Cliquez sur **Ajouter** pour sélectionner l'utilisateur ou le groupe à auditer puis cliquez sur **OK**.



- Dans la boîte de dialogue **Audit de l'entrée**, sélectionnez les cases à cocher des autorisations que vous voulez auditer. Ces dernières correspondent aux permissions NTFS spéciales. Éventuellement, modifiez l'étendue et cochez si besoin la case **Appliquer ces entrées d'audit uniquement aux objets et/ou aux conteneurs faisant partie de ce conteneur**.



Ne cochez que les autorisations qui peuvent avoir un sens, comme l'autorisation **Suppression** si vous voulez savoir grâce à l'audit quelle personne supprime un fichier.

- Cliquez quatre fois sur **OK**.

### c. Consulter le journal d'audit



Win

- Connectez-vous en tant qu'administrateur.

- Cliquez sur **Démarrer - Outils d'administration** puis **Observateur d'événements**.
- Dans le volet gauche de l'**Observateur d'événements**, développez l'arborescence en cliquant sur les noeuds **Journaux Windows - Sécurité**.
- Filtrez le journal pour ne faire apparaître que les événements de la catégorie **Système de fichiers**.

#### d. Gestion des audits à l'aide de l'utilitaire ligne de commande auditpol et SubInACL



Son cadre d'utilisation est principalement l'automatisation des audits. La granularité est plus fine qu'avec les stratégies de groupe.

- Affichez les noms des utilisateurs pour lesquels une stratégie d'audit est définie :

```
auditpol /list /user
```

- Activez un audit pour les systèmes de fichiers :

```
auditpol /set /subcategory : "File System /success:enable
```

- Affichez la liste de toutes les sous-catégories : **auditpol /list /subcategory :\***

Ensuite, il faut encore indiquer sur quel fichier et/ou dossier vous désirez auditer. Pour cela, il faut télécharger l'utilitaire SubInACL depuis le site de Microsoft puis saisir la commande suivante pour ajouter un audit en lecture pour les administrateurs sur le fichier c:\toto.txt :

```
SubInACL /file c:\toto.txt /sgrant=administrateur=R
```

# Systèmes de fichiers

## 1. Introduction

Windows Server 2008 supporte trois systèmes de fichiers, à savoir le système **FAT** (*File Allocation Table*), l'**exFAT** (*Extended File Allocation Table*) et le système **NTFS** (*New Technology File System*).

Le système de fichiers FAT, bien que largement répandu et utilisé par des systèmes d'exploitation et autres médias amovibles, se présente plus aujourd'hui comme un moyen universel d'échanger des fichiers que comme le système de fichiers des serveurs Windows. Ses limitations technologiques font de la FAT un reliquat qui a de la peine à disparaître.

L'ExFAT introduit par Microsoft dans Windows Embedded CE 6.0 permet de s'affranchir des limitations de la FAT.

Le tableau suivant montre les différences entre les systèmes de fichiers FAT, ExFAT et NTFS.

	<b>FAT ou FAT16</b>	<b>FAT32</b>	<b>exFAT</b>	<b>NTFS</b>
Taille maximale théorique d'une partition	2 Go	8 To	*	16 Eo
Taille maximale d'une partition	2 Go 4 Go (NT4)	32 Go	*	2 To (MBR) 256 To (GPT)
Taille minimale conseillée d'une partition	0 Mo	0 Mo	0 Mo	500 Mo
Taille maximale d'un fichier	2 Go	4 Go	16 Eo	16 Eo
Sécurité au niveau fichier	aucune	aucune	ACL**	NTFS
Nombre de bits utilisés pour l'adressage	16	32	64	64
Opérations auditables	Non	Non	Non	Oui
Compression transparente au niveau fichier	Non	Non	Non	Oui
Chiffrage transparent des fichiers	Non	Non	Non	Oui
Mise en œuvre des quotas	Non	Non	Non	Activable
Autoréparation	Non	Non	Non	Transparent
Transactionnel au niveau des fichiers	Non	Non	Oui	Oui
Limitation du nombre de fichiers ou dossiers à la racine du disque	Oui	Oui	Non	Non
Taille maximale d'un fichier	2 Go	4 Go	16 Eo	16 Eo

\* Pas d'infos.

\*\* Pas implémenté dans Windows Vista SP1 ni Windows Server 2008.

Il n'existe pas un système de fichiers FAT mais plusieurs dont la différence tient sur le nombre de bits utilisés par l'adressage des clusters de disque, donc sur la taille des volumes et le nombre de fichiers que l'on peut enregistrer.

La **FAT12** utilisée par les disquettes et certains supports amovibles de petite taille a tendance à disparaître au profit de la **FAT16** ou la **FAT32** qui utilisent respectivement 16 ou 32 bits pour l'adressage des clusters de disque.

La table d'allocation des fichiers est également lente car elle n'est pas indexée et la recherche d'un fichier peut prendre du temps, à l'inverse de NTFS qui utilise une structure en **B-arbre**. Son seul avantage est le peu de place que prend la table d'allocation des fichiers par rapport au NTFS qui demande au minimum 2 Mo.

 Sur un serveur, le choix s'arrête au système de fichiers NTFS !

➤ Si votre serveur est formaté en FAT, il est possible d'utiliser la commande suivante pour effectuer une conversion. Attention, elle ne fonctionne que de FAT vers NTFS : convert lecteur: /FS :NTFS

➤ Encore récemment, il m'a été rapporté par un client que sur un serveur contenant des données très confidentielles particulièrement capricieux, il préférait utiliser le système de fichiers FAT afin de pouvoir lire les données très facilement avec des outils simples en cas de crash et les restaurer sur un autre serveur !

## 2. Le système de fichiers exFAT

L'exFAT n'est supporté dans Windows Server 2008 que pour les disques amovibles.

Il utilise un système d'adressage de 64 bits ce qui, théoriquement, lui permet d'adresser 16 Eo.

Il permet de dépasser la limite des 32 Go de la FAT32, de gérer plus de 1000 fichiers par dossier et élimine la limite de 4 Go pour la taille d'un fichier.

La taille du cluster disque permet des implémentations jusqu'à 32 Mo.

exFAT a été conçu en tant que système de fichiers transactionnel **TFAT** (*Transaction-safe FAT*) ce qui signifie que les accès disque sont encapsulés dans des transactions qui assurent une garantie du résultat. Une transaction passe d'un état stable vers un autre état stable. Si l'état de destination ne peut être atteint (état instable), la transaction annule les opérations déjà effectuées et retourne à son état initial.

Il est considéré comme étant plus rapide que la FAT.

Enfin, Microsoft et ses partenaires devraient promouvoir ce type de fichiers pour les supports amovibles.

L'outil Gestion des disques reconnaît les disques amovibles et Windows Server 2008 peut les formater en exFAT.

## 3. Le système de fichiers NTFS

Les fonctionnalités essentielles du système NTFS sont résumées ici car le chapitre Mise en œuvre du serveur de fichiers est consacré au système de fichiers.

### a. Permissions NTFS

Le système de fichiers NTFS utilise des **ACLS** (*Access Control List*) pour sécuriser les fichiers et les dossiers des utilisateurs.

Chaque fois qu'un utilisateur tente d'accéder à un fichier, son jeton d'accès est contrôlé avec la liste **ACE** (*Access Control Entry*) des permissions **DACLs** (*Discretionary Access Control List*) ou simplement NTFS pour voir s'il dispose des permissions nécessaires, puis le processus continue en passant dans les **SACLs** (*Security Access Control List*) afin de vérifier s'il faut enregistrer un événement de sécurité appelé également audit. À la fin du processus, l'utilisateur soit obtient l'accès au fichier, soit l'accès est refusé et dans tous les cas, un ou plusieurs événements peuvent avoir été enregistrés.

Les permissions NTFS peuvent s'appliquer au niveau du dossier ou du volume et la granularité est le fichier.

### b. Compression NTFS

La compression permet de compresser de manière transparente pour l'utilisateur le contenu d'un dossier ou d'un volume dès son activation. La granularité est le fichier.

### c. Chiffrage EFS

Le chiffrement EFS des fichiers permet de limiter l'accès au fichier en ajoutant une signature numérique basée sur un certificat au fichier. Un utilisateur peut chiffrer un fichier ou un dossier avec EFS afin d'en restreindre l'accès. Une bonne formation des utilisateurs est à prévoir, et du côté des administrateurs il faut une bonne compréhension de la notion de certificats et de leur gestion.

NTFS a été conçu de manière à détecter des clusters défectueux et à les marquer comme tels afin d'éviter de perdre des données. Si le cluster contient une information, il déplace au préalable la donnée sur un autre cluster disque.

## d. Quotas NTFS

Il est possible de placer des quotas pour l'utilisation du disque par l'utilisateur. Ces quotas peuvent être restrictifs ou servir d'avertissement. La granularité pour activer les quotas est le volume.

Les quotas permettent de limiter l'espace disque utilisé pour chaque utilisateur.

## e. NTFS transactionnel

Le NTFS transactionnel est une nouvelle fonctionnalité qui permet aux programmeurs de créer des transactions pour des opérations de copie ou de déplacement de plusieurs fichiers et d'annuler ou d'approuver l'ensemble.

## 4. Le cluster disque

Comme il a été montré au début du chapitre, le cluster disque peut gaspiller de l'espace si la taille du cluster n'est pas adaptée à la taille des fichiers stockés sur le volume. Il est important d'avoir à l'esprit quels types de données seront stockés et quelles applications vont les utiliser.

 Le conseil qui indique que pour beaucoup de fichiers de petites tailles (moins de 2 Ko), il faudrait des clusters également petits mais au plus de 2 Ko est un conseil judicieux. Il faut également avoir à l'esprit que c'est un compromis entre place et performance.

Le tableau suivant indique la taille par défaut des clusters disque pour les systèmes de fichiers FAT et NTFS.

Taille d'une partition	FAT 16	FAT 32	NTFS
< 512 Mo	1 Ko - 8 Ko	0,5 Ko - 4 Ko	0,5 Ko
512 Mo - < 1 Go	16 Ko	4 Ko	1 Ko
1 Go - < 2 Go	32 Ko	4 Ko	2 Ko
2 Go - < 32 Go	Non supporté	4 Ko - 16 Ko	4 Ko
32 Go - < 2 To	Non supporté	Non supporté	4 Ko
2 To - < 4 To	Non supporté	Non supporté	4 Ko

En fonction de l'application, il est nécessaire d'adapter cette taille de clusters disque afin d'optimiser l'accès disque à l'information en gérant plus d'informations par accès disque.

Pour la base de données SQL Server, la plus petite information stockée sur le disque s'appelle une page et sa taille est de 8 Ko. Une taille de clusters disque de 8 Ko semble une bonne taille. Néanmoins, les pages sont agrégées en **extent** de 64 Ko soit 8 pages de 8 Ko. Il peut dès lors sembler séduisant de créer des clusters de disque de 64 Ko. En fait, seule une analyse très poussée des requêtes permettrait de choisir précisément entre 8 Ko et 64 Ko. Dans tous les cas, la taille d'un cluster de 8 Ko est recommandée.

L'utilitaire Diskmon de SysInternals peut être d'une aide précieuse pour déterminer la taille idéale des clusters disque pour une application ou un serveur de fichiers.

## 5. Le défragmenteur

### a. Introduction

Un fichier peut occuper plusieurs clusters disque. Si ces clusters sont contigus, les opérations de lecture et d'écriture sont rapides. À l'inverse, si la tête de lecture doit se déplacer à chaque fois de plusieurs pistes pour lire un cluster, l'accès au fichier devient lent.

Pour contrer cette problématique, Windows tente d'écrire les fichiers dans des espaces contigus. Malheureusement, ce n'est pas toujours possible et la fragmentation apparaît.

Plus un disque est fragmenté, plus ses performances baissent, il faut alors utiliser un logiciel de défragmentation.

Dans Windows Server 2008, il existe le Défragmenteur de disque qui permet de planifier cette tâche.

Cette version n'est plus aussi séduisante que dans Windows Server 2003 car le côté visuel a été enlevé.

Il existe également des outils tiers, souvent plus performants que le défragmenteur.

## b. Lancer le défragmenteur de disque

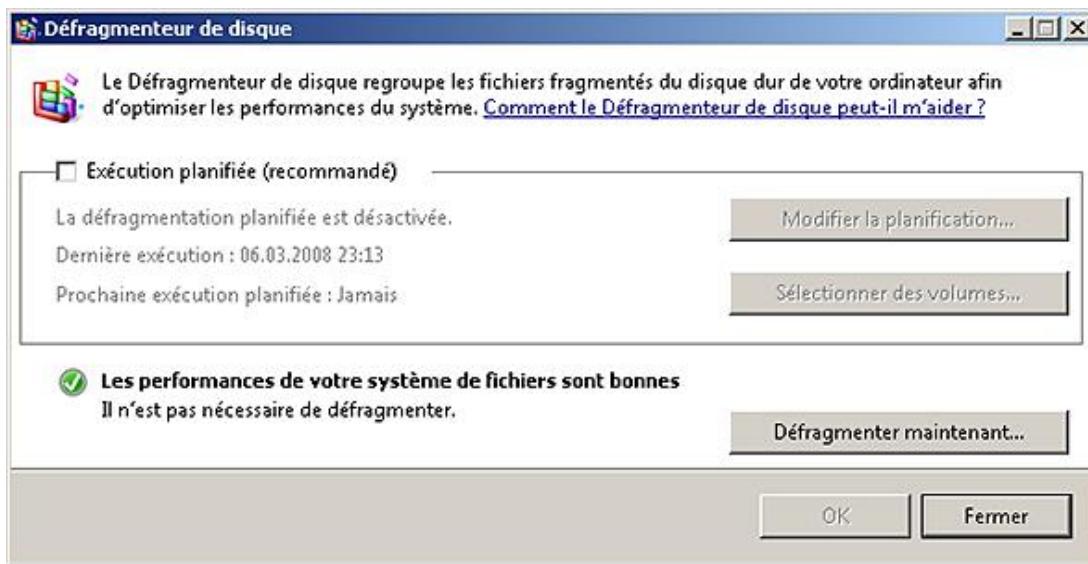


Win

Plusieurs méthodes pour lancer le défragmenteur sont possibles, la première consiste à saisir **Défragmenteur** dans la zone **Rechercher** du menu **Démarrer**.

- La seconde méthode consiste à ouvrir l'Explorateur et à cliquer avec le bouton droit de la souris sur un disque puis à choisir **Propriétés**.
- Dans la boîte de dialogue **Propriétés de**, cliquez sur l'onglet **Outils**. Cliquez sur le bouton **Défragmenter maintenant** de la section **Défragmentation**.
- Dans la boîte de dialogue **Défragmenteur de disque**, cliquez sur le bouton **Défragmenter maintenant**.

Le défragmenteur s'affiche et analyse les disques de votre système afin de déterminer s'ils ont besoin d'être défragmentés.



La défragmentation peut altérer les performances pendant le traitement, il est recommandé de planifier ces opérations en dehors des heures de travail des utilisateurs.

## c. Planifier une exécution du défragmenteur

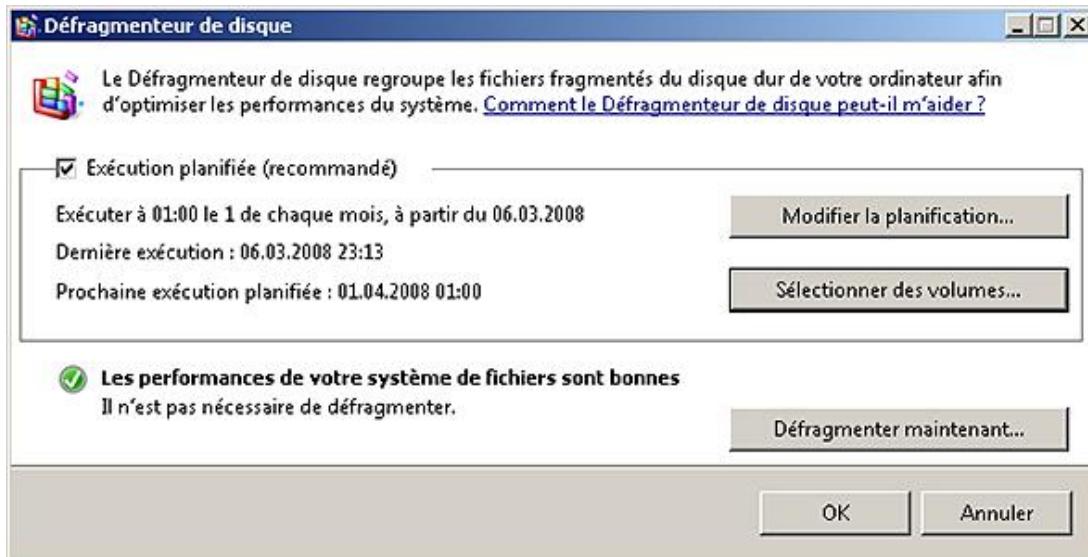


Win

- Lancez le défragmenteur.
- Dans la boîte de dialogue **Défragmenteur de disque**, cochez l'option **Exécution planifiée (recommandé)**.

Les boutons du groupe s'activent.

- Cliquez sur le bouton **Modifier la planification**.
- Dans la boîte de dialogue **Défragmenteur de disque : Modifier la planification**, sélectionnez une **Fréquence** (toutes les semaines, tous les mois ou tous les jours), éventuellement un **Jour** en fonction de la fréquence puis une **Heure**. Ensuite, cliquez sur **OK**.
- Dans la boîte de dialogue **Défragmenteur de disque**, cliquez sur le bouton **Sélectionner des volumes**.
- Dans la boîte de dialogue **Défragmenteur de disque : Options avancées**, sélectionnez les disques à défragmenter et activez l'option **Défragmenter automatiquement les nouveaux disques** puis cliquez sur **OK**.
- Dans la boîte de dialogue **Défragmenteur de disque**, contrôlez votre planification avant de cliquer sur **OK**.



#### d. Lancer la défragmentation via la ligne de commande



Cet utilitaire permet de défragmenter localement un volume ou le serveur comme le montre les exemples suivants :

- Effectue une défragmentation complète de l'ordinateur :

```
defrag -c -w
```

- Effectue une analyse sur le volume D. Le résultat est détaillé :

```
defrag d : -a -v
```

- Effectue une défragmentation partielle du lecteur E :

```
defrag e: -r
```

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre plusieurs objectifs décrits dans la section **Configuration des services fichiers et impression :**

### **Configurer un serveur de fichier**

Cela inclut, sans s'y limiter :

- publication des partages de fichiers ;
- mise en œuvre des fichiers hors connexion ;
- gestion des autorisations de partage ;
- gestion des autorisations NTFS ;
- mise en œuvre d'EFS (*Encrypting File System*).

### **Configurer DFS (Distributed File System)**

Cela inclut, sans s'y limiter :

- gestion des espaces de noms DFS ;
- mise en œuvre de DFS ;
- création et configuration de cibles DFS ;
- mise en œuvre de la réPLICATION DFS.

### **Configurer le service des clichés instantanés**

Cela inclut, sans s'y limiter :

- mise en œuvre des clichés instantanés ;
- planification des clichés instantanés ;
- gestion des emplacements de stockage.

### **Configurer la sauvegarde et la restauration**

Cela inclut, sans s'y limiter :

- comprendre les types de sauvegarde ;
- planification des sauvegardes ;
- mise en œuvre de l'administration à distance ;
- mise en œuvre de la restauration des données.

### **Administrer les quotas sur les disques**

Cela inclut, sans s'y limiter :

- mise en œuvre des quotas par volume ou par utilisateur ;

- gestion des entrées de quotas ;
- gestion des modèles de quotas.

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



## 3. Objectifs

La gestion des fichiers et des dossiers est un des points les plus difficiles et sensibles dans une entreprise. Sensible car rares sont les entreprises qui utilisent aujourd’hui une méthodologie pour classifier l’information et les documents, et difficile car sans une bonne méthodologie, et avec le poids de l’héritage, il n’est pas évident de gérer simplement les documents de l’entreprise.

Ce chapitre a pour objectif de vous présenter et d’expliquer le fonctionnement des permissions NTFS qui permettent de protéger les documents contre des accès non autorisés, que ce soit localement ou à travers un partage.

Ensuite, vous verrez les autres fonctionnalités que l’on peut trouver sur un serveur de fichiers comme la compression, les clichés instantanés, les quotas, le chiffrage EFS et les fichiers hors connexion.

La sauvegarde et sa mise en œuvre à l’aide des outils Microsoft sont également passées en revue car l’outil a été entièrement réécrit pour Windows 2008.

Le système de fichiers distribués (DFS) vous sera présenté et vous finirez l’étude avec l’installation et la présentation du rôle de serveur de fichiers.

# Validation des acquis : questions/réponses

## 1. Questions

### Questions triviales

- 1** Citez au moins deux phases pour l'acquisition d'une adresse IPv4.
- 2** À quoi correspondent les valeurs **T1** et **T2** ?
- 3** Quel type de message le client envoie-t-il au serveur ?
- 4** Est-ce qu'un serveur DHCP peut enregistrer auprès du serveur DNS un client Linux ?
- 5** Citez le nom d'au moins trois options qui sont toujours fournies par le serveur DHCP.
- 6** Citez le nom d'au moins trois options demandées par le client fournies par le serveur DHCP.
- 7** Que signifie la règle des 80/20 ?
- 8** Citez au moins deux phases pour l'acquisition d'une adresse IPv6.
- 9** Quel est l'emplacement de la base de données DHCP par défaut ?
- 10** Comment savoir si l'ordinateur local utilise une adresse IP dynamique ?
- 11** À quoi sert un agent relais DHCP ?
- 12** Que sauvegarde l'action **Sauvegarder** sur le nœud du serveur ?
- 13** Peut-on installer le rôle serveur DHCP sur un Server Core virtualisé ?

### Questions de compréhension

- 14** Comment pouvez-vous configurer un serveur DHCP de manière à ce qu'il utilise toutes les adresses du réseau 172.30.1.0/24 excepté les adresses allant de 1 à 30 et les adresses 22, 69 et 254 ?
- 15** Votre collègue installe et configure un serveur WDS, malheureusement aucun ordinateur client n'est capable de recevoir une adresse IP, pourquoi ?
- 16** Un de vos collègues ne comprend pas pourquoi l'adresse DNS fournie par un serveur DHCP à un ordinateur client ne correspond pas à l'adresse qu'il vient de configurer sur le serveur, pouvez-vous l'aider ?
- 17** Votre collègue vient d'installer et de configurer un serveur agent relais DHCP, malheureusement aucun ordinateur n'est capable de recevoir une adresse, pouvez-vous donner une raison ?
- 18** Votre collègue surveille votre réseau à l'aide d'un analyseur de réseau et ne comprend pas pourquoi il trouve des trames BOOTP provenant d'un autre segment de réseau, que pouvez-vous lui dire ?
- 19** Votre collègue veut installer un nouveau serveur DHCP pour gérer un groupe de travail indépendant du domaine de votre entreprise. Est-ce une bonne solution ?
- 20** Un ordinateur client vient d'être rallumé après avoir été éteint pendant plusieurs semaines ; votre collègue ne comprend pas pourquoi, à l'aide d'un analyseur réseau, il a trouvé des trames DHCP indiquant à l'ordinateur que son adresse n'était plus valide le forçant à recommencer le processus d'acquisition d'adresse IP, que lui répondez-vous ?
- 21** Un de vos collègues veut activer la tentative de détection de conflit au niveau du serveur, que lui répondez-vous ?

### Questions de mise en œuvre

- 22** Vous devez installer un serveur DHCP. Pendant l'installation du rôle, quelle est l'information à fournir obligatoirement dans l'assistant pour pouvoir installer ce rôle ?
- 23** Votre entreprise dispose de plusieurs serveurs DHCP et régulièrement vous constatez des erreurs dans l'enregistrement des adresses dynamiques DNS, comment pouvez-vous résoudre ce problème ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /23

Pour ce chapitre, votre score minimum doit être de 17 sur 23.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

### 3. Réponses

#### Questions triviales

- 1 Citez au moins deux phases pour l'acquisition d'une adresse IPv4.

*Vous pouvez citer DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPNACK et DHCPDECLINE.*

- 2 À quoi correspondent les valeurs **T1** et **T2** ?

*Elles correspondent au moment où le client doit tenter de renouveler son bail. La valeur T1 indique 50 % de la durée du bail et T2 87,5 %.*

- 3 Quel type de message le client envoie-t-il au serveur ?

*Lors de l'acquisition, le client utilise des messages de type BROADCAST. Lors du renouvellement, il utilise des messages de type UNICAST.*

- 4 Est-ce qu'un serveur DHCP peut enregistrer auprès du serveur DNS un client Linux ?

*Oui, les serveurs DHCP répondent aux demandes, pas à un client particulier.*

- 5 Citez le nom d'au moins trois options qui sont toujours fournies par le serveur DHCP.

*Vous pouvez citer PAD, masque de sous-réseau, nom de l'hôte, informations spécifiques au fournisseur, adresse demandée, durée du bail, type de message DHCP, identification du serveur, liste des paramètres demandés, durée T1, durée T2, identificateur client, mise à jour dynamique DNS et fin.*

- 6 Citez le nom d'au moins trois options demandées par le client fournies par le serveur DHCP.

*Routeur, serveur DNS, nom de domaine DNS, découvrir les routeurs, option d'itinéraire statique, nom du serveur WINS, type de nœud pour la résolution de nom NetBIOS sur TCP/IP, ID de l'étendue NetBIOS, itinéraires statiques sans classe.*

- 7 Que signifie la règle des 80/20 ?

*Si l'on crée une étendue sur plusieurs serveurs DHCP, il faut configurer 80 % des adresses sur le serveur principal et 20 % sur le serveur secondaire.*

- 8 Citez au moins deux phases pour l'acquisition d'une adresse IPv6.

*Vous pouvez citer SOLICIT, ADVERTISE, REQUEST et REPLY.*

- 9 Quel est l'emplacement de la base de données DHCP par défaut ?

*%systemroot%\system32\dhcp.*

- 10 Comment savoir si l'ordinateur local utilise une adresse IP dynamique ?

*En utilisant la commande ipconfig /all.*

- 11 À quoi sert un agent relais DHCP ?

*Il sert à écouter des requêtes DHCP provenant de clients sur le segment local afin de contacter un serveur DHCP connu placé sur un autre segment pour lui demander une adresse pour le client.*

- 12 Que sauvegarde l'action **Sauvegarder** sur le nœud du serveur ?

*Elle sauvegarde les informations d'étendue, les fichiers journaux, les clés du registre et de la configuration du serveur DHCP.*

- 13 Peut-on installer le rôle serveur DHCP sur un Server Core virtualisé ?

*Oui, tout à fait.*

#### Questions de compréhension

- 14 Comment pouvez-vous configurer un serveur DHCP de manière à ce qu'il utilise toutes les adresses du réseau 172.30.1.0/24 excepté les adresses allant de 1 à 30 et les adresses 22, 69 et 254 ?

*Une solution consiste à définir l'adresse de départ à 31 et la dernière à 253 puis à ajouter les exclusions pour les adresses 22 et 69.*

- 15 Votre collègue installe et configure un serveur WDS, malheureusement aucun ordinateur client n'est capable de recevoir une adresse IP, pourquoi ?

*Le protocole BOOTP n'est pas activé pour l'étendue.*

**16** Un de vos collègues ne comprend pas pourquoi l'adresse DNS fournie par un serveur DHCP à un ordinateur client ne correspond pas à l'adresse qu'il vient de configurer sur le serveur, pouvez-vous l'aider ?

*Les options fournies au niveau du serveur DHCP sont moins prioritaires que les options définies au niveau de l'étendue ou de la réservation. L'ordre de priorité d'utilisation des options est le suivant :*

- Réservation d'adresse IP
- Options en fonction de la classe
- Etendue
- Serveur

*Dans le cas présenté, l'adresse DNS est configurée à un niveau d'étendue ou un niveau de serveur et il doit y exister une option prioritaire définie à un niveau de la classe ou au niveau d'une réserve.*

**17** Votre collègue vient d'installer et de configurer un serveur agent relais DHCP, malheureusement aucun ordinateur n'est capable de recevoir une adresse, pouvez-vous donner une raison ?

*Il n'est sûrement pas configuré correctement. Après l'avoir installé, il faut encore le configurer.*

**18** Votre collègue surveille votre réseau à l'aide d'un analyseur de réseau et ne comprend pas pourquoi il trouve des trames BOOTP provenant d'un autre segment de réseau, que pouvez-vous lui dire ?

*Le routeur laisse passer les paquets de type BOOTP 67 et BOOTP 68, ce qui signifie que la RFC1542 est activée sur le routeur.*

**19** Votre collègue veut installer un nouveau serveur DHCP pour gérer un groupe de travail indépendant du domaine de votre entreprise. Est-ce une bonne solution ?

*Non car les serveurs DHCP vont répondre à toutes les demandes sans se soucier de l'origine du client. D'autre part, il est probable que le serveur DHCP autonome détecte le contrôleur DHCP de domaine et arrête de distribuer des adresses IP. Une solution consiste à n'utiliser qu'un serveur DHCP et à créer plusieurs étendues. Pour plus de sécurité, il faudrait intégrer ce serveur DHCP avec les technologies NAP.*

**20** Un ordinateur client vient d'être rallumé après avoir été éteint pendant plusieurs semaines ; votre collègue ne comprend pas pourquoi, à l'aide d'un analyseur réseau, il a trouvé des trames DHCP indiquant à l'ordinateur que son adresse n'était plus valide le forçant à recommencer le processus d'acquisition d'adresse IP, que lui répondez-vous ?

*La durée du bail a été atteinte et l'ordinateur client n'a pas pu renouveler son bail lorsqu'il est revenu sur le réseau et comme il ne peut plus utiliser cette adresse IP, il lui faut donc acquérir une nouvelle adresse IP.*

**21** Un de vos collègues veut activer la tentative de détection de conflit au niveau du serveur, que lui répondez-vous ?

*L'activation de la détection de conflit au niveau du serveur allonge considérablement le processus d'acquisition d'adresse IP. Elle ne devrait être activée que dans le cas où il existe des ordinateurs antérieurs à Windows 2000 et dans des environnements où il existe un risque de conflit.*

### **Questions de mise en œuvre**

**22** Vous devez installer un serveur DHCP. Pendant l'installation du rôle, quelle est l'information à fournir obligatoirement dans l'assistant pour pouvoir installer ce rôle ?

*Il est requis de fournir l'adresse d'un serveur DNS, ce dernier n'a pas besoin d'être atteignable.*

**23** Votre entreprise dispose de plusieurs serveurs DHCP et régulièrement vous constatez des erreurs dans l'enregistrement des adresses dynamiques DNS, comment pouvez-vous résoudre ce problème ?

*Chaque serveur DHCP ajoute un enregistrement DNS et devient le propriétaire de l'enregistrement. Lorsqu'un autre serveur DNS tente d'enregistrer la même adresse il se voit refuser l'enregistrement si la zone DNS est sécurisée. La bonne méthode pour éviter ce problème consiste à créer un utilisateur pour gérer les enregistrements DNS qui sont membres du groupe **DnsUpdateProxy** puis de l'ajouter dans les informations d'identification de chaque serveur DHCP.*

## Résumé du chapitre

Vous avez appris comment fonctionne un serveur DHCP, comment l'installer et le gérer dans l'environnement IPv4 éventuellement routé, sur une installation complète ou un **Server Core**. Vous avez également appris les différences essentielles entre les serveurs DHCPv4 et DHCPv6 et comment configurer une étendue IPv6.

## Travaux pratiques

Dans les travaux pratiques pour l'exercice 4, vous devrez effectuer les opérations suivantes :

- Installation du rôle DHCP sur plusieurs serveurs.
- Création d'étendues et configuration des options.
- Mise en œuvre d'une classe utilisateur.
- Autorisation dans l'Active Directory.
- Mise en œuvre et test d'un agent Relais DHCP.
- Configuration d'un serveur pour accepter des clients PXE et test à l'aide de clients PXE.

## Meilleures pratiques

- Utilisez la règle des 80/20 lorsque plusieurs serveurs DHCP servent la même étendue.
- Limitez le nombre de serveurs DHCP dans votre entreprise au minimum. Faut-il introduire de la redondance ?
- Réglez la durée des baux de manière à ce que les clients distants et sans fils disposent d'un bail court alors que les autres pourraient voir leur bail augmenter.
- Pour la mise à jour dynamique du DNS, préférez l'utilisation des préférences client par défaut.
- Ne désactivez une étendue que si vous désirez la supprimer définitivement sinon utilisez des plages d'exclusions.
- Intégrez le serveur DHCP avec d'autres services comme le DNS et le WINS.
- Sur de grands réseaux, contrôlez la diffusion des messages BOOTP en limitant leur portée en n'activant pas la RFC1542 sur certains routeurs.
- Activez la détection de conflit côté serveur sur les serveurs DHCP uniquement dans des environnements ayant des ordinateurs antérieurs à Windows 2000, si nécessaire. Cela rallonge la durée d'acquisition d'adresse IP.
- Si vous utilisez la réservation d'adresses et plusieurs serveurs DHCP pour servir l'étendue, alors il faut ajouter sur tous les serveurs DHCP la réservation.
- Prêtez une attention particulière au sous-système disque en en choisissant un rapide.

# Rôle DHCP sur un Server Core



## Installation du rôle Server DHCP

- Dans l'invite de commande, saisissez `start /w ocsetup DHCPServerCore` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que le serveur DHCP est bien installé puis appuyez sur [Entrée].

## Désinstallation du rôle Server DHCP

- Dans l'invite de commande, saisissez `start /w ocsetup DHCPServerCore /uninstall` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que le serveur DHCP est bien désinstallé puis appuyez sur [Entrée].

## Gestion

Pour la gestion du serveur DHCP, vous pouvez utiliser les commandes `netsh` en ayant pris soin d'insérer vos commandes à l'avance dans des scripts, ou à distance par l'intermédiaire de la console **DHCP**.

# Gestion d'un serveur DHCP

Pour assurer la gestion d'un serveur DHCP, il faut être membre du groupe **Administrateurs** ou membre du groupe **Administrateurs DHCP** des serveurs DHCP.

## 1. Migration de la base de données DHCP



Il peut être utile de déplacer le service DHCP d'un serveur à un autre ou de restaurer les informations d'un serveur DHCP sur un nouveau serveur. La procédure suivante décrit comment sauvegarder la base de données et comment la restaurer.

La langue du système d'exploitation doit être identique entre les deux serveurs.

### a. Sauvegarde de la base de données



- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur le nœud du serveur, puis sur **Sauvegarder**.
- Dans la boîte de dialogue **Rechercher un dossier**, déplacez-vous vers le dossier prévu pour la sauvegarde et cliquez sur **OK**.
- Arrêtez le service DHCP en cliquant avec le bouton droit de la souris sur le nœud du serveur, puis en cliquant sur **Toutes les tâches et Arrêter**.
- Déplacez le dossier qui contient la sauvegarde vers le nouvel ordinateur.

N'oubliez pas de désinstaller le rôle DHCP ou de vérifier que le service DHCP ne puisse pas démarrer au prochain démarrage.

Cette procédure sauvegarde les informations d'étendues, les fichiers journaux, les clés de registre et la configuration du serveur DHCP. C'est une bonne pratique que de l'exécuter à intervalles réguliers.

### b. Restauration de la base de données



- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.

- Cliquez avec le bouton droit de la souris sur le nœud du serveur, puis cliquez sur **Restaurer**.
  - Dans la boîte de dialogue **Rechercher un dossier**, déplacez-vous vers le dossier qui contient la sauvegarde et cliquez sur **OK**.
- Il est également possible d'utiliser la base de données de sauvegarde standard, soit le dossier **%systemroot%\system32\dhcp\backup**.
- Si une boîte de dialogue vous invite à arrêter les services, cliquez sur **Oui**.

## 2. Sauvegarde

Dans la procédure de sauvegarde du serveur, il ne faut pas oublier d'ajouter le dossier de la base de données DHCP, par défaut **%systemroot%\system32\dhcp** ainsi que le répertoire de sauvegarde **%systemroot%\system32\dhcp\backup**.

## 3. Statistiques



Il est possible d'afficher des statistiques pour les serveurs DHCPv4 et DHCPv6. La procédure est la suivante :

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur **IPv4** ou sur **IPv6** pour afficher les statistiques **IPv4** ou **IPv6**, puis sur **Afficher les statistiques**.

Statistiques du serveur 172.30.2.58	
Description	Détails
Heure de début	02.04.2008 21:50:05
Durée de fonctionnement	1 heures, 53 minutes, 4 secondes
Sollicitations	12
Publications	12
Demandes	12
Réponses	26
Renouvellements	9
Liaisons renouvelées	0
Confirmations	1
Refus	0
Libérations	1
Nombre total d'étendues	3
Nombre total d'adresses	18446744073709551613
- Utilisées	3 (0%)
- Disponibles	18446744073709551610 (100%)

**Actualiser**    **Fermer**

## 4. Gestionnaire de serveur



Win2

Le Gestionnaire de serveur complète la console DHCP car il permet de :

- Visualiser les événements liés au serveur DHCP.
- Gérer le service Serveur DHCP.
- Obtenir des informations supplémentaires.

The screenshot shows the Windows Server Management Console window titled "Gestionnaire de serveur". The main pane displays the "Serveur DHCP" role, which manages IP addresses for network clients. The interface includes several sections:

- Événements :** A section showing 0 events with a table for filtering by level, ID, date, and source.
- Services système :** Shows the "Serveur DHCP" service is running (en cours d'exécution) and set to automatic start. It includes a detailed description of the service's function.
- Ressources et support :** A section for recommendations, tasks, and best practices. It lists several items under "Recommandations" such as "Améliorer la tolérance de panne en fractionnant les étendues DHCP" and "Supprimer les mises à jour manuelles des enregistrements DNS en configurant la mise à jour dynamique". It also provides links for "Aide sur le rôle Serveur DHCP", "Centre communautaire Serveur DHCP", and "Envoyer des commentaires à Microsoft".

## 5. Commande netsh



La commande netsh dont l'intérêt principal est la création de scripts ou une utilisation sur un **Server Core** permet de gérer totalement le serveur DHCP.

### a. Ajout d'une étendue

Les commandes ci-dessous créent une étendue appelée Etendue4 avec des adresses allant de 172.30.1.50 à 172.30.1.59 avec un masque de 255.255.255.0 dont le bail est de 1 heure ; on y ajoute l'adresse du routeur et du DNS et à la fin, on active l'étendue.

```
REM Création de l'étendue
netsh dhcp server 172.30.1.170 add scope 172.30.1.0.255.255.255.0 Etendue4
"commentaire de l'étendue 4"
REM Ajout des adresses IP de l'étendue
netsh dhcp server 172.30.1.170 scope 172.30.1.0 add iprange
172.30.1.50 172.30.1.59
REM Modification de la durée du bail (1heure)
netsh dhcp server 172.30.1.170 scope 172.30.1.0 optionvalue 051 DWORD "3600"
REM Ajout du routeur
netsh dhcp server 172.30.1.170 scope 172.30.1.0 optionvalue 003
IPADDRESS 172.30.1.254
REM Ajout du DNS
netsh dhcp server 172.30.1.170 scope 172.30.1.0 optionvalue 006
IPADDRESS 172.30.1.170
REM Activation de l'étendue
netsh dhcp server 172.30.1.170 scope 172.30.1.0 set state 1
REM Affiche le contenu de la base DHCP
netsh dhcp server 172.30.1.170 scope 172.30.1.0 dump
```

### b. Autorisation d'un serveur DHCP auprès de l'Active Directory

Les serveurs DHCP Microsoft Windows doivent être autorisés par l'Active Directory pour distribuer des adresses s'ils font partie d'un domaine. Si un serveur DHCP ne faisant pas partie d'un domaine détecte qu'il se trouve sur un segment de réseau où existe un serveur DHCP de domaine, son service DHCP s'arrête.

Pour autoriser un serveur DHCP à distribuer des adresses :

```
netsh dhcp add server mondhcpserver.pfffc.ch 172.30.1.10
```

Pour interdire un serveur DHCP, la commande est la suivante :

```
netsh dhcp delete server mondhcpserver.pfffc.ch 172.30.1.10
```

# Configuration



## 1. Configuration de la base de données DHCP

Il est possible de modifier l'emplacement de la base de données du serveur DHCP et de la sauvegarde.

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur le nœud du serveur puis sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés**, saisissez le nouveau chemin pour la base de données ou utilisez le bouton **Parcourir**. Par défaut, le répertoire est **%systemroot%\system32\dhcp**.
- Saisissez le nouveau chemin pour la sauvegarde ou utilisez le bouton **Parcourir**. Par défaut, le répertoire est **%systemroot%\system32\dhcp\backup**.



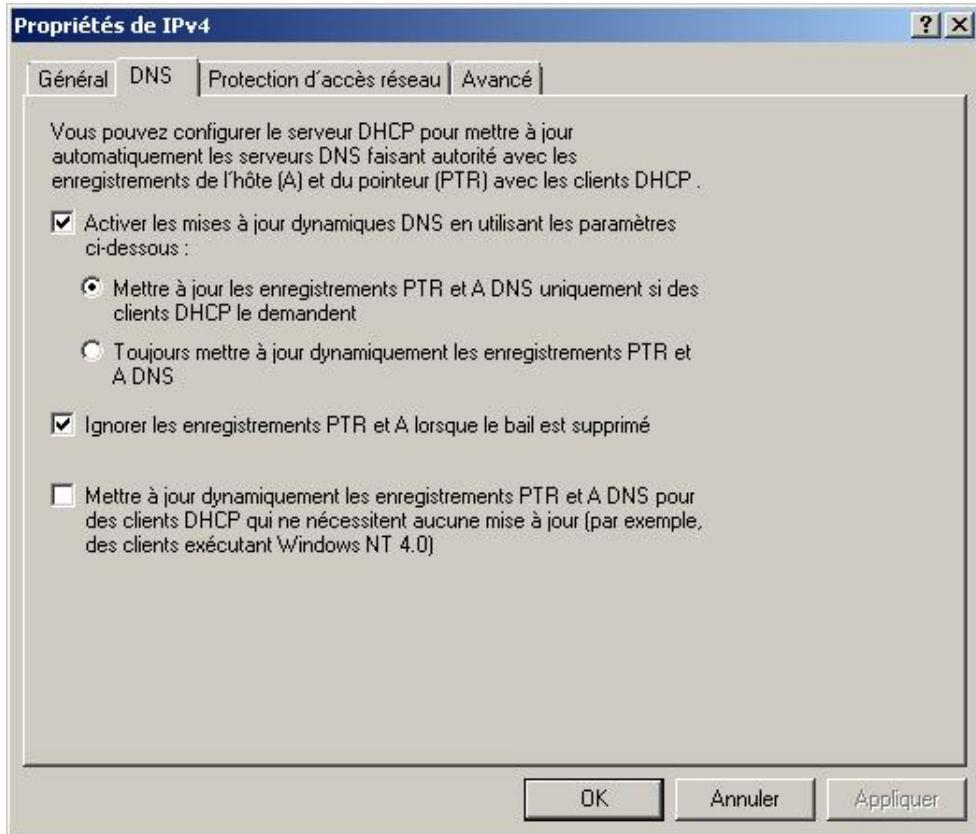
Une bonne méthode consiste à déplacer la sauvegarde sur un autre disque.

## 2. Intégration du DHCP avec DNS



La mise à jour des enregistrements DNS à partir du serveur DHCP est possible au niveau de l'étendue ou du serveur DHCPv4 ou DHCPv6. Il est recommandé de la paramétriser au niveau du serveur DHCP.

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez sur **IPv4** ou **IPv6** pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur **IPv4** ou **IPv6**, puis sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **DNS**.



Par défaut, il n'y a rien à modifier.

L'option **Activer les mises à jour dynamiques DNS en utilisant les paramètres** est prévue pour les clients postérieurs à NT4 qui demandent au serveur DHCP de mettre à jour les enregistrements ; vous pouvez également décider de toujours mettre à jour ces enregistrements à la place du client.

**Ignorer les enregistrements PTR et A lorsque le bail est supprimé** : ignorer signifie en réalité supprimer, c'est une mauvaise traduction. À ne pas modifier pour éviter d'avoir des fantômes dans le serveur DNS.

**Mettre à jour dynamiquement les enregistrements PTR et A DNS pour des clients DHCP qui ne nécessitent aucune mise à jour** est prévu pour les clients antérieurs à Windows 2000 uniquement. Cette case à cocher n'existe pas pour IPv6.

- Dans la boîte de dialogue **Propriétés**, cliquez sur l'onglet **Avancé**.

Par défaut, il n'y a rien à modifier.

Ne modifiez **Tentatives de détection de conflit** que dans des environnements où vous disposez d'ordinateurs antérieurs à Windows 2000. Il faut savoir que l'activation de la détection de conflit augmente la durée du processus d'acquisition d'adresse IP. Uniquement disponible pour le protocole IPv4.

Vous pouvez modifier le chemin d'accès du fichier journal d'audit.

En cliquant sur **Liaisons**, vous pouvez modifier les interfaces d'écoute pour le protocole DHCP.

En cliquant sur **Information d'identification**, vous pouvez sécuriser les inscriptions DNS effectuées par le serveur DHCP. Pour cela, il faut définir un compte d'utilisateur dédié qui doit être membre du groupe **DnsUpdateProxy** et ensuite ajouter son login à chaque serveur DHCP. Cela permet également d'éviter des erreurs d'enregistrement.

- 
- Il est également possible de modifier ces valeurs par étendue au lieu de serveur.
- 

### 3. Crédit d'une étendue IPv4



Win2

L'assistant de création d'une étendue post-installation est plus complet que celui proposé lors de l'installation du serveur DHCP.

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez sur **IPv4** pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur le nœud **IPv4**, puis sur **Nouvelle étendue**.
- Dans **Assistant Nouvelle étendue**, cliquez sur **Suivant**.
- Dans la page **Nom de l'étendue**, saisissez le **Nom** et éventuellement une **Description**.

➤ Saisissez un nom qui a un sens permettant d'identifier facilement les adresses comprises dans l'étendue comme **Etendue192.168.1.1 -> 199** qui indique l'adresse de début et de fin ou **172.30.1.0/24** qui indique que l'on utilise 254 adresses.

- Sur la page **Plage d'adresses IP**, saisissez une **Adresse IP de début**, une **Adresse IP de fin** puis soit la **Longueur** (suffixe IP), soit le **Masque de sous-réseau** puis cliquez sur **Suivant**.

The dialog box contains the following fields:  
- Input field: 'Adresse IP de début : 172 . 30 . 1 . 6' with a button 'Première adresse'.  
- Input field: 'Adresse IP de fin : 172 . 30 . 1 . 59' with a button 'Dernière adresse'.  
- Text area: 'Un masque de sous-réseau définit le nombre de bits d'une adresse IP à utiliser pour les ID de réseau/sous-réseau, ainsi que le nombre de bits à utiliser pour l'ID d'hôte. Vous pouvez spécifier le masque de sous-réseau en terme de longueur ou comme une adresse IP.'  
- Input field: 'Longueur : 24' with a dropdown arrow.  
- Input field: 'Masque de sous-réseau : 255 . 255 . 255 . 0'

- Sur la page **Ajout d'exclusions**, entrez éventuellement des adresses exclues, puis cliquez sur **Suivant**.

➤ Il n'est pas conseillé d'avoir des adresses exclues.

- Sur la page **Durée du bail** définissez la durée, par défaut elle est de 8 jours. Pour un bail de durée infinie, la configuration se fait après la création de l'étendue.
- Sur la page **Configuration des paramètres DHCP**, sélectionnez l'option **Oui** puis cliquez sur **Suivant**.
- Sur la page **Routeur (Passerelle par défaut)**, saisissez l'adresse de la passerelle par défaut puis cliquez sur **Ajouter**. Éventuellement, saisissez plusieurs passerelles si tous les clients sont des ordinateurs Windows Server 2008, puis cliquez sur **Suivant**.

- Sur la page **Nom de domaine et serveur DNS**, saisissez une à une les adresses des serveurs DNS puis cliquez sur **Ajouter**, cliquez ensuite sur **Suivant**.
- Sur la page Serveur **WINS**, saisissez éventuellement l'adresse d'un serveur WINS puis cliquez sur **Ajouter** avant de cliquer sur **Suivant**.
- Sur la page **Activer l'étendue**, cliquez sur **Oui** (défaut) pour l'activer immédiatement ou sur **Non** pour l'activer plus tard, puis cliquez sur **Suivant**.
- Sur la page **Fin de l'Assistant Nouvelle étendue**, cliquez sur **Terminer**.

## 4. Gestion d'une étendue



Win2

Les actions possibles à l'aide du menu **Action** de la console DHCP ou du menu contextuel pour une étendue sont les suivantes :

**Activer** : active une étendue désactivée, c'est-à-dire une étendue configurée mais que le serveur ne peut utiliser pour distribuer des adresses.

**Désactiver** : désactive une étendue activée.

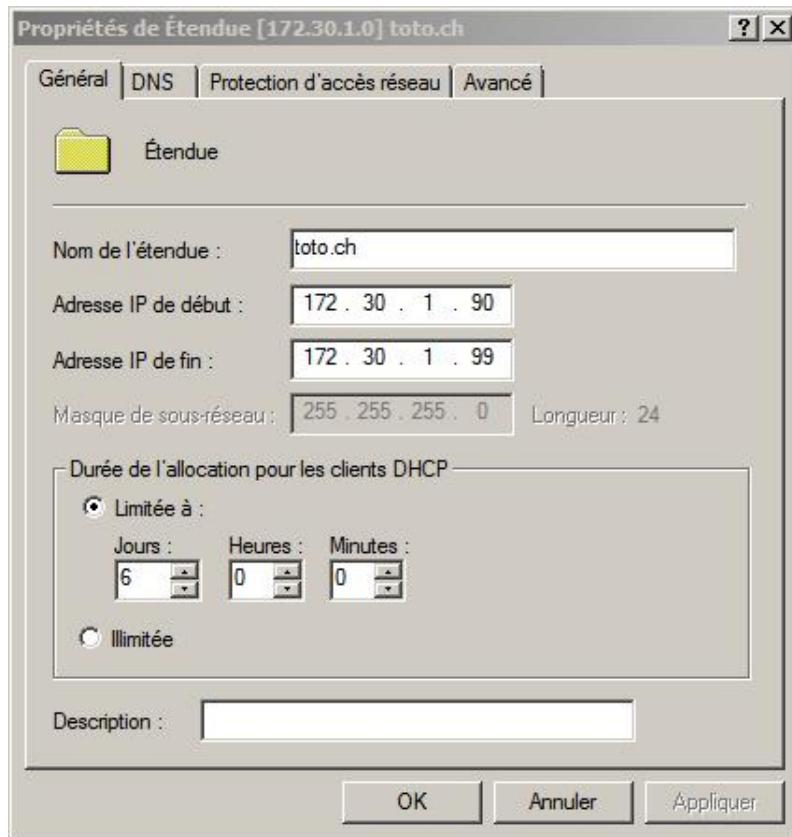
**Afficher les statistiques** : affiche les statistiques, c'est-à-dire le nombre d'adresses de la plage, le nombre d'adresses louées (en %) ainsi que le nombre d'adresses disponibles (en %).

**Réconcilier** : permet de réparer des inconsistances existantes pour l'étendue entre la base de données et le registre.

**Supprimer** : supprime l'étendue.

**Propriétés** : affiche la boîte de dialogue pour modifier des paramètres de l'étendue.

Il n'est pas possible de modifier le masque de sous-réseau de l'étendue. Il faudra détruire l'étendue pour la recréer avec un nouveau masque.



L'onglet **Avancé** permet d'activer le protocole BOOTP pour l'étendue.

La durée de bail de l'onglet **Avancé** n'est valide que pour le protocole BOOTP.

- Il faut activer le protocole BOOTP pour distribuer des images avec RIS ou WDS. Cela permet aux ordinateurs de démarrer sur le réseau si leur carte réseau est compatible PXE.

L'onglet **Protection d'accès réseau** permet d'indiquer si NAP s'applique à toutes les étendues et que faire lorsque le serveur NPS n'est pas joignable. Pour plus d'informations concernant NAP, consultez la section Présentation de la protection d'accès réseau (NAP) dans le chapitre Configuration des services réseaux avancés.

## 5. Création d'une réservation



Une réservation est un assignement permanent d'une adresse physique (*Mac Address*) d'un ordinateur client à une adresse IP de l'étendue. Certaines applications peuvent requérir que le client dispose toujours de la même adresse IP.

Pour créer une nouvelle réservation :

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez sur **IPv4** pour développer l'arborescence.
- Cliquez sur le nœud de l'étendue pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur **Réservations**, puis sur **Nouvelle réservation**.
- Dans la boîte de dialogue **Nouvelle réservation**, saisissez les informations demandées puis cliquez sur **Ajouter**.

Saisissez le **Nom de la réservation** afin de l'identifier.

L'**adresse IP** correspond à l'adresse IP attribuée à cette réservation.

L'**adresse MAC** correspond à l'adresse physique (*Mac Address*) de la carte réseau de l'hôte.

- Pour afficher l'adresse MAC de la carte locale, vous pouvez utiliser la commande `ipconfig /all`. La commande `arp -a` affiche les adresses MAC sur le même segment de réseau. Enfin, si le protocole NetBIOS est toujours activé, vous pouvez saisir `nbtstat -A <AdresseIP>` ou `nbtstat -a <nomIP>`.

La **Description** est facultative.

Les **Types pris en charge** sont les clients DHCP, BOOTP ou les deux.

Pour entrer un grand nombre de réservations, il est préférable d'utiliser un script spécialisé et/ou de recourir à la commande netsh.

## 6. Configuration des options



Il est possible de définir des options au niveau :

- du serveur IPv4 ;
- de l'étendue ;
- de la classe ;
- de la réservation.

Concernant les priorités des options, le niveau de la réservation est la plus prioritaire alors que le niveau serveur est le moins prioritaire.

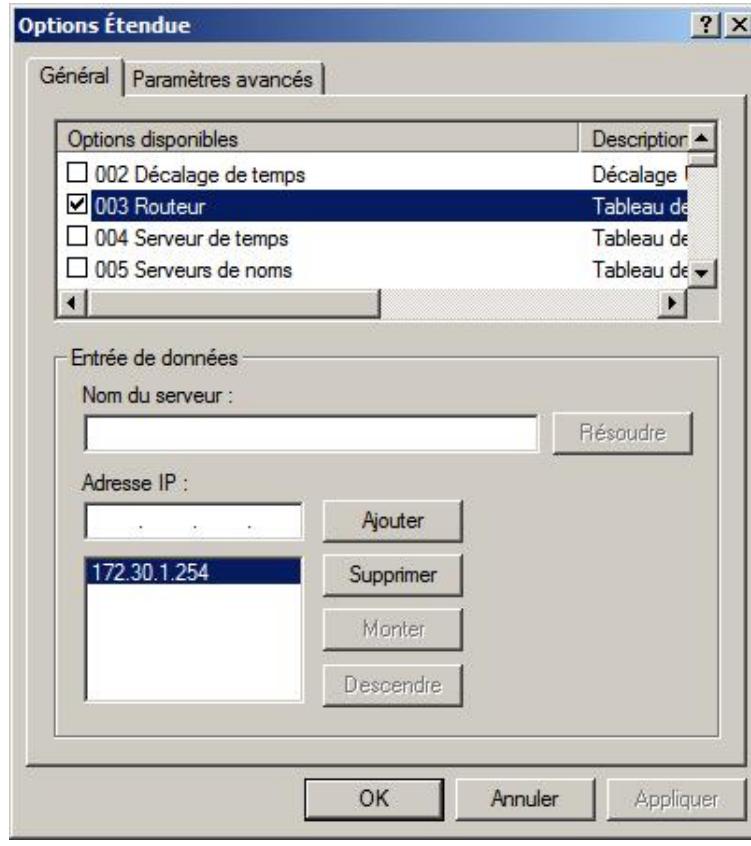
 La meilleure pratique veut qu'il faille définir les options globales valables pour toutes les étendues au niveau du serveur, comme les adresses de serveurs DNS, WINS, le nom de domaine, etc. Les options d'étendue peuvent disposer de l'adresse du routeur. Enfin, les options à placer au niveau de la réservation doivent être les exceptions.

 La procédure est la même pour gérer les options au niveau du serveur ou de la réservation.

Pour gérer les options au niveau de l'étendue :

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez sur **IPv4** pour développer l'arborescence.
- Cliquez sur le nœud de l'étendue pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur **Options d'étendue** puis choisissez **Configurer les options**.

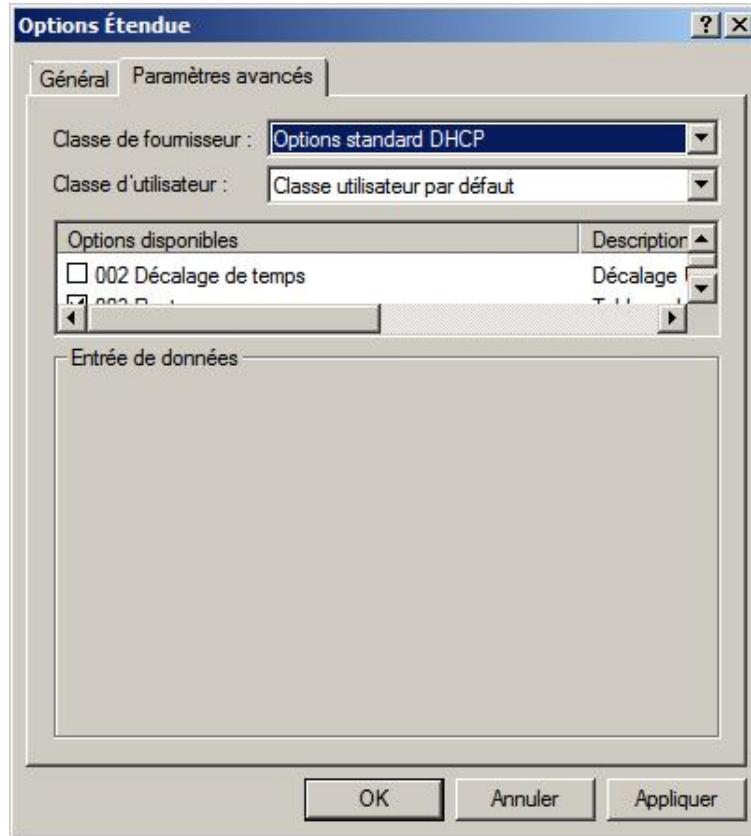
### **Onglet Général**



La sélection d'une option s'effectue en activant la case à cocher de l'option désirée. Ensuite, vous devez configurer l'option dans **Entrée de données**. Le cadre change pour chaque option.

- Les clients Windows ne supportent que peu d'options, pour la liste complète référez-vous à la section précédente. Si le client n'est pas un client Microsoft, il est possible de lui transmettre d'autres options.

#### **Onglet Paramètres avancés**



L'onglet **Paramètres avancés** diffère du fait qu'il est possible de restreindre les ordinateurs concernés par les options soit en utilisant une classe Fournisseur comme :

- Options Microsoft regroupe les classes Options Microsoft Windows 2000 et Options Microsoft Windows 98.
- Options Microsoft Windows 2000 uniquement pour Windows 2000 et supérieur.
- Options Microsoft Windows 98 pour Windows 98.
- Options standard DHCP (défaut), comme son nom l'indique.

---

► Cette notion de classe n'est plus vraiment utilisée.

---

Il est également possible de cibler le type de client en utilisant une classe d'utilisateur comme :

- Classe BOOTP par défaut pour les clients BOOTP uniquement.
- Classe de protection d'accès réseau par défaut qui correspond au client NAP.
- Classe de routage et d'accès distant par défaut qui correspond au client VPN.
- Classe utilisateur par défaut (défaut), soit les autres.

---

► Cette classe Utilisateur est plus intéressante que la classe Fournisseur car elle permet de définir clairement les options spécifiques à chaque type d'accès client.

---

## 7. Crédit d'une étendue IPv6



Win2

L'assistant de création d'une étendue post-installation est plus complet que celui proposé lors de l'installation du serveur DHCP.

- Connectez-vous en tant qu'administrateur.
- Lancez la console DHCP en cliquant sur **Démarrer - Outils d'administration** puis sur **DHCP**.
- Cliquez sur le nœud du serveur pour développer l'arborescence.
- Cliquez sur **IPv6** pour développer l'arborescence.
- Cliquez avec le bouton droit de la souris sur le nœud **IPv6**, puis cliquez sur **Nouvelle étendue**.
- Dans l'**Assistant Nouvelle étendue**, cliquez sur **Suivant**.
- Dans la page **Nom de l'étendue**, saisissez le **Nom** et éventuellement une **Description**.

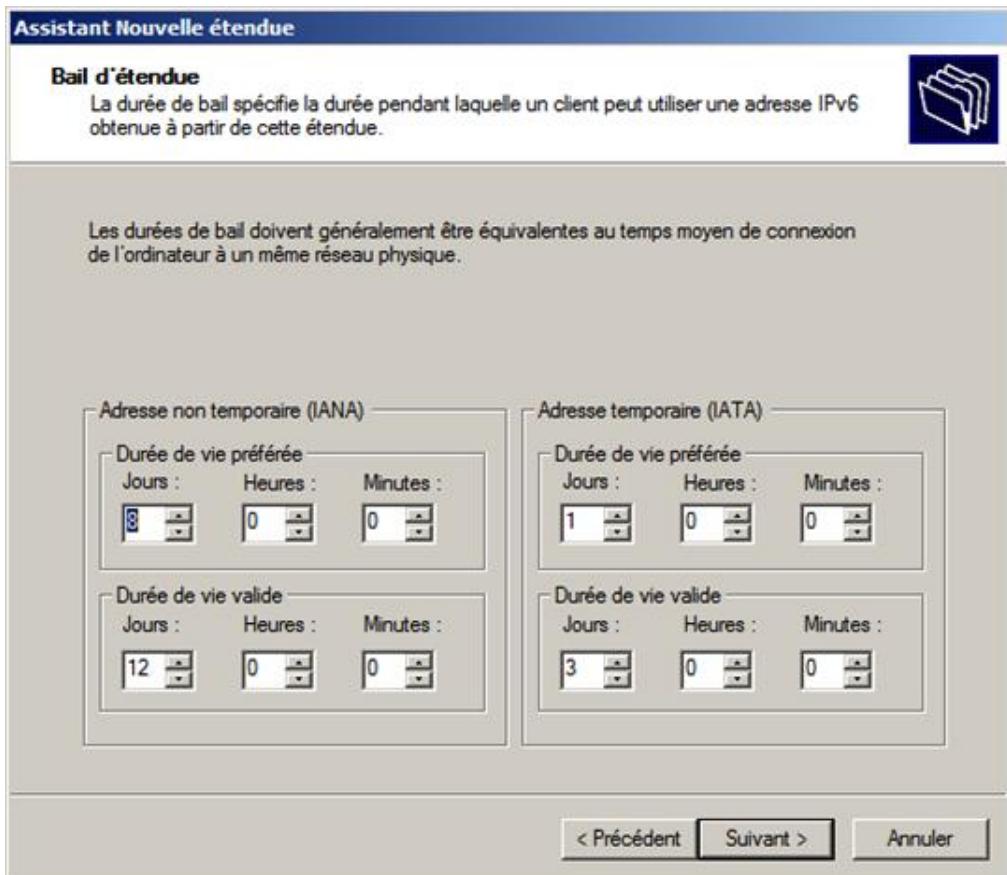
 Saisissez un nom qui a un sens permettant d'identifier facilement les adresses comprises dans l'étendue comme **EtenduePrefixe** qui indique le préfixe utilisé par l'étendue.

- Sur la page **Préfixe d'étendue**, saisissez un **Préfixe** et modifiez la **Préférence** (priorité par rapport aux autres étendues) si nécessaire puis cliquez sur **Suivant**.

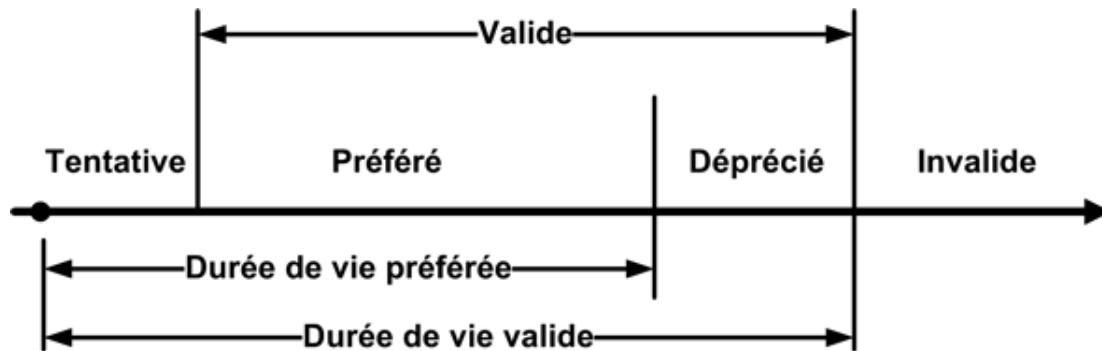
Entrez le préfixe IPv6 pour les adresses distribuées par l'étendue et la valeur de préférence pour cette étendue.

Préfixe	FC00:1234:: /64
Préférence	0

- Sur la page **Ajout d'exclusion**, ajoutez éventuellement une exclusion avant de cliquer sur **Suivant**.
- Sur la page **Bail d'étendue**, modifiez si nécessaire les durées de vie des adresses permanentes et temporaires puis cliquez sur **Suivant**.



Le schéma suivant montre la durée de vie d'une adresse DHCP IPv6.



- Sur la page **Fin de l'assistant Nouvelle étendue**, cliquez sur **Oui** pour activer l'étendue maintenant sinon cliquez sur **Non**, puis sur **Terminer**.

L'acquisition d'une adresse est légèrement différente par rapport à un client IPv4. Pour information, la figure suivante montre une capture des trames échangées durant l'acquisition.

Frame Summary							
Frame Number	Time Offset	Conv Id	Source	Destination	Protocol Name	Description	
32	13.279095		172.30.2.7	172.30.2.255	NbtNs	NbNs: Query Request for ISATAP.TOTO.CH	
33	14.030175		172.30.2.7	172.30.2.255	NbtNs	NbNs: Query Request for ISATAP.TOTO.CH	
34	14.661082		FE80:0:0:0:C... FF02:0:0:0:...	DHCPv6	DHCPv6: MessageType = SOLICIT		
35	14.661082		FC00:1234:0:0:...	FE80:0:0:0:C...	DHCPv6	DHCPv6: MessageType = ADVERTISE	
36	14.781255		172.30.2.7	172.30.2.255	NbtNs	NbNs: Query Request for ISATAP.TOTO.CH	
37	15.532335		172.30.2.7	172.30.2.255	NbtNs	NbNs: Query Request for ISATAP.TOTO.CH	
38	15.662522		FE80:0:0:0:C... FF02:0:0:0:...	DHCPv6	DHCPv6: MessageType = REQUEST		
39	15.662522		FC00:1234:0:0:...	FE80:0:0:0:C...	DHCPv6	DHCPv6: MessageType = REPLY	
40	15.662522		FE80:0:0:0:C... FF02:0:0:0:...	ICMPv6	ICMPv6: Version 2 Multicast Listener Report		
41	15.672536		FE80:0:0:0:C... FF02:0:0:0:...	ICMPv6	ICMPv6: Version 2 Multicast Listener Report		
42	15.672536		172.30.2.7	224.0.0.22	IGMP	IGMP: IGMPv3 Membership Report	

Le principe des options est identique à l'IPv4 soit :

- Options globales à IPv6.
- Options par étendue.
- Options par classe.
- Options par réservation.

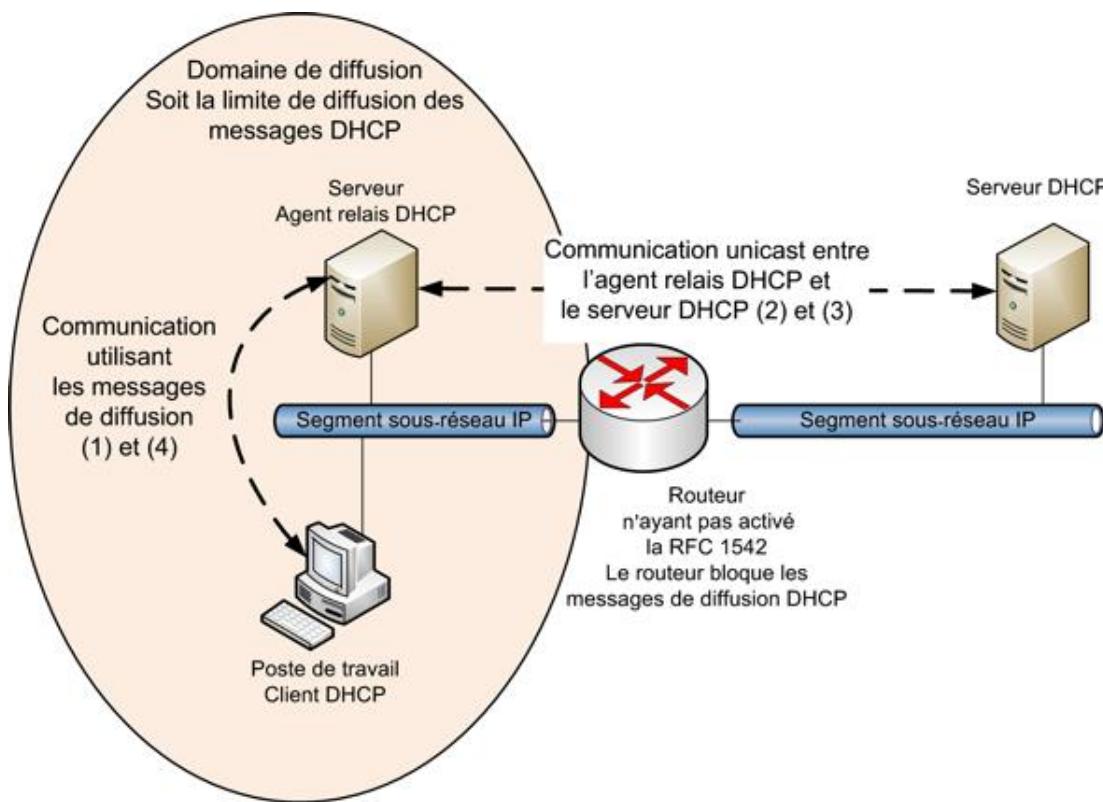
 Bien entendu, les options ne sont pas les mêmes.

## 8. Configuration du service DHCP dans un environnement routé

Par défaut, le serveur DHCP et le client doivent se trouver sur le même segment de réseau car les routeurs bloquent les messages de diffusion. Pour pallier ce problème et éviter de placer des serveurs DHCP sur chaque segment de réseau, il est possible d'activer le routage des messages de diffusion de type BOOTP (UDP 67 et 68) pour les routeurs intégrant la RFC 1542.

Si le routeur n'est pas compatible avec la RFC 1542, ou si les stratégies réseau empêchent l'activation de la RFC 1542 sur les routeurs, il est toujours possible d'installer un serveur Agent Relay DHCP.

Le serveur **Agent Relay DHCP** agit comme un proxy situé entre le client DHCP et le serveur DHCP. Il écoute les messages de diffusion BOOTP (1) sur le segment de réseau local et transmet la demande auprès d'un serveur DHCP (2) situé sur un autre segment de réseau en monodiffusion. Le serveur DHCP traite la demande s'il existe une étendue pour le segment de réseau considéré et renvoie la réponse à l'Agent Relay DHCP (3) qui diffuse la réponse sur le segment de réseau local (4), comme le montre le dessin suivant :



 Il n'est pas possible d'utiliser l'agent de relais DHCP sur un serveur DHCP ou un serveur NAT.

### a. Installation du service de rôle Routage



Win3

Si le service de rôle n'est pas encore installé :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur **Rôles**.
- Dans la fenêtre principale de **Rôles**, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez **Services de stratégie et d'accès réseau** puis cliquez sur **Suivant**.
- Sur la page **Stratégies et accès réseau**, cliquez sur **Suivant**.
- Sur la page **Services de rôle**, sélectionnez **Routage**.

---

Il est également possible d'ajouter l'agent relais DHCP en ajoutant le Service d'accès à distance.

---

- Dans la boîte de dialogue **Assistant Ajout de rôles**, cliquez sur le bouton **Ajouter les services de rôle requis**.
- Sur la page **Service de rôle**, cliquez sur **Suivant**.
- Sur la page **Confirmation**, cliquez sur **Installer**.
- Dès que la page **Résultats** apparaît, contrôlez que le rôle est bien installé, puis cliquez sur **Fermer**.

## b. Activation du service de routage



Win3

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez avec le bouton droit de la souris sur **Routage et accès distant** puis cliquez sur **Configurer et activer le routage et l'accès distant**.
- Sur la page **Bienvenue de l'assistant**, cliquez sur **Suivant**.
- Sur la page **Configuration**, cliquez sur **Configuration personnalisée** puis sur **Suivant**.
- Sur la page **Fin de l'Assistant Installation d'un serveur de routage et d'accès à distance**, cliquez sur **Terminer**.

- Dans la boîte de dialogue **Routage et accès distant**, cliquez sur **Démarrer le service**.

### c. Ajout de l'agent relais DHCP pour IPv4 ou IPv6



Win3

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez sur le nœud **IPv4** ou **IPv6** selon l'agent relais DHCP à activer.
- Si l'agent de relais DHCP n'est pas installé, cliquez avec le bouton droit de la souris sur **Général**, puis sur **Nouveau protocole de routage**.
- Dans la boîte de dialogue **Nouveau protocole de routage**, sélectionnez **Agent de relais DHCP** dans la liste **Protocoles de routage** puis cliquez sur **OK**.

L'agent relais DHCP apparaît sous routage IPv4 ou IPv6.

### d. Configuration de l'agent de relais DHCPv4



Win3

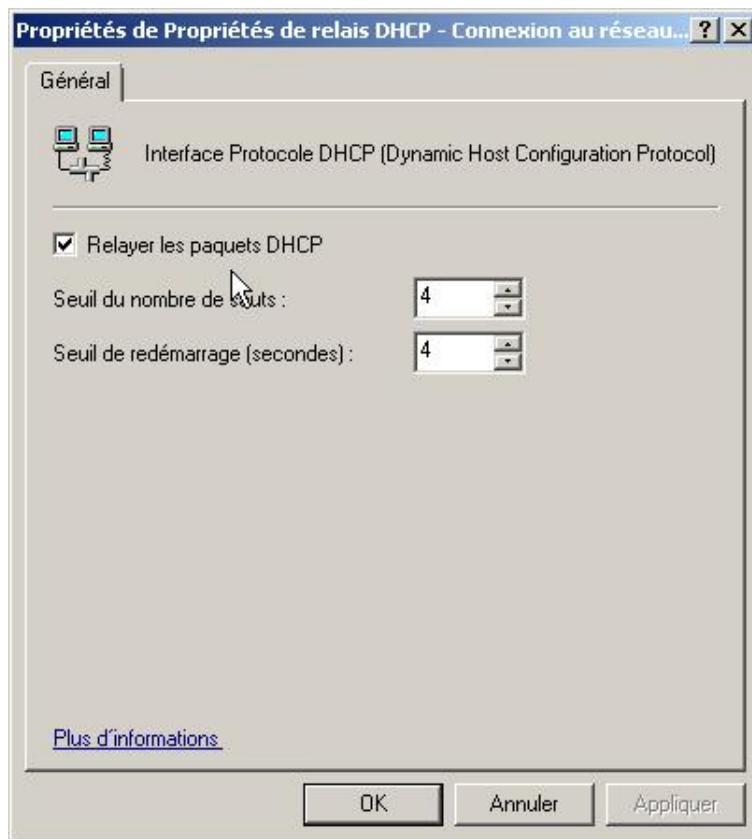
- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez sur le nœud **IPv4**.
- Cliquez avec le bouton droit de la souris sur **Agent de relais DHCP** puis sur **Propriétés**.
- Saisissez l'adresse du serveur DHCP disposant d'une étendue pour le sous-réseau, puis cliquez sur **Ajouter**. Répétez l'opération s'il existe d'autres serveurs DHCP. À la fin cliquez sur **OK**.

### e. Ajout et configuration des interfaces d'écoute pour l'agent de relais DHCPv4



Win3

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez sur le nœud **IPv4**.
- Cliquez avec le bouton droit de la souris sur **Agent de relais DHCP** puis sur **Nouvelle interface**.
- Dans la boîte de dialogue **Nouvelle interface pour Agent de relais DHCP**, sélectionnez l'interface d'écoute dans la liste des interfaces puis cliquez sur **OK**.
- Dans la boîte de dialogue **Propriétés de Propriétés de relais DHCP**, assurez-vous que la case à cocher **Relayer les paquets DHCP** est sélectionnée, puis cliquez sur **OK**.



**Seuil du nombre de sauts** : indique le nombre maximal d'agents relais DHCP qui géreront le trafic DHCP relayé (max. 16).

**Seuil de redémarrage (secondes)** : indique le temps d'attente avant d'envoyer la requête DHCP sur le serveur DHCP distant si aucune réponse locale n'a été reçue. Si aucun serveur DHCP n'est présent sur le segment local, diminuez cette valeur à 0.

## f. Configuration de l'agent de relais DHCPv6



Win3

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez sur le nœud **IPv6**.
- Cliquez avec le bouton droit de la souris sur **Agent de relais DHCP** puis sur **Propriétés**.

La boîte de dialogue **Propriétés** apparaît.

#### **Onglet Général**

L'onglet **Général** permet de définir les informations qui sont enregistrées dans le journal Système de l'Observateur d'événements.

#### **Onglet Serveurs**

- Saisissez l'adresse du serveur DHCP disposant d'une étendue pour le sous-réseau, puis cliquez sur **Ajouter**. Répétez l'opération s'il existe d'autres serveurs DHCP. À la fin, cliquez sur **OK**.

---

 L'agent relais DHCP doit disposer d'une adresse IPv6 globale !

---

### **g. Ajout et configuration des interfaces d'écoute pour l'agent de relais DHCPv6**



Win3

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud **Rôles**.
- Cliquez sur le nœud **Services de stratégie et d'accès distant**.
- Cliquez sur le nœud **IPv6**.
- Cliquez avec le bouton droit de la souris sur **Agent de relais DHCP** puis sur **Nouvelle interface**.
- Dans la boîte de dialogue **Nouvelle interface pour Agent de Relais DHCP**, sélectionnez l'interface d'écoute dans la liste des interfaces puis cliquez sur **OK**.
- Dans la boîte de dialogue **Propriétés de propriétés de Relais DHCP**, assurez-vous que la case à cocher **Relayer les paquets DHCP** est sélectionnée, puis cliquez sur **OK**.

**Seuil du nombre de sauts** : indique le nombre maximal d'agents relais DHCP qui géreront le trafic DHCP relayé (max. 16).

**Seuil de temps écoulé (centi-secondes)** : indique le temps d'attente avant d'envoyer la requête DHCP sur le serveur DHCP distant si aucune réponse locale n'a été reçue. Si aucun serveur DHCP n'est présent sur le segment local, diminuez cette valeur à 0.



L'utilisation d'un agent relais en support d'un serveur DHCP local est une bonne pratique en matière de tolérance de panne (règle des 80/20).

---

# Installation et désinstallation du rôle DHCP

## 1. Pré-requis



Le pré-requis pour l'installation du rôle DHCP est que le serveur dispose d'une adresse IP. Cette adresse devrait être statique (conseillé) sinon il faut s'assurer qu'elle ne peut pas être modifiée en effectuant une réservation auprès de son serveur DHCP (déconseillé). Car si l'adresse IP du serveur DHCP change, les clients DHCP ne peuvent renouveler leur bail, ce qui a pour conséquence de créer une interruption du réseau et une perte de toutes les connexions ouvertes.

Ce rôle peut fonctionner sur un serveur virtualisé. Dans ce cas, il est nécessaire de prêter une attention particulière aux cartes réseaux virtuelles ainsi qu'aux switch réseaux virtuels qui seront créés.

Il est possible de contrôler l'adresse IP du serveur avec la commande **ipconfig /all**.

## 2. Installation



L'assistant installe le service DHCP et permet également de configurer le serveur DHCP avec les options les plus courantes.

- Connectez-vous en tant qu'administrateur.
- Pour démarrer l'installation, lancez le Gestionnaire de serveur en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur **Rôles**.
- Dans **Rôles**, cliquez sur **Ajouter des rôles**.
- Dans l'**Assistant Ajout de rôles**, si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez le rôle **Serveur DHCP** puis cliquez sur **Suivant**.
- Sur la page **Serveur DHCP**, prenez connaissance si nécessaire des informations supplémentaires concernant le serveur DHCP puis cliquez sur **Suivant**.
- Sur la page **Liaisons de connexion réseau** de l'assistant, choisissez quelle(s) connexion(s) réseau traitera(ont) les demandes DHCP puis appuyez sur **Suivant**.

Un serveur DHCP disposant de plusieurs cartes réseau peut n'écouter les requêtes DHCP que sur certaines de ses cartes.

- Sur la page **Paramètres DNS IPv4**, spécifiez les options DNS que recevra un client DHCP, puis appuyez sur **Suivant**.

Les options entrées dans l'assistant sont enregistrées en tant qu'**Options de serveur**.

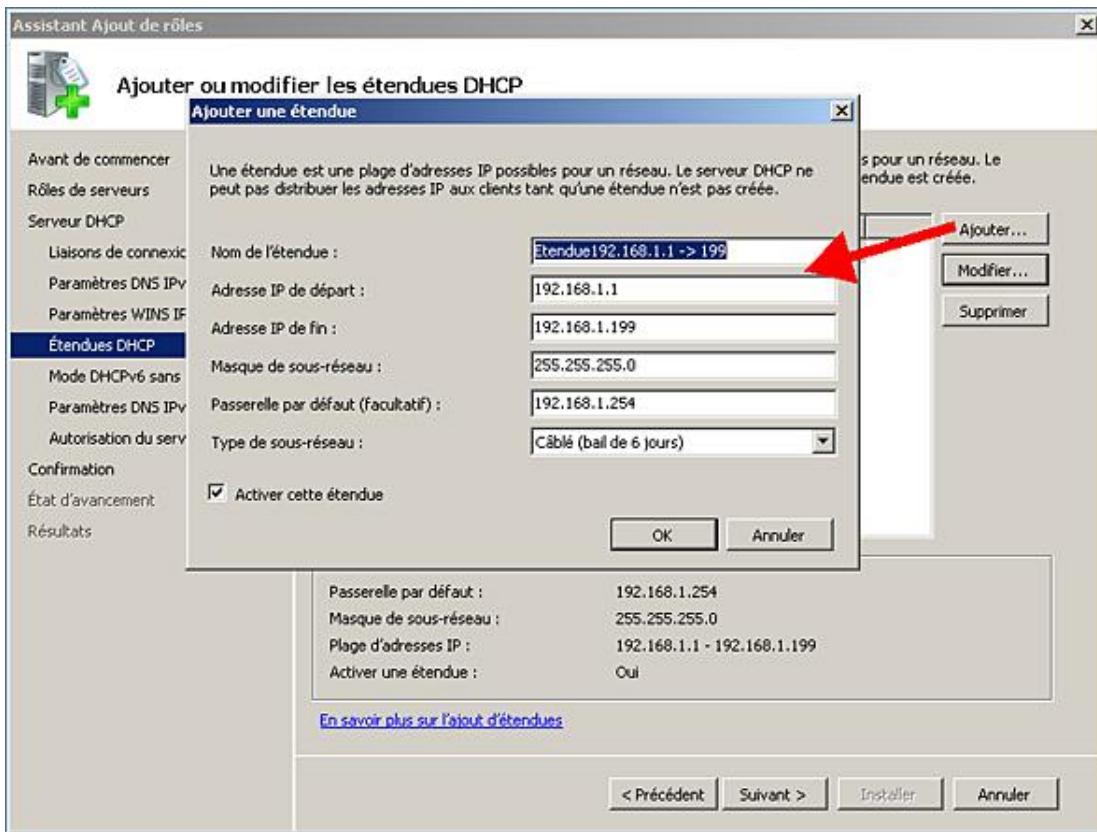
En cliquant sur le bouton **Valider**, l'assistant contrôle qu'un serveur DNS répond.

- Sur la page **Paramètres WINS IPv4**, spécifiez les options WINS c'est-à-dire les adresses des serveurs WINS que

recevra un client DHCP, puis appuyez sur **Suivant**.

- Un réseau moderne n'a plus besoin de serveurs WINS sauf si vous avez des ordinateurs clients Windows NT4.0 dans un environnement routé ou si vous utilisez certaines applications qui travaillent avec des requêtes NetBIOS.

- Sur la page **Étendues DHCP**, ajoutez au moins une étendue en cliquant sur le bouton **Ajouter**.
- Dans la boîte de dialogue **Ajouter une étendue**, saisissez les informations demandées comme dans l'exemple suivant :



**Nom de l'étendue** : saisissez un nom qui a un sens permettant d'identifier facilement les adresses comprises dans l'étendue comme **Etendue192.168.1.1 -> 199** qui indique l'adresse de début et de fin ou **172.30.1.0/24** qui indique que l'on utilise 254 adresses.

**Adresse IP de départ** : indique la première adresse de l'étendue.

**Adresse IP de fin** : indique la dernière adresse de l'étendue.

**Masque de sous-réseau** : comme son nom l'indique.

**Passerelle par défaut (facultatif)** : l'adresse du routeur.

**Type de sous-réseau** : permet de définir rapidement une durée de bail, soit 6 jours pour un ordinateur de bureau et 4 heures pour un ordinateur portable.

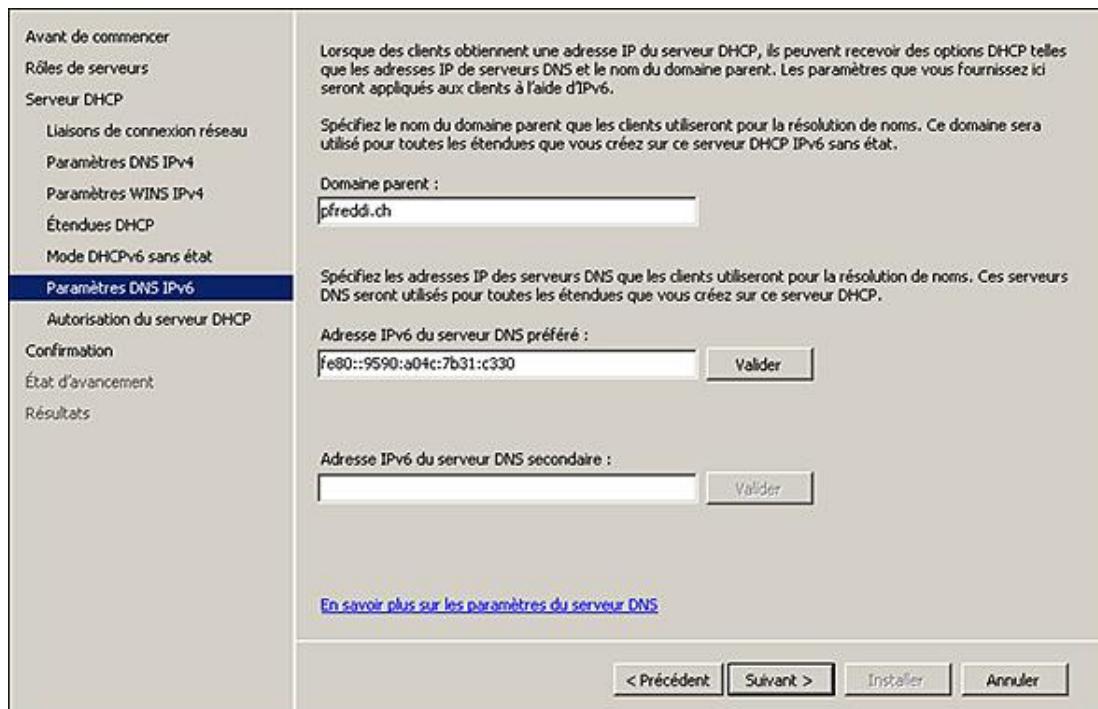
**Activer cette étendue** : indique si l'étendue une fois créée peut être utilisée par le serveur DHCP ou non.

- Lorsque vous appuyez sur **OK**, des contrôles sont effectués afin de garantir que les valeurs saisies sont correctes.

Dans la page **Mode DHCPv6 sans état**, vous pouvez activer le mode **stateless** DHCPv6 (choix par défaut) qui permet de fournir aux clients IPv6 les paramètres autres que l'adresse IP. Si vous voulez également fournir l'adresse IP ou activer le mode **stateful**, il faut sélectionner l'option **Désactiver le mode sans état DHCPv6 pour ce serveur**. À la fin,

cliquez sur **Suivant**.

La page **Paramètres DNS IPv6** n'apparaît que si le mode **sans état (stateless)** est sélectionné dans la page précédente. Saisissez les options de serveur avec les valeurs suivantes :



En cliquant sur le bouton **Valider**, l'assistant contrôle que le serveur DNS stipulé répond.

Sur la page **Autorisation du serveur DHCP**, il faut indiquer si c'est l'utilisateur actuel ou un utilisateur spécifique qui autorise le serveur DHCP à distribuer des adresses IP. Dans un environnement Active Directory, les serveurs DHCP doivent être autorisés à distribuer des adresses.

Cette protection sert plus à se prémunir contre une mauvaise configuration d'un serveur que contre des serveurs DHCP pirates, car seuls les serveurs DHCP Microsoft sont touchés.

► Lorsqu'un serveur DHCP autonome Windows Server 2008 détecte qu'il existe un serveur DHCP membre d'un domaine sur le même sous-réseau que lui et que ce dernier a été autorisé, alors le serveur DHCP autonome arrête de distribuer des adresses IP.

■ Si vous êtes **administrateur de domaine**, cliquez simplement sur **Suivant**, sinon spécifiez d'autres informations d'identification ou reportez l'autorisation à plus tard en sélectionnant **Ignorer l'autorisation de ce serveur DHCP dans les services de domaine Active Directory**.

► C'est une bonne méthode que d'ajouter les administrateurs DHCP ou les utilisateurs DHCP (consultations des informations du serveur DHCP) en utilisant une stratégie de groupe située dans **Configuration de l'ordinateur - Paramètres Windows - Paramètres de sécurité - Groupes restreints**. Il est nécessaire que l'utilisateur soit ajouté au groupe restreint ainsi qu'au groupe proprement dit.

■ La page **Confirmation** résume les paramètres entrés durant les différentes étapes de l'assistant. Prenez le temps de les vérifier puis cliquez sur **Installer**.

La page suivante, appelée **État d'avancement**, affiche un curseur montrant la progression de l'installation.

Enfin, la page **Résultats** indique si l'installation du serveur DHCP a réussi.

Dans ce cas, votre serveur DHCP est installé et opérationnel.

### 3. Désinstallation



Win

- Connectez-vous en tant qu'administrateur.
- Pour désinstaller le serveur DHCP, lancez le Gestionnaire de serveur en cliquant sur **Démarrer** puis sur **Outils d'administration** et enfin sur **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur **Rôles**.
- Dans **Rôles**, cliquez sur **Supprimer des rôles**.
- Dans l'**Assistant Suppression de rôles**, si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez le rôle **Serveur DHCP** puis cliquez sur **Suivant**.
- Sur la page **Confirmation**, vérifiez que vous supprimez le serveur DHCP puis cliquez sur **Supprimer**.

La page **Etat d'avancement** montre une barre de progression pour vous faire patienter pendant la suppression.

Enfin, la page **Résultats** indique que pour terminer la suppression du rôle, il faut redémarrer le serveur.

- Cliquez sur **Fermer**.
- Dans la boîte de dialogue **Assistant Suppression de rôle**, cliquez sur **Oui** pour redémarrer le serveur maintenant.

Lors de la prochaine connexion, l'assistant affiche le résultat de la suppression du serveur DHCP. Vérifiez que la suppression est réussie.

L'assistant de suppression du serveur DHCP ne supprime que les services et pas la base de données qui est toujours présente dans le répertoire **%systemroot%\system32\dhcp**. Effacez le répertoire pour une suppression complète.

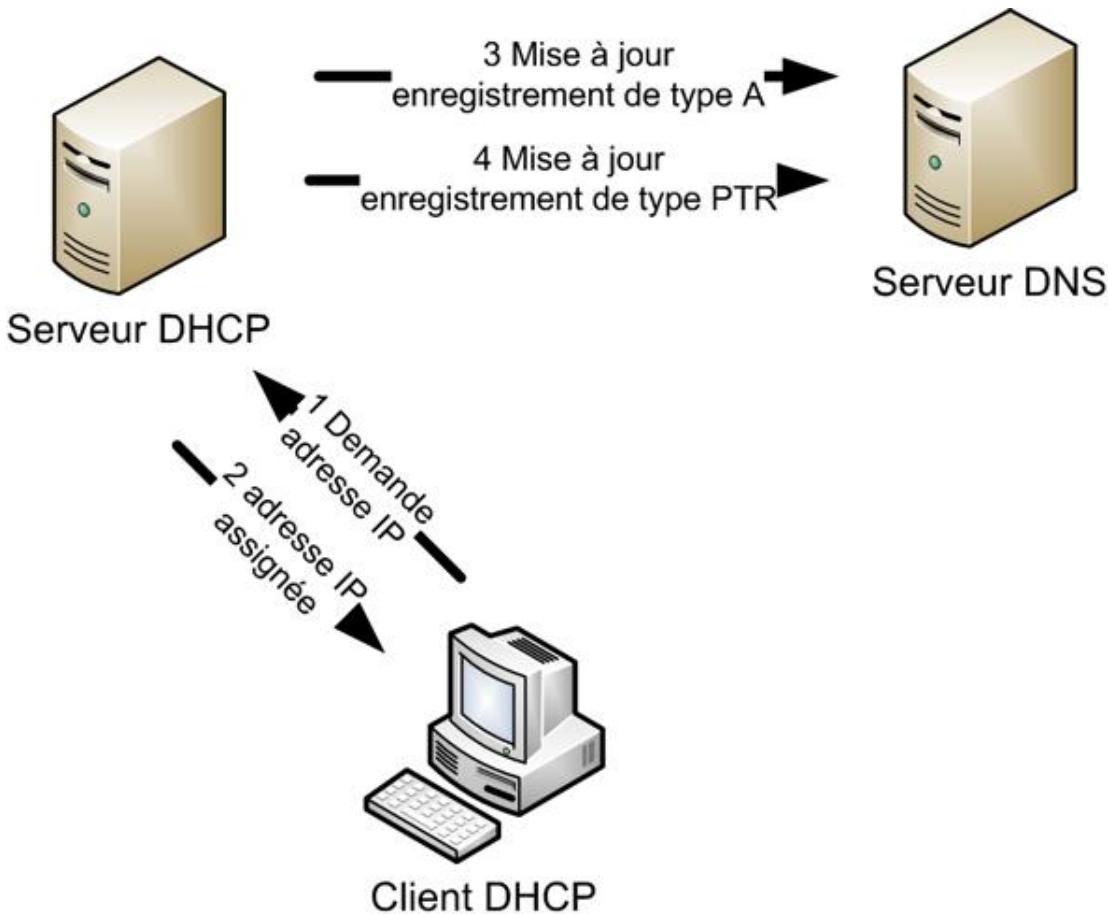
# Service DHCP de Windows

## 1. Introduction

Le rôle Microsoft DHCP implémente les RFC 2131 et 2132 pour le protocole TCP/IP v4 ainsi que la RFC 3315 pour le protocole TCP/IP v6.

Le service DHCP, s'il fonctionne dans un domaine, doit être autorisé par l'Active Directory, sinon le service ne démarre pas. Pour cela, le serveur DHCP envoie un message **DHCPINFORM** à l'Active Directory qui lui répond avec un message **DHCPPACK** ou **DHCPNACK**.

Le serveur DHCP peut mettre à jour le DNS au nom du client DHCP, comme montré sur la figure suivante, pour un client qui ne peut mettre à jour le serveur DNS ou si le client le demande.



Dans la figure précédente, si le client peut mettre à jour le serveur DNS, l'étape 3, voire l'étape 4, peut être effectuée par le client DHCP au lieu du serveur DHCP.

Dans certains réseaux, on voit parfois plusieurs sous-réseaux IP partager le même réseau physique. Le serveur DHCP permet de réunir ces différents réseaux IP pour créer une étendue globale de manière à ce que les clients DHCP se trouvant sur le réseau physique reçoivent une adresse provenant de l'un des sous-réseaux IP.

Il est fortement déconseillé d'avoir plusieurs réseaux IP sur le même réseau physique. Cet état n'est acceptable que durant une phase de surcharge ou de transition courte. Néanmoins l'utilisation d'une étendue globale présente un intérêt s'il existe plusieurs serveurs DHCP sur le même segment de réseau.

## 2. Les options

Parmi les quelques 80 options standardisées, les clients DHCP Windows n'utilisent par défaut que celles montrées dans le tableau suivant :

Nom de l'option	Code de l'option	Option rencontrée dans
PAD	0	Tous les messages DHCP
Masque de sous-réseau	1	Tous les messages DHCP
Routeur	3	Demandée par le client
Serveur DNS	6	Demandée par le client
Nom de l'hôte	12	Tous les messages DHCP
Nom de Domaine DNS	15	Demandée par le client
Découvrir les routeurs*	31	Demandée par le client
Option d'itinéraire statique*	33	Demandée par le client
Informations spécifiques au fournisseur	43	Tous les messages DHCP
Nom du serveur Wins	44	Demandée par le client
Type de nœud pour la résolution de nom NetBIOS sur TCP/IP	46	Demandée par le client
ID de l'étendue NetBIOS	47	Demandée par le client
Adresse demandée	50	Tous les messages DHCP
Durée du bail	51	Tous les messages DHCP
Type de message DHCP	53	Tous les messages DHCP
Identificateur du serveur	54	Tous les messages DHCP
Liste des paramètres demandés	55	Tous les messages DHCP
Durée T1	58	Tous les messages DHCP
Durée T2	59	Tous les messages DHCP
Identificateur client	61	Tous les messages DHCP
Mise à jour DNS dynamique	81	Tous les messages DHCP
Itinéraires statiques sans classe*	121	Demandée par le client
Itinéraires statiques sans classe*	249	Demandée par le client
Fin	255	Tous les messages DHCP

\*Pour des clients postérieurs à Windows 2000

 Concernant les itinéraires statiques sans classe, l'option 249 était utilisée pour les versions antérieures à Windows Vista. Windows Vista et Windows Server 2008 utilisent les deux options, à savoir 121 et 249, comme vous pouvez le voir dans l'image suivante.

Pour recevoir d'autres options provenant du serveur DHCP, le client DHCP doit explicitement les demander en ajoutant l'option désirée dans la **liste des paramètres demandés** (code de l'option 55). Pour le client Microsoft, la

procédure consiste à passer par la programmation, en d'autres termes il faut un programme pour modifier la **liste des paramètres demandés**.

L'image suivante montre le détail des options DHCP d'une capture effectuée avec un moniteur réseau.

```
Dhcp: Boot Request, MsgType = REQUEST, TransactionID = 0x12DAAE49
  OpCode: Boot Request, 1(0x01)
  HardwareType: Ethernet
  HardwareAddressLength: 6 (0x6)
  HopCount: 0 (0x0)
  TransactionID: 316321353 (0x12DAAE49)
  Seconds: 0 (0x0)
  Flags: 32768 (0x8000)
  ClientIP: 0.0.0.0
  YourIP: 0.0.0.0
  ServerIP: 0.0.0.0
  RelayAgentIP: 0.0.0.0
  ClientHardwareAddress: 00-03-FF-C7-6A-CF
  ServerHostName:
  BootFileName:
  MagicCookie: 99.130.83.99
  MessageType: REQUEST
  clientID: (Type 1)
    Code: Client-identifier, 61(0x3D)
    Length: 7 UINT8(s)
    Type: HardwareAddress(1)
    ClientID: Binary Large Object (6 Bytes)
  RequestedIPAddress: 172.30.1.105
  HostName: WIN-SOT94GFZGLA
  FullyQualifiedDomainName:
  VendorClassIdentifier: MSFT 5.0
  ParameterRequestList:
    Code: Parameter Request List, 55(0x37)
    Length: 12 UINT8(s)
    Parameter: Subnet Mask, 1(0x01)
    Parameter: Domain Name, 15(0x0F)
    Parameter: Router, 3(0x03)
    Parameter: Domain Name Server, 6(0x06)
    Parameter: NetBIOS over TCP/IP Name Server, 44(0x2C)
    Parameter: NetBIOS over TCP/IP Node Type, 46(0x2E)
    Parameter: NetBIOS over TCP/IP Scope, 47(0x2F)
    Parameter: Perform Router Discovery, 31(0x1F)
    Parameter: Static Route, 33(0x21)
    Parameter: Classless Static Route Option, 121(0x79)
    Parameter: Classless Static Route, 249(0xF9)
    Parameter: Vendor specific information, 43(0x2B)
  End:
```

Dans le cas où le serveur DHCP distribue des adresses à des clients Microsoft ayant besoin d'options particulières, il est tout à fait possible de créer des options personnalisées basées sur des classes utilisateurs ou fournisseurs.

### 3. Les nouveautés de Windows Server 2008

Le support du protocole DHCPv6 signifie qu'il est possible de définir des étendues et de distribuer des adresses IPv6.

Le support du protocole NAP permet de contrôler la distribution d'adresses IP de manière à ce qu'un client non conforme ne puisse recevoir toutes les options DHCP et soit renvoyé vers le réseau de remédiation.

## 4. Les outils de configuration

Les outils de configuration et de gestion sont :

- La console DHCP, soit une console MMC permettant de gérer un ou plusieurs serveurs DHCP.
- Les commandes **netsh** permettent également d'effectuer une gestion efficace d'un serveur DHCP.

## 5. Meilleures pratiques

- Créer des étendues de manière à ne pas utiliser d'exception.
- Prévoir des baux de 7 jours pour les ordinateurs de bureau.
- Prévoir des baux de 2 heures pour les ordinateurs portables.
- Pour une haute disponibilité, prévoir un second serveur en partageant les adresses IP sur les deux serveurs avec la règle des 80/20.
- Éviter la création d'étendues globales.
- Configurer correctement les options à utiliser.
- Activer le protocole BOOTP pour les clients RIS ou WDS.
- Gérer la redondance avec un cluster pour disposer d'une gestion totalement centralisée, tolérante aux pannes.

# Présentation du protocole DHCP

## 1. Introduction

DHCP est un protocole client/serveur qui fournit automatiquement à un hôte IP une adresse IP et d'autres paramètres de configuration comme le masque de sous-réseau.

On utilise les termes de **client** ou **client DHCP** pour l'hôte IP qui reçoit une adresse IP provenant d'un **serveur DHCP**.

Le serveur DHCP peut être un routeur ADSL, donc basé sur du matériel, ou un logiciel comme le rôle DHCP de Windows Server 2008.

Le serveur DHCP gère et distribue de manière centralisée et automatique les adresses IP sur un réseau donné. Le réseau peut être local ou distant.

Ses avantages principaux sont :

- Le gain de productivité car il n'est plus nécessaire à un technicien de passer sur chaque ordinateur pour configurer son adresse IP.
- La modification du système d'adressage IP est également simplifiée.
- Les erreurs de configuration sont impossibles en production.
- Il est possible de réserver une adresse pour un client afin qu'il utilise toujours la même adresse.

Sur un réseau, il peut coexister des hôtes clients DHCP et des hôtes configurés manuellement.

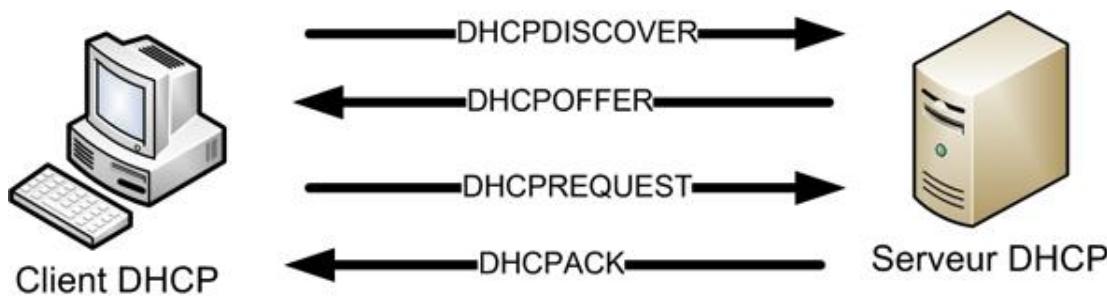
On parle également d'adresse dynamique pour un client DHCP et d'adresse statique pour une configuration manuelle.

Le protocole DHCP est une extension du protocole BOOTP (*Bootstrap Protocol*). Il diffère principalement de ce dernier par le fait que le client DHCP peut renouveler son bail et pas le client BOOTP. Le protocole BOOTP est encore utilisé par les clients PXE (*Preboot eXecution Environment*) lors d'un déploiement du système d'exploitation via un serveur RIS (*Remote Installation Services*) ou son successeur WDS (*Windows Deployment Services*).

## 2. Processus d'acquisition d'une adresse IPv4

Le processus d'acquisition d'une adresse IP permet à un hôte de recevoir une adresse IP automatiquement.

Ce processus comporte quatre phases comme montré dans la figure suivante :



Lorsque l'hôte se connecte sur un réseau, il envoie un message de diffusion appelé **DHCPDISCOVER** du port UDP 68 vers le port UDP 67 pour demander une adresse IP.

Tout serveur DHCP recevant le message DHCPDISCOVER doit traiter cette requête.

Le serveur DHCP commence par déterminer dans quelle étendue se trouve le demandeur puis il recherche dans les adresses réservées si le client est connu et lui assigne son adresse IP, sinon il lui assigne une adresse provenant des adresses libres de l'étendue. L'envoi de l'adresse du serveur au client se fait au moyen d'un message de diffusion appelé **DHCPOFFER** depuis le port UDP 67 vers le port UDP 68 contenant l'adresse IP, le masque de sous-réseau, la durée du bail et les options définies.

Le client est tenu d'accepter la première adresse IP provenant d'un DHCPOFFER quel que soit le serveur DHCP et de retourner un message de diffusion appelé **DHCPREQUEST** du port UDP 68 vers le port UDP 67 auprès du serveur DHCP afin de lui signifier qu'il veut utiliser l'adresse IP reçue.

Le serveur DHCP concerné retourne auprès du client un message appelé **DHCPACK** en utilisant le port UDP 67 vers le port UDP 68, ce qui permet au client d'utiliser l'adresse IP pendant la durée du bail. Si la réponse est un **DHCPNACK**, le client doit recommencer entièrement le processus d'acquisition d'une adresse IP.

À partir de Windows 2000, le client DHCP contrôle également si l'adresse IP n'est pas déjà utilisée après avoir reçu le DHCPACK. Si elle est utilisée, il envoie auprès du serveur DHCP, un message DHCPDECLINE et il recommence le processus d'acquisition.

L'image suivante montre l'enregistrement des trames réseau par un moniteur réseau lors de l'acquisition d'une adresse IP par un client DHCP. La trame 16 teste si l'adresse est utilisée, la réponse n'a pas été enregistrée par le moniteur réseau mais il y a eu une réponse et l'adresse est donc utilisée car la trame 18 envoie un DHCPDECLINE.

Fra...	Source	Destination	Protocol Name	Description
11	0.0.0.0	255.255.255.255	DHCP	DHCP: Boot Request, MsgType = DISCOVER, TransactionID = 0x986D377D
12	172.30.1.1	255.255.255.255	DHCP	DHCP: Boot Reply, MsgType = OFFER, TransactionID = 0x986D377D
13	172.30.1.170	255.255.255.255	DHCP	DHCP: Boot Reply, MsgType = OFFER, TransactionID = 0x986D377D
14	0.0.0.0	255.255.255.255	DHCP	DHCP: Boot Request, MsgType = REQUEST, TransactionID = 0x986D377D
15	172.30.1.1	255.255.255.255	DHCP	DHCP: Boot Reply, MsgType = ACK, TransactionID = 0x986D377D
16	0.0.0.0	172.30.1.103	ARP	ARP: Request, 0.0.0.0 asks for 172.30.1.103
17	FE80:0:0:0:... FF02:0:0:0:1	UDP	UDP: SrcPort = 61585, DstPort = Linklocal Multicast Name Resolution(5355)	
18	0.0.0.0	255.255.255.255	DHCP	DHCP: Boot Request, MsgType = DECLINE, TransactionID = 0x986D377D
19	FF02:0:0:0:1 FF02:0:0:0:1	UDP	UDP: SrcPort = 61585, DstPort = Linklocal Multicast Name Resolution(5355)	

**Frame Details**

```

Frame:
  + Ethernet: Etype = Internet IP (IPv4)
  + Ipv4: Next Protocol = UDP, Packet ID = 253, Total IP Length = 354
  + Udp: SrcPort = BOOTP client(68), DstPort = BOOTP server(67), Length = 334
    - SourcePort: BOOTP client(68), 68(0x44)
    - DestinationPort: BOOTP server(67), 67(0x43)
    - TotalLength: 334 (0x14E)
    - Checksum: 12301 (0x300D)
  + Dhcp: Boot Request, MsgType = REQUEST, TransactionID = 0x986D377D
    - OpCode: Boot Request, 1(0x01)
    - Hardwaretype: Ethernet
    - HardwareAddressLength: 6 (0x6)
    - HopCount: 0 (0x0)
  
```

Il est également intéressant de constater qu'il existe deux serveurs DHCP sur ce réseau selon les trames 12 et 13 et que le client DHCP a bien accepté la première requête reçue.

### 3. Processus de renouvellement d'une adresse IP

Il intervient dans les deux cas suivants :

- Pour renouveler le bail.
- Chaque fois que la carte réseau se reconnecte au réseau.

En cas de reconnexion, si l'expiration du bail n'est pas atteinte, le client DHCP envoie un message de diffusion DHCPREQUEST pour obtenir le DHCPACK du serveur et utiliser l'adresse IP louée. Il n'y a pas de contrôle pour savoir si l'adresse est utilisée par un autre hôte.

Pour le renouvellement, le client doit tenter de renouveler son adresse IP au temps **T1**, soit à la moitié de la durée du bail. Si le serveur DHCP n'est pas disponible, il essaiera de nouveau au temps **T2**, soit à 87,5 % de la durée de bail. Si le bail n'a pas pu être renouvelé, le client DHCP doit libérer l'adresse IP à l'expiration et recommencer le processus d'acquisition d'une adresse IP. Une interruption du trafic réseau et la perte des connexions sont possibles.

Le renouvellement utilise des messages UNICAST pour la demande DHCPREQUEST et la réponse DHCPACK provenant du serveur DHCP.

Les valeurs de T1 et T2 sont fournies en tant qu'options DHCP.

### 4. Les options

Le terme d'option est utilisé pour définir un paramètre de configuration complétant l'adresse IP comme le masque de sous-réseau, l'adresse du routeur, le serveur DNS. Il existe des options standardisées ainsi que des options que l'on peut définir. Les options sont assignées en même temps que l'adresse IP.



# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre plusieurs objectifs décrits dans les sections :

### Configuration des services et de l'adressage IP

Configurer DHCP (*Dynamic Host Configuration Protocol*).

Cela inclut, sans s'y limiter :

- d'installer et gérer un serveur DHCP ;
- d'autoriser un serveur DHCP dans l'Active Directory ;
- de créer et gérer des étendues ;
- d'exclure des adresses d'une étendue ;
- de gérer les options DHCP ;
- de créer de nouvelles options DHCP ;
- de comprendre la portée d'une étendue et de mettre en œuvre le cas échéant un serveur agent relais DHCP ;
- démarrage à l'aide du client PXE ;
- virtualisation et serveur DHCP.

### Configuration de la résolution de noms

Configurer les enregistrements DNS.

Cela inclut, sans s'y limiter :

- mises à jour des enregistrements DNS via le serveur DHCP.

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



## 3. Objectifs

Gérer efficacement, simplement et de manière centralisée l'adressage IP est une opération aisée grâce à l'utilisation d'un serveur DHCP (*Dynamic Host Configuration Protocol*). Sa mise en œuvre est des plus simples, néanmoins dans une configuration réseau moderne avec des routeurs, elle est un peu plus délicate. En effet, il faut pouvoir également distribuer des adresses dans le bon segment de réseau IP.

Le début du chapitre présente le protocole DHCPv4 et la manière dont un client reçoit une adresse en IPv4. Sont également présentés et expliqués les différents termes et paramètres utiles d'un serveur DHCP.

Ensuite, vous verrez comment installer, configurer et gérer un serveur DHCP pour IPv4 et IPv6 avec les explications nécessaires pour comprendre les différences entre les deux protocoles. Enfin, vous verrez comment installer et gérer un Server Core.

# Validation des acquis : questions/réponses

## 1. Questions

### Questions triviales

- 1 Qu'est-ce qu'un espace de noms ?
- 2 Qu'appelle-t-on un FQDN ?
- 3 Pourquoi est-il possible que deux entreprises possèdent un nom identique mais avec une extension différente comme eni.fr et eni.com ?
- 4 À quoi sert le TTL ?
- 5 Comment créer un serveur de cache DNS ?
- 6 Comment faire pour répondre à des requêtes DNS ne provenant que d'une seule interface sur un serveur multirésident ?
- 7 Quelle est la différence entre un **redirecteur conditionnel** et une **zone de stub** ?
- 8 Indiquez plusieurs avantages au stockage d'une zone dans l'Active Directory.
- 9 Indiquez à quoi sert un enregistrement de type **MX** et donnez un exemple d'utilisation.
- 10 Indiquez à quoi sert un enregistrement de type **DNAME** et donnez un exemple d'utilisation.
- 11 Indiquez à quoi sert un enregistrement de type **SRV** et donnez un exemple d'utilisation.
- 12 Pourquoi le transfert de zone d'une zone intégrée Active Directory est plus sécurisé que le transfert de zone DNS ?
- 13 Quelle différence y-a-t-il entre une **zone de recherche directe** et une **zone de recherche inversée** ?
- 14 Quelle différence y-a-t-il entre une **recherche itérative** et une **recherche récursive** ?
- 15 Pourquoi créer une **zone déléguée** au lieu d'un simple **sous-domaine** ?
- 16 Qu'est-ce qu'une zone **GlobalNames** ?
- 17 Est-il recommandé d'installer un serveur DNS sur un Server Core ?
- 18 Indiquez le nom d'au moins deux utilitaires en ligne de commande, pour gérer un serveur DNS.
- 19 À quoi sert la commande **dnscmd localhost /info** ?
- 20 Indiquez un pré-requis pour installer un serveur DNS.
- 21 Qu'appelle-t-on la recherche du réseau ?
- 22 Indiquez au moins trois éléments utilisés par le résolveur TCP/IP.
- 23 Qu'est-ce qu'un type de nœud ?

### Questions de compréhension

- 24 Expliquez la différence entre une **zone principale**, une **zone secondaire** et une **zone intégrée Active Directory**.
- 25 Votre collègue a créé des enregistrements pour des serveurs de tests dans le serveur DNS ; bien que les serveurs n'existent plus depuis près d'une année, les enregistrements ne sont jamais supprimés, pourquoi ?
- 26 L'adresse IP d'un serveur a changé, certains utilisateurs se plaignent de ne pouvoir s'y connecter. Quelle solution leur proposez-vous pour résoudre leur problème ?
- 27 Indiquez quelques avantages à utiliser un serveur de cache externe et quelle serait la stratégie à utiliser.
- 28 Un de vos collègues aimerait limiter le trafic dû au transfert de zone entre le siège et un bureau distant. Il préconise l'utilisation d'un serveur DNS de cache, alors qu'un autre préconise l'utilisation d'une zone de stub, enfin un troisième propose la création d'un sous-domaine. Quel est votre avis sur les solutions proposées et quelle serait votre solution ?
- 29 Vous devez modifier l'adresse IP d'un serveur sensible, quelle serait la procédure à effectuer pour garantir qu'il n'y aura pas une interruption de service ?
- 30 Vous devez déplacer un serveur sensible d'un site A vers un site B, il est requis de limiter au maximum l'interruption du serveur, quelle procédure mettez-vous en œuvre ?

- 31** Des utilisateurs se plaignent qu'ils n'arrivent pas à se connecter au serveur applicatif. Comment pouvez-vous être sûr qu'il s'agit d'un problème de résolution de noms et pas d'un problème réseau ?
- 32** L'entreprise de sécurité mandatée pour un audit indique qu'il existe un problème au niveau du transfert des zones DNS, quelle pourrait en être la cause ?
- 33** L'entreprise de sécurité mandatée pour un audit indique dans son rapport qu'il est possible de connaître la topologie de votre réseau, donnez une explication possible.
- 34** Vous devez implémenter une solution simple mais sécurisée pour permettre aux utilisateurs d'un groupe de travail d'avoir accès aussi bien aux ordinateurs de leur entreprise qu'à Internet, quelle serait une solution possible ?
- 35** Un de vos collègues ne trouve pas d'enregistrement dans le DNS concernant un serveur. Il propose de l'ajouter manuellement, que lui dites-vous ?

### **Questions de mise en œuvre**

- 36** Dans votre entreprise, composée d'environ 3000 ordinateurs, il existe un bureau distant qui dispose d'un serveur et de 10 postes de travail. Généralement, les utilisateurs se plaignent de la lenteur lorsqu'ils accèdent à des ressources situées sur le réseau de l'entreprise alors que les performances sont bonnes sur leur réseau distant. Vous avez déterminé que la bande passante est presque saturée et avez observé des transferts de zone. Pouvez-vous améliorer un peu la bande passante en modifiant la configuration du serveur DNS, justifiez votre réponse ?

## **2. Résultats**

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /36

Pour ce chapitre, votre score minimum doit être de 27 sur 36.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

## **3. Réponses**

### **Questions triviales**

- 1** Qu'est-ce qu'un espace de noms ?

*Un espace de noms est une arborescence qui contient des objets (des nœuds et des sous-domaines) sur laquelle le serveur DNS a autorité.*

- 2** Qu'appelle-t-on un FQDN ?

*Le FQDN est un nom complet identifiant une ressource depuis ses parents jusqu'à la racine. Chaque point étant un séparateur hiérarchique. [www.eni.fr](http://www.eni.fr). est un FQDN.*

- 3** Pourquoi est-il possible que deux entreprises possèdent un nom identique mais avec une extension différente comme eni.fr et eni.com ?

*Le nom de domaine doit être unique dans le domaine dans lequel il se trouve (règle d'unicité). Vous pouvez donc avoir eni.fr qui appartient à l'entreprise X et eni.com qui appartient à l'entreprise Y, vous êtes invité à faire le test via nslookup ou un navigateur.*

- 4** À quoi sert le TTL ?

*Le TTL ou Time To Live définit la durée de vie d'un enregistrement DNS. Normalement cette valeur est définie pour la zone, mais il est possible de la définir pour un enregistrement particulier. Le **TTL** permet de modifier l'adresse IP d'un nœud facilement, car dès que la valeur du **TTL** change il est possible de garantir qu'à la fin du délai les ordinateurs seront capables de basculer vers la nouvelle adresse automatiquement.*

- 5** Comment créer un serveur de cache DNS ?

*Il faut simplement installer le rôle Serveur DNS, bien sûr les clients doivent pointer dessus.*

- 6** Comment faire pour ne répondre à des requêtes DNS provenant que d'une seule interface sur un serveur multirésident ?

*Il est nécessaire de désactiver l'écoute de requêtes DNS pour les adresses IP du serveur qui sont sur les autres interfaces.*

- 7** Quelle est la différence entre un **directive conditionnel** et une **zone de stub** ?

Bien que les deux permettent de rediriger les requêtes de certains domaines vers des serveurs DNS spécifiques, la différence essentielle tient au fait que pour les redirecteurs conditionnels, il faut inscrire et mettre à jour manuellement les enregistrements des serveurs DNS, alors que pour la zone de stub il suffit d'ajouter manuellement les adresses des serveurs DNS, toutes les modifications s'effectueront automatiquement.

**8** Indiquez plusieurs avantages au stockage d'une zone dans l'Active Directory.

Parmi tous les avantages, on peut citer la sécurité du stockage puisqu'elle est stockée dans la base Active Directory, l'utilisation de la réPLICATION Active Directory, le choix et la portée de la partition utilisée pour stocker la zone DNS dans l'Active Directory, le chargement en arrière-plan de la zone Active Directory.

**9** Indiquez à quoi sert un enregistrement de type **MX** et donnez un exemple d'utilisation.

Un enregistrement MX permet de trouver des serveurs SMTP (messagerie e-mail) pour un domaine particulier. Les enregistrements MX sont généralement enregistrés sur un serveur DNS externe à l'entreprise afin que les collaborateurs puissent être joignables par des utilisateurs externes à celle-ci.

**10** Indiquez à quoi sert un enregistrement de type **DNAME** et donnez un exemple d'utilisation.

Un enregistrement DNAME permet de créer un alias de domaine pour, par exemple, migrer une entreprise d'un ancien nom de domaine vers le nouveau nom, ou pour intégrer une entreprise nouvellement acquise dans un holding.

**11** Indiquez à quoi sert un enregistrement de type **SRV** et donnez un exemple d'utilisation.

Les enregistrements SRV permettent de définir des enregistrements de ressources utilisables par des applications. Par exemple l'enregistrement SRV \_gc pour le catalogue global permet de trouver des catalogues globaux de notre forêt.

**12** Pourquoi le transfert de zone d'une zone intégrée Active Directory est plus sécurisé que le transfert de zone DNS.

Le transfert de zone est plus sécurisé car il utilise la réPLICATION Active Directory qui ne réplique les informations que vers des contrôleurs de domaine de la forêt. D'autre part, les informations sont cryptées durant le transfert.

**13** Quelle différence y-a-t-il entre une **zone de recherche directe** et une **zone de recherche inversée** ?

La zone de recherche directe est utilisée pour résoudre des noms en adresse IP alors que la zone de recherche inversée permet la résolution d'adresse IP en nom.

**14** Quelle différence y-a-t-il entre une **recherche itérative** et une **recherche récursive** ?

Dans la recherche itérative, on accepte une demi réponse qui est une indication pour contacter un autre serveur, alors qu'avec une recherche récursive seule la réponse correcte est acceptée, soit résolue ou non résolue.

**15** Pourquoi créer une **zone déléguée** au lieu d'un simple **sous-domaine** ?

Le plus simple est de créer un sous-domaine, néanmoins lorsque pour des raisons de bande passante disponible le trafic dû au transfert de zone est pénalisant, il est préférable de déléguer ce sous-domaine à un serveur DNS qui aura autorité pour le sous-domaine, et il n'y aura plus de transfert de zone entre les serveurs DNS.

**16** Qu'est-ce qu'une zone **GlobalNames** ?

La zone GlobalNames est une alternative au serveur WINS lorsque l'on se retrouve dans des environnements où ;

- L'on ne veut pas installer des serveurs WINS mais où l'on a besoin de pouvoir contacter des serveurs par leur nom sans ajouter de suffixes.
- Lorsque l'on a des hôtes disposant uniquement de la pile IPv6. Ils ne sont pas capables de dialoguer avec un serveur WINS.

**17** Est-il recommandé d'installer un serveur DNS sur un Server Core ?

Oui, c'est même une excellente pratique. Il faudrait que le Server Core soit également contrôleur de domaine.

**18** Indiquez le nom d'au moins deux utilitaires en ligne de commande pour gérer un serveur DNS.

Vous pouvez citer Nslookup, DnsCmd, DnsLint.

**19** À quoi sert la commande **dnscmd localhost /info** ?

Cette commande sert à afficher des informations sur le serveur DNS local.

**20** Indiquez un pré-requis pour installer un serveur DNS.

Il faut que l'adresse IP du serveur DHCP soit une adresse IP fixe ou une adresse IP réservée. En fait elle ne doit pas pouvoir changer.

**21** Qu'appelle-t-on la recherche du réseau ?

La recherche du réseau correspond à l'implémentation du protocole LLMNR qui remplace la recherche par diffusion du protocole NetBIOS par une recherche purement TCP/IP utilisant des adresses Multicast. La recherche du réseau est compatible avec le protocole IPv6 alors que la diffusion ne l'est pas. Elle remplace l'explorateur d'ordinateurs.

**22** Indiquez au moins trois éléments utilisés par le résolveur TCP/IP.

Vous pouvez citer le nom local, le cache local, le fichier HOSTS, le serveur DNS et bien sûr la recherche LLMNR.

**23** Qu'est-ce qu'un type de noeud ?

*Un type de nœud permet de définir pour une recherche NetBIOS comment la diffusion et le serveur WINS seront utilisés.*

### **Questions de compréhension**

**24** Expliquez la différence entre une **zone principale**, une **zone secondaire** et une **zone intégrée Active Directory**.

*Une zone principale est une zone qui est accessible en lecture et en écriture alors qu'une zone secondaire n'est accessible qu'en lecture. Pour disposer d'une zone secondaire, il est nécessaire de disposer d'au moins une zone principale pour le nom de domaine considéré. Ces deux zones sont stockées dans un fichier. Pour un domaine particulier, il ne peut exister qu'un serveur hébergeant une zone principale, les autres serveurs pour ce domaine doivent être configurés en zone secondaire. Une zone intégrée Active Directory est accessible en lecture et en écriture sur plusieurs serveurs. La zone est stockée dans l'Active Directory. La réPLICATION est gérée par la réPLICATION de l'Active Directory. Une zone intégrée Active Directory est plus sécurisée car il est possible de restreindre les mises à jour dynamiques uniquement aux membres de l'Active Directory.*

**25** Votre collègue a créé des enregistrements pour des serveurs de tests dans le serveur DNS ; bien que les serveurs n'existent plus depuis près d'une année, les enregistrements ne sont jamais supprimés, pourquoi ?

*Les enregistrements sont statiques et par conséquent ils ne sont jamais supprimés. Il faut les supprimer manuellement.*

**26** L'adresse IP d'un serveur a changé, certains utilisateurs se plaignent de ne pouvoir s'y connecter. Quelle solution leur proposez-vous pour résoudre leur problème ?

*Il faut vider le cache local du résolveur de l'ordinateur client. Bien que la commande soit **ipconfig /flushdns**, elle doit être exécutée avec des priviléges élevés sur un ordinateur Windows Vista mais fonctionne parfaitement pour Windows XP.*

**27** Indiquez quelques avantages à utiliser un serveur de cache externe et quelle serait la stratégie à utiliser.

*L'utilisation d'un cache externe évite au serveur DNS d'effectuer directement des recherches sur Internet ; il passe par le serveur de cache, il est donc moins exposé. En terme de sécurité, l'ouverture du port 53 sur le pare-feu n'est activée que du serveur DNS interne vers le serveur de cache externe. Enfin les utilisateurs passent par le serveur DNS interne pour obtenir une réponse à leurs requêtes.*

**28** Un de vos collègues aimerait limiter le trafic dû au transfert de zone entre le siège et un bureau distant. Il préconise l'utilisation d'un serveur DNS de cache, alors qu'un autre préconise l'utilisation d'une zone de stub, enfin un troisième propose la création d'un sous-domaine. Quel est votre avis sur les solutions proposées et quelle serait votre solution ?

*Le serveur DNS de cache pourrait être une solution si le nombre d'ordinateurs est faible. Il faudrait néanmoins garantir que les ordinateurs du site distant soient enregistrés dans le serveur DNS. Un inconvénient de cette solution est que s'il existe un problème réseau entre le site distant et le siège, les utilisateurs du site distant ne peuvent pas accéder à un ordinateur du site distant par son nom si l'information n'est pas dans le cache du serveur DNS. Néanmoins le trafic DNS reste limité si le TTL est élevé.*

*La zone de stub redirige toutes les requêtes vers les serveurs DNS distants, cette solution est moins bonne que le serveur de cache car le trafic DNS est plus important.*

*La création d'un sous-domaine ne diminue en rien le trafic DNS dû au transfert de zone, donc ce n'est pas une bonne solution. Néanmoins il peut être envisagé d'effectuer une délégation du sous-domaine ce qui diminue fortement le trafic DNS entre les deux sites.*

*En résumé, en fonction du nombre d'utilisateurs, le choix serait un serveur de cache pour quelques utilisateurs et une zone déléguée pour un nombre plus important.*

**29** Vous devez modifier l'adresse IP d'un serveur sensible, quelle serait la procédure à effectuer pour garantir qu'il n'y aura pas une interruption de service ?

*Il n'est demandé que de modifier l'adresse IP alors il faut utiliser la procédure suivante :*

- Ajouter la nouvelle adresse IP sur le serveur.
- Modifier l'adresse IP de l'enregistrement A sur le serveur DNS
- À la fin du délai TTL, supprimer l'ancienne adresse IP.

**30** Vous devez déplacer un serveur sensible d'un site A vers un site B, il est requis de limiter au maximum l'interruption du serveur, quelle procédure mettez-vous en œuvre ?

*Si vous ne pouvez disposer d'un second serveur, il y aura une interruption de service, il faut donc effectuer le déménagement durant une période creuse comme la nuit ou un week-end.*

*La procédure pourrait être la suivante :*

- Diminuer la valeur du TTL pour l'enregistrement à une valeur minimale.
- Prévoir le déménagement au plus tôt à la fin de l'ancien délai du TTL.

- Déménager le serveur.
- Contrôler que l'enregistrement est bien modifié dans le serveur DNS.
- Augmenter la valeur du TTL à son ancienne valeur.

**31** Des utilisateurs se plaignent qu'ils n'arrivent pas à se connecter au serveur applicatif. Comment pouvez-vous être sûr qu'il s'agit d'un problème de résolution de noms et pas d'un problème réseau ?

*Vous pouvez utiliser la commande **ping <adresse IP>** et si vous recevez une réponse alors le problème ne vient pas du réseau. Ensuite vous pouvez "pinger" le nom DNS, s'il n'y a pas de réponse il est probable que le nom ne pointe pas sur la bonne adresse IP.*

**32** L'entreprise de sécurité mandatée pour un audit indique qu'il existe un problème au niveau du transfert des zones DNS, quelle pourrait en être la cause ?

*Une des causes probables serait que le transfert de zone est autorisé vers n'importe quel serveur. Il faudrait sécuriser le transfert en permettant un transfert uniquement vers une liste de serveurs spécifiés ou modifier le type zone pour utiliser uniquement des zones intégrées Active Directory.*

**33** L'entreprise de sécurité mandatée pour un audit indique dans son rapport qu'il est possible de connaître la topologie de votre réseau, donnez une explication possible.

*Il est probable que le pare-feu laisse entrer des requêtes DNS vers le serveur DNS interne et que ce dernier réponde. Il peut même être envisagé que des transferts de zone soient possibles.*

**34** Vous devez implémenter une solution simple mais sécurisée pour permettre aux utilisateurs d'un groupe de travail d'avoir accès aussi bien aux ordinateurs de leur entreprise qu'à Internet, quelle serait une solution possible ?

*Comme on parle de groupe de travail, il y a au maximum 10 ordinateurs. On peut utiliser le serveur DNS du fournisseur d'accès Internet car les résolutions de noms locales s'effectueront via le protocole LLMNR. Une autre solution consiste à utiliser un serveur DNS de cache en interne et à lui créer une zone pour l'entreprise dans laquelle on ajouterait les ordinateurs du groupe de travail. Cette solution semble plus intéressante pour une évolution future.*

**35** Un de vos collègues ne trouve pas d'enregistrement dans le DNS concernant un serveur. Il propose de l'ajouter manuellement, que lui dites-vous ?

*S'il l'enregistre manuellement, il faudra le supprimer manuellement. Dans ce cas, il faut soit redémarrer le serveur, lui redemander une adresse IP ou mieux utiliser la commande **ipconfig /registerdns**.*

### **Questions de mise en œuvre**

**36** Dans votre entreprise, composée d'environ 3000 ordinateurs, il existe un bureau distant qui dispose d'un serveur et de 10 postes de travail. Généralement, les utilisateurs se plaignent de la lenteur lorsqu'ils accèdent à des ressources situées sur le réseau de l'entreprise alors que les performances sont bonnes sur leur réseau distant. Vous avez déterminé que la bande passante est presque saturée et avez observé des transferts de zone. Pouvez-vous améliorer un peu la bande passante en modifiant la configuration du serveur DNS, justifiez votre réponse ?

*En modifiant le serveur DNS pour qu'il soit uniquement un serveur DNS de cache. De cette manière, la réPLICATION DNS n'existe plus et seules les demandes spécifiques qui ne sont pas dans le cache utiliseront de la bande passante.*

## Résumé du chapitre

Dans ce chapitre, vous avez abordé la théorie concernant le service DNS, spécifiquement comment fonctionnent les espaces de noms et les zones. Les mécanismes utilisés pour la résolution de noms ont également été présentés.

Vous avez appris comment installer un serveur DNS, à le configurer et à le gérer. Enfin vous avez vu quels sont les outils de type ligne de commandes qu'il est possible d'utiliser pour configurer ou dépanner un serveur DNS.

## Travaux pratiques

Dans les travaux pratiques pour l'exercice 5, vous devrez effectuer les opérations suivantes :

- Installation d'un serveur DNS sur plusieurs serveurs.
- Configuration d'un serveur DNS de cache.
- Création de plusieurs zones y compris une zone stub.
- Mise en œuvre de la délégation de zone.
- Mise en œuvre de la réPLICATION.
- Mise en œuvre d'une zone GlobalNames.
- Utilisation des outils ligne de commande.
- Gestion des paramètres du DNS via une stratégie de groupe.
- Mise en œuvre de redirecteur conditionnel.

# Résolution de noms pour les ordinateurs clients

Dans cette section, vous allez examiner comment les ordinateurs clients ou serveurs résolvent les noms en adresse IP.

## 1. Nom d'hôte

Comme vous l'avez déjà entrevu, le nom d'hôte est un nom associé à une adresse TCP/IP. Il est défini dans les RFCs et est considéré comme étant un FQDN. Le nom d'hôte peut contenir les lettres allant de a à z (majuscule ou minuscule), les chiffres de 1 à 9 et le tiret. **www.eni.fr** est un nom d'hôte valide. La longueur maximale est de 255 caractères dont chaque partie doit être comprise en 1 et 63 caractères.

## 2. Nom NetBIOS

Le nom NetBIOS est également un nom mais dont la définition est différente car il est limité à seize caractères dont quinze composent le nom, le dernier servant à identifier un service. Il peut se composer de caractères alphanumériques, excepté l'espace et les caractères \ /: \*? <>; |. Les noms d'hôtes ont une hiérarchie alors que les noms NetBIOS sont tous au même niveau. Les noms NetBIOS ne se composent que d'une seule partie. **TOTO** est un nom NetBIOS valide.

Bien que Windows ait abandonné l'utilisation des noms NetBIOS en tant que noms principaux, ils sont encore largement utilisés par certaines applications. Voici quelques exemples de valeurs pour le seizième caractère. Pour disposer d'une liste complète, veuillez consulter la KB163409.

- 00 service Station de travail
- 03 Service Messenger
- 20 Service de fichiers
- 1B Maitre d'exploration de domaine
- 1C Contrôleur de domaine
- 1D Maître d'exploration

## 3. Fichier HOSTS

Le fichier HOSTS qui se trouve dans le répertoire **%systemroot%\system32\drivers\etc** est l'ancêtre des serveurs DNS et permet la résolution de noms d'hôtes en adresses IP.

Si vous devez l'utiliser, il suffit simplement de l'éditer avec un éditeur de texte comme le Bloc-notes. L'image suivante montre le fichier HOSTS avec les valeurs par défaut :

```
# Copyright (c) 1993-2006 Microsoft Corp.  
#  
# This is a sample HOSTS file used by Microsoft TCP/IP for windows.  
#  
# This file contains the mappings of IP addresses to host names. Each  
# entry should be kept on an individual line. The IP address should  
# be placed in the first column followed by the corresponding host name.  
# The IP address and the host name should be separated by at least one  
# space.  
#  
# Additionally, comments (such as these) may be inserted on individual  
# lines or following the machine name denoted by a '#' symbol.  
#  
# For example:  
#  
#      102.54.94.97    rhino.acme.com        # source server  
#      38.25.63.10    x.acme.com            # x client host  
  
127.0.0.1      localhost  
::1            localhost
```

Dès que vous avez modifié ce fichier, sauvez-le et à la prochaine requête, il sera de nouveau utilisé.

Sauf pour des cas bien précis, ce fichier n'est que rarement modifié.

## 4. Fichier LMHOSTS

Le fichier LMHOSTS est le pendant du fichier HOSTS mais pour les noms NetBIOS. Il se trouve également dans le répertoire %systemroot%\system32\drivers\etc, il est l'ancêtre des serveurs. Par défaut, ce fichier s'appelle **lmhosts.sam**. Pour l'utiliser il faut le renommer en **lmhosts**. Il est plus puissant que son homologue car il permet d'y intégrer non seulement des services mais également d'inclure un fichier provenant du réseau. Comme pour le fichier HOSTS, on le modifie à l'aide du Bloc-notes. La capture d'écran suivante montre une partie du fichier IMHOSTS.

```
# The #BEGIN_ and #END_ALTERNATE keywords allow multiple #INCLUDE  
# statements to be grouped together. Any single successful include  
# will cause the group to succeed.  
#  
# Finally, non-printing characters can be embedded in mappings by  
# first surrounding the NetBIOS name in quotations, then using the  
# \0xnn notation to specify a hex value for a non-printing character.  
#  
# The following example illustrates all of these extensions:  
#  
# 102.54.94.97    rhino      #PRE #DOM:networking  #net group's DC  
# 102.54.94.102   "appname"  \0x14                 #special app server  
# 102.54.94.123   popular     #PRE                  #source server  
# 102.54.94.117   localsrv   #PRE                  #needed for the include  
#  
# #BEGIN_ALTERNATE  
# #INCLUDE \\localsrv\public\lmhosts  
# #INCLUDE \\rhino\public\lmhosts  
# #END_ALTERNATE
```

Actuellement il est possible d'utiliser des zones DNS GlobalNames pour se passer de ce fichier.

## 5. Diffusion

L'utilisation du protocole NetBIOS permet d'utiliser des messages de diffusion comme une méthode possible pour la résolution du nom. Bien que cette méthode soit surtout efficace dans les petits réseaux pour des demandes locales, elle est encore principalement utilisée avec la résolution NetBIOS.

## 6. Recherche du réseau LLMNR (Link-Local Multicast Name Resolution)

LLMNR défini par la RFC 4795 permet la résolution de noms dans des environnements locaux où il n'existe pas de serveurs DNS, son principe est semblable à la diffusion mais les messages utilisés sont des messages de multidiffusion. Pour en bénéficier, il faut utiliser un ordinateur exécutant au moins Windows Vista ou Windows Server 2008.

Le principal avantage de LLMNR réside dans le fait qu'il supporte les protocoles IPv4 et IPv6 alors que le résolveur NetBT (NetBIOS) qui passe par la diffusion n'est pas supporté par le protocole IPv6.

Il faut également noter qu'il est possible d'activer ou de désactiver LLMNR via la stratégie de groupe suivante **Turn off Multicast Name Resolution (Configuration Ordinateur\Modèles d'administration\Réseau\Client DNS)**.

LLMNR utilise le port 5355/UDP et l'adresse de multicast IPv4 224.0.0.252 et comme adresse de destination multicast 33-33-00-01-00-03 et en IPv6 FF02::1:3 avec comme adresse de destination multicast 01-00-5E-00-00-FC.

 La **recherche du réseau** rend obsolète le **service d'exploration d'ordinateurs** qui était basé sur des messages de diffusion. Ce service est enfin désactivé par défaut.

## 7. Protocole PnrP (Peer Name Resolution Protocol)

**PnrP** est un protocole conçu par Microsoft adapté aux réseaux postes à postes qui permet de résoudre des noms d'ordinateurs ou d'autres types d'informations dans des réseaux locaux voire sur Internet en adresses IPv6. Il effectue des opérations qui dépassent largement ce que fait LLMNR et a été conçu pour :

- Fonctionner dans des environnements distribués sans serveurs évolutifs et devant mettre en œuvre un niveau de sécurité élevé.
- Publier sans effort des noms sans utiliser des outils tiers comme l'utilisation d'un serveur DNS.
- Permettre les mises à jour en temps réel à l'inverse du serveur DNS qui utilise un cache.
- Fournir des informations supplémentaires autres que le nom et l'adresse soit le port, le nom du service, etc.
- Publier les noms de manière sécurisée ou non en fonction des besoins.

Il est également conçu pour être intégré dans des applications.

Il est disponible pour Windows XP SP2, Windows Vista et Windows Server 2008. La version actuelle est la 2.1.

Les ordinateurs sont réunis dans des nuages, ce qui permet de retrouver les autres ordinateurs appartenant au nuage. Par défaut, un ordinateur appartient au nuage global et au nuage de lien local mais vous pouvez créer vos propres nuages.

Cette méthode est encore peu utilisée et répandue, elle est juste citée ici comme moyen existant pour effectuer la résolution de noms.

## 8. Résolution NetBIOS et type de nœud

La résolution NetBIOS utilise quatre éléments, à savoir :

Élément	Commande utile	Description
cache local	nbtstat -c nbtstat -R	Affiche le contenu du cache Purge et recharge le cache
diffusion		Peut être activée en fonction du type de nœud
fichier LMHOSTS	Bloc-notes	Édite le fichier

	nbtstat -R	Purge et recharge le cache Peut être désactivé dans les paramètres WINS de la carte réseau.
Serveur WINS		Peut être activé en fonction du type de nœud

Normalement, le cache local est toujours utilisé ainsi que le fichier LMHOSTS. Par contre, la diffusion et le serveur WINS peuvent être désactivés par la valeur **Type de nœud**. Le type de nœud indique comment ces éléments sont utilisés. On les gère grâce à une stratégie de groupe ou via le serveur DHCP. Les valeurs admissibles sont :

Type de nœud	Explication
B-node 0x01	Uniquement la diffusion.
P-node 0x02	Uniquement le serveur WINS.
M-Node 0x04	Mode mixte soit la diffusion puis le serveur WINS.
H-node	Mode hybride soit le serveur WINS puis la diffusion (conseillé).

Donc pour résoudre un nom, le résolveur recherche dans l'ordre suivant et s'arrête dès que le nom est résolu :

- Cache local ;
- En fonction du type de nœud (Wins et diffusion) ;
- Fichier LMHOSTS (s'il n'est pas désactivé).

## 9. Résolution TCP/IP

La résolution TCP/IP utilise depuis Windows Vista et Windows Server 2008 les cinq éléments dans l'ordre suivant, à savoir :

Élément	Commande utile	Description
Nom est local		La source et la destination sont locales, il n'y a pas d'accès à la carte réseau
cache local	ipconfig /displaydns ipconfig /flushdns	Affiche le contenu du cache Purge et recharge le cache
fichier HOSTS	Bloc-notes	Édite le fichier
Serveur DNS		S'il est défini, il est utilisé
LLMNR		S'il est activé

Ensuite, si la résolution de noms NetBIOS est activée et que le nom n'a pas été résolu, le résolveur TCP/IP passe la main au résolveur NetBIOS.

 Il faut également se souvenir que l'ordre de recherche des suffixes DNS peut être modifié (cf. le chapitre Configuration de base des services réseau). Il est dès lors normal que plusieurs requêtes DNS soient envoyées. Il faut donc être vigilant lorsque l'on modifie l'ordre des suffixes.

Pour enregistrer l'ordinateur local auprès du serveur DNS défini, il faut saisir la commande ipconfig /registerdns.

## 10. Quel résolveur choisir ?

Par défaut, c'est le résolveur TCP/IP qui est utilisé sauf si le nom est constitué d'un seul bloc sans point de moins de 16 caractères ou qu'une application typiquement NetBIOS est appelée, pour autant que le protocole NetBIOS n'a pas été désactivé.

En fait, le résolveur TCP/IP est utilisé dans la grande majorité des cas et il n'est pas rare que dans les entreprises les administrateurs tentent de désactiver le protocole NetBIOS. Il faut néanmoins rester prudent car certaines applications réseau inattendues demandent parfois d'utiliser une résolution de type NetBIOS que l'on peut simplifier au maximum en utilisant un fichier LMHOSTS et en utilisant un P-node comme type de nœud, mais en n'indiquant aucun serveur WINS.

## 11. Gestion des paramètres du client via une stratégie de groupe

Voici la liste des paramètres DNS qu'il est possible de gérer via une stratégie de groupes. Le fichier s'appelle **DnsClient.admx**.

 Pour obtenir une liste complète des stratégies, il faut télécharger le fichier **WindowsServer2008andWindowsVistaSP1GroupPolicySettings.xls**.

- Allow DNS Suffix Appending to Unqualified Multi-Label Name Queries
- Connection-Specific DNS Suffix
- DNS Servers
- DNS Suffix Search List
- Dynamic Update
- Primary DNS Suffix
- Primary DNS Suffix Devolution
- Register DNS records with connection-specific DNS suffix
- Register PTR Records
- Registration Refresh Interval
- Replace Addresses In Conflicts
- TTL Set in the A and PTR records
- Turn off Multicast Name Resolution
- Update Security Level
- Update Top Level Domain Zones

C'est une excellente méthode que de gérer les paramètres DNS via une stratégie de groupe.

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre les objectifs suivants décrits dans la section **Configuration des services fichiers et impression**.

### Configurer et surveiller les services d'impression

Cela inclut, sans s'y limiter :

- mettre en œuvre un partage d'imprimante ;
- publier les imprimantes dans Active Directory ;
- gérer les autorisations d'impression ;
- déployer une connexion d'imprimante ;
- installer des pilotes d'impression ;
- exporter et importer des files d'attente d'impression et des paramètres d'imprimante ;
- mettre en œuvre les groupes d'impression (Pool d'imprimante) ;
- gérer les priorités de l'impression.

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



## 3. Objectifs

Disposer d'une version papier de l'information électronique est un besoin des utilisateurs. En effet, dans les entreprises, le besoin en documents imprimés ne cesse d'augmenter et par conséquent les coûts liés à l'utilisation des imprimantes. Afin de rationaliser au mieux et de tenter d'endiguer ces coûts, il faut définir une stratégie d'impression dans l'entreprise qui peut consister à fournir une imprimante par utilisateur ou une imprimante par service. Leur gestion peut également devenir délicate car elle est souvent décentralisée et il faut se connecter sur chacun des serveurs d'impression. Enfin, les utilisateurs deviennent de plus en plus exigeants et ils aimeraient pouvoir imprimer sur les imprimantes de l'entreprise tout en étant à l'extérieur de l'entreprise.

Dans ce chapitre, vous allez apprendre le vocabulaire à utiliser pour gérer des imprimantes sous Windows Server 2008, puis comment installer et gérer une imprimante locale ou en réseau. Ensuite, vous examinerez comment installer et utiliser le rôle Serveur d'impression. Enfin, vous verrez comment gérer les impressions en utilisant l'impression Internet.

# Validation des acquis : questions/réponses

## 1. Questions

### Questions triviales

- 1 Indiquez une méthode pour ouvrir le **Gestionnaire des tâches**.
- 2 Est-il possible d'afficher une tâche 16 bits ?
- 3 Quelle différence existe-t-il entre **Terminer un processus** et **Terminer l'arborescence de processus** ?
- 4 Quelle est la priorité par défaut pour une application qui dispose du focus ?
- 5 Indiquez la commande pour afficher l'équivalent de l'onglet **Services** du **Gestionnaire des tâches**.
- 6 Quel serait l'outil qui vous permettrait de visualiser un goulet d'étranglement sans devoir configurer quoi que ce soit ?
- 7 Comment s'appelle l'outil qui établit des rapports sur la stabilité du système ?
- 8 Comment s'appelle l'outil qui permet de créer des rapports systèmes ?
- 9 Comment s'appelle le premier fichier qui s'exécute au démarrage de Windows Server 2008 ?
- 10 Quelle est la procédure pour démarrer au plus vite le service **Windows Defender** ?

### Questions de compréhension

- 11 Vous désirez visualiser d'un seul coup d'œil les informations concernant le processeur, le disque et la mémoire, quel outil vous semble le plus approprié et pourquoi ?
- 12 Votre collègue doit rédiger un rapport sur les performances d'un serveur. Il utilise l'analyseur de performance et le configure comme désiré. Ensuite il effectue une capture de l'écran puis à l'aide d'un logiciel de dessin ne sélectionne que la partie qui l'intéresse pour l'inclure dans son rapport. D'après-vous, serait-il possible de faire autrement et comment procéderiez-vous ?
- 13 Votre collègue aimerait modifier plusieurs paramètres au démarrage de Windows Server 2008 et il ne trouve pas le fichier boot.ini. Comment pouvez-vous l'aider ?
- 14 Votre collègue aimerait modifier des éléments au démarrage de Windows Server 2008, il ne sait pas comment procéder. Comment pouvez-vous l'aider ?
- 15 Quelle pourrait être la cause d'un problème si celui-ci survient après l'enregistrement d'un événement particulier propre à la carte réseau ?
- 16 Durant une discussion, votre collègue soutient mordicus que tous les systèmes de gestion utilisent uniquement le protocole SNMP pour interroger les systèmes. Quel est votre point de vue ?
- 17 Vous avez configuré un serveur SQL pour utiliser l'authentification mixte afin de permettre à des utilisateurs externes à l'entreprise de pouvoir utiliser une application qui en a besoin. Vous utilisez MBSA pour contrôler si vos serveurs sont sécurisés et pour le serveur SQL, concernant l'authentification, vous recevez un score qui indique que le test a échoué mais n'est pas critique. Qu'en pensez-vous ?

### Questions de mise en œuvre

- 18 Un de vos collègues met à jour des pilotes pour un serveur Windows Server 2008 qui demande un redémarrage. Une fois que celui-ci a redémarré, un écran bleu survient ainsi qu'à chaque redémarrage ultérieur. Votre collègue sollicite votre aide afin de résoudre ce problème, comment pouvez-vous l'aider ?
- 19 Votre entreprise dispose de trois serveurs Windows Server 2008 et sept postes de travail Vista. Vous désirez traiter les événements sur un seul ordinateur, comment pouvez-vous procéder ?
- 20 Un événement en erreur n'est pas très explicite, indiquez une solution pour obtenir des informations supplémentaires ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /20

Pour ce chapitre, votre score minimum doit être de 15 sur 20.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

### 3. Réponses

#### Questions triviales

1 Indiquez une méthode pour ouvrir le **Gestionnaire des tâches**.

*Vous pouvez citer :*

- [Ctrl] [Shift] [Echap]
- [Ctrl] [Alt] [Suppr] puis sélectionner **Gestionnaire des tâches**.
- Cliquer avec le bouton droit de la souris dans la barre des tâches du Bureau puis cliquer sur **Gestionnaire des tâches** dans le menu contextuel.
- Cliquer sur **Démarrer**, saisir **taskmgr** dans la zone **Rechercher** et appuyer sur [Entrée].

2 Est-il possible d'afficher une tâche 16 bits ?

*Oui, c'est une des actions possible du menu contextuel de l'onglet Processus du Gestionnaire des tâches.*

3 Quelle différence existe-t-il entre **Terminer un processus** et **Terminer l'arborescence de processus** ?

*Terminer une arborescence de processus ferme également les processus dépendants du processus sélectionné.*

4 Quelle est la priorité par défaut pour une application qui dispose du focus ?

*La priorité est Normale + 2.*

5 Indiquez la commande pour afficher l'équivalent de l'onglet **Services** du **Gestionnaire des tâches**.

*Vous pouvez citer :*

- tasklist /svc
- sc query
- sc query ex
- net start

*Bien entendu la première commande est celle dont le résultat se rapproche le plus de l'onglet Services.*

6 Quel serait l'outil qui vous permettrait de visualiser un goulet d'étranglement sans devoir configurer quoi que ce soit ?

*Le **moniteur de ressources** correspond mieux que l'**analyseur de performances**.*

7 Comment s'appelle l'outil qui établit des rapports sur la stabilité du système ?

*Le moniteur de fiabilité.*

8 Comment s'appelle l'outil qui permet de créer des rapports systèmes ?

*La section rapport de **Fiabilité et performances** ou, en fonction du nom, **Ensemble de collecteurs de données et rapports**.*

9 Comment s'appelle le premier fichier qui s'exécute au démarrage de Windows Server 2008 ?

*Ce fichier s'appelle **bootmgr.exe**.*

10 Quelle est la procédure pour démarrer au plus vite le service **Windows Defender** ?

*Il faudrait utiliser l'une des commandes suivantes qui est bien plus rapide que de passer par l'interface graphique.*

- net start "Windows Defender"
- sc start "windows Defender"

## **Questions de compréhension**

- 11** Vous désirez visualiser d'un seul coup d'œil les informations concernant le processeur, le disque et la mémoire, quel outil vous semble le plus approprié et pourquoi ?  
*Le moniteur de ressources correspond mieux que l'analyseur de performances car aucune configuration n'est requise.*
- 12** Votre collègue doit rédiger un rapport sur les performances d'un serveur. Il utilise l'analyseur de performance et le configure comme désiré. Ensuite il effectue une capture de l'écran puis à l'aide d'un logiciel de dessin ne sélectionne que la partie qui l'intéresse pour l'inclure dans son rapport. D'après-vous, serait-il possible de faire autrement et comment procéderiez-vous ?  
*Oui, il faudrait enregistrer le contenu de l'analyseur de performances en tant qu'image GIF. Pour cela, il suffit d'utiliser la commande **Enregistrer l'image sous** du menu contextuel de l'analyseur de performances.*
- 13** Votre collègue aimerait modifier plusieurs paramètres au démarrage de Windows Server 2008 et il ne trouve pas le fichier boot.ini. Comment pouvez-vous l'aider ?  
*Le fichier boot.ini est remplacé par BCD. Il faut passer par un utilitaire comme bcdedit de Microsoft ou VistaBootPro voire EaysBcd.*
- 14** Votre collègue aimerait modifier des éléments au démarrage de Windows Server 2008, il ne sait pas comment procéder. Comment pouvez-vous l'aider ?  
*Il faudrait utiliser l'outil **Configuration du système** qui permet de modifier des paramètres de démarrage ou de revenir à l'état initial.*
- 15** Quelle pourrait être la cause d'un problème si celui-ci survient après l'enregistrement d'un événement particulier propre à la carte réseau ?  
*Vous pourriez utiliser le planificateur de tâches afin de faire démarrer une application lorsque l'événement survient. Ici, le moniteur réseau pourrait être l'outil idéal.*
- 16** Durant une discussion, votre collègue soutient mordicus que tous les systèmes de gestion utilisent uniquement le protocole SNMP pour interroger les systèmes. Quel est votre point de vue ?  
*Que c'était vrai il y a 20 ans mais que maintenant les APIS WMI sont plus utilisées par les logiciels modernes. Néanmoins SNMP peut encore rendre quelques services.*
- 17** Vous avez configuré un serveur SQL pour utiliser l'authentification mixte afin de permettre à des utilisateurs externes à l'entreprise de pouvoir utiliser une application qui en a besoin. Vous utilisez MBSA pour contrôler si vos serveurs sont sécurisés et pour le serveur SQL, concernant l'authentification, vous recevez un score qui indique que le test a échoué mais n'est pas critique. Qu'en pensez-vous ?  
*Les recommandations effectuées par MBSA ne prennent pas en compte l'environnement. Il est donc nécessaire de relativiser l'importance de certaines recommandations comme celle citée. Pour améliorer la sécurité, il est peut-être nécessaire de modifier l'application ce qui n'est pas une opération aisée.*

## **Questions de mise en œuvre**

- 18** Un de vos collègues met à jour des pilotes pour un serveur Windows Server 2008 qui demande un redémarrage. Une fois que celui-ci a redémarré, un écran bleu survient ainsi qu'à chaque redémarrage ultérieur. Votre collègue sollicite votre aide afin de résoudre ce problème, comment pouvez-vous l'aider ?  
*C'est un cas typique où il est nécessaire de redémarrer avec la dernière bonne configuration connue.*
- 19** Votre entreprise dispose de trois serveurs Windows Server 2008 et sept postes de travail Vista. Vous désirez traiter les événements sur un seul ordinateur, comment pouvez-vous procéder ?  
*Comme tous les ordinateurs utilisent le nouveau système d'événements, il est possible de rediriger ces événements sur un seul ordinateur et de les traiter à partir de ce dernier.*  
*Une autre solution consiste à utiliser une application de type **System Center Operation Manager**.*
- 20** Un événement en erreur n'est pas très explicite, indiquez une solution pour obtenir des informations supplémentaires ?  
*Vous pouvez consulter le site de Microsoft, voire le site [www.eventid.net](http://www.eventid.net)*

## Résumé du chapitre

Dans ce chapitre vous avez appris quels sont les éléments matériels importants qui peuvent causer des goulets d'étranglement et qu'il faut analyser en priorité lorsque vous avez des problèmes de performances.

Pour y arriver, vous avez appris à utiliser les outils que sont le gestionnaire des tâches et le moniteur de fiabilité et de performances. Vous avez appris à utiliser l'observateur d'événements y compris les nouvelles fonctionnalités comme la redirection des événements et le déclenchement du planificateur de tâche sur un événement particulier. Vous avez examiné l'utilisation de l'analyseur de performances pour détecter des goulets d'étranglement, voire améliorer les performances globales du serveur. Le protocole SNMP a également été introduit ainsi que la notion d'agent. Le moniteur réseau, qui permet l'analyse des trames, a été présenté afin de pouvoir l'utiliser. Enfin les moyens pour mettre à jour Windows, voire d'autres produits, et pour être sécurisé ont été présentés avec WSUS et MBSA. Enfin, des outils supplémentaires mais très utiles vous ont été présentés comme le fonctionnement du processus de démarrage de Windows Server 2008, l'utilisation de l'assistance à distance, l'utilisation de la console des services, l'utilisation de la configuration système, la mise en œuvre de la dernière bonne configuration connue. Vous avez vu à quoi servent les différentes options de démarrage de Windows, appris à utiliser l'outil diagnostics de la mémoire, le registre, l'observateur d'événements, le planificateur de tâches, à connaître l'utilité des paramètres du panneau de configuration et à utiliser pleinement les outils de type ligne de commande.

## Travaux pratiques

Dans les travaux pratiques dans différents exercices, vous devrez effectuer les opérations suivantes :

- Gestion des événements de l'observateur d'événements (Exercice 13).
- Redirection des événements (Exercice 13).
- Exécution d'une tâche planifiée déclenchée par un événement (Exercice 13).
- Gestion des journaux de l'observateur d'événements (Exercice 13).
- Installation et mise en œuvre de SNMP (Exercice 13).
- Analyse des trames à l'aide du moniteur réseau (Plusieurs exercices).
- Installation d'un serveur WSUS (Exercice 14).

# Outils supplémentaires de type ligne de commandes

## 1. runas



La commande **runas** permet de lancer une application sous une autre identité.

```
c:\>runas

Syntaxe de RUNAS :

RUNAS [ [/noprofile | /profile] [/env] [/savecred | /netonly] ]
      /user:<Nom_utilisateur> programme

RUNAS [ [/noprofile | /profile] [/env] [/savecred] ]
      /smartcard [/user:<Nom_utilisateur>] programme

RUNAS /trustlevel:<niveau_approbation> programme

/noprofile      spécifie que le profil de l'utilisateur ne devrait pas
                être chargé. Cela permet le chargement plus rapide
                de l'application, mais peut provoquer le dysfonctionnement
                de certaines applications.
/profile        spécifie que le profil de l'utilisateur devrait être
                chargé. Il s'agit de l'option par défaut.
/env            pour utiliser l'environnement en cours à la place de
                celui de l'utilisateur.
/netonly        à utiliser si les informations d'identification spécifiées
                sont pour l'accès à distance uniquement.

.
/savecred       pour utiliser les informations d'identification
                précédemment sauvegardées par l'utilisateur.
                Cette option n'est pas disponible dans Windows Vista
                Edition Familiale ou Windows Vista Starter Edition
                et sera ignorée.
/smartcard      utiliser si les informations d'identification sont
                fournies à partir d'une carte à puce.
/user           <NomUtilisateur> sous la forme UTILISATEUR@DOMAINE ou
                DOMAINE\UTILISATEUR
/showtrustlevels affiche les niveaux d'approbation qui peuvent être
                 utilisés comme arguments au /trustlevel.
/trustlevel     <Niveau> devrait être un des niveaux énumérés
                 dans /showtrustlevels.
program        ligne de commande pour EXE. Veuillez voir les exemples ci-dessous

Exemples :
> runas /noprofile /user:mymachine\administrator cmd
> runas /profile /env /user:mydomain\admin "mmc %windir%\system32\dsa.msc"
> runas /env /user:utilisateur@domaine.microsoft.com "notepad \"fichier.txt\""
```

- Pour démarrer l'invite de commandes en tant qu'administrateur, saisissez :

```
runas /user:myDomain\administrateur cmd
```

## 2. start

La commande **start** ouvre une fenêtre et exécute le programme ou la commande spécifié.

```
c:\>start /?
```

Ouvre une fenêtre et exécute le programme ou la commande spécifiée.

```
START ["titre"] [/D chemin] [/I] [/MIN] [/MAX] [/SEPARATE | /SHARED]
  [/LOW | /NORMAL | /HIGH | /REALTIME | /ABOVENORMAL | /BELOWNORMAL]
  [/AFFINITY <affinité_hexa>] [/WAIT] [/B] [commande/programme]
  [paramètres]
```

"titre" Titre de la fenêtre.  
chemin Répertoire de départ.  
B Lance l'application sans créer de fenêtre. L'arrêt par ^C n'est pas pris en charge dans l'application.  
Si l'application n'autorise pas la détection de ^C, ^Pause est la seule façon d'arrêter l'application.  
I Le nouvel environnement sera l'environnement original passé à cmd.exe, et non pas l'environnement actuel.  
MIN Démarrer avec la fenêtre réduite.  
MAX Démarrer avec la fenêtre agrandie.  
SEPARATE Démarrer les programmes Windows 16 bits dans un espace mémoire distinct.  
SHARED Démarrer les programmes Windows 16 bits dans un espace mémoire partagé.  
LOW Démarrer l'application dans la classe de priorité IDLE.  
NORMAL Démarrer l'application dans la classe de priorité NORMAL.  
HIGH Démarrer l'application dans la classe de priorité HIGH.  
REALTIME Démarrer l'application dans la classe de priorité REALTIME.  
ABOVENORMAL Démarrer l'application dans la classe de priorité ABOVENORMAL.  
BELOWNORMAL Démarrer l'application dans la classe de priorité BELOWNORMAL.  
AFFINITY La nouvelle application aura le masque d'affinité de processeur spécifié, exprimé en tant que valeur hexadécimale.  
WAIT Lancer l'application et attendre qu'elle mette fin à la commande ou au programme.  
S'il s'agit d'une commande interne ou d'un fichier batch, le processeur de commandes est exécuté avec le commutateur /K pour cmd.exe.  
Ceci signifie que la fenêtre reste ouverte après exécution de la commande.

Paramètres Spécifie les paramètres à passer à la commande ou au programme.

- Pour démarrer une autre invite de commandes, saisissez : start.
- Pour démarrer le Bloc-notes avec une priorité haute dans une fenêtre réduite, saisissez : start /min /high notepad.

### 3. tasklist

Cet utilitaire affiche la liste des processus fonctionnant sur le serveur local ou sur un serveur distant.

```
C:\>tasklist /?

TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]
  [/M [module] | /SVC | /V] [/FI filtre] [/FO format] [/NH]

Description :
  Cet outil affiche une liste des processus actuellement en cours sur
  un ordinateur local ou un ordinateur distant.

Liste de paramètres :
  /S    système          Spécifie le système distant auquel se connecter.
```

```

/U  [domaine\]utili. Spécifie le contexte utilisateur sous lequel
     la commande doit exécuter.

/P  [mot_passe]      Spécifie le mot de passe pour le contexte
                      utilisateur donné. Il est demandé s'il est omis.

/M  [module]         Liste toutes les tâches utilisant le nom de
                      fichier exe ou dll donné. Si le nom de module
                      n'est pas spécifié, tous les modules chargés
                      sont affichés.

/SVC                  Affiche les services hébergés dans chaque processus.

/V                   Affiche les informations de tâches détaillées.

/FI  filtre          Affiche un ensemble de tâches qui correspond
                      au critère spécifié par le filtre.

/FO  format           Spécifie le format de la sortie.
                      Valeurs valides : "TABLE", "LIST", "CSV".

/NH                  Spécifie que les en-têtes de colonnes ne
                      être affichée sur la sortie.
                      Valide uniquement pour les formats
                      "TABLE" et "CSV".

/?                  Affiche ce message d'aide.

```

**Filtres :**

Nom du filtre	Opérateurs valides	Valeurs valides
STATUS	eq, ne	RUNNING   NOT RESPONDING   UNKNOWN
IMAGENAME	eq, ne	Nom d'image
PID	eq, ne, gt, lt, ge, le	Valeur PID
SESSION	eq, ne, gt, lt, ge, le	Numéro de session
SESSIONNAME	eq, ne	Nom de session
CPUTIME	eq, ne, gt, lt, ge, le	Heure valide au format hh:mm:ss. hh - heures mm - minutes, ss - secondes
MEMUSAGE	eq, ne, gt, lt, ge, le	Mémoire utilisée, en Ko
USERNAME	eq, ne	Nom d'utilisateur [domaine\]utilisateur
SERVICES	eq, ne	Nom de service
WINDOWTITLE	eq, ne	Titre de la fenêtre
MODULES	eq, ne	Nom de DLL

Remarque : les filtres "WINDOWTITLE" et "STATUS" ne sont pas pris en charge lors de recherches sur un ordinateur distant.

- Pour afficher la liste des services de chaque processus et l'enregistrer dans un fichier au format CSV, saisissez : tasklist /svc /FO csv > MonFichier.csv.
- Pour afficher la liste des services qui ont utilisé plus d'une minute de temps processeur, saisissez : tasklist /FI "cputime gt 00:01:00".

## 4. tskill

Cet utilitaire permet d'arrêter un processus tournant soit sur l'ordinateur local, soit sur l'ordinateur distant.

```

C:\>tskill /?
Arrête un processus.

TSKILL IDprocessus | NomProcessus [/SERVER:NomServeur] [/ID:IDsession | /A] [/V]

```

ID_processus	ID du processus devant être arrêté.
NomProcessus	Nom du processus devant être arrêté.
/SERVER:NomServeur	Serveur contenant l'ID de processus <ID actuel par défaut>. /ID ou /A doit être spécifié lorsqu'un nom de processus et /SERVER sont utilisés.
/ID:ID_session	Arrêt du processus exécuté au cours de la session spécifiée.
/A	Arrêt du processus exécuté au cours de TOUTES les sessions.
/V	Affichage d'informations sur les actions exécutées.

C:\>

- Pour arrêter le processus 1060, saisissez : tskill 1060.

 L'utilisation de cette commande sur certains processus comme **crss** peut provoquer des écrans bleus.

## 5. taskkill

L'utilitaire **taskkill** permet d'arrêter un processus. La syntaxe est similaire à celle de l'utilitaire **tasklist**.

- Pour arrêter le Bloc-notes, saisissez : taskkill /im notepad.exe.

 Si plusieurs instances du Bloc-notes sont lancées, alors toutes les instances sont arrêtées.

- Pour arrêter plusieurs processus, saisissez : taskkill /PID 1060 /PID 1280.

## 6. Liste non exhaustive des outils de type ligne de commande

**ASSOC** : affiche ou modifie les applications associées aux extensions de fichiers.

**ATTRIB** : affiche ou modifie les attributs d'un fichier.

**BREAK** : active ou désactive le contrôle étendu de CTRL+C.

**BCDEDIT** : définit les propriétés dans la base de données de démarrage pour le contrôle du chargement d'amorçage.

**CACLS** : affiche ou modifie les listes de contrôles d'accès aux fichiers.

**CALL** : appelle un fichier de commandes à partir d'un autre fichier de commandes.

**CD** : modifie le répertoire ou affiche le répertoire actif.

**CHCP** : modifie ou affiche le numéro de la page de code active.

**CHDIR** : modifie le répertoire ou affiche le nom du répertoire actif.

**CHKDSK** : vérifie un disque et affiche un rapport d'état.

**CHKNTFS** : affiche ou modifie la vérification du disque au démarrage.

**CLS** : efface l'écran.

**CMD** : exécute une nouvelle instance de l'interpréteur de commandes de Windows.

**COLOR** : modifie les couleurs de premier plan et de l'arrière-plan de la console.

**COMP** : compare les contenus de deux fichiers ou groupes de fichiers.

**COMPACT** : modifie ou affiche la compression des fichiers sur une partition NTFS.

**CONVERT** : convertit des volumes FAT en volumes NTFS. Vous ne pouvez pas convertir le lecteur en cours d'utilisation.

**COPY** : copie un ou plusieurs fichiers.

**DATE** : affiche ou définit la date.

**DEL** : supprime un ou plusieurs fichiers.

**DIR** : affiche la liste des fichiers et des sous-répertoires d'un répertoire.

**DISKCOMP** : compare les contenus de deux disquettes.

**DISKCOPY** : copie le contenu d'une disquette sur une autre.

**DISKPART** : affiche ou configure les propriétés d'une partition de disque.

**DOSKEY** : modifie les lignes de commande, rappelle des commandes Windows et crée des macros.

**DRIVERQUERY** : affiche l'état et les propriétés du pilote de périphérique en cours d'utilisation.

**ECHO** : affiche des messages ou active/désactive l'affichage des commandes.

**ENDLOCAL** : stoppe la localisation des modifications d'environnement dans un fichier de commandes.

**ERASE** : supprime un ou plusieurs fichiers.

**EXIT** : quitte l'interpréteur de commandes (CMD.EXE).

**FC** : compare deux fichiers ou groupes de fichiers et affiche les différences.

**FIND** : recherche une chaîne de caractères dans un ou plusieurs fichiers.

**FINDSTR** : cherche des chaînes dans les fichiers.

**FOR** : exécute une commande sur chaque fichier d'un ensemble de fichiers.

**FORMAT** : formate un disque devant être utilisé avec Windows.

**FSUTIL** : affiche ou configure les propriétés du système de fichiers.

**FTYPE** : affiche ou modifie les types de fichiers utilisés dans les associations d'extensions.

**GOTO** : indique pour l'exécution d'un fichier de commandes le déplacement vers une ligne identifiée par une étiquette.

**GPRESULT** : affiche les informations de stratégie de groupe pour un ordinateur ou un utilisateur.

**GRAFTABL** : permet à Windows d'afficher un jeu de caractères en mode graphique.

**HELP** : affiche des informations sur les commandes de Windows.

**ICACLS** : pour afficher, modifier, sauvegarder ou restaurer les listes de contrôle d'accès pour les fichiers et les répertoires.

**IF** : effectue un traitement conditionnel dans un fichier de commandes.

**LABEL** : crée, modifie ou supprime le nom de volume d'un disque.

**MD** : crée un répertoire.

**MKDIR** : crée un répertoire.

**MKLINK** : créer des liens symboliques et des liens réels.

**MODE** : configure un périphérique du système.

**MORE** : affiche la sortie écran par écran.

**MOVE** : déplace un ou plusieurs fichiers d'un répertoire à un autre.

**OPENFILES** : affiche les fichiers partagés ouverts à distance par les utilisateurs.

**PATH** : affiche ou définit le chemin de recherche des fichiers exécutables.

**PAUSE** : interrompt l'exécution d'un fichier de commandes et affiche un message.

**POPD** : restaure la valeur précédente du répertoire actif enregistrée par PUSHD.

**PRINT** : imprime un fichier texte.

**PROMPT** : modifie l'invite de commande de Windows.

**PUSHD** : enregistre le répertoire actif puis le modifie.

**RD** : supprime un répertoire.

**RECOVER** : récupère l'information lisible d'un disque défectueux.

**REM** : insère un commentaire dans un fichier de commandes ou CONFIG.SYS.

**REN** ou **RENAME** : renomme un ou plusieurs fichiers.

**REPLACE** : remplace des fichiers.

**RMDIR** : supprime un répertoire.

**ROBOCOPY** : utilitaire avancé pour copier les fichiers et les arborescences de répertoires.

**SET** : affiche, définit ou supprime des variables d'environnement Windows.

**SETLOCAL** : commence la localisation des modifications d'environnement dans un fichier de commandes.

**SC** : affiche ou configure les services (processus en arrière-plan).

**SCHTASKS** : planifie les commandes et les programmes à exécuter sur l'ordinateur.

**SHIFT** : modifie la position des paramètres remplaçables dans un fichier de commandes.

**SHUTDOWN** : permet un arrêt local ou distant correct de l'ordinateur.

**SORT** : trie les entrées.

**START** : ouvre une fenêtre séparée pour l'exécution d'un programme ou d'une commande spécifique.

**SUBST** : associe un chemin d'accès à une lettre de lecteur.

**SYSTEMINFO** : affiche les propriétés et la configuration spécifiques de l'ordinateur.

**TASKLIST** : affiche toutes les tâches en cours d'exécution, y compris les services.

**TASKKILL** : termine ou interrompt un processus ou une application en cours d'exécution.

**TIME** : affiche ou définit l'heure du système.

**TITLE** : définit le titre de la fenêtre pour une session CMD.EXE.

**TREE** : affiche le graphisme de la structure de répertoire d'un lecteur ou d'un chemin d'accès.

**TYPE** : affiche le contenu d'un fichier texte.

**VER** : affiche la version de Windows.

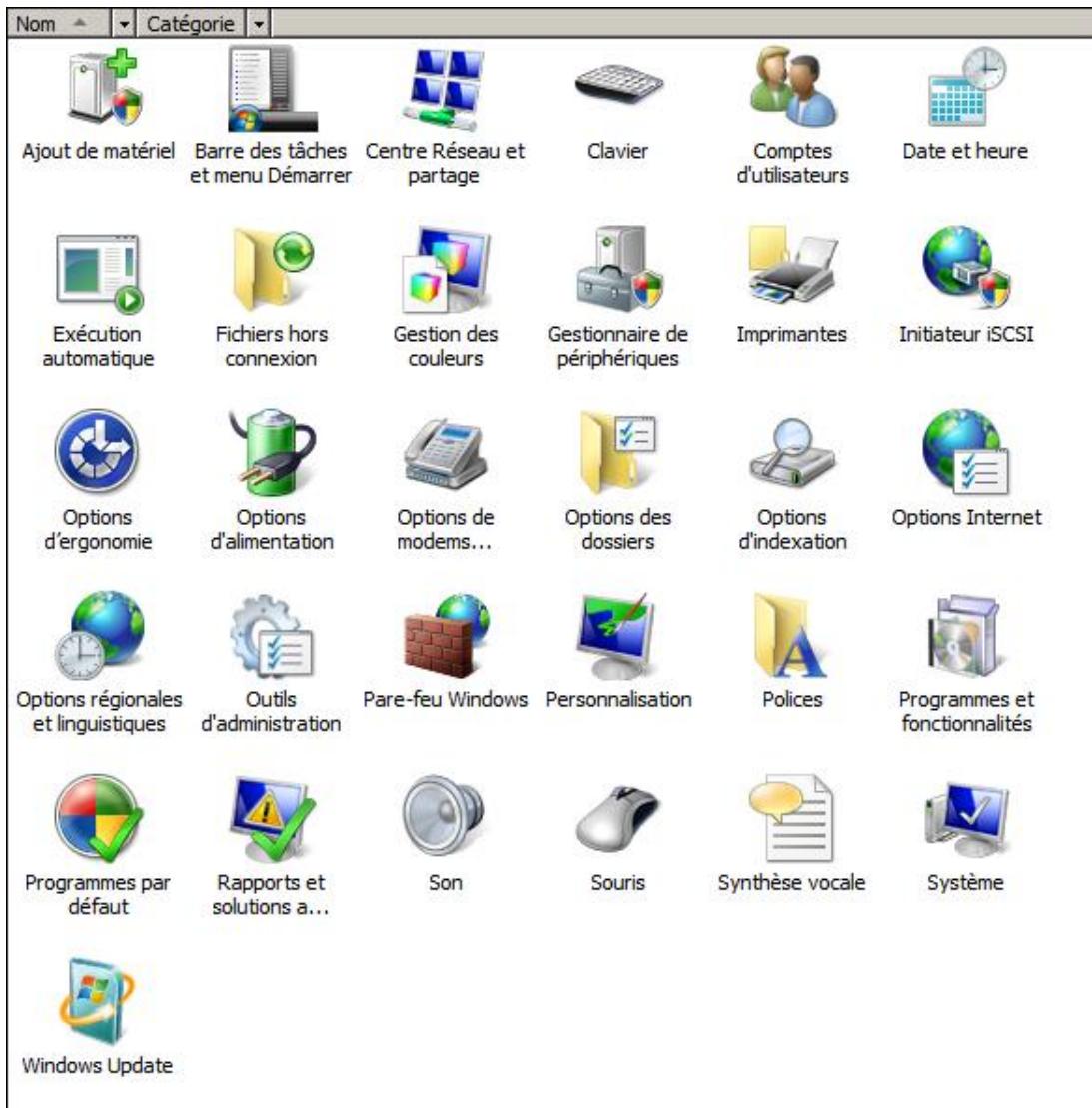
**VERIFY** : demande à Windows de vérifier si les fichiers sont correctement écrits sur le disque.

**VOL** : affiche le nom et le numéro de série d'un volume de disque.

**XCOPY** : copie les fichiers et les arborescences de répertoires.

**WMIC** : affiche les informations WMI dans l'interface de commande interactive.

# Le Panneau de configuration



Dans le Panneau de configuration, vous pouvez configurer un nombre important de paramètres pour la configuration de Windows. Certaines applications créent leur propre application de configuration et la placent également dans le Panneau de configuration.

Sur un Server Core, il n'existe pas d'équivalent au panneau de configuration.

- Il faut utiliser la commande **control** suivie du nom de l'applet pour le démarrer dans une invite de commande comme par exemple **control ncpa.cpl**.

La liste suivante donne une description des différentes catégories de paramètres du Panneau de configuration.

**Ajout de matériel** : permet d'ajouter un matériel. Ce paramètre est important.

**Barre des tâches et menu Démarrer** : permet de gérer la barre des tâches et le menu **Démarrer**. Ce paramètre est moyennement important.

**Centre Réseau et partage** : permet de gérer l'accès aux réseaux. Ce paramètre est important.

**Clavier** : permet de gérer le clavier. Ce paramètre est peu important.

**Comptes d'utilisateurs** : permet de gérer les utilisateurs locaux ainsi que l'activation du contrôle des comptes

d'utilisateurs (UAC). Les utilisateurs locaux doivent être une exception dans un domaine. Ce paramètre est moyennement important. L'UAC doit être géré via les stratégies de groupe.

**Date et heure** : permet de gérer la date, l'heure et le fuseau horaire. La date et l'heure devraient se synchroniser par rapport à un serveur de temps. Ce paramètre est important.

**Exécution automatique** : permet de gérer le démarrage automatique de logiciels provenant de médias amovibles. Ce paramètre est peu important.

**Fichiers hors connexion** : permet de gérer la partie cliente des fichiers hors connexion. Ce paramètre est peu important.

**Gestion des couleurs** : permet de créer des profils de couleur. Ce paramètre est peu important.

**Gestionnaire de périphériques** : permet de gérer des périphériques et les pilotes de ces derniers. Ce paramètre est important.

**Imprimantes** : permet de gérer localement des imprimantes. Ce paramètre est important.

**Initiateur iSCSI** : permet de configurer l'initiateur iSCSI. Ce paramètre est important.

**Options d'ergonomie** : permet d'activer des paramètres qui peuvent aider certains utilisateurs. Ce paramètre est important.

**Options d'alimentation** : permet de définir un mode de gestion de l'alimentation. Ce paramètre est moyennement important.

**Options de modems** : permet de définir les options des modems. Ce paramètre est moyennement important.

**Options des dossiers** : permet de définir les options de dossiers et l'affichage. Ce paramètre est moyennement important.

**Options d'indexation** : permet de définir les emplacements à indexer. Excepté pour un serveur de fichiers, ce paramètre devrait être désactivé. Ce paramètre est moyennement important.

**Options Internet** : permet de définir les options Internet. Ce paramètre est important mais devrait être géré via une stratégie de groupes.

**Options régionales et linguistiques** : permet de définir le format de l'affichage des nombres, le type de clavier utilisé, etc. Ce paramètre est important.

**Outils d'administration** : affiche la liste des outils d'administration (plus longue à ouvrir que de passer via le menu Démarrer). Ce paramètre est important.

**Pare-feu Windows** : permet de gérer le pare-feu standard de Windows. À NE PAS UTILISER, lui préférer le pare-feu avec fonctions avancées de sécurité. Ce paramètre est important.

**Personnalisation** : permet de gérer l'apparence et les sons. Ce paramètre est peu important, excepté pour gérer l'affichage écran de l'ordinateur.

**Police** : permet de gérer les polices de l'ordinateur. Ce paramètre est peu important.

**Programmes et fonctionnalités** : permet d'installer, de modifier et de désinstaller un programme. Ce paramètre est moyennement important.

**Programmes par défaut** : permet de définir des programmes par défaut basés sur des extensions, des protocoles, etc. Ce paramètre est peu important.

**Rapports et solutions aux problèmes** : permet de définir comment utiliser l'envoi de rapports pour solutionner un problème. Ce paramètre est important mais devrait être géré via une stratégie de groupes.

**Son** : permet de gérer les sons de l'ordinateur. Ce paramètre est peu important.

**Souris** : permet de configurer les paramètres de la souris de l'ordinateur. Ce paramètre est peu important.

**Synthèse vocale** : permet à l'ordinateur de lire du texte en utilisant une voix. Ce paramètre est peu important.

**Système** : permet de consulter des informations sur le système d'exploitation, changer la clé du produit et ouvrir le Gestionnaire de périphériques, les paramètres d'utilisation à distance, les paramètres avancés du système et Windows Update. Ce paramètre est important mais devrait être géré via une stratégie de groupes.

**Windows Update** : permet de configurer comment recevoir les mises à jour Windows, voire d'autres produits. Ce paramètre est important mais devrait être géré via une stratégie de groupes.

# Planificateur de tâches



Le Planificateur de tâches permet de différer l'exécution de programmes selon un calendrier.

## 1. Démarrer le Planificateur de tâches

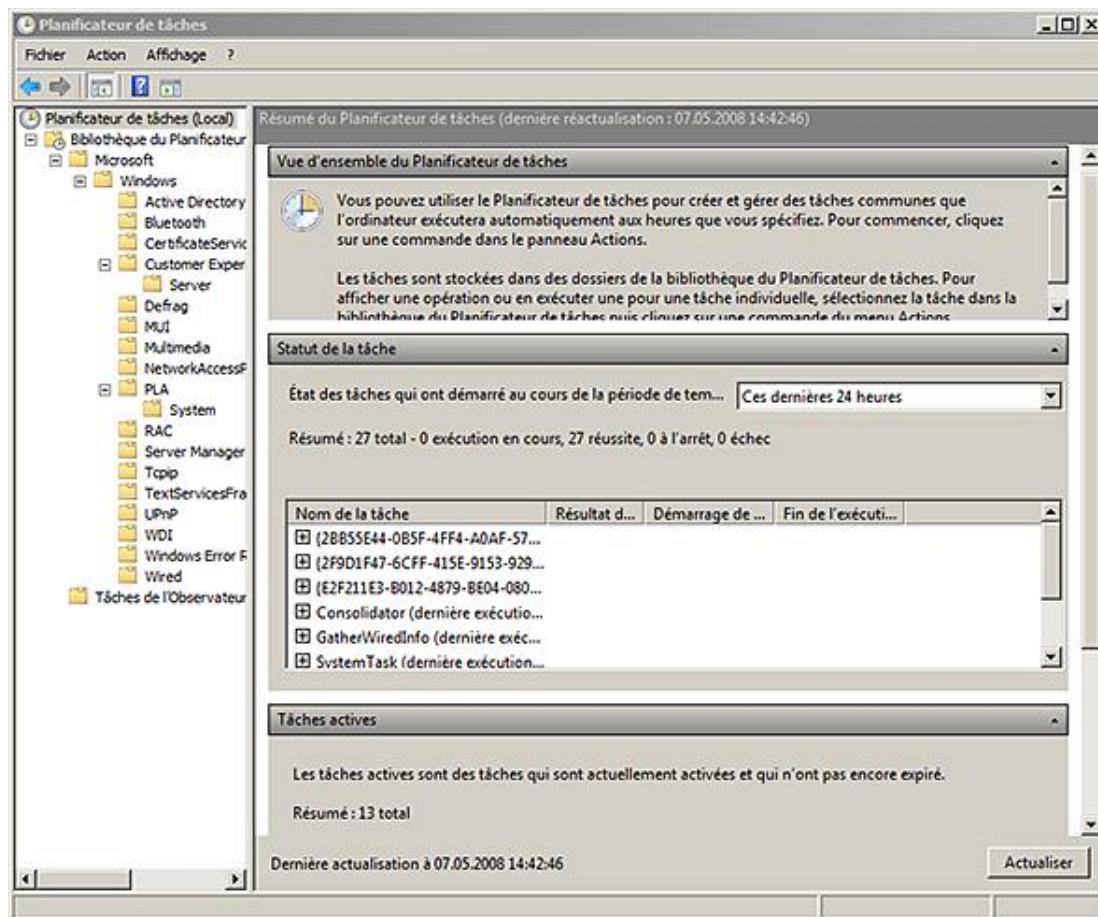
- Connectez-vous sur l'ordinateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Planificateur de tâches**.

Sur la fenêtre principale, la première section affiche des informations sur ce que peut faire le Planificateur de tâches, la seconde section affiche des informations sur le statut, l'heure de démarrage et d'arrêt des tâches qui ont démarré au cours de la dernière heure, des dernières 24 heures, des 7 derniers jours ou des 30 derniers jours. Enfin, la troisième section affiche des informations sur les tâches actives comme le nom de la tâche, la prochaine exécution et l'emplacement du fichier exécutable.

Le volet de gauche affiche une structure arborescente de dossiers contenant des tâches planifiées. L'arborescence peut être personnalisée.

## 2. Création d'une tâche

- Dans le volet gauche du Planificateur de tâches, sélectionnez le dossier dans lequel vous voulez stocker la tâche.

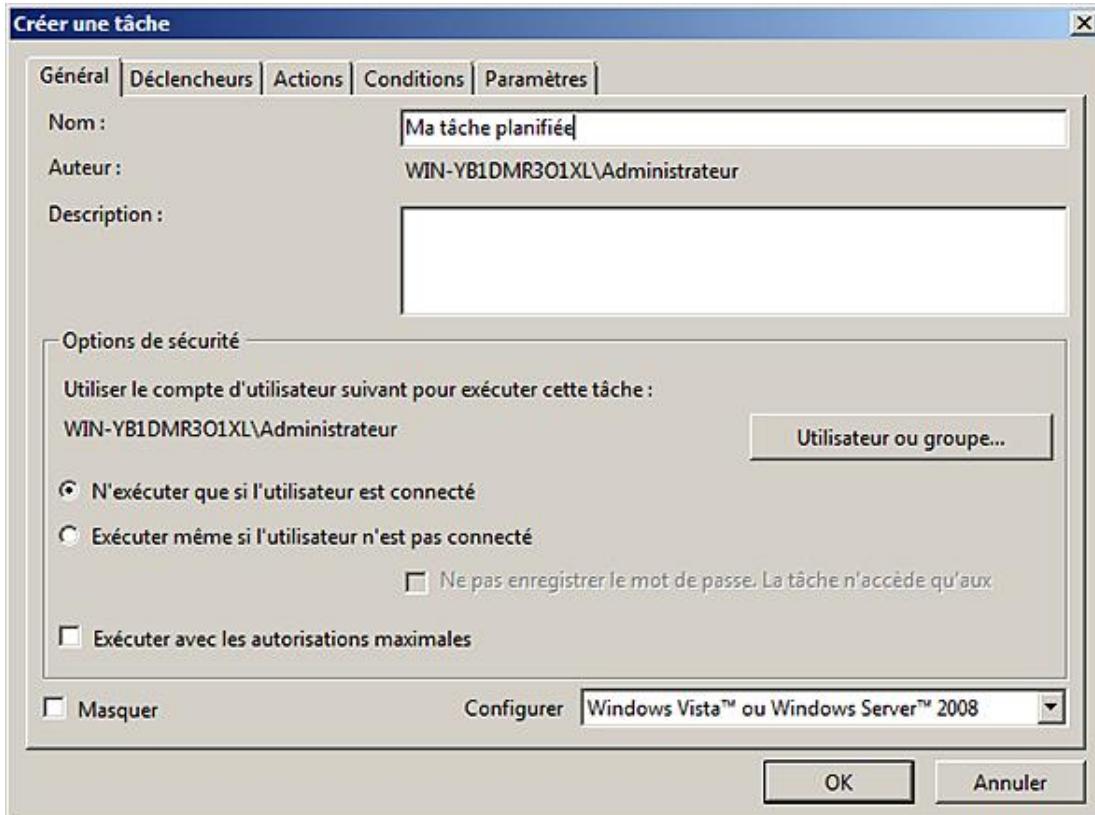


- Cliquez avec le bouton droit de la souris sur le dossier puis cliquez soit sur **Créer une tâche de base** soit **Créer une tâche** (présenté ici).

 Une tâche de base diffère d'une tâche uniquement lors de sa création. L'assistant pour la création d'une tâche est réduit à son minimum pour la tâche de base.

- Dans l'assistant **Créer une tâche**, passez d'un onglet à l'autre pour définir la tâche. Il faut au minimum saisir un **Nom** dans l'onglet **Général** et une action dans l'onglet **Actions**. Cliquez ensuite sur **OK**.

### Onglet Général



Le bouton **Utilisateur ou groupe** permet de définir dans quel contexte de sécurité la tâche va s'exécuter. Par défaut, elle s'exécute dans le contexte de l'utilisateur connecté.

 Si vous êtes connecté avec un compte d'utilisateur qui n'est pas administrateur, le bouton **Utilisateur ou groupe** est modifié en **Utilisateur**.

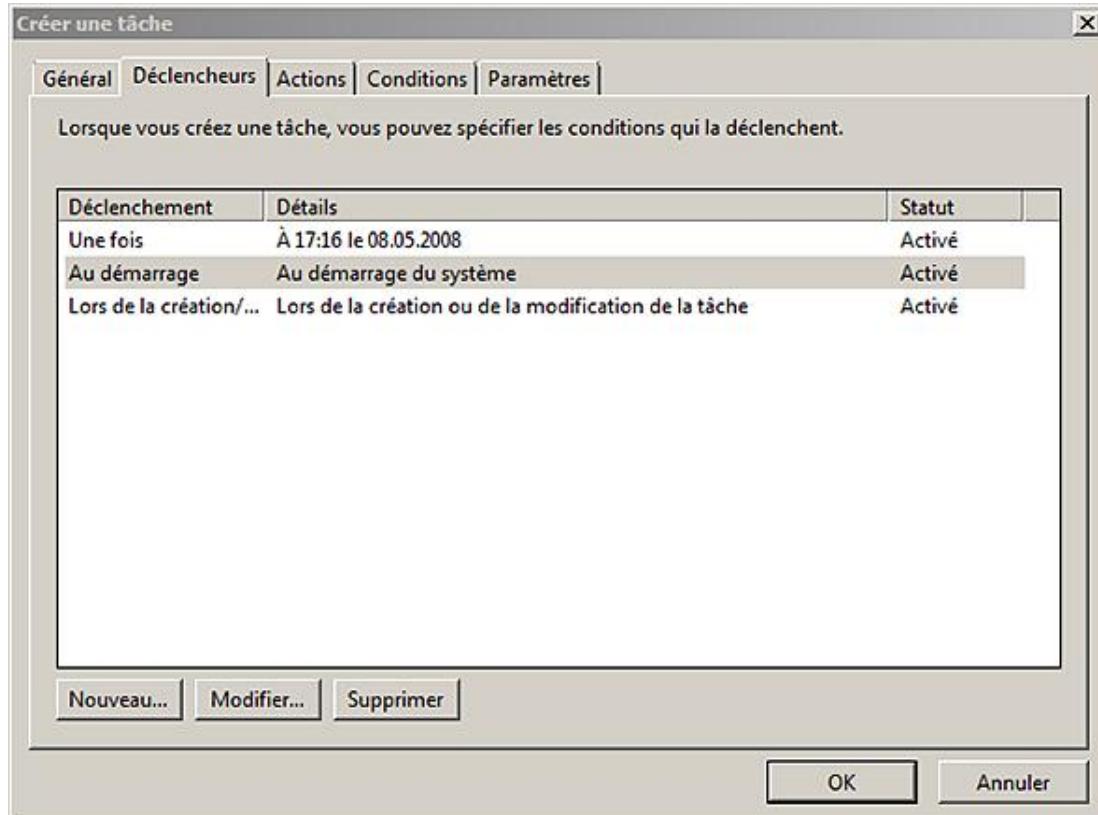
Le bouton radio permet de définir si la tâche peut s'exécuter si l'utilisateur n'est pas connecté ; dans ce cas, pour améliorer la sécurité, vous pouvez sélectionner la case à cocher **Ne pas enregistrer le mot de passe** qui a pour conséquence d'exécuter la tâche dans un contexte de sécurité de l'utilisateur restreint aux ressources locales. Cette méthode est conforme à la norme RFC 1510 qui définit les extensions Kerberos S4U (Services à l'utilisateur).

L'option **Exécuter avec les autorisations maximales** s'utilise principalement avec un compte d'administrateur afin d'augmenter ses priviléges en administrateur selon l'UAC (Contrôle du compte utilisateur).

La case à cocher **Masquer** n'affiche plus la tâche dans l'affichage standard du Planificateur de tâches ; pour la rendre à nouveau visible, soit vous décochez cette case, soit vous cliquez sur l'action **Afficher les tâches masquées** du menu **Affichage** du Planificateur de tâches.

La liste déroulante **Configurer** permet de créer des tâches soit au format **Windows Vista ou Windows Server 2008**, soit au format **Windows Server 2003, Windows XP ou Windows 2000**. Après la création de la tâche, il n'est possible que de passer de l'ancien format vers le format supporté par Windows Server 2008 et Windows Vista.

### Onglet Déclencheurs



L'onglet **Déclencheurs** permet de définir les conditions qui permettront de faire démarrer la tâche.

S'il existe plusieurs déclencheurs, la tâche s'exécute dès qu'un des déclencheurs est actionné.

Le bouton **Nouveau** permet de définir un nouveau déclencheur.

Le bouton **Modifier** permet de modifier le déclencheur sélectionné.

Le bouton **Supprimer** permet de supprimer le déclencheur sélectionné. En pressant la touche [Ctrl], vous pouvez sélectionner plusieurs déclencheurs et les supprimer en une opération.

Les déclencheurs sont présentés ci-après :

- **Sur une planification** : l'exécution se base sur le calendrier pour démarrer la tâche une fois ou selon une périodicité journalière, hebdomadaire ou mensuelle. L'intervalle de la fréquence peut être également choisi.
- **À l'ouverture d'une session** : l'exécution se déclenche dès qu'un utilisateur spécifique ou un utilisateur membre d'un groupe spécifique se connecte.
- **Au démarrage** : l'exécution se déclenche lorsque l'ordinateur démarre.
- **En période d'inactivité** : l'exécution se déclenche lorsque l'ordinateur est inactif selon la configuration définie sous l'onglet **Conditions**.
- **Sur un événement (\*)** : l'exécution se déclenche sur un événement particulier ou basé sur un filtre d'événements.
- **Lors de la création/modification d'une tâche (\*)** : l'exécution se déclenche lors de la création ou de la modification de la tâche.
- **Connexion à une session utilisateur (\*)** : l'exécution se déclenche lors de la connexion d'un utilisateur local ou via le Bureau distant. L'utilisateur peut être tout utilisateur, un utilisateur spécifique ou un utilisateur membre d'un groupe spécifique.
- **Lors de la déconnexion d'une session utilisateur (\*)** : l'exécution se déclenche lors de la déconnexion d'un utilisateur local ou via le Bureau distant. L'utilisateur peut être tout utilisateur, un utilisateur spécifique ou un utilisateur membre d'un groupe spécifique.

- **Lors du verrouillage du poste de travail** (\*) : l'exécution se déclenche lorsque l'utilisateur verrouille sa session. L'utilisateur peut être tout utilisateur, un utilisateur spécifique ou un utilisateur membre d'un groupe spécifique.
- **Lors du déverrouillage du poste de travail** (\*) : l'exécution se déclenche lorsque l'utilisateur déverrouille sa session. L'utilisateur peut être tout utilisateur, un utilisateur spécifique ou un utilisateur membre d'un groupe spécifique.

(\*) Conditions non disponibles pour un déclencheur configuré pour Windows Server 2003, Windows XP ou Windows 2000.

Pour chaque tâche, en plus des paramètres spécifiques au déclencheur, vous pouvez définir des **Paramètres avancés** tels que ceux décrits ci-dessous :

- **Retarder la tâche** : permet de retarder l'exécution de la tâche entre le moment où elle se déclenche et la valeur définie dans cette option. Le déclenchement est alors aléatoire et il n'est pas possible de déterminer avec précision le moment exact du déclenchement.
- **Répéter la tâche tous les** : permet de définir une fréquence de répétition pendant une certaine durée.
- **Arrêter la tâche qui s'exécute plus longtemps que** : permet d'arrêter la tâche après un certain temps d'activité prédéfini allant de 30 mn à 1h, 2h, 4h, 8h, 12h, 1j ou 3j.
- **Activer** : permet d'activer la tâche à partir d'une certaine date.
- **Expiration** : permet d'arrêter l'exécution de la tâche à partir d'une certaine date.
- **Activée** : permet d'activer ou non la tâche manuellement.

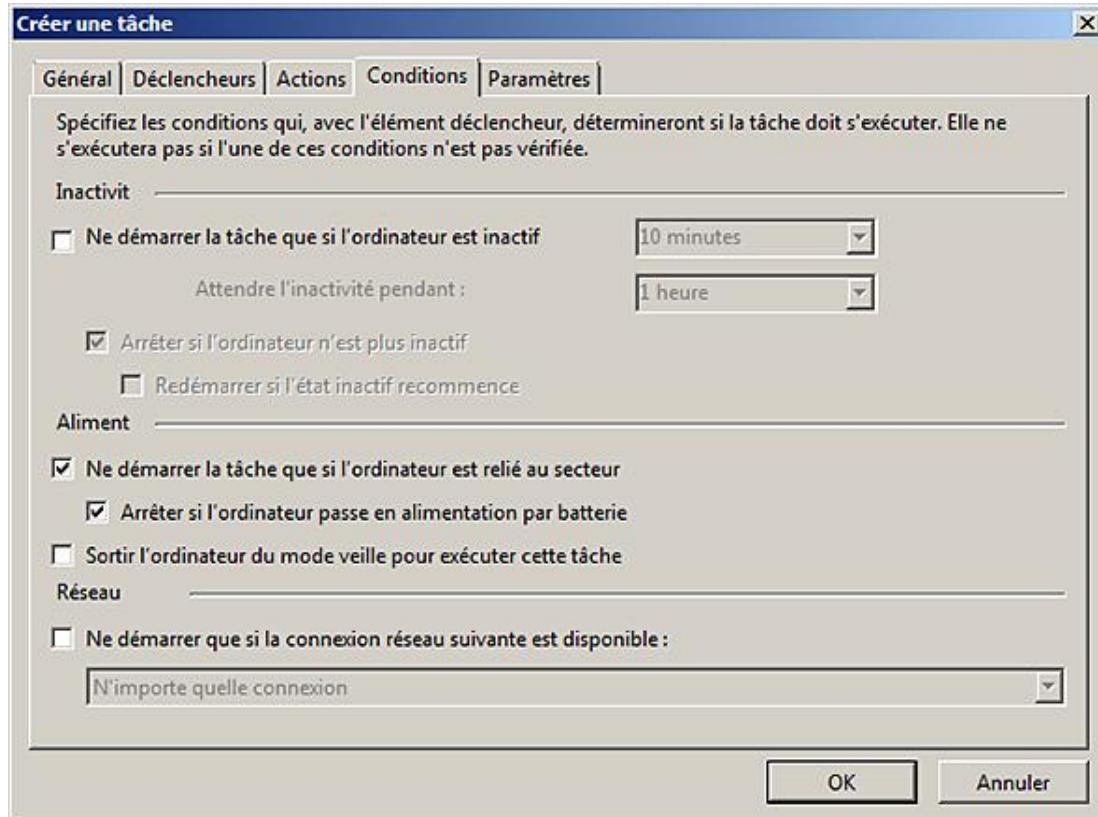
### **Onglet Actions**

L'onglet **Actions** permet de définir une ou plusieurs actions (maximum 32) qui s'exécuteront dans l'ordre défini lorsque la tâche est déclenchée.

Les actions possibles sont :

- **Démarrer un programme**.
- **Envoyer un courrier électronique** au format SMTP. Cette action n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.
- **Afficher un message** affiche un message et est disponible uniquement si l'utilisateur est connecté. Elle n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.

### **Onglet Conditions**

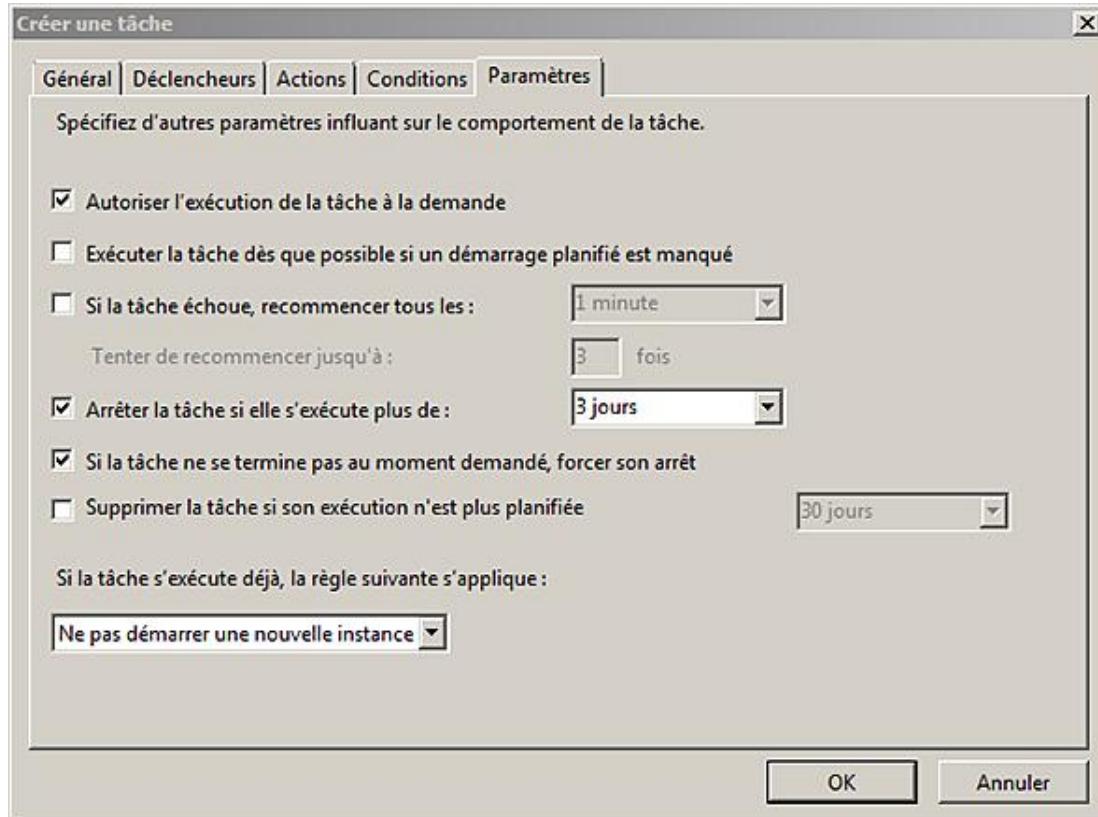


Cet onglet permet de définir les conditions pour le déclenchement de la tâche.

Vous pouvez définir trois types de conditions :

- **Inactivité** : par défaut, un système est considéré comme inactif si l'utilisation de l'unité centrale est 0 % et les entrées/sorties sont à 0 % pendant au moins 90 % d'une durée de 15 minutes. Vous pouvez indiquer vos propres valeurs.
- **Alimentation** : utile pour les portables s'ils sont déconnectés du réseau électrique.
- **Réseau** : pour les tâches devant impérativement disposer du réseau, vous pouvez démarrer la tâche uniquement si le réseau est disponible. Cette option n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.

### **Onglet Paramètres**



Cet onglet permet de définir le cadre d'exécution de la tâche.

**Autoriser l'exécution de la tâche à la demande** permet à un utilisateur de démarrer l'exécution de la tâche sans utiliser de déclencheur. Cette option n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.

**Exécuter la tâche dès que possible si un démarrage planifié est manqué** permet d'exécuter la tâche en cas d'ordinateur éteint, de tâche non activée, etc., lorsque le Planificateur de tâches est de nouveau disponible après un délai de 10 minutes. Ce choix n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.

**Si la tâche échoue** il est possible d'effectuer, après un certain délai, un certain nombre de tentatives. Cette option n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.

**Arrêter la tâche si elle s'exécute plus de** permet de définir la durée maximale d'exécution. Pour garantir l'arrêt, sélectionnez l'option **Si la tâche ne se termine pas au moment désiré, forcer son arrêt**. Ce dernier paramètre n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000.

**Supprimer la tâche si son exécution n'est plus planifiée** permet de supprimer la tâche après un délai, à déconseiller !

Enfin, vous pouvez définir la règle à appliquer **Si la tâche s'exécute déjà :**

- Ne pas démarrer une nouvelle instance.
- Exécuter une nouvelle instance en parallèle.
- Mettre une nouvelle instance en file d'attente.
- Arrêter l'instance existante

Cette option n'est pas disponible pour une tâche configurée pour Windows Server 2003, Windows XP ou Windows 2000 car les tâches sont configurées pour ne pas démarrer une nouvelle instance.

### 3. Importer une tâche

- Dans le volet gauche du **Planificateur de tâches**, sélectionnez le dossier dans lequel vous voulez stocker la tâche.

- Cliquez avec le bouton droit de la souris sur le dossier puis cliquez sur **Importer une tâche**.
- Dans la boîte de dialogue **Ouvrir**, sélectionnez le fichier XML de la tâche et cliquez sur **Ouvrir**. La tâche est importée.

 Cette procédure est utile pour déplacer des tâches d'un dossier à un autre sur le même ordinateur ou entre ordinateurs.

## 4. Exporter une tâche

- Dans le volet gauche du Planificateur de tâches, cliquez sur le dossier qui contient la tâche. La tâche apparaît dans la fenêtre principale.
- Dans la fenêtre principale, cliquez avec le bouton droit de la souris sur la tâche puis cliquez sur **Exporter**.
- Dans la boîte de dialogue **Enregistrer sous**, sélectionnez l'emplacement où vous allez stocker le fichier XML de la tâche et donnez-lui un nom, puis cliquez sur **Enregistrer**.

## 5. Gestion d'une tâche

- Dans le volet gauche du Planificateur de tâches, cliquez sur le dossier qui contient la tâche. La tâche apparaît dans la fenêtre principale.
- Dans la fenêtre principale, cliquez avec le bouton droit de la souris sur la tâche puis cliquez sur l'une des actions suivantes :

**Exécuter** : lance manuellement l'exécution de la tâche

**Fin** : arrête l'exécution de la tâche.

**Désactiver/Activer** : active ou désactive le déclenchement de la tâche.

**Propriétés** : permet de modifier les paramètres de la tâche.

**Supprimer** : supprime la tâche.

Lorsqu'une tâche est sélectionnée, la fenêtre centrale affiche en lecture les différents paramètres de la tâche, plus l'onglet **Historique** qui permet de consulter le journal d'exécution de la tâche.

Sur un Server Core, il faut utiliser la commande **schtasks**. Comme la syntaxe de schtasks peut être laborieuse, il peut être utile d'utiliser le planificateur de tâches sur un autre serveur exécutant une installation complète de Windows Server 2008, puis de l'exporter au format XML et de l'importer avec la commande suivante :

```
schtasks /create */xml myfile.xml /tn NomDeLaTache
```

Pour créer une tâche s'exécutant chaque jour sur le serveur Zens, la tâche consiste à ouvrir le Notepad, la commande est la suivante :

```
schtasks /create /S Zens /U Administrateur /P MotDePasse /Ru  
ExecuteEnTantQu'utilisateur /RP ExecuteMotDePasse /SC DAILY /TN Ma Tache  
/TR notepad
```

Supprime la tâche MaTache :

```
schtasks /delete / S Zens/ U Administrateur /P MotDePasse /TN MaTache /F
```

# Base de registre ou registre



## 1. Introduction

La base de registre est une base de données contenant des informations sur le système d'exploitation, les applications Windows et des applications tierces.

Sa structure hiérarchique permet de définir des clés que l'on peut comparer aux dossiers d'un système de fichiers qui stockent au niveau feuille des valeurs dont le contenu a une signification précise. Le contenu d'une valeur est typé, c'est-à-dire qu'elle n'accepte que le type de données défini. Seuls les types de données suivants sont possibles :

- **Valeur chaîne** accepte une chaîne de caractères composée des caractères affichables de l'alphabet y compris les chiffres.
- **Valeur binaire** accepte tous les caractères, y compris ceux qui ne s'affichent pas. La signification de la chaîne n'est pas forcément compréhensible.
- **Valeur DWORD 32 bits** accepte un nombre entier dont la plus grande valeur est égale à 4294967295 en décimal ou ffffffff en hexadécimal.
- **Valeur QWORD 64 bits** accepte un nombre entier dont la plus grande valeur est égale à 18446744073709551615 en décimal ouffffffffffff en hexadécimal.
- **Valeurs de chaînes multiples** accepte des chaînes de caractères, y compris des nombres, séparées par un retour à la ligne.
- **Valeur de chaîne extensible** peut contenir une variable dont le contenu est remplacé lors de l'appel. %systemroot% est un exemple de variable.

---

Pour définir une clé, il ne faut définir que son nom alors que pour définir une valeur, il faut indiquer le nom de la valeur ainsi que la donnée de la valeur.

---

## 2. La structure en nid d'abeille

Les clés sont organisées en branches, chaque branche est composée de sous-clés, voire de valeurs.

Le tableau suivant résume les branches principales du registre :

Branche	Description
HKEY_CLASSES_ROOT	Enregistre des informations concernant les applications comme l'association des fichiers, les liens OLE, les logiciels composants enfichables, etc.
HKEY_CURRENT_USER	Contient toutes les informations sur la session de l'utilisateur connecté, c'est une copie des informations de l'utilisateur contenues dans HKEY_USERS.
HKEY_LOCAL_MACHINE	Contient des informations concernant le système d'exploitation, les applications, les services, les utilisateurs locaux et la sécurité.
HKEY_USERS	Contient toutes les informations des utilisateurs.
HKEY_CURRENT_CONFIG	Contient des informations collectées lors du démarrage de l'ordinateur, ces

informations résident uniquement en mémoire RAM et ne sont jamais enregistrées.

Le registre a été créé pour centraliser les informations provenant des différents fichiers d'initialisation disposant d'une extension ini. Dès le début, le nombre important de clés et le manque d'informations de référence conduisent à disposer d'un système Windows qui n'est pas toujours optimisé pour le matériel sur lequel fonctionne le système d'exploitation. D'autre part, le souci d'être compatible avec le maximum de matériel conduit les ingénieurs de Microsoft à rajouter un nombre incroyable de clés totalement inutiles pour votre matériel. Il est dès lors difficile de déterminer quelle clé est réellement utile.

Les éditeurs de logiciels, quant à eux, utilisent le registre pour y stocker un nombre incroyable d'informations mais oublient souvent de le nettoyer ou laissent des traces dans le registre lors de la désinstallation du logiciel.

Cet état permet à des spywares et autres virus de s'y loger à votre insu et ils deviennent difficilement détectables.

 Il n'est pas recommandé de modifier les permissions sur les clés même si certaines clés ne sont pas accessibles aux administrateurs mais seulement au compte système.

### 3. L'outil regedit

 La modification du registre n'est pas anodine, elle peut amener à rendre inutilisable l'ordinateur !

L'outil à utiliser pour se déplacer et modifier le registre s'appelle **regedit**. Il n'affiche que les clés pour lesquelles l'administrateur a des droits en lecture. Chaque clé est protégée par des permissions DACLs.

Pour vous connecter au registre local ou situé sur un autre ordinateur, utilisez la procédure suivante :

- Connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.
- Cliquez sur **Démarrer**, puis saisissez **regedit** dans la zone **Rechercher** et appuyez sur [Entrée]. Vous êtes connecté au registre local.
- Pour se connecter au registre d'un autre ordinateur, cliquez sur **Fichier** puis **Connexion au Registre réseau**.
- Dans la boîte de dialogue **Sélectionnez Ordinateur**, saisissez le nom de l'ordinateur désiré ou bien cliquez sur le bouton **Avancé** pour rechercher l'ordinateur désiré, puis cliquez sur **OK**.

### 4. Sauvegarde et restauration du registre

Il est recommandé de sauvegarder le registre avant toute modification de celui-ci. Pour cela, il faut utiliser l'utilitaire de sauvegarde.

Vous pouvez également exporter la totalité du registre ou une partie en utilisant la commande **Exporter** du menu **Fichier**. Cette méthode est plutôt conseillée pour sauvegarder uniquement une partie du registre dans le but de revenir à l'état d'origine après avoir effectué des modifications.

Pour restaurer le registre, vous pouvez utiliser la commande **Importation** du menu **Fichier**, utiliser la dernière configuration valide connue ou effectuer une restauration de votre système.

### 5. Modifier une valeur du registre

- Connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.
- Cliquez sur **Démarrer**, saisissez **regedit** dans la zone **Rechercher** puis appuyez sur [Entrée].
- Si vous ne connaissez pas le chemin pour atteindre la valeur, appuyez sur la touche [F3] pour faire apparaître la boîte de dialogue **Rechercher**, sinon cliquez sur les clés dans le volet gauche.
- Dans la boîte de dialogue **Rechercher**, saisissez le nom de la clé, de la valeur ou de la donnée dans la zone de

texte **Rechercher**, éventuellement décochez les options **Clés**, **Valeurs** ou **Données** afin de limiter l'étendue de la recherche puis cliquez sur **Suivant**.

- Si l'occurrence montrée n'est pas la bonne, appuyez sur la touche [F3] pour passer à la prochaine occurrence.
- Dès que l'occurrence est trouvée, double cliquez sur la valeur, modifiez la valeur et cliquez sur **OK**. La nouvelle valeur est enregistrée dans la base de registre.

---

 Il faut garder à l'esprit que pour certains paramètres du système d'exploitation, il n'est pas besoin de redémarrer l'ordinateur pour que les nouvelles valeurs soient opérationnelles, donc l'état du système peut devenir instable.

---

 Il est important de ne modifier que les valeurs pour lesquelles vous connaissez les données possibles.

---

## 6. Ajouter une valeur ou une clé

Il est possible d'ajouter une valeur ou une clé à tous les niveaux. Si l'orthographe est incorrecte, cela n'a pas d'incidence sur le fonctionnement du système, excepté si le nom correspond à une autre valeur. Dans ce cas, la donnée de la valeur peut rendre le système inutilisable.

## 7. Cadre d'utilisation

Le registre est utile pour contrôler une valeur et peut dans ce cas être utilisé. Bien qu'il soit possible de modifier directement une valeur par l'intermédiaire de l'outil regedit, ce n'est pas la méthode conseillée car cette modification est souvent non documentée. Il est préférable d'utiliser une stratégie de groupes pour effectuer cette modification.

# Outil Diagnostics de la mémoire



## 1. Introduction

Les erreurs les plus difficiles à diagnostiquer concernent la mémoire RAM. Une erreur de ce type peut apparaître seulement après quelques minutes de fonctionnement et non pendant les tests effectués au démarrage de l'ordinateur par le BIOS.

Windows Server 2008 peut détecter automatiquement un problème de mémoire et demander le lancement de l'outil de diagnostics de la mémoire.

 Il n'est pas improbable que Windows détecte un faux positif, c'est-à-dire qu'il détecte une erreur alors que l'outil **Diagnostics de la mémoire** ne détecte rien par la suite. Si cela se produit, il faut consigner le nom du serveur, la date, l'application dans laquelle l'erreur s'est produite et le résultat de l'outil.

Cet outil est manquant sur un Server Core.

## 2. Lancement manuel de l'outil

Il est également possible de le lancer manuellement :

- Cliquez sur **Démarrer**, puis sur **Outil Diagnostics de la mémoire** dans **Outils d'administration**.
- Dans la boîte de dialogue **Outil Diagnostics de la mémoire Windows**, choisissez soit d'effectuer le test immédiatement en redémarrant l'ordinateur, soit de programmer la tâche au prochain redémarrage.

Dans les deux cas, au prochain redémarrage, l'outil se lance automatiquement. Deux passes de vérification de la mémoire sont effectuées, puis le système redémarre ; après le login de l'utilisateur, le système notify le résultat du test dans la zone de notification de la barre des tâches.

Une bonne méthode consiste à rechercher dans le journal des événements **Système** les événements dont la source est MemoryDiagnostics-Results.

**Système** 2'964 Événements

Niveau	Date et heure	Source	ID de l'...	Catégo...
⚠ Avertissement	12.06.2008 00:18:28	Time-S...	12	Aucun
ⓘ Information	12.06.2008 00:18:16	Memor...	1201	Aucun
ⓘ Information	12.06.2008 00:18:16	Memor...	1101	Aucun
ⓘ Information	12.06.2008 00:18:16	DfsSvc	14531	Aucun
ⓘ Information	12.06.2008 00:18:16	DfsSvc	14533	Aucun

## Événement 1101, MemoryDiagnostics-Results

[Général](#) | [Détails](#) |

L'outil Diagnostics de la mémoire Windows a testé la mémoire de l'ordinateur et n'a détecté aucune erreur.

Journal : Système  
Source : MemoryDiagnostics-Results Connecté : 12.06.2008 00:18:16  
Événement : 1101 Catégorie : Aucun  
Niveau : Information Mots-clés :  
Utilisateur : SYSTEM Ordinateur : AD1.artvinum.com  
Opcode : Informations  
Informations : [Aide sur le Journal](#)

## Options de démarrage avancées



Les options avancées de démarrage permettent de dépanner le démarrage d'un système.

- Au démarrage de l'ordinateur, après le démarrage du BIOS, appuyez sur [F8] pour faire apparaître les options de démarrage avancées.

Les options de démarrage avancées sont les suivantes :

**Mode sans échec** : le mode sans échec lance le système uniquement avec les services et les pilotes minimum nécessaires. Seul un pilote carte graphique VGA standard est démarré. Il existe trois modes sans échec, à savoir :

- le mode invite de commandes,
- le mode Bureau local sans prise en charge du réseau,
- le mode Bureau local avec prise en charge du réseau.

**Inscrire les événements de démarrage dans le journal** : dans ce mode, Windows crée un fichier ntbtlog.txt qui contient la liste de tous les pilotes chargés au démarrage, y compris le dernier avant un problème.

**Démarrage en VGA** : dans ce mode, Windows démarre en basse résolution soit 640\*480. Il est surtout utilisé sur des stations de travail pour résoudre des problèmes de mauvaise configuration de la résolution entre la carte réseau et l'écran.

**Mode restauration des services d'annuaire** : démarre un contrôleur de domaine sans lancer les services d'annuaire. Très utile dans les versions précédentes, son intérêt est désormais limité car il est possible d'arrêter et de démarrer les services Active Directory sans redémarrer le serveur.

**Mode débogage** : ce mode permet d'utiliser un autre ordinateur pour déterminer l'origine d'un problème sur un serveur. Complexé à mettre en œuvre et à interpréter, ce mode sert surtout pour déterminer l'origine d'un problème sur des serveurs très couteux.

**Empêcher le redémarrage automatique** : cette option empêche Windows de redémarrer après un incident.

**Désactiver le contrôle des signatures** : par défaut, sur une version 64 bits, il n'est pas possible de démarrer Windows avec des pilotes en mode noyau non signés. Bien qu'il ne soit pas conseillé de désactiver le contrôle obligatoire des signatures, il est possible d'effectuer des tests ou de résoudre des problèmes avec ce mode.

## Dernière configuration valide connue



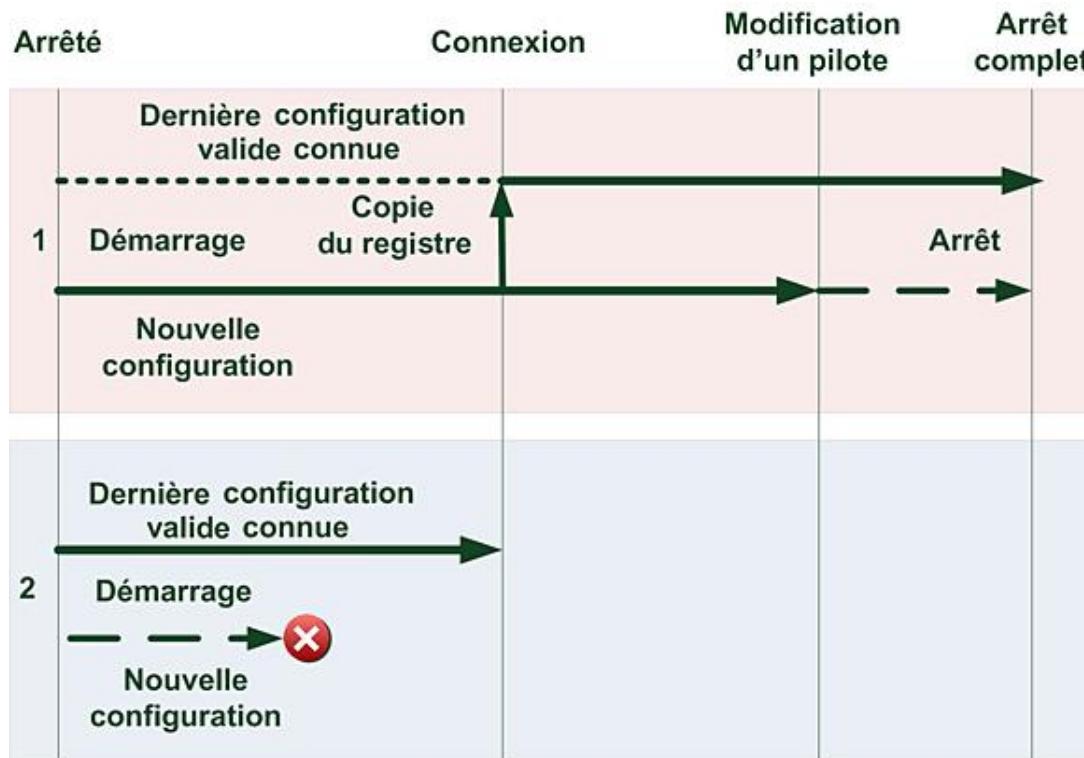
Il ne s'agit pas à proprement dit d'un outil de dépannage mais plutôt d'une fonctionnalité qui permet de résoudre un problème survenu lors d'une modification du système ayant entraîné un redémarrage, et un écran bleu lors du démarrage.

Sur la figure suivante, au point 1, au démarrage, la configuration de la base de registres stockée dans la **dernière configuration valide connue** est différente de la **configuration actuelle** jusqu'au moment où un utilisateur se connecte.

À ce moment, la dernière configuration valide connue est écrasée et la configuration actuelle est copiée. Les deux configurations sont identiques.

Après un certain temps, l'utilisateur met à jour un pilote critique. Après la mise à jour, il faut redémarrer le serveur, ce qui est fait. À l'arrêt, la dernière configuration valide connue et la configuration actuelle sont différentes.

Au démarrage du serveur au point 2, un écran bleu survient à cause du nouveau pilote. Comme il n'est plus possible de démarrer, la seule solution est d'utiliser la dernière configuration valide connue. Cela ramène le serveur à l'état du dernier démarrage, c'est-à-dire lors de la connexion de l'utilisateur après le démarrage du point 1.



Pour cela, il faut exécuter la procédure suivante :

- Au démarrage de l'ordinateur, après le démarrage du BIOS, appuyez sur [F8] pour faire apparaître les options de démarrage avancées.
- Avec les touches [Flèche en haut] ou [Flèche en bas], sélectionnez la commande **Dernière configuration valide connue (option avancée)** puis appuyez sur [Entrée].

➤ Après la modification d'un pilote, il est recommandé d'attendre le chargement complet de tous les pilotes pour éviter d'avoir un écran bleu et dans ce cas, d'utiliser la dernière configuration valide connue. Ce conseil s'applique pour tout démarrage après installation d'un pilote ou d'une application.

# Configuration du système



Win

## 1. Présentation

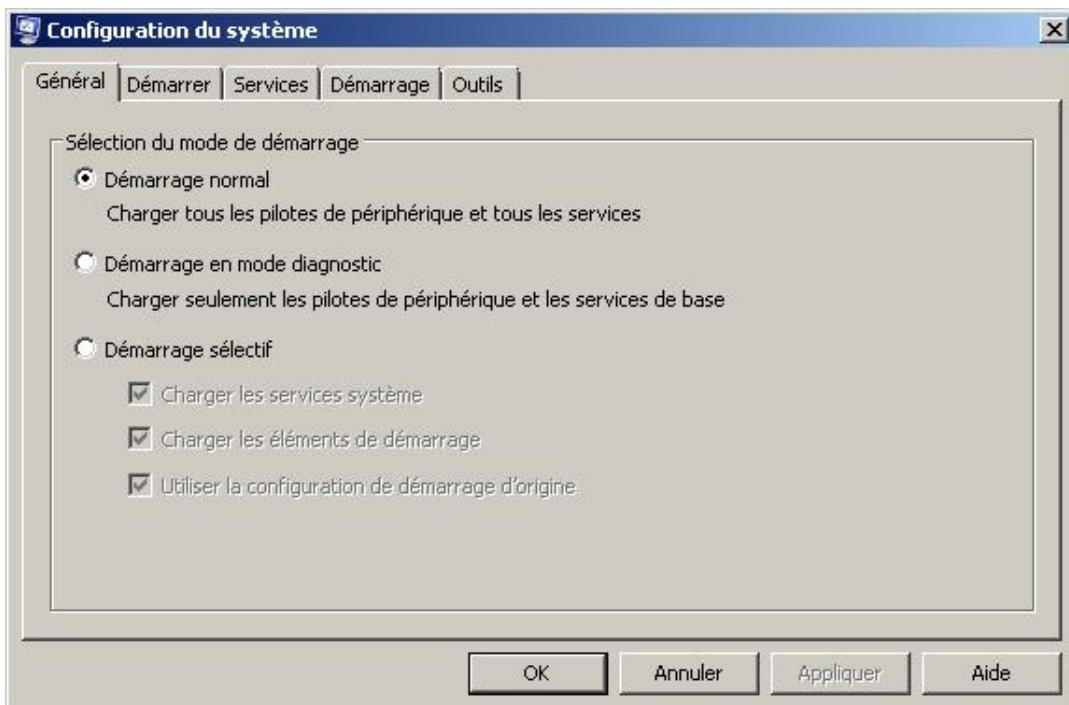
L'outil **Configuration du système** sert principalement à modifier la configuration de démarrage de Windows afin de résoudre des problèmes provenant du chargement des services et des applications.

Le principe de dépannage à utiliser est simple, il faut commencer par désactiver les services et applicatifs pour isoler le service ou l'application qui pose problème.

Cet outil est absent sur un Server Core.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Configuration du système**.

### Onglet Général



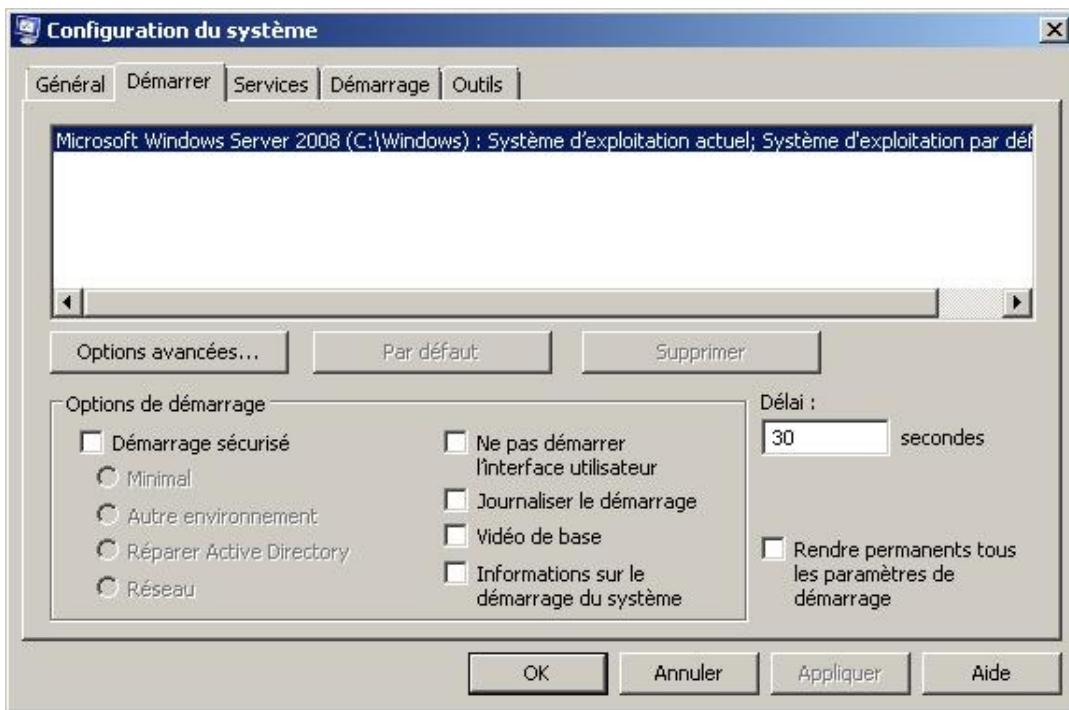
**Démarrage normal** est le mode de fonctionnement normal, à sélectionner à la fin du dépannage.

**Démarrage en mode diagnostic** permet d'exclure un problème de fichiers de Windows. Il démarre uniquement avec les services et pilotes de base.

**Démarrage sélectif** étend le mode diagnostic en permettant de sélectionner d'autres services et programmes. Les onglets **Services** et **Démarrage** permettent d'activer/désactiver les services et applications concernés.

- 
- À la fin du dépannage, n'oubliez pas de sélectionner le mode normal.
- 

### Onglet Démarrer



Cet onglet permet de sélectionner un système d'exploitation au démarrage et de lui appliquer certains paramètres pour le dépanner. Cela revient à préconfigurer le prochain démarrage pour une utilisation de la touche [F8] avec un plus grand contrôle.

#### Démarrage sécurisé :

- **Minimal** est équivalent à un mode sans échec sans prise en charge du réseau.
- **Autre environnement** est équivalent à une invite de commande en mode sans échec sans prise en charge du réseau.
- **Réparer Active Directory** est équivalent au mode de restauration des services d'annuaire.
- **Réseau** est équivalent à un mode sans échec avec prise en charge du réseau.

Les autres options de démarrage sont :

- **Ne pas démarrer l'interface utilisateur**, c'est-à-dire toujours utiliser une invite de commande.
- **Journaliser le démarrage** dans le fichier %systemroot%\ntbtlog.txt.
- **Vidéo de base** : démarre en mode VGA minimal.
- **Informations sur le démarrage du système** : affiche le nom des pilotes pendant leur chargement.

La sélection de la case à cocher **Rendre permanents tous les paramètres de démarrage** ne permet plus de restaurer les modifications avec le mode **Démarrage normal** de l'onglet **Général**.

Le bouton **Options avancées** permet de modifier le matériel en diminuant le nombre de processeurs, la quantité de mémoire RAM, les verrous PCI et forcer la détection de la HAL (*Hardware Abstraction Layer*). Il est également possible d'envoyer les informations de débogage sur un second ordinateur afin de traiter des problèmes comme les écrans bleus en envoyant les fichiers **dump** correspondant aux bons services techniques.

#### Onglet Services

Cet onglet permet de sélectionner quels services vont être désactivés lors du prochain redémarrage. Le bouton **Désactiver tout** laisse quelques services requis par le système en fonctionnement. Toutefois, il peut être dangereux de désactiver des services dont dépendent d'autres services !

### **Onglet Démarrage**

Cet onglet permet de sélectionner quelles applications vont être désactivées lors du prochain redémarrage. Le bouton **Désactiver tout** les désactive toutes.

### **Onglet Outils**

Cet onglet propose une liste d'autres outils qu'il est possible d'utiliser pour le dépannage. Il suffit de sélectionner l'outil et de cliquer sur **Exécuter**.

## **2. Cadre d'utilisation**

L'outil **Configuration du système** peut être utilisé pour dépanner tous les problèmes rencontrés lors du démarrage d'un serveur. Il s'utilise surtout si le serveur peut démarrer en mode sans échec.

# Les services

Un service est une application qui tourne en tâche de fond sans interaction avec l'utilisateur. Généralement, les services sont lancés au démarrage et stoppés à l'arrêt du serveur.

Il peut être utile de gérer un service pendant l'exécution de Windows soit pour modifier son démarrage, soit pour l'arrêter ou le configurer lorsqu'une erreur survient.

## 1. La console Services



Win

La console Services est un snap-in.

- Pour démarrer la console, connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Services**.

À partir de la console, vous pouvez gérer les services de cet ordinateur ou d'un ordinateur distant. Pour cela, sélectionnez **Services** dans le volet gauche puis cliquez avec le bouton droit de la souris et sélectionnez **Se connecter à un autre ordinateur**.

L'onglet **Standard** de la fenêtre principale n'affiche pas les informations sur l'état du service et sa description donc il est à déconseiller.

Dans la fenêtre principale, est affichée la liste des services. Il est possible de la trier selon le titre d'une des colonnes si vous cliquez sur ce titre. Vous pouvez aussi modifier l'ordre des colonnes en sélectionnant le titre et en effectuant un glisser/déplacer, ou bien **Ajouter/supprimer des colonnes** via l'option correspondante du menu **Affichage**.

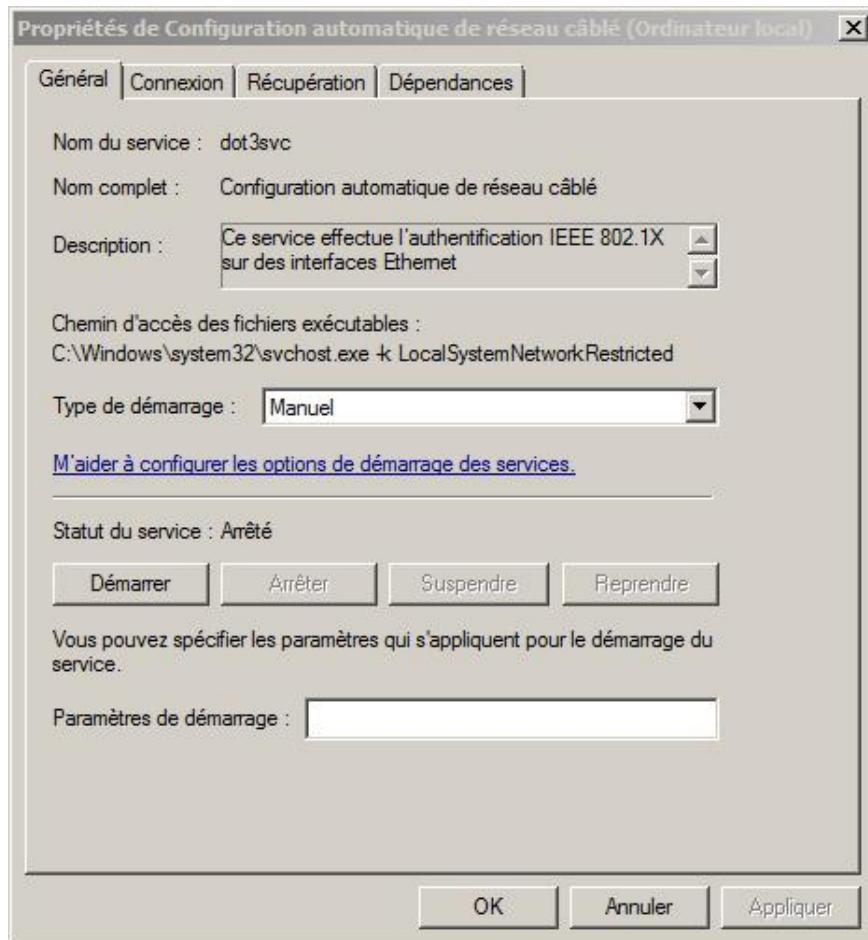
Dès qu'un service est sélectionné, il est possible d'effectuer les actions suivantes via le menu contextuel ou le menu **Action** :

- Démarrer
- Arrêter
- Suspendre
- Reprendre
- Redémarrer

Vous pouvez également afficher les **Propriétés** du service. Les onglets de la boîte de dialogue **Propriétés** sont présentés dans la section suivante.

## 2. Propriétés des services

### Onglet Général



Les informations suivantes sont affichées :

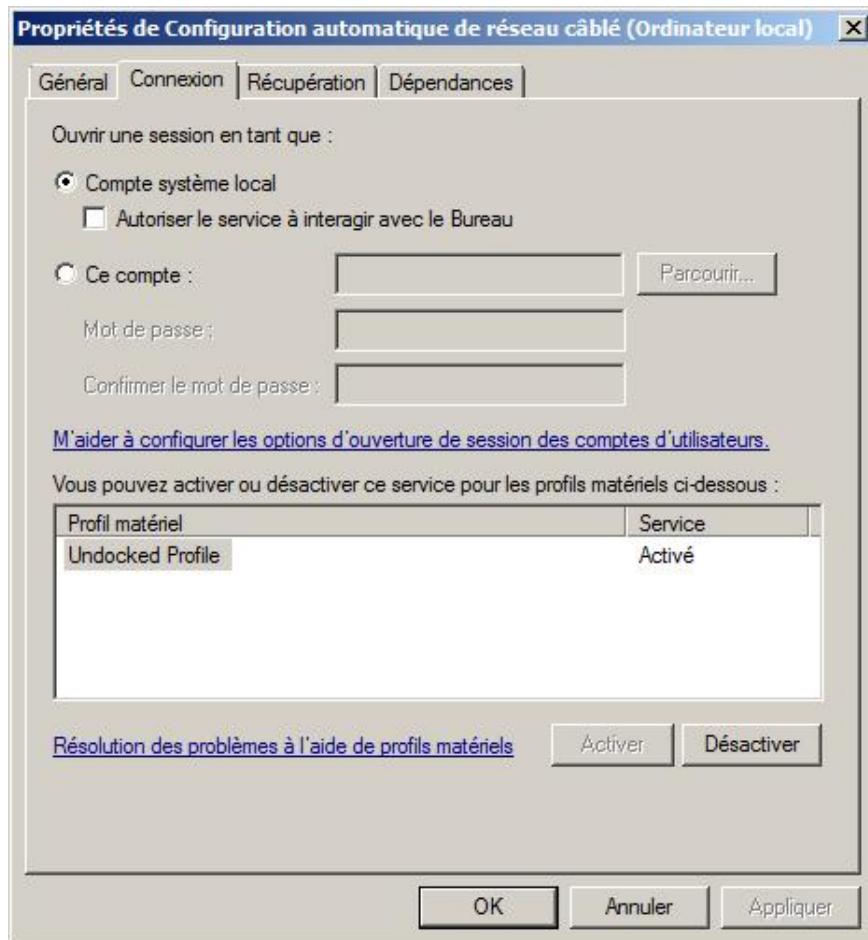
- Le **Nom du service** qui peut être utilisé avec les commandes **net start** ou **net stop**.
- Le **Nom complet** ou le nom long.
- Une **Description** du service.
- Le nom et le **Chemin d'accès** complet du fichier du service.

Le **Type de démarrage** peut prendre une des valeurs suivantes :

- **Automatique (début différé)** : le démarrage a lieu en même temps que celui de Windows mais après que les services non différés auront démarré.
- **Automatique** : le service démarre avec Windows.
- **Manuel** : le service démarre uniquement si une application en a besoin.
- **Désactivé** : le service ne démarre pas.

Les boutons de la zone **Statut du service** permettent respectivement de démarrer, arrêter, mettre en pause ou reprendre le service. Les **Paramètres de démarrage** permettent d'indiquer les options prévues par l'éditeur de service.

### Onglet Connexion



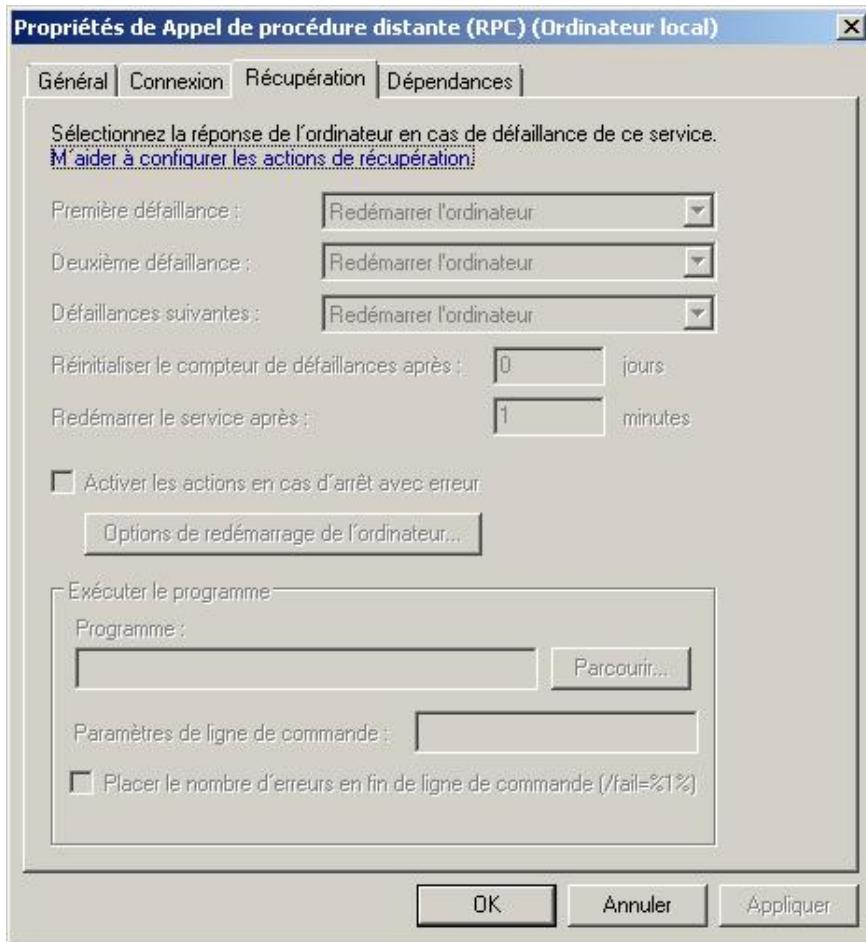
Cet onglet permet de définir sous quel compte d'utilisateur le service fonctionne. Il peut s'agir d'un compte utilisateur créé ou d'un compte système ou système restreint.

Les comptes système restreints sont apparus afin de limiter les droits de certains services avec pour conséquence de diminuer la surface d'attaque. Avec Windows Server 2008, il est possible de gérer les services suivants :

- **LocalSystem** est le compte qui a le plus de droits et de permissions sous Windows Server 2008 et il dépasse même l'administrateur. Un service s'exécutant sous ce compte peut avoir accès à tout le système d'exploitation. Les services suivants fonctionnent sous ce compte : BITS, Themes, Rasman, TrkWks, Error Reporting, 6to4, Task scheduler, RemoteAccess, Rasauto, WMI.
- **LocalSystem restreint avec le pare-feu** permet un meilleur contrôle de LocalSystem. Il suffit de restreindre le service dans le pare-feu. Les services suivants fonctionnent sous ce compte : WMI Perf Adapter, Automatic Updates, Secondary Logon, App Management, Wireless Configuration.
- **Network Service réseau restreint** est un compte limité car il n'a pas plus de droits qu'un utilisateur mais il a accès au réseau. Les services suivants fonctionnent sous ce compte : Cryptographic Services, Telephony, PolicyAgent, Nlasvc.
- **Network Service totalement restreint** est encore plus limitatif. Les services suivants fonctionnent sous ce compte : DNS Client, ICS, DHCP Client, Browser, Server, W32time.
- **Local Service sans accès au réseau** est un compte limité car il n'a pas plus de droits qu'un utilisateur et n'a pas accès au réseau. Les services suivants fonctionnent sous ce compte : System Event Notification, Network Connections, Shell Hardware Detection, COM+ Event System.
- **Local Service totalement restreint** est encore plus limitatif. Les services suivants fonctionnent sous ce compte : Windows Audio, TCP/IP NetBIOS helper, WebClient, SSDP, Event Log, Workstation, Remote registry.

 C'est au démarrage du service qu'il faut spécifier comment le compte prédéfini doit être utilisé, par exemple svchost.exe -k LocalServiceNoNetwork.

## Onglet Récupération



Cet onglet permet de définir comment réagir en cas de défaillance du service.

L'action définie par défaut est **Ne rien faire**, mais vous pouvez :

- **Redémarrer le service** après un délai défini, 2 minutes par défaut.
- **Exécuter un programme** permet de lancer un script ou un programme spécifique éventuellement avec des paramètres ainsi que la valeur de l'erreur rencontrée.
- **Redémarrer l'ordinateur** est l'option la plus radicale. Pour cette option, vous pouvez définir la durée avant de redémarrer l'ordinateur et demander l'envoi d'un message aux autres ordinateurs connectés au réseau en utilisant le bouton **Options de redémarrage de l'ordinateur** et en l'activant avec la case à cocher correspondante.

Vous pouvez configurer des actions jusqu'à la troisième défaillance du service durant un certain laps de temps après avoir déterminé que le service est défaillant.

## Onglet Dépendances

Cet onglet montre les dépendances qui existent entre les services.

Regardez toujours cet onglet avant d'arrêter un service car comme spécifié sur l'écran précédent, tous les services présents dans la liste du bas s'arrêtent si vous arrêtez le service.

En dépannage, cet onglet est utile pour vérifier si tous les services dont dépend le service concerné ont bien démarré.

 À ma connaissance, il n'existe pas d'outil qui permette d'afficher une arborescence hiérarchique des services et leurs dépendances.

### 3. La commande sc



La commande **sc** permet de gérer les services via l'invite de commandes, la syntaxe de cette commande est la suivante :

The screenshot shows a Windows Command Prompt window titled "Invite de commandes - sc". The command entered is "C:\>sc". The output provides detailed information about the "sc" command, including its description, usage, and a comprehensive list of available commands and their descriptions. The commands listed include query, queryex, start, pause, interrogate, continue, stop, config, description, failure, failureflag, sidtype, privs, qc, qdescription, qfailure, qfailureflag, qsidtype, qprivs, delete, create, control, sdshow, sdset, showsid, GetDisplayName, GetKeyName, and EnumDepend. It also includes sections for boot options like "ok" and "bad", and service management commands like Lock and QueryLock.

```
C:\>sc
DESCRIPTION :
    SC est un utilitaire de ligne de commande utilisé pour
    communiquer avec le Gestionnaire de contrôle des services et les
    services.

UTILISATION :
    sc <serveur> [commande] [nom service] <option1> <option2>...

L'option <serveur> se présente au format « \\\NomServeur »
Pour obtenir de l'aide sur une commande, entrez : « sc [commande] »

Commandes :
    query----- Interroge l'état d'un service ou
                énumère l'état de types de services.
    queryex----- Interroge l'état étendu d'un service ou énumère
                l'état de types de services.
    start----- Démarrer un service.
    pause----- Envoie une demande de contrôle PAUSE à un service.
    interrogate---- Envoie une demande de contrôle INTERROGATE à un
                    service.
    continue----- Envoie une demande de contrôle CONTINUE à
                    un service.
    stop----- Envoie une demande STOP à un service.
    config----- Modifie la configuration d'un service (persistant).
    description---- Modifie la description d'un service.
    failure----- Modifie les actions entreprises par un service en
                cas d'échec.
    failureflag---- Modifie l'indicateur des actions d'échec
                    d'un service.
    sidtype----- Modifie le type de SID d'un service.
    privs----- Modifie les priviléges nécessaires d'un service.
    qc----- Interroge les informations de configuration
            d'un service.
    qdescription---- Interroge la description d'un service.
    qfailure----- Interroge les actions entreprises par un service
            en cas d'échec.
    qfailureflag---- Interroge l'indicateur des actions d'échec
                    d'un service.
    qsidtype----- Interroge le type de SID d'un service.
    qprivs----- Interroge les priviléges nécessaires d'un service.
    delete----- Supprime un service (du Registre).
    create----- Crée un service (en l'ajoutant au Registre).
    control----- Envoie un contrôle à un service.
    sdshow----- Affiche le descripteur de sécurité d'un service.
    sdset----- Définit le descripteur de sécurité d'un service.
    showsid----- Affiche la chaîne du SID de service correspondant à
                un nom arbitraire.
    GetDisplayName-- Récupère le nom affiché d'un service.
    GetKeyName---- Récupère le nom de clé d'un service.
    EnumDepend---- Énumère les dépendances d'un service.

Les commandes suivantes ne nécessitent pas de nom de service :
    sc <serveur> <commande> <option>
        boot----- (ok | bad) Indique si le dernier démarrage doit
                    être enregistré comme la dernière configuration
                    valide connue
        Lock----- Verrouille la base de données des services
        QueryLock---- Interroge l'état de verrouillage d'une base de
                    données du Gestionnaire de contrôle des services
```

#### Quelques exemples

- Saisissez `sc start <MonService>` pour démarrer un service.
- Saisissez `sc stop <MonService>` pour arrêter un service.
- Saisissez `sc query <MonService>` pour afficher des informations concernant un service.

### 4. Cadre d'utilisation

La console Services permet de définir comment les services doivent démarrer. Néanmoins il est préférable de gérer les services via les stratégies de groupe. Il est recommandé d'utiliser cet outil pour afficher la configuration actuelle et

en dépannage.

# Assistance à distance



Win

L'assistance à distance permet à une personne chargée du support, appelée expert ou conseiller, de fournir une aide sur un ordinateur particulier à un utilisateur appelé novice ou utilisateur. L'assistance à distance est différente du Bureau distant du fait que l'affichage et le contrôle du Bureau de l'ordinateur à dépanner sont partagés entre l'expert et le novice. Par défaut, l'expert ne peut que visualiser le Bureau du novice sans pouvoir interagir.

Même si la fonctionnalité Assistance à distance n'est pas installée, il est toujours possible d'activer et d'utiliser le Bureau distant.

Il existe deux possibilités pour démarrer une assistance. Pour la première, le novice demande de l'aide en créant un fichier MsRcIncident qui pourra être envoyé en tant que fichier joint par courrier électronique, placé sur un partage réseau ou sur un média spécifique, voire en utilisant la messagerie instantanée. Cette méthode s'appelle l'**Assistance à distance sollicitée** alors que l'autre méthode, où l'expert propose son aide au novice soit directement, soit via la messagerie instantanée, s'appelle **Assistance à distance non sollicitée**.

Les membres du groupe Administrateurs du domaine ne font plus partie par défaut de la liste des experts.

Des fichiers de journalisation sont créés afin d'augmenter la sécurité. Ces derniers sont enregistrés dans le répertoire **users\Nom\_utilisateur\Documents\Remote Assistance Logs**.

Dans un environnement de domaine, la gestion de l'assistance à distance se fait via les stratégies de groupe situées dans l'emplacement suivant **Configuration de l'ordinateur - modèles d'administration - Système - assistance à distance** :

- Assistance à distance sollicitée.
- Proposer l'Assistance à distance.
- Autoriser uniquement les connexions Vista ou ultérieures.
- Personnaliser les messages d'avertissement.
- Activer la journalisation de session.
- Activer l'optimisation de la bande passante.

Le composant de cette fonctionnalité est **Remote-Assistance**.

Cette fonctionnalité est absente sur un Server Core.

## 1. Configuration de l'assistance à distance

Après avoir installé la fonctionnalité, vous pouvez à tout moment autoriser ou refuser l'assistance à distance.

- Sur le serveur Windows 2008, cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage est en mode classique, cliquez sur **Système**, sinon cliquez sur **Système et maintenance** puis sur **Système**.
- Sous **Tâches**, cliquez sur **Paramètres d'utilisation à distance**.
- Sélectionnez ou désélectionnez l'option **Autoriser les connexions d'assistance à distance vers cet ordinateur**.

Si vous cliquez sur le bouton **Options avancées**, il est possible de définir les paramètres suivants :

- Autoriser l'expert à prendre le contrôle de cet ordinateur.
- Gérer la durée maximale de validité des invitations.
- Autoriser uniquement des ordinateurs exécutant Windows Vista ou ultérieur à se connecter en tant qu'expert (améliore la sécurité).

## 2. Utilisation de l'assistance à distance

Ce scénario décrit la procédure qu'un novice doit effectuer pour solliciter une assistance en créant un fichier MsRcIncident qu'il placera sur un partage réseau.

- Sur le serveur Windows 2008, cliquez sur **Démarrer** puis saisissez **msra** dans la zone de recherche avant d'appuyer sur [Entrée].
- Dans la boîte de dialogue **Voulez-vous demander une assistance ou en proposer ?**, cliquez sur **Invitez une personne de confiance à vous aider**.
- Dans la boîte de dialogue **Comment souhaitez-vous inviter quelqu'un à vous aider ?**, cliquez sur **Enregistrer cette invitation en tant que fichier**.
- Dans la boîte de dialogue **Enregistrez l'invitation en tant que fichier**, saisissez un chemin réseau de type UNC puis un mot de passe et confirmez le mot de passe avant de cliquer sur **Terminer**.

L'expert n'a pas besoin de disposer d'un compte de login sur l'ordinateur à dépanner. Il doit seulement connaître le mot de passe que le novice lui aura transmis par un moyen comme le téléphone pour se connecter. Une fois connecté sur celui-ci, même s'il est administrateur, l'expert dispose des mêmes droits que le novice !

Concernant les pare-feu, une configuration spécifique doit être prévue.

L'expert doit disposer d'un ordinateur tournant au minimum sous Windows Vista pour aider le novice sinon le fonctionnement risque d'être aléatoire.

## 3. Cadre d'utilisation

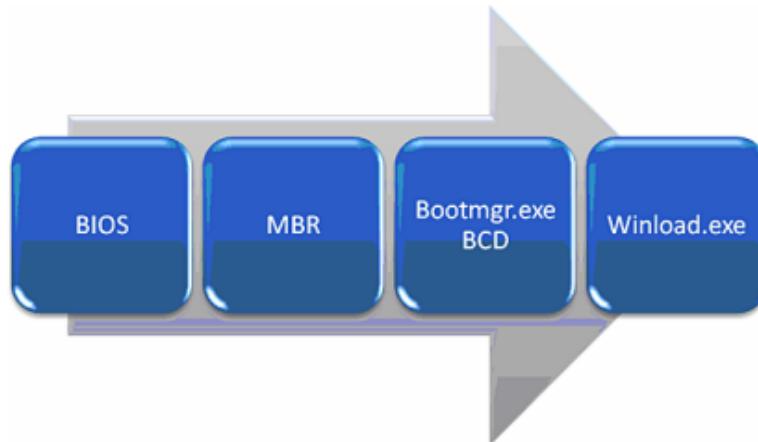
Pour un serveur, cette fonctionnalité est utile pour demander de l'aide à d'autres administrateurs de l'entreprise afin qu'ils puissent fournir de l'aide à distance.

# Processus de démarrage de Windows Server 2008



## 1. Déroulement du processus

La séquence de démarrage de Windows Server 2008 est la suivante :



Lorsque le serveur est allumé, le système démarre et le CMOS charge le **BIOS** et exécute le POST ; ensuite, le système cherche le secteur appelé **MBR** - pour *Master Boot Record* - qui contient entre autres le nom du fichier de démarrage appelé **bootmgr.exe** situé à la racine de la partition active.

**Bootmgr** se charge en mémoire et lit les données du magasin **BCD** (*Boot Configuration Data*) du répertoire **boot** de la partition active. Puis, en fonction du système d'exploitation, il charge **winload.exe** (%systemroot%\system32) pour **Windows Vista** ou **Windows 2008** ou **ntoskrnl.exe** pour des versions de Windows antérieures, Windows 2000/2003.

---

➤ Si le système est en mode d'hibernation, **winload** est remplacé par **winresume** (%systemroot%\system32).

---

**Winload** charge les pilotes qui sont configurés pour démarrer au boot puis il transfère le contrôle au noyau de Windows **ntoskrnl.exe** (%systemroot%\system32).

Enfin le Shell affiche l'écran de connexion.

---

➤ Il est possible de copier les fichiers bootmgr.exe et boot sur un autre média et de démarrer à partir de ce média, mais cette procédure n'est actuellement pas supportée par Microsoft.

---

Le processus de démarrage n'utilise plus de fichier texte **boot.ini** sensible à des attaques, mais BCD - pour *Boot Configuration Data* - aussi appelé magasin de données de configuration de démarrage. En plus d'être mieux sécurisé, il est compatible avec d'autres plates-formes et permet de gérer un plus grand nombre de paramètres.

L'utilitaire fourni par Microsoft pour gérer BCD s'appelle **bcdedit**. Il s'agit d'un utilitaire de type ligne de commande simple à utiliser mais dont les paramètres peuvent être complexes.

```
C:\>bcdedit
Gestionnaire de démarrage Windows
{
    {bootmgr}
        device      partition=C:
        description Windows Boot Manager
        locale     fr-FR
        inherit    {globalsettings}
        default   {current}
        displayorder {current}
        toolsdisplayorder {nemdiag}
        timeout    30
}

Chargeur de démarrage Windows
{
    {current}
        device      partition=C:
        path       \Windows\system32\winload.exe
        description Microsoft Windows Server 2008
        locale     fr-FR
        inherit    {bootloadersettings}
        osdevice   partition=C:
        systemroot \Windows
        resumeobject {6608cb51-04a9-11dd-ac17-857fbef7f2f}
        nx        OptOut
}

C:\>
```

Il existe plusieurs outils graphiques gratuits ou payants comme VistaBootPro ou EasyBcd qui permettent de gérer BCD plus facilement.

## 2. Cadre d'utilisation

Le processus de démarrage est à utiliser lorsque vous disposez de plusieurs systèmes d'exploitation comme cela peut être le cas pour une station de travail sous Windows Vista.

Pour un serveur, ce sera surtout pour dépanner le système au démarrage.

# Windows Server Update Services



WSUS est un service additionnel gratuit de Windows dont l'objectif est de gérer de manière centralisée le déploiement des mises à jour prévues par Microsoft via Windows Update pour des ordinateurs utilisant un système d'exploitation Windows au sein de l'entreprise.

Son principal avantage, et également sa principale différence par rapport à Windows Update, tient au fait que l'administrateur peut décider quelles seront les mises à jour à installer pour des groupes d'ordinateurs. Avec WSUS, il est possible de conserver Windows Update comme source de téléchargement pour chaque ordinateur car la configuration des méthodes de mise à jour dépend des paramètres des stratégies de groupe (GPO) configurées et appliquées.

 Bien que WSUS soit conseillé à partir d'un réseau comportant dix ordinateurs, il est conseillé de l'utiliser dès que l'on dispose d'une Active Directory.

WSUS est l'outil qui s'intercale entre Windows Update, plus adapté à une gestion discrète, et System Center Management Center prévu pour de grandes entreprises.

Dans une entreprise de moyenne importance disposant de bureaux distants, WSUS permet, si l'architecture le demande, d'utiliser plusieurs serveurs WSUS en cascade dont le premier sert de serveur maître.

WSUS supporte non seulement la distribution de mise à jour pour les systèmes d'exploitation Windows mais également pour d'autres produits comme SQL-Server, Exchange, Biztalk, etc. y compris le moniteur réseau. Il est également possible d'y ajouter d'autres produits.

## 1. Installation et configuration initiale de WSUS

Dans Windows Server 2008, WSUS est un rôle supplémentaire qu'il faut rechercher sur Internet.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** et **Gestionnaire de serveur**.
- Dans la zone **Résumé Serveur** du Gestionnaire de serveur, cliquez sur l'action **Rechercher de nouveaux rôles** de la section **Informations sur la sécurité**.
- Une boîte de dialogue vous informe qu'un ou plusieurs nouveaux rôles sont disponibles, cliquez sur **Ouvrir Windows Update**.
- Dans **Windows Update**, cliquez sur **Afficher les mises à jour disponibles**.
- Assurez-vous que **Mise à jour pour le Gestionnaire de serveur Windows Server 2008 (KB940518)** est sélectionnée puis cliquez sur **Installer**.
- Une fois les mises à jours installées et éventuellement après avoir redémarré le serveur, ouvrez le **Gestionnaire de serveur** puis cliquez sur **Rôles**.
- Cliquez sur **Ajouter des rôles**.
- Dans l'assistant, sélectionnez le rôle **Windows Server Update Services** puis cliquez sur **Suivant**. Si la boîte de dialogue **Ajouter les services de rôle requis pour l'installation de Windows Server Update Services** s'ouvre, cliquez sur **Ajouter les services de rôle requis**. Ensuite, cliquez deux fois sur **Suivant**.
- Contrôlez les services de rôles qui seront installés puis cliquez deux fois sur **Suivant**.
- Sur la page **Confirmation**, cliquez sur **Installer**.

- Dès que la partie IIS est installée, l'assistant d'installation de WSUS apparaît, cliquez sur **Suivant** pour commencer.
- Sur la page **Contrat de licence**, lisez le contenu de la licence avant de sélectionner l'option **j'accepte les termes du contrat de licence**, puis cliquez deux fois sur **Suivant**.
- Sur la page **Selectionner la source des mises à jour**, si vous désirez stocker localement les mises à jour, veillez à disposer d'un espace disque au format NTFS d'au moins 6 Go et modifiez éventuellement le dossier de stockage proposé. Ensuite, cliquez sur **Suivant**, sinon désélectionnez la case à cocher **Stocker les mises à jour localement**.
- Sur la page **Options de base de données**, vous pouvez utiliser la base de données SQL proposée et installée avec WSUS (défaut), éventuellement modifier le dossier de stockage, celui-ci doit être au format NTFS avec au minimum 2 Go. Vous pouvez également choisir d'utiliser un serveur de base de données SQL Server existant sur le même ordinateur ou un ordinateur distant. Ensuite, cliquez sur **Suivant**.
- Sur la page **Sélection du site Web**, vous pouvez soit utiliser le site Web par défaut existant (recommandé) soit créer un site Web pour WSUS, il utilisera un port différent du port 80 pour y accéder. Ensuite cliquez sur **Suivant**.
- Sur la page **Prêt pour l'installation de Windows Server Update Services 3.0 SP1**, contrôlez les informations de configuration avant de cliquer sur **Suivant**.
- L'installation commence. Une fois installé, l'assistant de configuration apparaît. Si vous désirez l'exécuter plus tard, vous pourrez toujours le faire via la console MMC en utilisant la page **Options**. Avant de cliquer sur **Suivant**, assurez-vous que les trois opérations citées sont déjà effectuées.
- Sur la page **S'inscrire au Programme d'amélioration de Microsoft Update**, si vous ne désirez pas participer désélectionnez la case à cocher puis cliquez sur **Suivant**.
- Sur la page **Choisir le serveur en amont**, il vous faut décider si le serveur se synchronise avec Windows Update ou via un autre serveur WSUS. Ensuite cliquez sur **Suivant**.
- Sur la page **Définir le serveur Proxy**, si vous en avez besoin remplissez les informations demandées sinon cliquez sur **Suivant**.
- Sur la page **Se connecter au serveur en amont**, cliquez sur **Démarrer la connexion** et attendez que le bouton **Suivant** s'active avant de cliquer dessus.
- Sur la page **Choisir les langues**, sélectionnez la ou les langues utilisées par les ordinateurs qui seront mis à jour par votre serveur WSUS, puis cliquez sur **Suivant**.
- Sur la page **Choisir les produits**, sélectionnez les applications qui pourront être mises à jour par le serveur WSUS puis cliquez sur **Suivant**.



Ne sélectionnez que les produits dont vous disposez, il peut être utile de désélectionner Windows 2000 si vous n'utilisez plus ce système d'exploitation.

- 
- Sur la page **Choisir les classifications**, indiquez quelles sont les mises à jour que vous allez effectuer via le serveur WSUS avant de cliquer sur **Suivant**. Par défaut Microsoft propose une classification minimale à utiliser, vous pouvez par exemple tout sélectionner puis décider par la suite des éléments que vous voulez mettre à jour.
  - Sur la page **Définir la planification de la synchronisation**, vous pouvez choisir une synchronisation manuelle ou la planifier jusqu'à une fois par heure, ensuite, cliquez sur **Suivant**.
  - Sur la page **Terminé**, vous pouvez désélectionner la synchronisation initiale avant de cliquer sur **Suivant**.
  - Sur la page **Et maintenant**, quelques sujets vous sont proposés afin d'améliorer l'utilisation du système, cliquez sur **Terminer**.
  - Vous revenez sur l'assistant **Ajout de rôles** et devez voir que l'installation a réussi. Cliquez sur **Fermer**.

Vous devez maintenant attendre la fin de la synchronisation pour voir les mises à jour et définir s'il faut les installer.

Il est également nécessaire d'installer la visionneuse de rapport Report Viewer (Microsoft Report Viewer 2005 Redistribuable) qu'il faut au préalable télécharger à partir du site de Microsoft.

Si l'approbation est automatique votre serveur est opérationnel. Dans le cas contraire, il faut le configurer comme nous le verrons dans le chapitre des travaux pratiques.

Concernant les clients WSUS, il faut maintenant utiliser les stratégies de groupe pour paramétrer la stratégie de groupe, du modèle d'administration Windows Update afin que les ordinateurs soient redirigés vers le serveur WSUS pour télécharger les mises à jour. C'est un exercice du chapitre réservé aux travaux pratiques.

# Baseline Security Analyser (MBSA)



MBSA est un outil simple adapté aux petites et moyennes entreprises permettant de déterminer si les recommandations concernant les éléments de sécurité définis par Microsoft sont installées sur les ordinateurs de l'entreprise. Dans le cas contraire, MBSA indique les moyens pour y remédier.

MBSA peut analyser les composants et logiciels suivants :

- Windows 2000, Windows XP, Windows 2003 et Windows 2008.
- Microsoft Internet Information Server (IIS) 5.0, 5.1, 6.0 et 7.0.
- Microsoft Internet Explorer 5.01, 5.5, 6.0 et 7.0

La version supportée par Windows Server 2008 est MBSA 2.1.

Il est possible de remplacer MBSA dans des entreprises plus importantes par WSUS qui sera introduit dans une prochaine section, ou par System Center Management Server dans des organisations encore plus importantes.

## 1. Installation de MBSA

- Il faut au préalable télécharger MBSA 2.1 à partir du site de Microsoft (<http://www.microsoft.com/mbsa>) puis double cliquer sur l'icône MBSASetup-x86-Fr.msi.
- Sur la page **Bienvenue dans l'outil Microsoft Baseline Security Analyzer**, cliquez sur **Suivant**.
- Sur la page **Contrat de licence**, lisez le contrat puis sélectionnez l'option **J'accepte le contrat de licence** avant de cliquer sur **Suivant**.
- Sur la page **Dossier de destination**, modifiez éventuellement l'emplacement du dossier de destination puis cliquez sur **Suivant**.
- Sur la page **Démarrer l'installation**, cliquez sur **Installer**, puis attendez la fin de l'installation pour voir apparaître la boîte de dialogue suivante et cliquez sur **OK**.



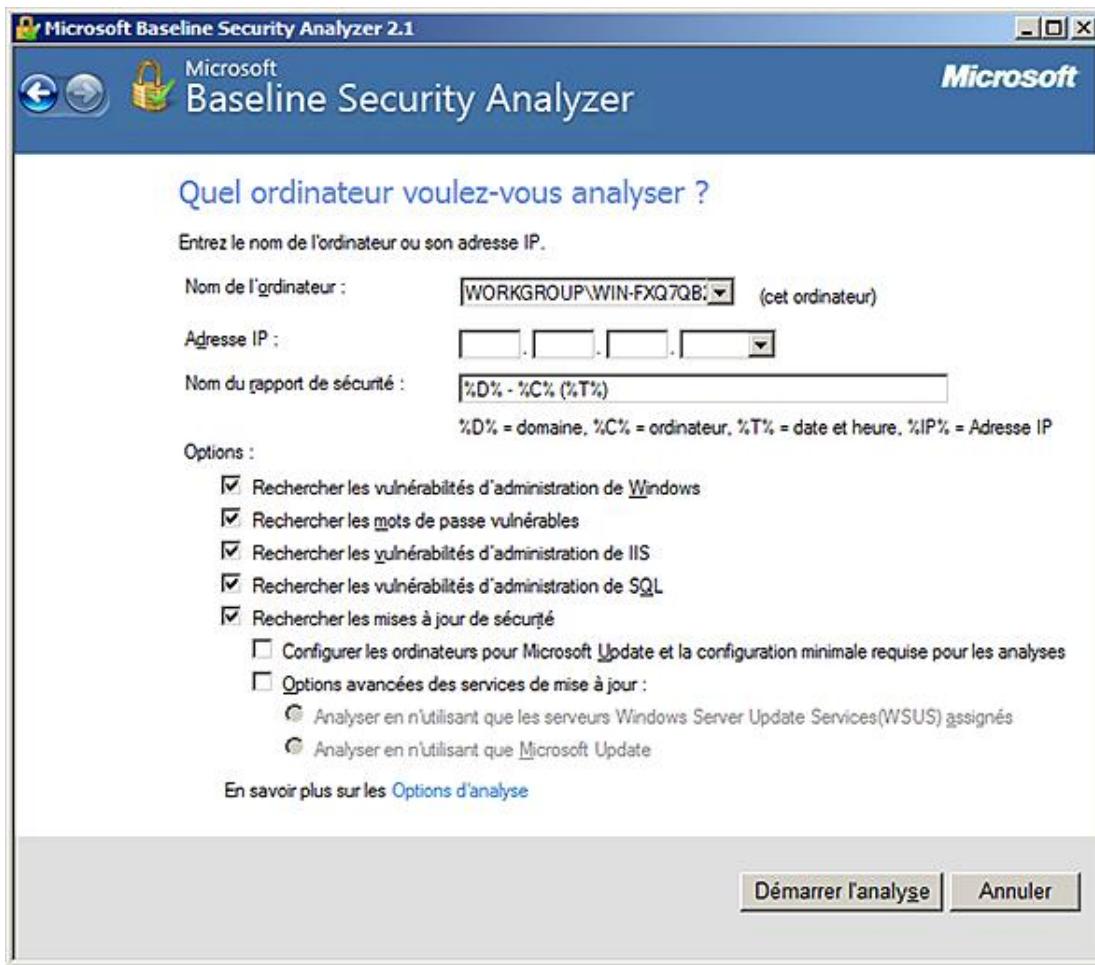
## 2. Lancement de l'analyse sur l'ordinateur local et affichage du rapport

Pour effectuer cette opération, il faut être connecté à l'Internet.

- Cliquez sur **Démarrer - Tous les programmes** et **Microsoft Baseline Security Analyzer 2.1**.
- Dans la fenêtre **Internet**, cliquez sur **Analyser un ordinateur**, soit sous **Tâches** à gauche, ou dans la partie

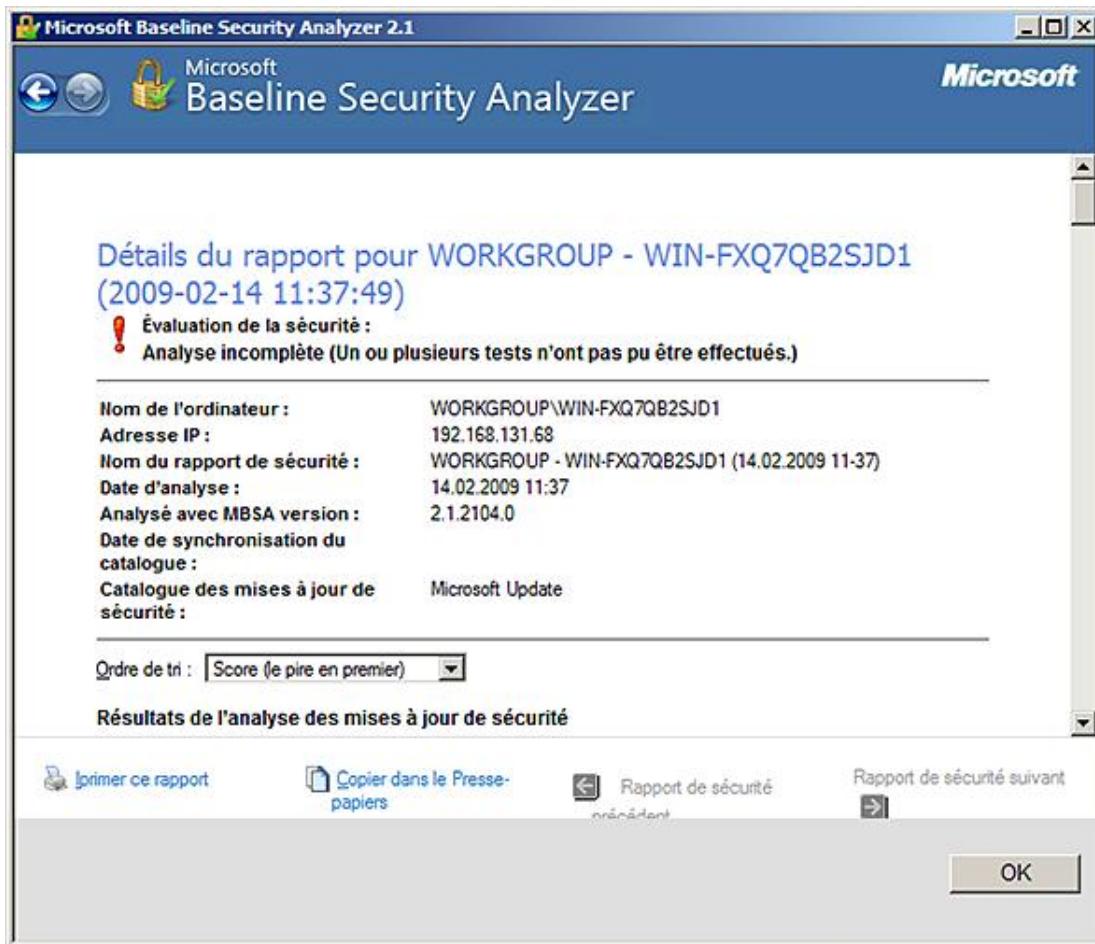
centrale.

- Sur la page suivante montrée ci-après, cliquez sur **Démarrer l'analyse**. Notez que par défaut toutes les options sont sélectionnées.



Si vous recevez un message d'erreur qui indique que le catalogue est endommagé, c'est que vous n'êtes pas connecté à Internet. L'analyse commence par télécharger le catalogue **wsusscn2.cab**, soit un fichier d'environ 13 Mo avant d'analyser l'ordinateur.

La page suivante montre le rapport détaillé. La première partie présente des informations issues de l'ordinateur qui a été analysé.



Puis, pour les sections suivantes, des informations en colonnes basées sur un score, une catégorie et un résultat.

Les scores sont les suivants :

Score	Catégorie	Résultat
	Windows - Mises à jour de sécurité	18 mises à jour de sécurité sont absentes. 1 Service Packs ou correctifs cumulatifs sont absents. <a href="#">Afficher les ressources analysées</a> <a href="#">Détails</a> <a href="#">Comment corriger le problème</a>

L'icône précédente correspond à un test critique qui a échoué. Il faudrait corriger le problème immédiatement car l'ordinateur présente un risque de sécurité maximal. Cela peut être une mise à jour de sécurité manquante, une configuration manquante, etc.

Dans tous les cas, vous pouvez savoir ce qui a été analysé sous **Afficher les ressources analysées** et obtenir les informations nécessaires pour corriger cet état sous **Détails**. Dans le cas où des patchs de sécurité sont manquants, les liens sont également donnés. Le lien **Comment corriger le problème** donne la procédure globale de résolution.

Score	Catégorie	Résultat
	Expiration des mots de passe	Certains comptes d'utilisateurs (3 sur 4) ont un mot de passe n'expirant pas. <a href="#">Afficher les ressources analysées</a> <a href="#">Détails</a> <a href="#">Comment corriger le problème</a>

Ce score correspond à un test qui a échoué mais qui n'est pas critique, donc un problème potentiel de sécurité. En fait l'élément est bien configuré mais ne correspond pas aux recommandations de sécurité Microsoft. La configuration actuelle peut avoir un sens dans certaines configurations. Concernant les correctifs cumulatifs et les services packs, ce score indique qu'ils sont manquants.

Score	Catégorie	Résultat
	SQL Server - Mises à jour de sécurité	Aucune mise à jour de sécurité n'est absente. <a href="#">Afficher les ressources analysées</a> <a href="#">Détails</a>

Ce score indique que l'élément analysé est conforme aux attentes de sécurité définies par Microsoft, il a donc réussi les tests.

Score	Catégorie	Résultat
	Services	Certains services potentiellement superflus sont installés. <a href="#">Afficher les ressources analysées</a> <a href="#">Détails</a> <a href="#">Comment corriger le problème</a>

Ce score indique une recommandation ou une information supplémentaire à mettre en œuvre pour augmenter la sécurité.

Score	Catégorie	Résultat
	État des services IIS	Les fichiers communs IIS ne sont pas installés sur l'ordinateur local. Vérifiez la configuration requise spécifiée dans l'aide en ligne de Microsoft Baseline Security Analyzer. <a href="#">Afficher les ressources analysées</a> <a href="#">Comment corriger le problème</a>

Ce score indique que l'analyse est impossible car un élément nécessaire à l'analyse est manquant. Cela ne signifie pas que c'est un risque potentiel pour la sécurité.

Score	Catégorie	Résultat
	Sécurité des macros	Aucun produit Microsoft Office pris en charge n'est installé.

Ce score indique que le test n'a pas été effectué pour la raison indiquée.

- Examinez avec soin chaque résultat puis évaluez son impact positif ou négatif sur votre ordinateur. Un test manqué peut être correct et normal dans certaines configurations.

### 3. Lancement en ligne de commande

Pour lancer MBSA en mode ligne de commande, il faut utiliser la commande **mbsacli.exe**. Il est possible de scanner un ordinateur, une étendue d'ordinateurs, un domaine ou de se baser sur un fichier de configuration. L'invite de commande permet de gérer plus efficacement les ordinateurs d'un parc réseau car elle peut être placée dans un script.

Exécute MBSA sur l'ordinateur local en omettant les tests indiqués :

```
mbsacli /n Password+IIS+SQL
```

Exécute MBSA pour les adresses IP spécifiées, le login à utiliser étant passé en paramètre :

```
mbsacli /r 172.30.1.100-172.30.1.150 /ld /u MyUser /p MyPassword
```

Lancement de l'analyse en mode déconnecté :

```
mbsacli /catalog c:\wsusscn2.cab /ia /nvc
```

Le catalogue wsusscn2.cab s'installe par défaut dans le dossier **C:\Users\Administrateur\AppData\Local\Microsoft\MBSA\2.1** lorsque vous lancez MBSA en mode graphique.

# Protocole SNMP



Le protocole SNMP (*Simple Network Management Protocol*) est un protocole de gestion utilisé pour surveiller des périphériques. Il est encore largement répandu et utilisé par différentes applications de surveillance dans des environnements gérés.

Conceptuellement, le périphérique surveillé, qui peut être un routeur physique, un switch, une imprimante réseau, un ordinateur, etc., s'appelle l'**agent SNMP** et il est en contact avec un ou plusieurs gestionnaires SNMP également appelés applications de console de gestion comme snmputil, MOM, SCOM, HP Openview, etc.

SNMP peut être utilisé pour :

- Configurer des périphériques distants à partir d'un système de gestion.
- Surveiller les performances du réseau à partir d'un système de gestion qui interroge régulièrement les périphériques.
- Déetecter des erreurs réseau ou des accès inappropriés à partir des agents qui envoient des messages au système de gestion lorsqu'un événement spécifique intervient.
- Auditer l'utilisation du réseau.

Une base de données appelée **MIB** (*Management Information Database*) décrit les objets ou les informations gérées par l'agent. Cette base est hiérarchique et débute toujours par l'espace de nom 1.3.6.1.4.1.311 pour les ordinateurs Windows Server 2008. Puis chaque objet utilise un identificateur d'objet appelé **OID** (*Object Identifier*) pour garantir son unicité.

SNMP utilise le protocole UDP pour communiquer entre les agents et le système de gestion. Pour disposer de plusieurs systèmes de gestion et faciliter l'administration des agents, il faut créer des communautés, soit des groupes auxquels appartiennent les agents et les systèmes de gestion, afin que l'agent ne réponde qu'aux demandes des systèmes de gestion provenant des communautés auxquelles il appartient.

Les commandes utilisées sont simples. Le système de gestion utilise **Get-Request**, **Get-next-request**, **GetBulk-request** et **Set-Request** alors que l'agent répond aux demandes avec **Get-Response** ou envoie des messages aux systèmes de gestion en utilisant **Trap**.

## 1. Installation du protocole SNMP

Le protocole SNMP est une fonctionnalité. Dans Windows Server 2008, il est possible d'installer l'agent SNMP, ainsi qu'une interface de programmation sous WMI afin d'automatiser certaines recherches dans des scripts par exemple.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** et **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur **Fonctionnalités**.
- Sur la page principale **Fonctionnalités**, cliquez sur **Ajouter des Fonctionnalités**.
- Sélectionnez **Services SNMP**. Éventuellement, désélectionnez **Fournisseur WMI SNMP** si vous ne désirez pas permettre l'envoi d'interruptions SNMP en tant qu'événements WMI. Ensuite cliquez sur **Suivant**.
- Sur la page de **Confirmation**, contrôlez les éléments qui seront installés avant de cliquer sur **Installer**.
- Attendez la fin de l'installation pour contrôler que l'installation est effectuée correctement.
- Avant le Service Pack 1 de Windows Server 2008, il existe un bug qui initialise incorrectement le service SNMP. Vous

pouvez le vérifier en ouvrant le journal Application de l'observateur d'événements qui fait apparaître les événements d'erreurs ou d'avertissemens suivants. Il est nécessaire de télécharger et d'appliquer le correctif **950923**.

Application 3'280 Événements				
Niveau	Source	ID de l'événement	Catégorie de la tâche	Date et heure
Information	SRMSVC	8202	Aucun	22.02.2009...
Information	SRMSVC	8202	Aucun	22.02.2009...
Information	EvntAgnt	2020	Aucun	22.02.2009...
Erreur	EvntAgnt	2019	Aucun	22.02.2009...
Erreur	EvntAgnt	1020	Aucun	22.02.2009...
Erreur	EvntAgnt	2019	Aucun	22.02.2009...
Avertissement	EvntAgnt	3001	Aucun	22.02.2009...
Avertissement	EvntAgnt	3001	Aucun	22.02.2009...
Erreur	EvntAgnt	3003	Aucun	22.02.2009...
Information	MSSQLSERVER	958 (2)		22.02.2009...

- Sur un Server Core, il n'est possible que d'installer le service SNMP.

## 2. Configuration de l'agent SNMP

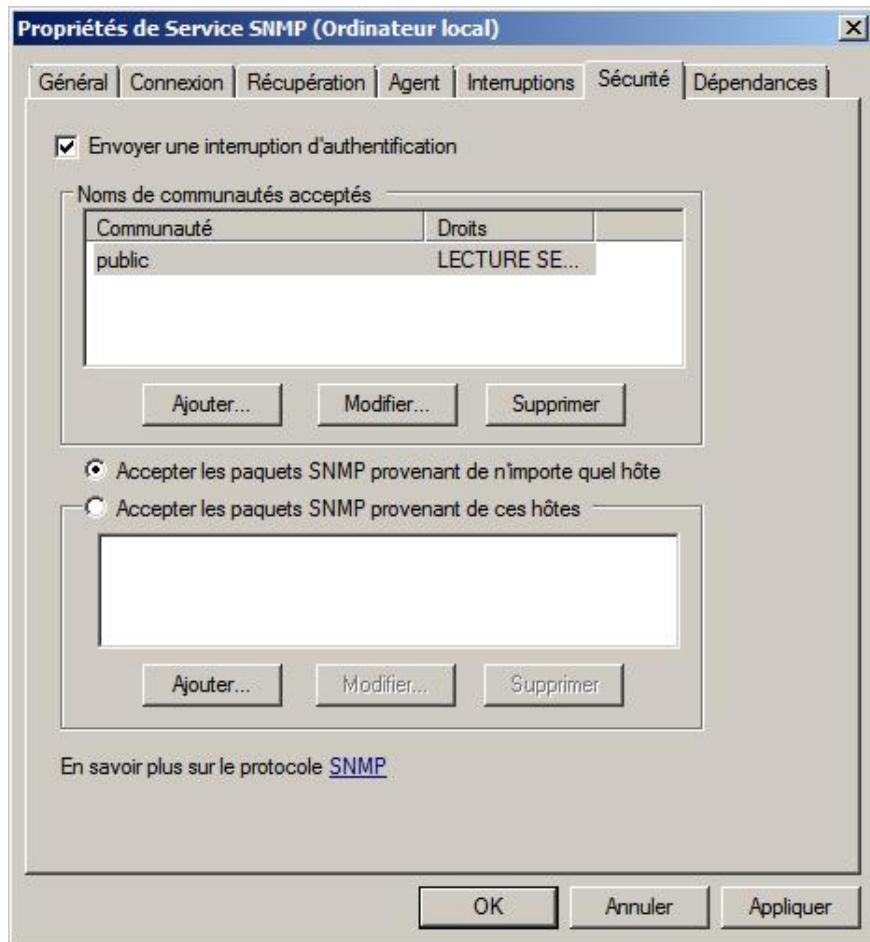
La configuration de l'agent SNMP utilise des onglets supplémentaires attachés à l'application services.msc.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration et Services**.
- Dans la liste des services, cliquez avec le bouton droit de la souris sur **Propriétés de Services SNMP**.
- Sélectionnez l'onglet **Agent** pour définir le contact soit le nom de l'administrateur, l'emplacement physique ainsi que les informations sur les services que gère l'hôte SNMP.

**Physique** indique que l'ordinateur gère des périphériques physiques comme un disque dur. **Applications** pour des applications TCP/IP tournant sur l'ordinateur. **Liaison de données et sous-réseau** si l'ordinateur est utilisé comme pont réseau. **Internet** pour indiquer qu'il s'agit d'un routeur et **Bout en bout** pour indiquer qu'il s'agit d'un hôte IP.

- Sélectionnez l'onglet **Interruptions** pour définir les communautés auxquelles appartient l'hôte. Par défaut il appartient à la communauté **public**. Pour chaque communauté, vous pouvez définir le ou les systèmes de gestion qui vont recevoir les interruptions (messages Trap) provenant de l'agent.
- Sélectionnez l'onglet **Sécurité** pour définir si l'agent doit répondre à toutes les demandes. Il est d'usage de garantir un minimum de sécurité afin de ne répondre qu'aux messages des communautés nommées explicitement et d'y ajouter les droits correspondants. Vous pouvez également restreindre les demandes à certains hôtes.

Les droits sont **Aucun** pour ne pas répondre, **Notifier** pour envoyer des interruptions, **Lecture seule** pour répondre à des demandes d'objets, **Lecture Ecriture** comme Lecture seule mais permettant également de modifier le contenu de l'objet et **Lecture Création** comme Lecture Ecriture mais également permettant de créer de nouveaux objets.



# Introduction au Moniteur réseau



Le moniteur réseau est un outil indispensable qui permet d'analyser les trames qui circulent sur un réseau. Bien que d'apparence simple, l'interprétation des trames peut vite s'avérer difficile car il est nécessaire de connaître la structure des trames se rapportant aux protocoles applicatifs pour en déterminer la signification. Dans cette section, vous apprendrez à reconnaître les éléments principaux des trames jusqu'au niveau de la couche 4 du modèle OSI (*Open System Interconnection*).

Il permet l'analyse de trames provenant d'une connexion réseau LAN (*Local Area Network*) câblée, d'une connexion RAS/VPN ou d'une connexion sans fil (Wi-Fi). Quel que soit le type de connexion, il faut savoir qu'il écoute toutes les trames de diffusion, de multidiffusion, de monodiffusion dont il est l'émetteur ou le destinataire. Pour écouter une trame monodiffusion adressée à un autre ordinateur, il faut activer le mode **promiscuité** appelé ici **P-mode**. Bien entendu, si l'ordinateur exécutant le moniteur réseau est relié à un **switch**, il faut également configurer sur ce dernier le port qui est relié à votre serveur d'analyse afin que toutes les trames passant sur le switch lui soient renvoyées en activant le mode promiscuité.

- Si vous installez le moniteur réseau dans un environnement virtuel, il faut faire attention à la portée de chaque type de switch virtuel créé, car l'écoute, et donc le trafic analysé, peut être totalement différente.

## 1. Installation du moniteur réseau

Il vous faut au préalable télécharger la bonne version du Microsoft Network Monitor, soit au minimum la version 3.2 du centre de téléchargement de Microsoft. Seule la version anglaise est disponible.

- Double cliquez sur l'icône **NM32\_AAA\_setup.exe** pour démarrer l'installation. Remplacez **AAA** par l'édition 32 ou 64 bits.
- Dans la boîte de dialogue vous avertissant que vous allez installer le moniteur réseau, cliquez sur **Oui**.
- Sur la page de bienvenue de l'assistant, cliquez sur **Next**.
- Sur la page de la licence, lisez l'agrément, sélectionnez l'option **I accept the terms in the licence agreement** puis cliquez sur **Next**.
- Sur la page **Use Microsoft Update to help keep your computer secure and up to date**, sélectionnez une des options puis cliquez sur **Next**.
- Sur la page **Choose a setup type**, cliquez sur l'icône **Complete**.
- Sur la page **Ready to install**, cliquez sur **Install**. Ensuite l'installation commence.
- Sur la page **Completing the Setup Wizard**, contrôlez que l'installation s'est correctement déroulée puis cliquez sur **Finish**.

- Bien qu'il soit possible de lancer le moniteur réseau avec n'importe quelle identité, il est nécessaire de le lancer avec les droits d'administration pour pouvoir réaliser une capture.

## 2. Capture et analyse

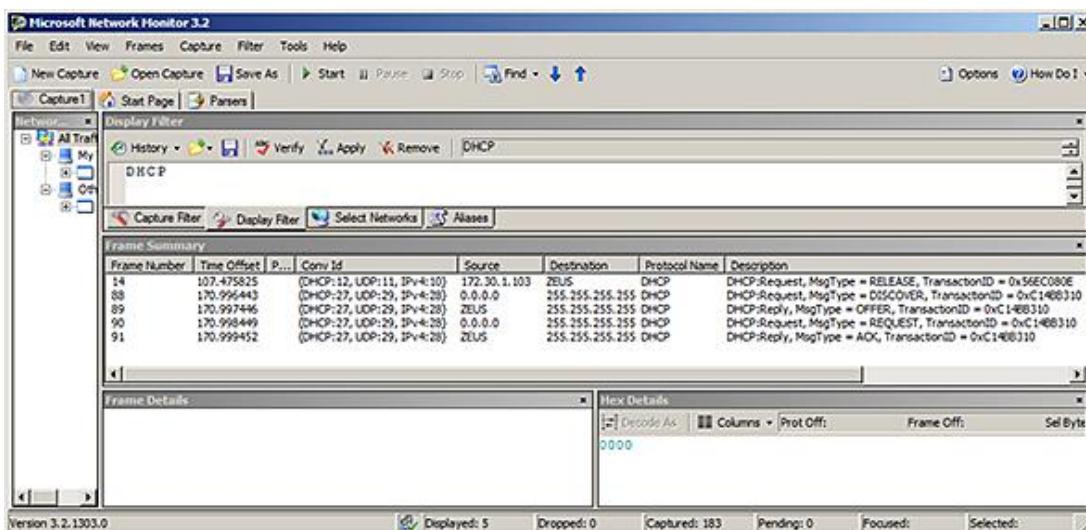
- Démarrez le moniteur réseau en cliquant avec le bouton droit de la souris sur l'icône **Microsoft Network Monitor**

### 3.2

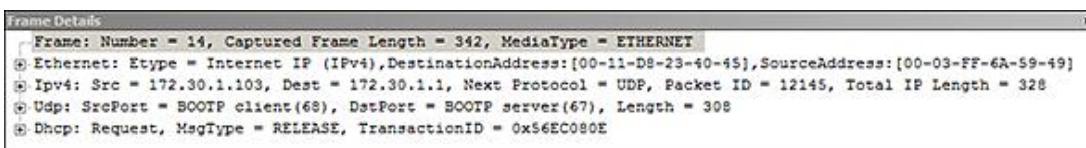


puis sur **Exécuter en tant qu'administrateur**.

- Si la boîte de dialogue **Microsoft Update Opt-In** apparaît, désélectionnez éventuellement la case à cocher puis cliquez soit sur **Yes** ou sur **No**.
- Dans la région **Select a Network**, contrôlez que la connexion au réseau local est bien sélectionnée.
- Dans la barre d'outils, cliquez sur **New Capture**.
- Dans la barre d'outils, cliquez sur **Start**. Les trames capturées s'affichent dans la région **Frame Summary**.
- Ouvrez une invite de commande puis saisissez **ipconfig /release** et appuyez sur [Entrée] ensuite saisissez **ipconfig /renew** puis appuyez sur [Entrée].
- Retournez dans le moniteur réseau et cliquez sur **Stop** dans la barre d'outils.
- Dans la région **Frame Summary**, vous notez un nombre important de trames qui ont été capturées, il est nécessaire d'utiliser un filtre pour n'afficher que celles qui nous intéressent à savoir, celles utilisant le protocole **DHCP**. Pour cela, cliquez dans la région **Display Filter**, puis saisissez uniquement **DHCP** et cliquez dans la barre d'outils de la région **Display Filter** sur **Apply**. Les trames suivantes devraient apparaître.



- Cliquez sur la première trame DHCP. Les régions **Frame Details** affichent le contenu en fonction de la couche du modèle OSI, et **Hex Details**, qui affiche les octets de la trame, exprimés soit en hexadécimal soit en ASCII, se remplissent. Examinez que la trame DHCP utilise la couche 2 (Ethernet), la couche 3 (IPv4), la couche 4 (UDP) et la couche applicative du modèle TCP/IP reprenant les couches 5, 6 et 7 du modèle OSI (DHCP). Si vous cliquez sur **Frame**, vous obtenez les informations de la Frame soit la longueur en octets et le type : **Ethernet**.



- En cliquant sur le nœud **Ethernet**, il est possible de déterminer les **adresses MAC** source et destination (elles sont situées dans le même réseau de diffusion), ainsi que le protocole qui sera utilisé dans la couche au dessus (IPv4 0x800), ainsi que le nombre d'octets restants.
- En cliquant sur le nœud **IPv4**, il est possible de déterminer les adresses IP source et de destination, le TTL (*Time To Live*) qui donne une indication sur le nombre de routeurs passés si la valeur est inférieure à 128 pour un ordinateur Windows, ainsi que le protocole qui sera utilisé dans la couche au-dessus.

- En cliquant sur le nœud **Udp**, il est possible de connaître le port source et le port de destination.
- Enfin, en cliquant sur le nœud **Dhcp**, il est possible de connaître des informations propres au protocole applicatif utilisé. Ici, il s'agit du protocole **Dhcp**, et le type de message est DHCP Release.



The screenshot shows the 'Frame Details' pane of NetworkMiner. The selected frame is a DHCP message (Frame 14) with the following details:

- Ethernet:** Etype = Internet IP (IPv4), DestinationAddress:[00-11-D8-23-40-45], SourceAddress:[00-03-FF-6A-59-49]
- Ipv4:** Src = 172.30.1.103, Dest = 172.30.1.1, Next Protocol = UDP, Packet ID = 12145, Total IP Length = 328
- Dhcp:** Request, MsgType = RELEASE, TransactionID = 0x56EC080E
- OpCode:** Request, 1(0x01)
- HardwareType:** Ethernet
- HardwareAddressLength:** 6 (0x6)
- HopCount:** 0 (0x0)
- TransactionID:** 1458309134 (0x56EC080E)
- Seconds:** 768 (0x300)
- Flags:** 0 (0x0)
  - ClientIP:** 172.30.1.103
  - YourIP:** 0.0.0.0
  - ServerIP:** 0.0.0.0
  - RelayAgentIP:** 0.0.0.0
- ClientHardwareAddress:** 00-03-FF-6A-59-49
- ServerHostName:**
- BootFileName:**
- MagicCookie:** 99.130.83.99
- MessageType:** RELEASE - Type 53
- ServerIdentifier:** 172.30.1.1 - Type 54
- clientID:** (Type 1) - Type 61
- End:**

### 3. Sélection des interfaces et du mode promiscuité

- Démarrez le moniteur réseau en cliquant avec le bouton droit de la souris sur l'icône **Microsoft Network Monitor**
- 3.2  puis sur **Exécuter en tant qu'administrateur**.
- Dans la région **Select a Network**, cliquez dans la barre d'outils sur **P-Mode**. Vous pouvez également double cliquer sur la connexion réseau où il faut activer le mode promiscuité pour activer la case à cocher **P-Mode** de la boîte de dialogue qui apparaît.

### 4. Lancement en mode ligne de commandes

Vous pouvez utiliser la commande **nmcap.exe** pour capturer des trames. La commande est plus efficace et performante que son homologue graphique. Voici un exemple qui enregistre toutes les trames TCP de toutes les cartes réseaux dans un fichier. Pour arrêter la capture, appuyez sur [Ctrl]+C.

```
nmcap /network * /capture tcp /File c:\tcp.cap
```

# Observateur d'événements



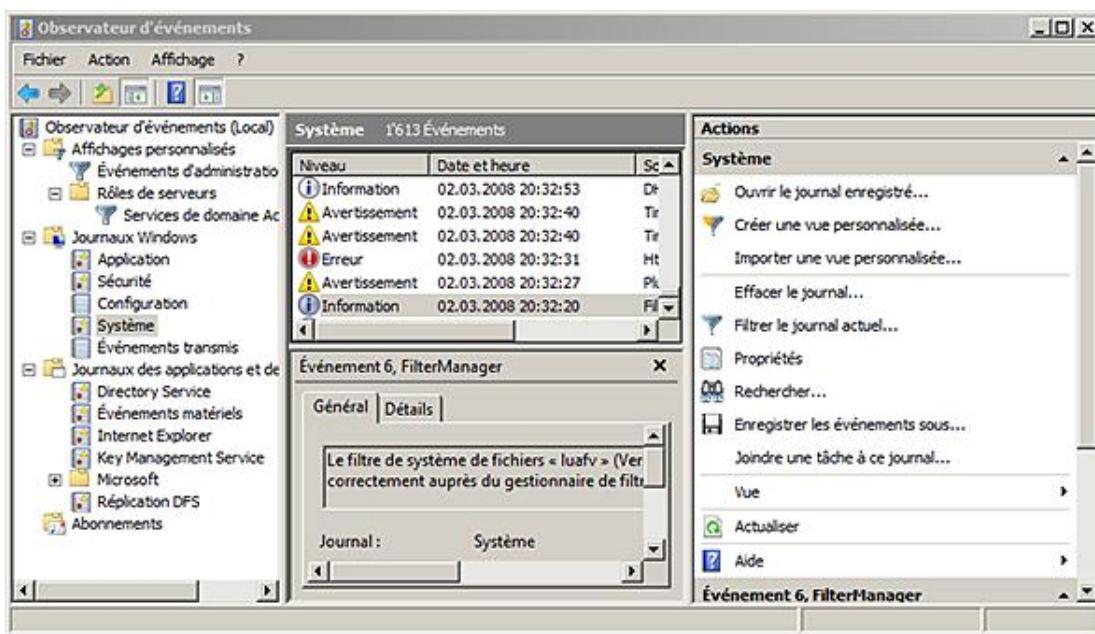
L'Observateur d'événements permet d'afficher les différents journaux des événements créés par le système d'exploitation : la sécurité ou les applications.

Un événement est généré par l'application ou le système durant son exécution si le développeur a inclus les instructions correspondantes afin d'indiquer une information utile à l'administrateur. Une lecture attentive soit manuelle, soit automatique avec l'aide de logiciels comme **SCOM** (*System Center Operation Manager*) permet de détecter et/ou de résoudre rapidement des problèmes.

Dans Windows Server 2008, il est également possible de centraliser les événements vers un serveur particulier.

## 1. Ouverture de l'Observateur d'événements local ou distant

- Connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.
- Cliquez sur **Démarrer - Outils d'administration - Observateurs d'événements**.



## 2. Ouverture des journaux

Dans Windows Server 2008, le nombre de journaux a augmenté et en plus des journaux déjà disponibles dans les versions précédentes, à savoir :

- **Système** qui contient des événements provenant du système d'exploitation.
- **Sécurité** qui contient les tentatives d'ouverture de session et l'accès à des ressources.
- **Application** qui contient les événements provenant des applications.

Il contient également les journaux suivants :

- **Événements transmis** qui sont les événements collectés provenant d'autres ordinateurs.

- **Configuration** qui contient des informations sur l'installation des applications.

De plus, les Journaux des applications et des services constituent une nouvelle catégorie de journaux des événements. Ils contiennent des événements provenant d'une application ou d'un composant système. Ils sont divisés en quatre types :

- **Journal d'administration**, principalement destiné à l'utilisateur final, il fournit des informations pour la résolution du problème.
- **Journal opérationnel** qui permet d'analyser et de diagnostiquer un problème en démarrant un programme par exemple.
- **Journal d'analyse** qui décrit le fonctionnement d'un programme.
- **Journal de débogage** qui par défaut est caché. Il permet à des développeurs d'isoler et de résoudre des problèmes applicatifs. Pour afficher ces journaux et les journaux d'analyse, il faut cliquer sur l'action **Afficher les journaux d'analyse et de débogage** du menu **Affichage**. Ensuite, il faut les activer en passant par les **Propriétés** du journal, en sélectionnant **Activer la journalisation**.

---

 Il existe des journaux spécialisés pour un nombre important de composants du système d'exploitation.

---

 Dès qu'un rôle a une fonctionnalité qui dispose d'un fichier de log compatible avec l'observateur d'événements, celui-ci est automatiquement visible dans les journaux des applications et de services comme le serveur DNS ou PowerShell.

---

### 3. Affichage d'un événement

- Dans le volet gauche de l'**Observateur d'événements**, cliquez sur le journal souhaité.

Les événements apparaissent dans la fenêtre principale. Cette fenêtre est divisée en deux, la partie haute affiche la liste des événements et la partie basse affiche les informations concernant l'événement sélectionné.

Par défaut, la vue simplifiée affichée dans l'onglet **Général** vous fournit déjà une description de l'événement et beaucoup d'informations comme le montre la prochaine image. Néanmoins si vous devez approfondir votre recherche, il faut utiliser l'onglet **Détails** dans lequel vous pourrez visualiser d'autres paramètres comme :

- L'ID du processus.
- L'ID du thread.
- L'ID du processeur.
- L'identificateur de session.
- Le temps d'exécution pour les instructions en mode noyau, exprimé en unité de temps processeur.
- Le temps d'exécution pour les instructions en mode utilisateur, exprimé en unité de temps processeur.
- Le temps d'exécution pour les instructions, exprimé en unité de temps processeur.
- L'ID de corrélation qui montre les relations entre les événements.
- L'identificateur de corrélation relatif qui identifie une activité associée dans un processus avec lequel l'événement est impliqué.

Si vous devez rechercher des événements basés sur ces paramètres, il est conseillé de modifier le filtre XML pour les faire apparaître dans une vue filtrée, d'utiliser un outil tiers ou de les importer dans une base de données et de les filtrer à l'aide de requêtes SQL.

L'écran suivant s'affiche en cliquant sur le lien **Propriétés de l'événement** dans le volet droit ou en double cliquant sur l'événement :



**Journal** : nom du journal dans lequel l'événement a été enregistré.

**Source** : logiciel ayant enregistré l'événement.

**Événement** : ID de l'événement.

**Niveau** : **Information** indique qu'une modification s'est produite généralement suite à un succès. **Avertissement** indique qu'une erreur s'est produite ; bien que bénigne, elle peut dégénérer en erreur si aucune action n'est entreprise. **Erreur** indique qu'une erreur s'est produite ; plus grave que l'avertissement, elle peut dégénérer en critique si aucune action n'est entreprise. **Critique** indique qu'une erreur s'est produite. **Succès de l'audit** indique que l'accès a été autorisé. **Échec de l'audit** indique qu'une tentative d'accès en échec a été enregistrée.

**Utilisateur** : nom de l'utilisateur à l'origine de l'événement.

**Code opérationnel (Opcode)** : valeur numérique qui identifie l'activité ou un point précis de l'activité.

**Informations** : permet d'afficher des informations supplémentaires provenant du TechNet sur l'événement.

**Connecté** : date et heure de l'enregistrement de l'événement.

**Catégorie** : représente un sous-composant ou une activité. Est utilisé par certains événements.

**Mots-clés** : mots-clés définis par les programmeurs.

**Ordinateur** : nom de l'ordinateur sur lequel l'événement est apparu.

En dépannage, il n'est pas évident de trouver la signification d'un événement. Vous pouvez consulter l'aide en ligne, la bibliothèque du TechNet, les kits de ressources techniques mais également le site Web [www.eventid.net](http://www.eventid.net) dont la partie gratuite peut déjà vous indiquer des pistes de recherche.

## 4. Créer une vue personnalisée

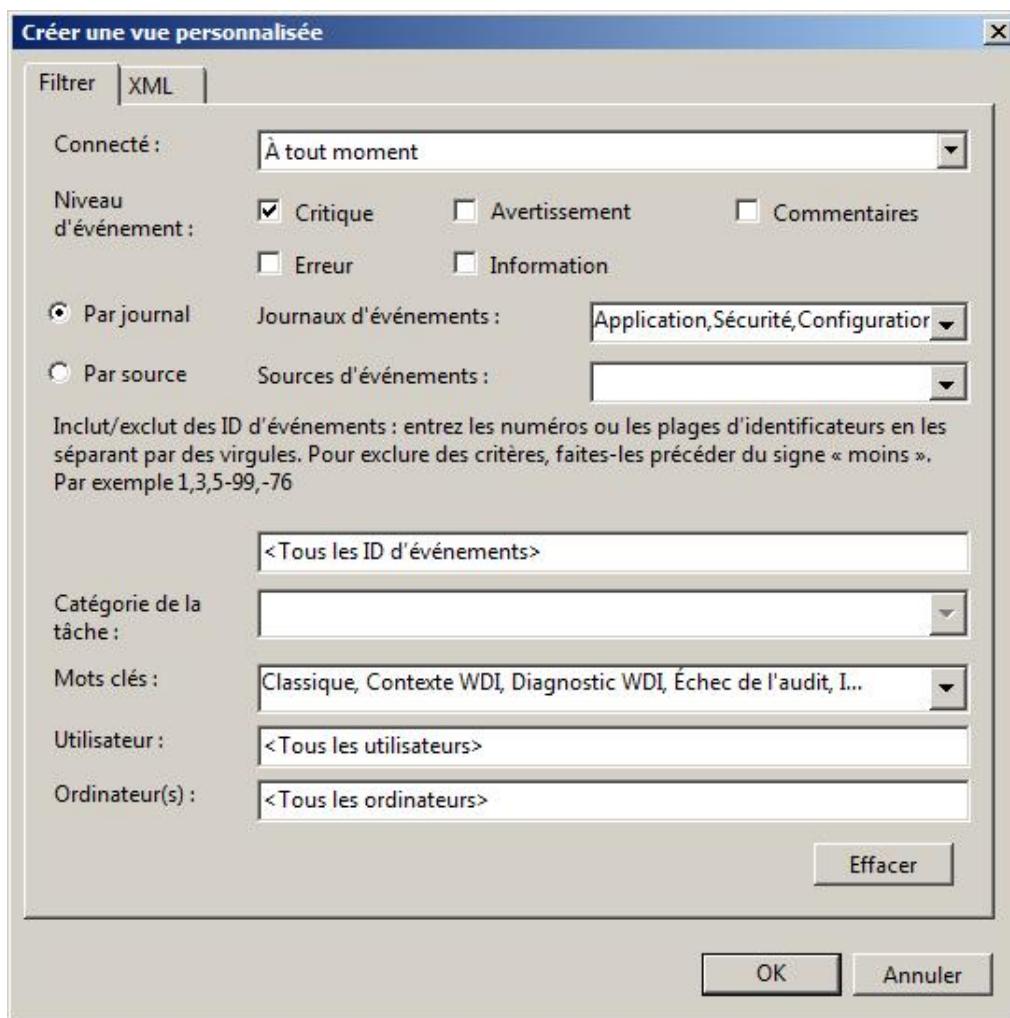
Dans Windows Server 2008, la méthodologie pour la lecture des événements a été modifiée de manière à ce que l'administrateur crée ses propres vues pour le traitement des événements.

Pour créer une vue personnalisée :

- Dans le volet gauche de l'**Observateur d'événements**, cliquez avec le bouton droit de la souris sur **Affichages personnalisés** puis cliquez sur **Créer une vue personnalisée**.

- Dans la boîte de dialogue **Créer une vue personnalisée**, dans l'onglet **Filtrer** sélectionnez les éléments correspondant à la vue souhaitée ou ajoutez un filtre XML en cliquant sur l'onglet **XML**.

### Onglet Filtrer



L'option **Connecté** permet de définir la plage temporelle pour l'affichage des événements, celle-ci peut être prédéfinie ou personnalisée.

**Niveau d'événement** permet de sélectionner les événements selon le niveau de gravité de l'événement.

**Par journal** permet de créer un filtre d'affichage des événements non limité à un journal.

**Par source** permet de créer un filtre sur une source d'événements précise.

---

Vous ne pouvez filtrer que par journal ou par source mais pas sur les deux critères en même temps.

---

La zone de saisie **Inclut/exclut des ID d'événements** permet de définir quels événements vous voulez inclure ou exclure en utilisant leur ID. Pour exclure un événement, saisissez le signe moins devant l'ID de l'événement. Séparez les ID par une virgule.

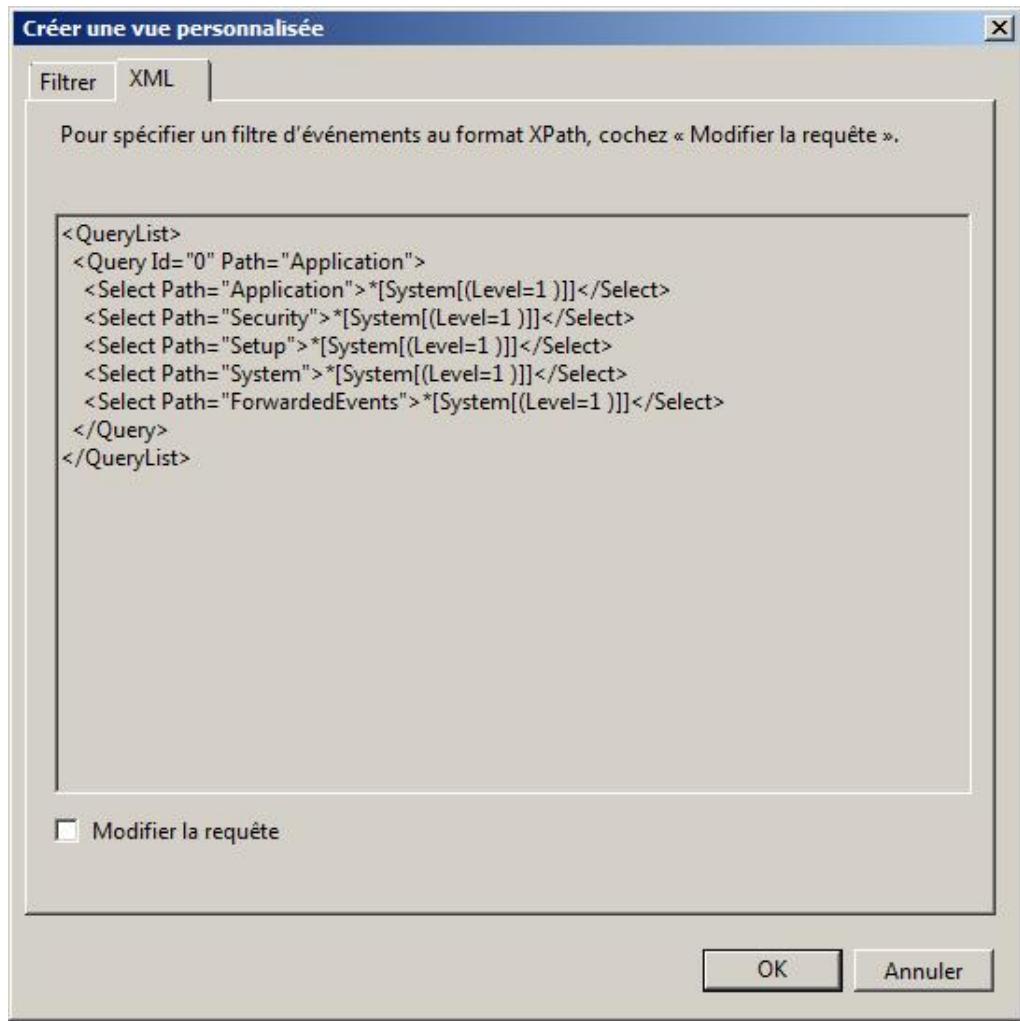
**Catégorie de la tâche** permet de filtrer sur un sous-composant ou une activité.

**Mots clés** permet de filtrer sur les mots clés définis dans les événements.

**Utilisateur** permet de filtrer par utilisateur.

**Ordinateur** permet de filtrer par ordinateur.

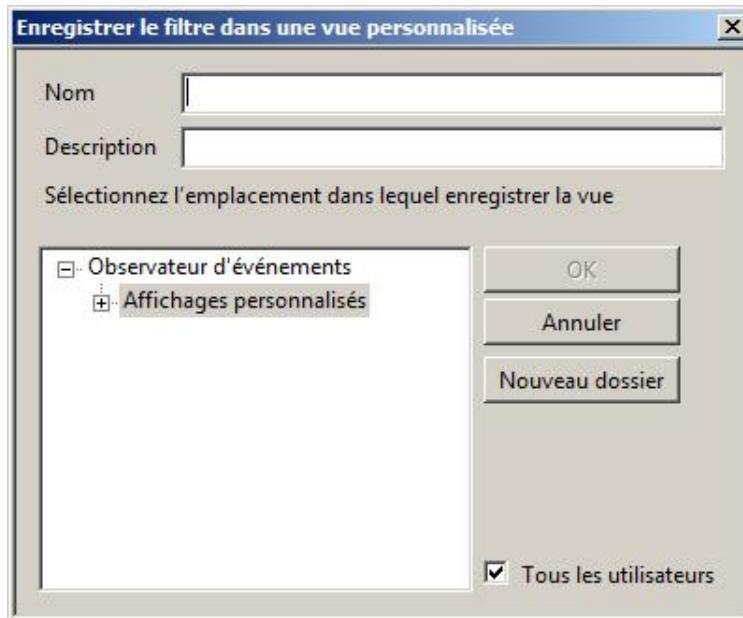
### Onglet XML



Dans cet onglet, vous pouvez **Modifier la requête** en cochant la case correspondante.

■ Enregistrez la vue.

Lorsque vous validez les options du filtre, la boîte de dialogue **Enregistrer le filtre dans une vue personnalisée** s'affiche à l'écran.



- Saisissez le **Nom** de la vue personnalisée et éventuellement une **Description**. Par défaut, la vue est enregistrée dans le dossier **Affichages personnalisés** mais vous pouvez créer des sous-dossiers afin d'organiser vos vues. Enfin, cliquez sur **OK**.

Vous pouvez à tout moment modifier votre vue en cliquant sur l'option **Propriétés** du menu contextuel de la vue.

## 5. Filtrer et rechercher un événement

Filtrer un journal permet d'afficher uniquement les événements qui correspondent à des critères comme pour une vue personnalisée, à la différence que le filtre est temporaire. Le filtre à utiliser est identique à celui utilisé pour une vue personnalisée.

Pour cela, cliquez sur le lien **Filtrer le journal actuel** dans le volet droit Actions.

- 
- Il est possible d'enregistrer le filtre en tant qu'affichage personnalisé.

Dans ce même volet, le lien **Rechercher** permet d'afficher un à un les événements selon une valeur de recherche. Cette valeur est une chaîne de caractères et la recherche s'effectue dans tous les paramètres de l'événement.

## 6. Associer une tâche à un événement

Associer une tâche à un événement est une des méthodes pour planifier une tâche dont le déclencheur est l'événement. Cette méthode n'offre pas la souplesse de l'assistant car il n'est pas possible de modifier le journal, la source et l'ID de l'événement. Pour bénéficier de toutes les possibilités, il faut utiliser le Planificateur de tâches.

Il est possible d'associer une tâche à une vue personnalisée.

- Cliquez avec le bouton droit de la souris sur l'événement puis cliquez sur **Joindre une tâche à cet événement**.
- Sur la page **Créer une tâche de base** de l'**Assistant Créer une tâche de base**, saisissez un **Nom** et éventuellement une **Description** avant de cliquer sur **Suivant**.
- Sur la page **Si un événement spécifique est enregistré**, cliquez sur **Suivant**.
- Sur la page **Action**, sélectionnez un des trois types d'action possibles puis cliquez sur **Suivant**.
- En fonction de l'action choisie, remplissez la page de l'action correspondante puis cliquez sur **Suivant**.
- Sur la page **Terminer**, contrôlez les informations. Vous pouvez faire apparaître la page **Propriétés** de la nouvelle tâche si vous sélectionnez la case à cocher **Ouvrir les propriétés de cette tâche quant j'aurai cliqué sur Terminer**. Si tout est correct, cliquez sur **Terminer**.

Les tâches sont enregistrées dans le dossier Tâches de l'Observateur d'événements de la bibliothèque du planificateur.

## 7. Centraliser des événements

Pour centraliser des événements, il faut disposer d'un ordinateur fonctionnant au moins sous Windows Vista ou Windows Server 2008.

Il faut préparer les ordinateurs pour transférer et recueillir les événements, puis il faut créer des abonnements.

Il est possible d'effectuer cette procédure dans un domaine ou dans un groupe de travail, bien que la procédure soit dans ce dernier cas plus délicate à mettre en œuvre.

Pour configurer l'ordinateur qui collecte les événements (collecteur) :

- Connectez-vous en tant qu'administrateur sur l'ordinateur collecteur.
- Ouvrez une invite de commandes avec les priviléges élevés.

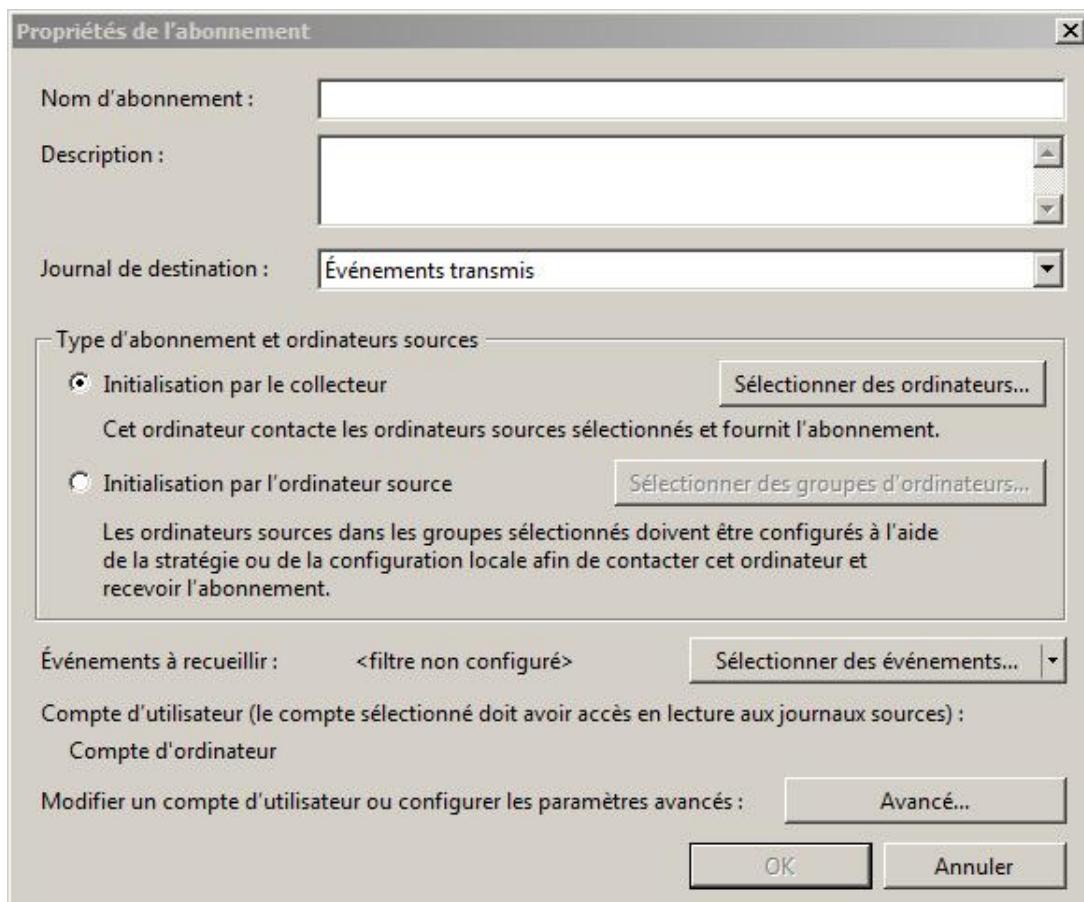
- Saisissez **wecutil qc** dans l'invite de commandes.

Pour configurer l'ordinateur sur lequel seront collectés les événements (source) :

- Connectez-vous en tant qu'administrateur sur l'ordinateur source.
- Ouvrez une invite de commandes avec les privilèges élevés.
- Saisissez **winrm quickconfig** dans l'invite de commandes.
- Vous devez ajouter le compte de l'ordinateur collecteur au groupe local **Administrateurs**.

Pour s'abonner à un événement :

- Connectez-vous en tant qu'administrateur sur l'ordinateur collecteur et ouvrez l'**Observateur d'événements**.
- Dans le volet gauche de l'**Observateur d'événements**, cliquez avec le bouton droit de la souris sur **Abonnements** puis cliquez sur **Créer un abonnement**. Si le service Collecteurs d'événements n'est pas démarré, vous serez invité à le faire démarrer pour continuer.
- Dans la boîte de dialogue **Propriétés de l'abonnement**, saisissez les informations nécessaires puis cliquez sur **OK**.



Saisissez au moins un **Nom d'abonnement**, voire une **Description**. Indiquez le **Journal de destination** du collecteur des événements.

Vous pouvez sélectionner l'ordinateur ou les ordinateurs source en cliquant sur **Initialisation par le collecteur** puis sur **Sélectionner des ordinateurs**. L'autre possibilité est de permettre l'**Initialisation par l'ordinateur source**, c'est-à-dire de configurer les ordinateurs sources à l'aide d'une stratégie de groupe pour qu'ils contactent l'ordinateur collecteur. Il faut configurer l'ordinateur collecteur de manière à ne pas recevoir des événements provenant d'ordinateurs non désirés.

Vous pouvez filtrer les événements à recueillir avec un filtre identique à celui d'une vue personnalisée.

Enfin, les paramètres avancés permettent de définir le protocole à utiliser pour transmettre les événements, le protocole HTTP ou le protocole HTTPS. Vous pouvez également définir l'utilisation de la bande passante selon un des paramètres suivants :

- Normale
- Réduire la bande passante
- Minimiser la latence
- Personnalisée

## 8. Cadre d'utilisation

Les événements produits par le système devraient systématiquement être traités par l'administrateur soit manuellement, ou mieux automatiquement pour la plupart des événements, et manuellement pour une petite partie.

Pour l'automatisation, vous pouvez utiliser une base de données dans laquelle vous importez et gérez les événements à l'aide d'ordres SQL mais vous pouvez également utiliser des outils comme SCOM qui offrent l'avantage de pouvoir être programmés pour réagir immédiatement à l'arrivée d'un événement particulier, ce qui vous amène vers une gestion proactive.

# Moniteur de fiabilité et de performances

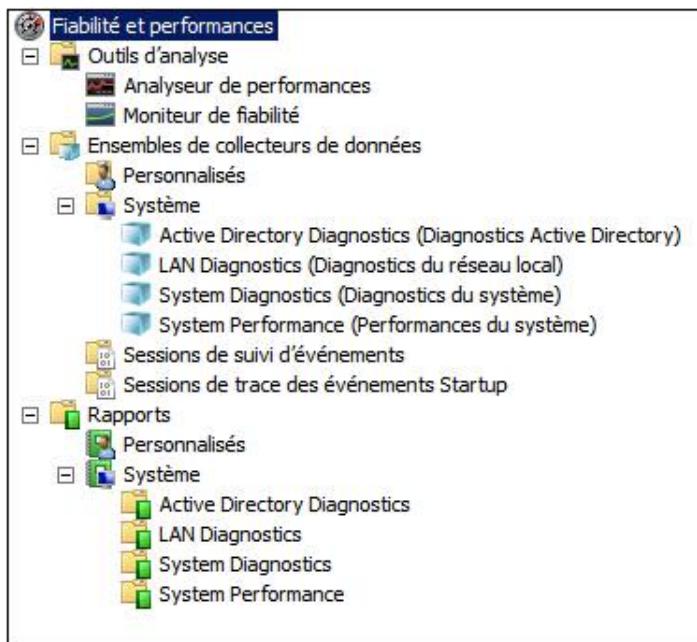


C'est un nouvel outil qui remplace avantageusement l'outil **Performances** de Windows 2003. Il est composé de plusieurs snap-ins placés judicieusement.

Pour démarrer l'outil **Moniteur de fiabilité et de performances** :

- Connectez-vous en tant qu'administrateur sur l'ordinateur Windows Server 2008.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Moniteur de fiabilité et de performances**.

La figure suivante montre l'arborescence de la console de cet outil.



L'outil **Fiabilité et performances** regroupe plusieurs outils d'analyse, de collecte de données et de rapports) tels que l'Analyseur de performances, le Moniteur de fiabilité, les Collecteurs et l'affichage des Rapports.

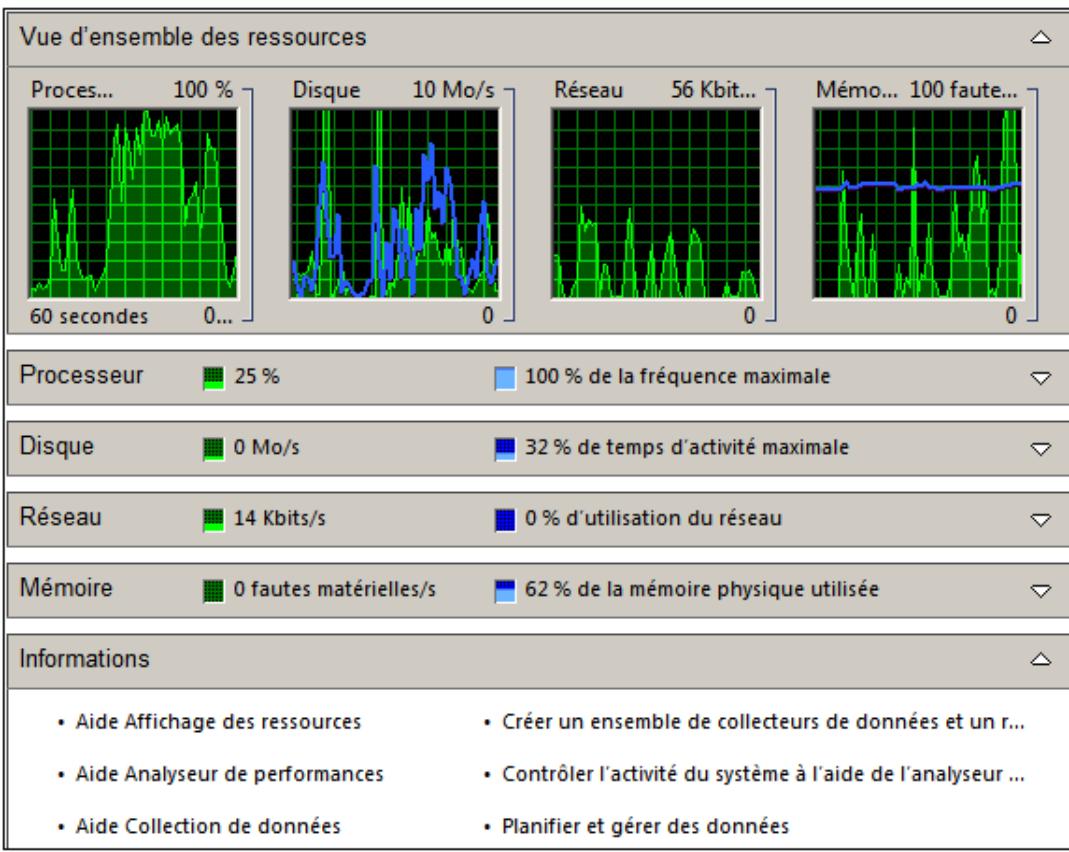
► Il est possible d'analyser un autre ordinateur via le menu **Action - Se connecter à un autre ordinateur**.

## 1. Moniteur de ressources

Le Moniteur de ressources permet de visualiser et analyser en temps réel les quatre sous-systèmes importants :

- Processeur,
- Disque,
- Réseau,
- Mémoire.

La figure suivante montre l'affichage à l'ouverture de cet utilitaire.



Les actions possibles de cet utilitaire sont **Arrêter le moniteur de ressources** et **Démarrer le moniteur de ressources**, par les boutons correspondants sur la barre d'outils.

Cet outil est très utile et fournit à l'administrateur une synthèse des quatre éléments à étudier pour proposer une optimisation.

En cliquant sur les barres grises, vous affichez ou masquez les informations concernant la section courante.

Pour chaque section, il est possible de trier les valeurs par colonne en cliquant sur l'en-tête de la colonne. Il est également possible de modifier l'ordre des colonnes en les sélectionnant et en les déplaçant vers l'endroit désiré.

### Vue d'ensemble des ressources

Cette section présente quatre graphiques, à savoir :

- **Processeur** qui affiche en vert le pourcentage d'utilisation du processeur et en bleu le pourcentage de la fréquence maximale.
- **Disque** qui affiche en vert l'activité du disque en Ko/s et en bleu le pourcentage de temps d'activité maximale.
- **Réseau** qui affiche en vert l'activité du réseau et en bleu le pourcentage d'utilisation du réseau.
- **Mémoire** qui affiche en vert le nombre de fautes matérielles par seconde et en bleu le pourcentage de la mémoire utilisée.

La granularité est le sous-système affiché et pas l'élément physique unitaire.

Vous pouvez constater sur la figure précédente qu'au moment de la pagination, l'activité disque a augmenté ainsi que l'activité du processeur. Dans ce cas, la pagination n'est pas un problème car elle n'intervient qu'une seule fois et qu'il reste suffisamment de mémoire libre avant la saturation.

### Processeur

Processeur	7 %	100 % de la fréquence maximale			
Image	PID	Description	Threads	Processeur	UC moyenne
csrss.exe	476	Processus d'exécution clien...	7	0	0.32
explorer.exe	252	Explorateur Windows	17	0	0.07
mmc.exe	2844	Microsoft Management Con...	17	3	1.59
perfmon.exe	3064	Moniteur de fiabilité et de p...	9	1	5.12
SnagIt32.exe	3928	SnagIt 8	6	2	0.53
svchost.exe (rapisrv)	2508	Processus hôte pour les serv...	9	0	0.02
System	4	NT Kernel & System	92	0	0.07
taskeng.exe	472	Moteur du Planificateur de t...	11	0	0.03
vmsvrc.exe	2268	Virtual Machine User Services	3	0	0.02

Cette section permet d'afficher des informations concernant le processeur :

- **Image** indique le nom du fichier exécutable de l'application.
- L'identificateur de processus **PID** est le numéro qui identifie le processus.
- La **Description** de l'application.
- Le nombre de **Threads** actuellement en cours dans l'application.
- Le **Processeur** affiche le nombre de cycles en cours pour l'application.
- L'**UC moyenne** affiche le pourcentage de la charge totale utilisée par l'application au cours des 60 dernières secondes.

## Disque

Disque	0 Ko/s	5 % de temps d'activité maximale				
Image	PID	Fichier	Lecture (octets/min)	Écriture (octets/min)	Priorité d'E/S	Temps de réponse (ms)
System	4	C:\Users\Administrateur	0	16 384	Normale	19
svchost.exe (LocalServiceNetworkRestricted)	928	C:\Windows\System32\adlsc...	16 384	0	Normale	13
System	4	C:\Users\Administrateur\ntu...	0	63 339	Normale	12
System	4	C:\Users\Administrateur\Ap...	0	4 096	Normale	12
System	4	C:\Windows\System32\confi...	0	776 027	Normale	9
System	4	C:\Windows\System32\wine...	0	8 192	Normale	8
System	4	C:\Users\Administrateur\Ap...	0	36 664	Normale	8
System	4	C:\Windows\System32\wine...	0	12 288	Normale	4
lsass.exe	572	C:\Windows\NTDS\ntds.dit	9 085 342	16 384	Normale	4
System	4	C:\Windows\System32\wine...	0	8 192	Normale	4

Cette section permet d'afficher des informations concernant le réseau :

- **Image** indique le nom du fichier exécutable de l'application.
- L'identificateur de processus **PID** est le numéro qui identifie le processus.
- **Fichier** affiche le nom et le chemin complet du fichier actuellement ouvert.
- **Lecture (octets/min)** affiche le débit en lecture.
- **Écriture (octets/min)** affiche le débit en écriture.
- **Priorité d'E/S** affiche la priorité de l'application.
- **Temps de réponse (ms)** affiche le temps de réponse de l'activité du disque.

## Réseau

Réseau	1 Kbits/s	0 % d'utilisation du réseau				
Image	PID	Adresse	Envoi (octets/min)	Réception (octets/min)	Total (octets/min)	
System	4	ZEUS	13956	9397	23353	
svchost.exe (NetworkService)	1168	AD1	0	756	756	
dns.exe	1708	AD1	0	756	756	
System	4	AD1	0	484	484	
svchost.exe (NetworkService)	1168	224.0.0.252	378	0	378	
svchost.exe (NetworkService)	1168	F02:1:3	0	378	378	
dns.exe	1708	AD1	0	338	338	
System	4	224.0.0.252	300	0	300	
svchost.exe (NetworkService)	1168	AD1	41	118	159	
dns.exe	1708	AD1	118	41	159	

Cette section permet d'afficher des informations concernant le réseau :

- **Image** indique le nom du fichier exécutable de l'application.
- L'identificateur de processus **PID** est le numéro qui identifie le processus.
- L'**Adresse** de destination IP ou le FQDN.
- **Envoi (octets/min)** : le nombre d'octets envoyés par min.
- **Réception (octets/min)** : le nombre d'octets reçus par min.
- Le nombre **Total (octets/min)** devrait être égal au nombre d'octets envoyés et reçus.

## Mémoire

Mémoire	0 fautes matérielles/s	70 % de la mémoire physique utilisée					
Image	PID	Fautes matérielles/min	Validation (Ko)	Plage de travail (Ko)	Partageable (Ko)	Privé (Ko)	
dns.exe	1708	0	6144	7784	5168	2616	
svchost.exe (LocalService)	1056	0	4256	8596	6016	2500	
svchost.exe (LocalSystem\NetworkRestricted)	1112	0	6860	8236	5856	2380	
svchost.exe (rpcess)	848	0	2724	5336	3632	2204	
services.exe	560	0	4836	8072	5876	2196	
svchost.exe (GPSvcGroup)	968	0	3604	7528	5368	2160	
msdtc.exe	3592	0	2756	6732	4620	2112	
taskeng.exe	472	2	2616	7696	5712	1984	
taskeng.exe	1508	0	2156	6364	5200	1664	
dfssvc.exe	1948	0	2220	5956	4396	1560	

Cette section permet d'afficher les informations concernant la mémoire :

- **Image** indique le nom du fichier exécutable de l'application.
- L'identificateur de processus **PID** est le numéro qui identifie le processus.
- **Fautes matérielles/min** définit le défaut de page, soit une page mémoire se trouvant sur le fichier de pagination et non en mémoire RAM. Un nombre de fautes élevé indique qu'il faut ajouter de la RAM.
- **Validation (Ko)** indique la plage mémoire allouable.
- **Plage de travail (Ko)** correspond à la mémoire actuellement utilisée par l'application.
- **Partageable (Ko)** correspond à un espace mémoire qui peut être utilisé par d'autres applications.
- **Privé (Ko)** correspond à un espace mémoire privé.

## Informations

Cette section permet d'accéder à des pages de l'aide en ligne.

 Vous pouvez lancer le Moniteur de ressources à l'aide de la commande **perfmon /res**.

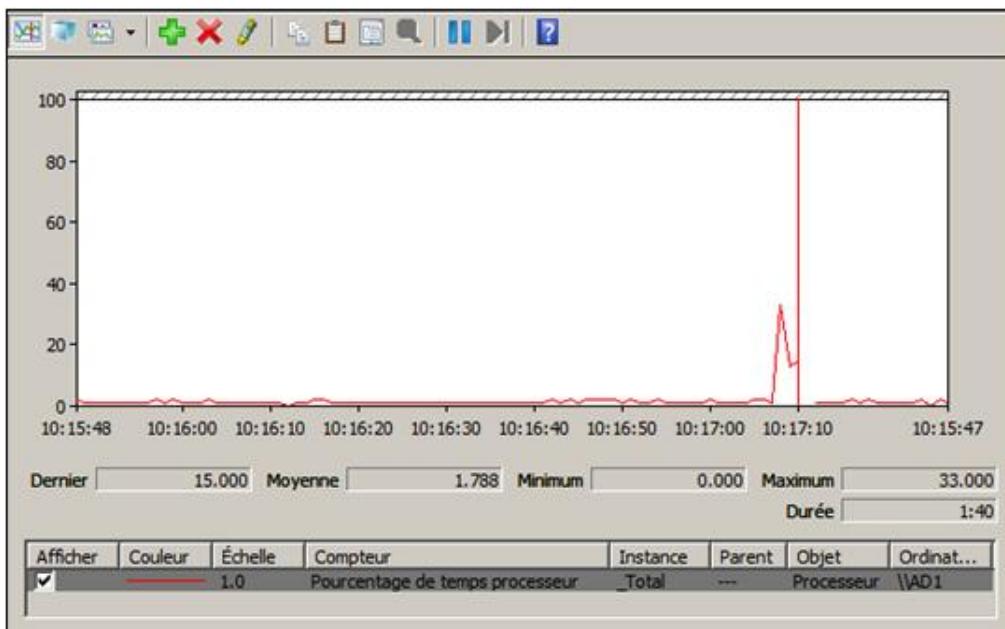
## 2. Analyseur de performances



L'Analyseur de performances est l'outil le plus complet pour examiner les performances. Sa compréhension et son utilisation permettent à l'administrateur de déterminer d'où proviennent les problèmes de performance et de réagir.

L'interprétation des valeurs n'est pas toujours évidente, elle dépend du matériel utilisé, du système d'exploitation et demande une bonne expérience de l'administrateur.

C'est également le plus complexe des outils placés dans le Moniteur de fiabilité et de performances.



Les actions possibles peuvent être catégorisées de la manière suivante :

- Modifier les compteurs.
- Modifier l'affichage de la présentation et la source des données. Vous pouvez travailler avec les données du journal ou l'activité en cours.
- Enregistrer les données pour une utilisation future.

### a. Modification des compteurs

Un compteur affiche le résultat de l'analyse d'un élément particulier. La valeur d'un compteur est soit une valeur absolue allant de 0 à n, soit un pourcentage allant de 0 à 100. Chaque compteur est prédéfini et a été programmé pour afficher l'information.

Pour ajouter un compteur, il faut commencer par définir quel ordinateur l'on veut analyser puis pour l'ordinateur considéré, quel compteur il faut ajouter en sélectionnant le compteur d'une famille de compteurs. Puis il faut sélectionner l'instance ou les instances existantes, avant de cliquer sur le bouton **Ajouter**.

Il est possible d'ajouter plusieurs compteurs provenant de plusieurs objets en même temps.

Pour ajouter un compteur, vous pouvez :

- Cliquer sur dans la barre d'outils.
- Utiliser le menu contextuel de la fenêtre **Analyseur de performances** puis cliquer sur **Ajouter des**

## **compteurs.**

Pour supprimer un ou plusieurs compteurs, vous pouvez :

- Cliquer sur  dans la barre d'outils pour supprimer les compteurs sélectionnés.
- Utiliser le menu contextuel de la fenêtre **Analyseur de performances** puis cliquer sur **Supprimer tous les compteurs**.

## **b. Modification de l'affichage**

Il est possible de modifier l'affichage du graphique en utilisant l'icône suivante  . Les types de graphiques possibles sont :

- **Ligne**, qui est l'affichage le plus utilisé.
- **Barre d'histogramme**.
- **Rapport**.

Pour chaque compteur, vous pouvez modifier l'échelle utilisée, le style du trait, sa largeur et sa couleur en sélectionnant l'onglet **Données** des **Propriétés** de l'Analyseur de performances. Pour le faire apparaître, cliquez avec le bouton droit de la souris dans la zone du graphique puis cliquez sur **Propriétés**.

 Bien que séduisante, la personnalisation des compteurs prend du temps.

## **c. Enregistrement des données**

Vous pouvez enregistrer une image au format **GIF** de la fenêtre d'enregistrement et des compteurs en utilisant le menu contextuel de la fenêtre d'enregistrement et en cliquant sur l'action **Enregistrer l'image sous**.

Dans le but de créer des analyses prêtées à l'emploi, procédez de la manière suivante :

- Dans la console **Analyseur de performances**, ajoutez les compteurs dont vous avez besoin.
- Cliquez avec le bouton droit de la souris sur la zone d'enregistrement puis cliquez sur **Enregistrer les paramètres sous**.
- Sélectionnez un emplacement sur un serveur, indiquez un nom de fichier et vérifiez que le format est **Page Web (\*.htm ; \*.html)** puis cliquez sur **Enregistrer**.

Pour démarrer l'analyse, il suffit maintenant de se placer sur un ordinateur puis de suivre la procédure suivante :

- Connectez-vous en tant qu'administrateur sur l'ordinateur à analyser.
- Depuis cet ordinateur, connectez-vous sur le partage qui contient les fichiers Page Web des compteurs que vous avez enregistrés.
- Double cliquez sur un compteur **Page Web**. Une page Web avec les compteurs figés au moment de l'enregistrement apparaît.
- Cliquez sur l'icône **Mettre à jour les données**  ou sur l'icône **Libérer l'affichage**  pour démarrer l'analyse.

 La procédure précédente est parfaitement adaptée pour tous les compteurs qui touchent la mémoire, le processeur, les disques et le réseau, mais peut ne pas fonctionner pour des compteurs applicatifs sur certains ordinateurs si l'application, donc les compteurs, ne sont pas installés.

#### d. Cadre d'utilisation

L'Analyseur de performances est à utiliser sans modération. Néanmoins, il faut disposer d'une référence pour interpréter les valeurs des compteurs. Il est recommandé de se baser sur les valeurs indiquées dans le kit de ressources techniques du système d'exploitation utilisé pour connaître les valeurs acceptables ou inacceptables des compteurs.

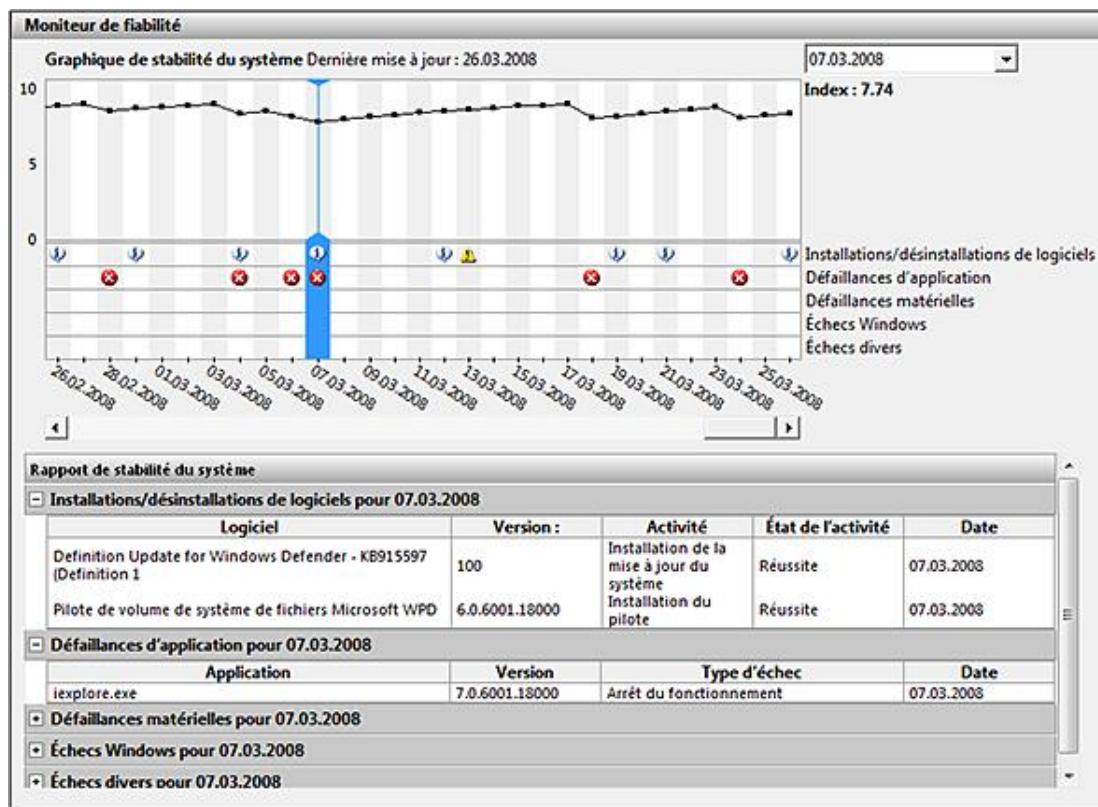
Les valeurs suivantes peuvent être considérées comme acceptables dans tous les cas de figure :

- Un pourcentage de temps processeur toujours supérieur à 80 % indique qu'il faut songer à disposer d'un processeur plus puissant, soit en le mettant à jour, soit en changeant de serveur.
- Un nombre de défauts de page par seconde élevé accompagné d'un nombre d'octets disponibles très faible et d'un accès disque important indique qu'il faut ajouter de la mémoire RAM au système.
- Une file d'attente des disques dont la longueur augmente et qui reste longtemps active indique que le contrôleur ou le disque n'arrive pas à traiter les demandes et qu'il faudrait disposer d'un contrôleur plus rapide, ou d'un disque plus rapide.

Pour différencier une optimisation concernant le disque ou le contrôleur, vous pouvez également utiliser la notion du débit, soit le nombre d'octets disque par seconde. L'architecture de la carte mère de l'ordinateur peut également être le goulet d'étranglement pour ce type de problèmes.

- Moins de 20 % de mémoire RAM disponible peut ralentir entièrement le système, il peut s'agir ici d'un goulet d'étranglement. Avant d'ajouter de la mémoire, contrôlez que des applications parasites ne fonctionnent pas, et si par hasard il n'est pas possible d'arrêter un instant certains services afin de libérer de la mémoire qui n'est jamais relâchée.

### 3. Moniteur de fiabilité



Le Moniteur de fiabilité établit des rapports sur la stabilité du système et les catégorise de la manière suivante :

- Installations/désinstallations de logiciels
- Défaillances d'application
- Défaillances matérielles
- Échecs Windows
- Échecs divers

Il ne permet que la lecture des informations.

L'indice de stabilité affiché dans le graphique est une valeur allant de 1 à 10 qui est le résultat d'un calcul de pondération prenant en compte le nombre de pannes observées pendant une période historique continue.



L'indice peut être considéré comme fiable à partir de 30 jours de collecte d'information.

Dans l'exemple de la figure précédente, pour le jour considéré, l'indice a chuté à cause d'un arrêt de fonctionnement d'Internet Explorer. La défaillance étant considérée comme peu importante, l'indice a peu chuté, alors que la défaillance suivante devait être plus importante.

L'étude de l'indice permet de visualiser certains problèmes récurrents rencontrés par l'ordinateur et de déterminer ce qui a pu les déclencher et à partir de quelle date.



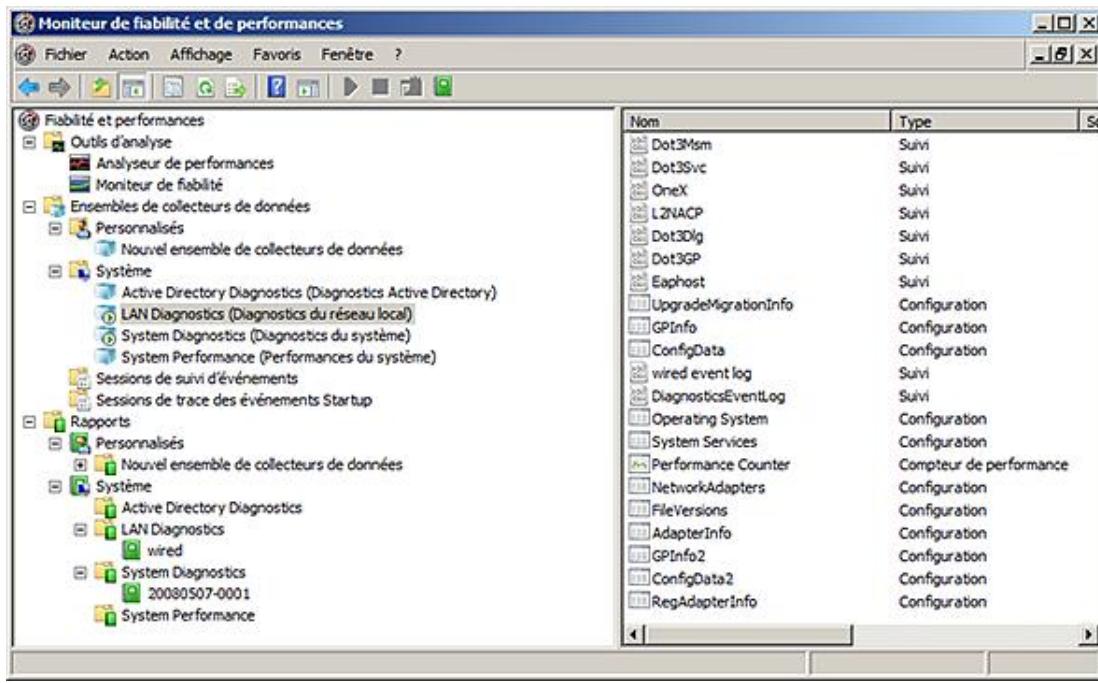
Vous pouvez lancer le Moniteur de fiabilité à l'aide de la commande **perfmon /rel**.

## 4. Ensemble de collecteurs de données et rapports

Le collecteur de données enregistre les données pour un usage différé et crée automatiquement des rapports pour une lecture plus aisée.

Le collecteur de données permet d'enregistrer des informations provenant des :

- Compteurs de performance.
- Données de suivi d'événements.
- Informations de configuration du système.
- Alertes de compteur de performance.



## a. Création d'un ensemble de collecteurs de données

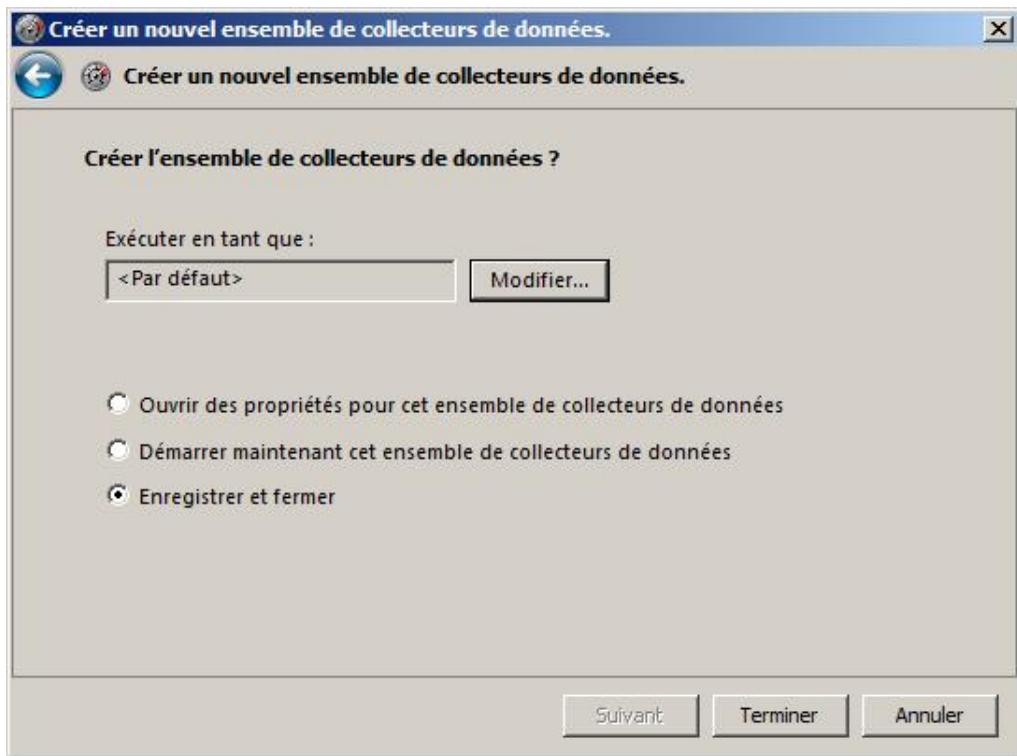
Les ensembles de collecteurs de données sont subdivisés en 4 sous-sections :

- **Personnalisés** permet d'ajouter des ensembles personnalisés.
- **Système** affiche les collecteurs prédéfinis. Ils ne peuvent être modifiés.
- **Sessions de suivi d'événements** permet de créer des ensembles basés sur les suivis d'événements.
- **Sessions de trace des événements Startup** permet de créer des ensembles basés sur les suivis d'événements au démarrage.

L'emplacement idéal pour créer un ensemble de collecteurs de données se trouve dans la sous-section **Personnalisés**.

- Dans la console **Ensembles de collecteurs de données**, cliquez avec le bouton droit de la souris sur **Personnalisés** pour faire apparaître le menu contextuel puis cliquez sur **Nouveau - Ensemble de collecteurs de données**.
- Dans l'assistant **Créer un nouvel ensemble de collecteurs de données**, saisissez un nom explicite puis sélectionnez **Créer à partir d'un modèle** si vous voulez utiliser un de vos modèles ou un de ceux proposés, sinon sélectionnez **Créer manuellement** puis cliquez sur **Suivant**. L'utilisation de modèles permet de gérer des ensembles de collecteurs entre ordinateurs.
- Sur la page **Quel type de données inclure ?**, vous pouvez soit créer des alertes de compteur de performance, soit créer des journaux de données pouvant inclure des compteurs de performance, des données de suivi d'événements et des informations de la configuration système. Sélectionnez le type de données à inclure puis cliquez sur **Suivant**.
- En fonction des types de données choisis, des pages vous proposent d'ajouter les données propres à chaque type de données. Ajoutez les données dont vous avez besoin puis cliquez sur **Suivant**.
- Sur la page **Où enregistrer les données ?**, saisissez le chemin complet et le nom du fichier, ou utilisez le bouton **Parcourir** pour choisir l'emplacement puis cliquez sur **Suivant**.
- Sur la page **Créer l'ensemble de collecteurs de données ?**, vous pouvez modifier le compte d'utilisateur employé pour collecter les données et déterminer le comportement de l'ensemble de collecteurs de données à la fin de

l'assistant. Ensuite, cliquez sur **Terminer**.



Vous pouvez également ajouter des collecteurs de données supplémentaires à un ensemble de collecteurs de données.

Dès qu'un ensemble de collecteurs de données est créé, le rapport associé est automatiquement créé. Le contenu du rapport se base sur les données collectées et pour cela, il faut au préalable collecter des données puis arrêter la collecte pour afficher le rapport afin que les valeurs aient un sens.

Certains rapports permettent un affichage pendant la collecte.

### b. Enregistrer le modèle

Une fois qu'un ensemble de collecteurs de données est créé, vous pouvez le sauvegarder en tant que modèle pour en disposer ultérieurement ou l'exporter vers un autre ordinateur. Le fichier généré est au format XML.

- Dans la console **Ensembles de collecteurs de données**, sélectionnez l'ensemble que vous voulez sauvegarder en tant que modèle.
- Cliquez avec le bouton droit de la souris pour faire apparaître le menu contextuel puis cliquez sur **Enregistrer le modèle**.
- Dans la boîte de dialogue **Enregistrer sous**, sélectionnez un emplacement et saisissez un nom de fichier puis cliquez sur **Enregistrer**.

### c. Démarrer/arrêter

Pour démarrer ou arrêter l'enregistrement des compteurs, suivez cette procédure :

- Dans la console **Ensembles de collecteurs de données**, sélectionnez l'ensemble concerné.
  - Cliquez avec le bouton droit de la souris pour faire apparaître le menu contextuel puis cliquez sur **Démarrer** ou sur **Arrêter**.
- 
-  Si l'ensemble de collecteurs de données n'est pas démarré ou arrêté, fermez la console et rouvrez-la.

Vous pouvez planifier le démarrage et/ou l'arrêt en passant par la boîte de dialogue **Propriétés** de l'ensemble de collecteurs de données, dans l'onglet **Planification**.

#### d. Rapport System Diagnostics

Parmi les rapports prédéfinis, ce rapport est le plus intéressant car il attire votre attention sur des valeurs d'indicateurs pouvant signaler des problèmes. Pour les avertissements, la cause et les détails sont indiqués et une solution pour y remédier vous est proposée.

La figure suivante montre une vue détaillée du rapport dans lequel l'indicateur pour l'utilisation de la mémoire est au rouge, ce qui se traduit par une pagination excessive. Les résultats des requêtes WQL (*WMI Query Language*) concernant les logiciels anti-espions et antivirus n'ont pas retourné de valeur, ce qui se traduit par une information dans le rapport sur l'absence de ces logiciels.

The screenshot displays the 'Performances' section of the System Diagnostics report. It shows a table for resource usage:

Composant	Statut	Utilisation	Détails
Processeur	Normale	25 %	Charge processeur normale.
Réseau	Inactif	0 %	La carte réseau la plus chargée est inférieure à 15 %. <input checked="" type="checkbox"/>
Disque	Inactif	13/sec	Le nombre d'E/S disque est inférieur à 100 (opérations de lecture/écriture) par seconde sur le disque 0. <input checked="" type="checkbox"/>
Mémoire	Occupé	90 %	49 Mo disponibles.

Below this, the 'Configuration du logiciel' section is shown, followed by 'Vérifications du système d'exploitation'. The 'Informations sur le système d'exploitation' section contains two WQL queries:

Demande	Résultat de requête
root\cimv2:SELECT * FROM Win32_OperatingSystem	0x0
root\cimv2:SELECT * FROM Win32_ComputerSystem	0x0

The 'Informations du Centre de sécurité' section is present, but its content is mostly redacted. The 'Informations de logiciel anti-espion' section shows a single query with a result code of 0x8004100e:

Demande	Résultat de requête
root\SecurityCenter:SELECT * FROM AntiSpywareProduct	0x8004100e

The 'Informations antivirus' section also shows a single query with a result code of 0x8004100e:

Demande	Résultat de requête
root\SecurityCenter:SELECT * FROM AntiVirusProduct	0x8004100e

#### e. Cadre d'utilisation

Cet outil peut sembler séduisant, néanmoins il faut garder à l'esprit que les collecteurs et leur traitement ont une incidence négative sur les performances de l'ordinateur et que certains ensembles de collecteurs de données prédéfinis ou personnalisés peuvent devenir difficiles à interpréter, voire illisibles.

Il s'agit de l'outil le plus difficile à mettre en œuvre, dès lors il est à utiliser avec précaution excepté pour les rapports prédéfinis dont l'utilité n'est plus à démontrer. Ces rapports devraient être produits sur la base d'un calendrier et analysés avec soin par un administrateur.

## Gestionnaire des tâches

Le Gestionnaire des tâches est un outil installé en standard sur toutes les versions de Windows. Son utilisation est simple et son usage permet aussi bien d'arrêter un programme ou un service que de visualiser des utilisateurs connectés ou la charge du réseau.



**Process Explorer**, un autre utilitaire Microsoft provenant du rachat de Sysinternals peut être un outil plus précis.

Pour ouvrir le Gestionnaire des tâches, utilisez l'une de ces méthodes :



- Tapez [Ctrl] [Shift] [Echap].
- Tapez [Ctrl] [Alt] [Suppr] puis sélectionnez **Gestionnaire des tâches**.
- Cliquez avec le bouton droit de la souris dans la barre des tâches du Bureau puis cliquez sur **Gestionnaire des tâches** dans le menu contextuel.
- Cliquez sur **Démarrer**, saisissez **taskmgr** dans la zone **Rechercher** et appuyez sur [Entrée].

Pour ouvrir le Gestionnaire des tâches sur un Server Core :

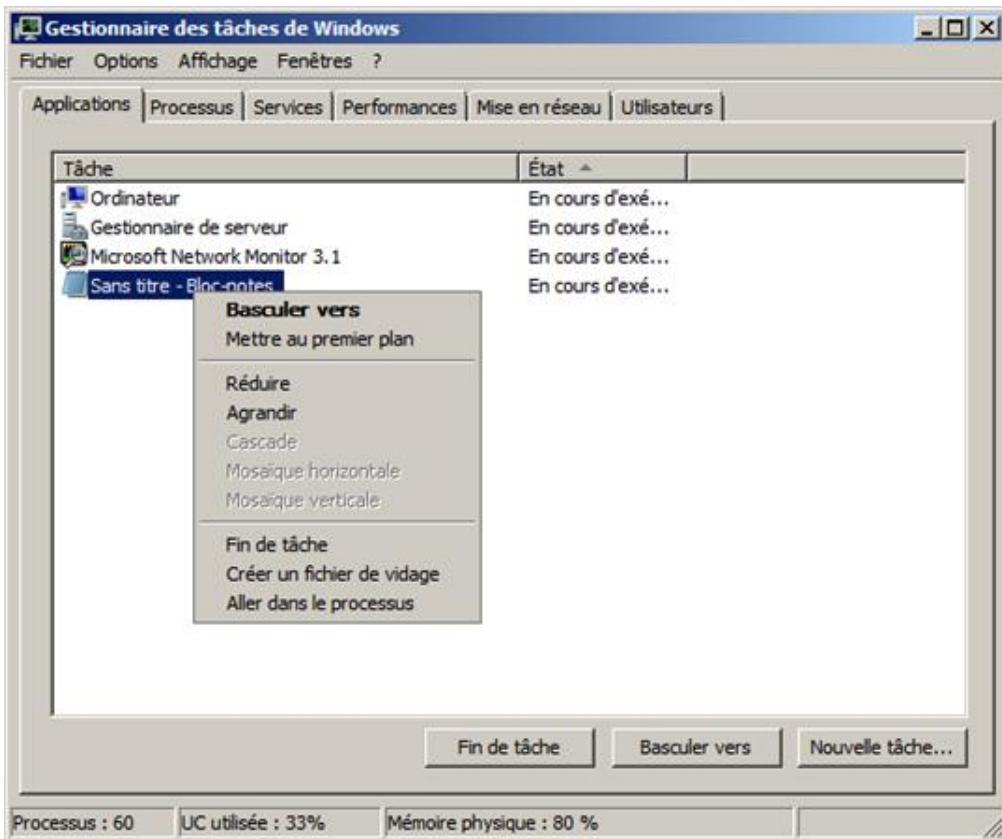


- Tapez [Ctrl] [Shift] [Echap].
- Tapez [Ctrl] [Alt] [Suppr] puis sélectionnez **Gestionnaire des tâches**.



Si vous double cliquez dans un graphique, l'affichage du graphique change de manière à occuper tout l'espace de la fenêtre disponible. Pour revenir à l'état normal, il faut également double cliquer.

### Onglet Applications



L'onglet **Applications** affiche les applications actuellement lancées par l'utilisateur connecté.

La liste affiche les applications en cours d'exécution. Les termes possibles pour l'État sont **En cours d'exécution** si l'application fonctionne normalement et **Pas de réponse** si l'application ne répond pas, ce qui peut indiquer un problème.

Les actions possibles depuis le menu, le menu contextuel ou les boutons sont :

**Basculer vers** : cache le Gestionnaire des tâches si l'application sélectionnée est au premier plan.

**Mettre au premier plan** : affiche l'application sélectionnée au premier plan.

**Réduire** : minimise toutes les fenêtres.

**Agrandir** : maximise toutes les fenêtres.

**Cascade** : dispose les fenêtres en cascade sur le Bureau.

**Mosaïque horizontale** : dispose les fenêtres en mosaïque horizontale.

**Mosaïque verticale** : dispose les fenêtres en mosaïque verticale.

**Fin de tâche** : termine l'application sélectionnée.

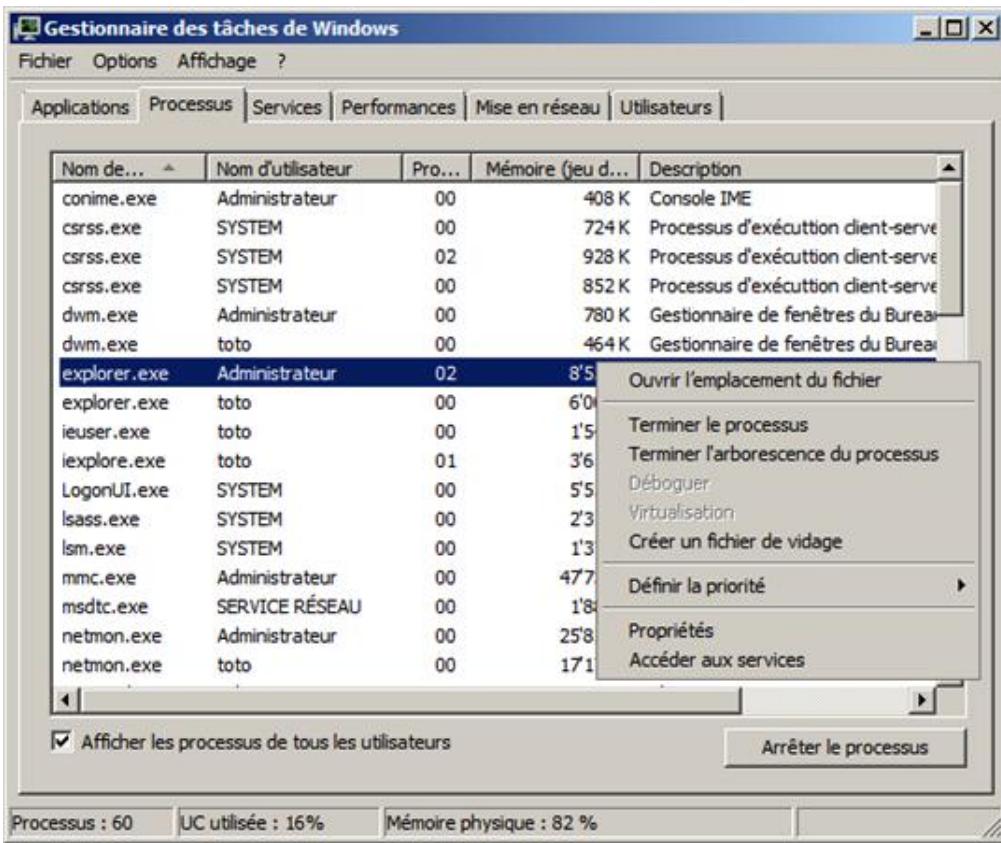
**Créer un fichier de vidage** : crée un fichier de vidage **nom de l'image.DMP** pour l'application sélectionnée. Le chemin de stockage est donné lorsque le fichier est créé. Le fichier de vidage contient des informations sur la mémoire qui peuvent être lues en utilisant des outils comme Dumpcheck, à télécharger à partir du site Microsoft, pour déterminer pourquoi l'ordinateur a cessé de répondre.

**Aller dans le processus** : pour l'application sélectionnée, affiche le processus correspondant dans l'onglet **Processus**.

**Nouvelle tâche** : permet de lancer une nouvelle application soit en saisissant directement son nom, soit en sélectionnant son exécutable à l'aide du bouton **Parcourir**.

### Onglet Processus

L'onglet **Processus** affiche la liste de tous les processus qui tournent actuellement sur le serveur.



La liste affiche les processus en cours et l'utilisation du processeur sollicité. L'observation de cet onglet permet de déterminer si un processus peut poser des problèmes.

Pour trier la liste dans un autre ordre, cliquez sur l'en-tête d'une autre colonne. Le nombre de colonnes ainsi que l'ordre des colonnes sont modifiables.

Les actions possibles depuis le menu, le menu contextuel ou les boutons sont :

**Afficher les tâches 16 bits** : affiche directement les processus 16 bits au lieu de les montrer dans le processus ntvdm.

**Ouvrir l'emplacement du fichier** : affiche une fenêtre explorateur du dossier qui contient le fichier du processus sélectionné.

**Terminer le processus** : permet de fermer le processus sélectionné.

**Terminer l'arborescence du processus** : permet de fermer le processus et les processus dépendants du processus sélectionné.

**Déboguer** : permet de déboguer le processus sélectionné.

**Virtualisation** : indique l'état de virtualisation du processus. Un processus est virtualisé uniquement s'il n'a pas été conçu pour fonctionner sous Windows Vista ou Windows Server 2008.

**Créer un fichier de vidage** : crée un fichier de vidage nom de l'image.DMP pour l'application sélectionnée. Le chemin de stockage est donné lorsque le fichier est créé.

**Définir la priorité** : permet de modifier la priorité du processus allant de **Basse, Inférieure à la normale, Normale, Supérieure à la normale, Haute** et **Temps réel**. La priorité **Normale** étant le niveau standard. Évitez la priorité **Temps réel** car le clavier et la souris ne répondent plus, leur niveau de priorité étant plus faible, un redémarrage du système est alors nécessaire pour reprendre la main.

Une application se trouvant sur l'**avant plan**, soit celle qui a le focus, augmente temporairement son niveau de +2.

**Définir l'affinité** : permet de privilégier l'exécution du processus sur un ou plusieurs processeurs sélectionnés. Par défaut, l'affinité est définie pour utiliser tous les processeurs.

**Propriétés** : affiche la boîte de dialogue **Propriétés** de l'exécutable.

**Accéder aux services** : affiche l'onglet **Services** et éventuellement le service associé au processus sélectionné.

Le bouton **Arrêter le processus** permet d'arrêter le processus sélectionné.

La case à cocher **Afficher les processus de tous les utilisateurs** permet d'afficher les processus de l'utilisateur courant et de tous les utilisateurs.

## Onglet Services

L'onglet **Services** fournit le moyen le plus simple pour consulter l'état des services du serveur Windows Server 2008.

- La commande **tasklist /svc** est similaire en mode ligne de commandes.

The screenshot shows the Windows Task Manager window titled "Gestionnaire des tâches de Windows". The "Services" tab is selected. The main area is a grid table with columns: Nom, PID, Description, État, and Groupe. The table lists various system services. At the bottom of the window, there is a status bar showing "Processus : 41", "UC utilisée : 53%", and "Mémoire physique : 59%". A "Services..." button is located at the bottom right of the grid area.

Nom	PID	Description	État	Groupe
VSS		Cliché instantané de volume	Arrêté	N/D
gpsvc	916	Client de stratégie de groupe	En cours d'exécution	N/D
TrkWks	1060	Client de suivi de lien distribué	En cours d'exécution	LocalSystem\NetworkRestricted
Dhcp	892	Client DHCP	En cours d'exécution	LocalService\NetworkRestricted
Dnscache	1112	Client DNS	En cours d'exécution	NetworkService
Websvc		Collecteur d'événements de Wind...	Arrêté	NetworkService
dot3svc		Configuration automatique de rés...	Arrêté	LocalSystem\NetworkRestricted
SessionEnv		Configuration des services Termin...	Arrêté	netsvcs
NlaSvc	1112	Connnaissance des emplacements ...	En cours d'exécution	NetworkService
Netman	1060	Connexions réseau	En cours d'exécution	LocalSystem\NetworkRestricted
MSDTC	1964	Coordinateur de transactions dist...	En cours d'exécution	N/D
vds		Disque virtuel	Arrêté	N/D
SSDPSRV		Découverte SSDP	Arrêté	LocalService
UI0Detect		Détection de services interactifs	Arrêté	N/D
ShellHWDet...	928	Détection matériel noyau	En cours d'exécution	netsvcs
ProtectedSt...		Emplacement protégé	Arrêté	
Browser		Explorateur d'ordinateurs	Arrêté	netsvcs

Pour trier la liste dans un autre ordre, cliquez sur l'en-tête d'une autre colonne. Le nombre de colonnes n'est pas modifiable mais l'ordre des colonnes est modifiable.

La liste des services affiche le **Nom**, l'identificateur du processus (**PID**), l'**État** du service (arrêté ou en cours d'exécution) et le **Groupe**.

Le fichier **svchost** est un processus d'hôte générique qui exécute dans son processus un ou plusieurs services que l'on appelle groupe ou groupe de services. L'association entre le service et le groupe est créée avec la commande **svchost -k svcgroup** où **svcgroup** représente le groupe de services de la colonne **Groupe**.

La définition des noms de groupe et des services associés au groupe est enregistrée dans la clé de registre suivante :

**HKEY\_LOCAL\_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Svchost**

Si vous sélectionnez un service avec le menu contextuel, il est possible :

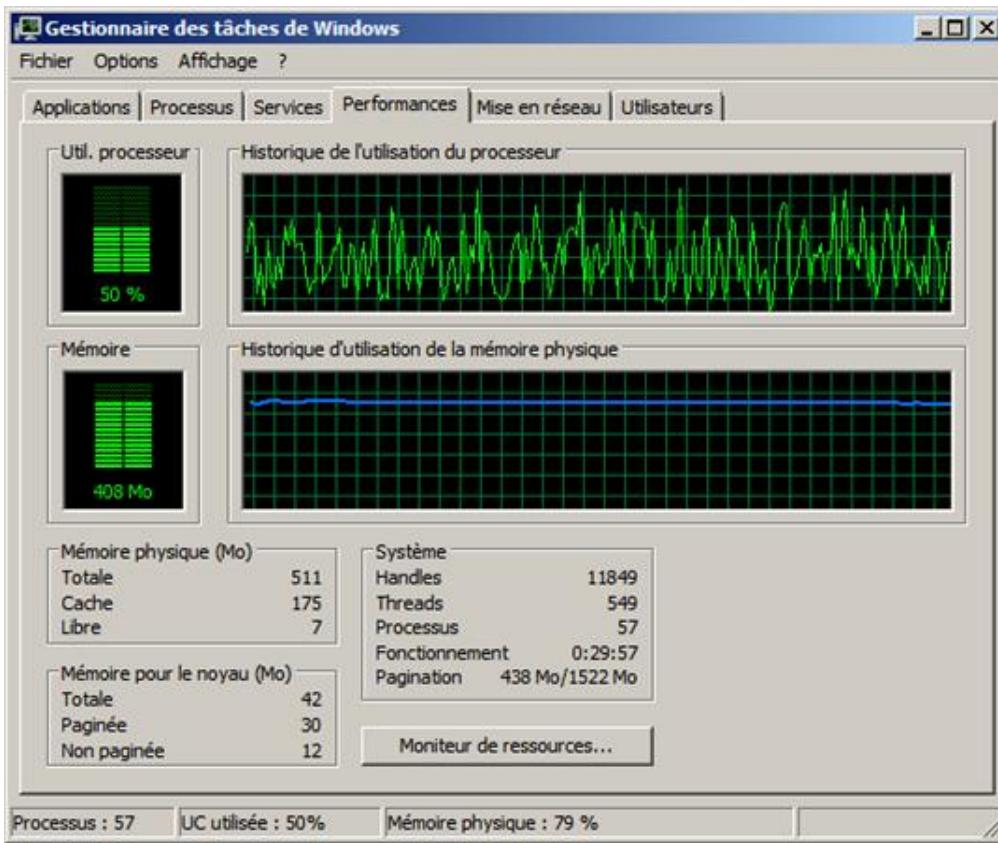
- de démarrer le service.
- d'arrêter le service.
- d'aller dans le processus associé au service.

Le bouton **Services** permet de lancer la console MMC Services.

- En cas de conflit entre services, l'utilisateur ou Windows Server 2008 peut désactiver un des services.

## Onglet Performances

L'onglet **Performances** est sûrement l'onglet le plus intéressant.



La section **Util. processeur** indique le pourcentage actuel d'utilisation du processeur alors que l'historique affiche la courbe des dernières valeurs.

La section **Mémoire** indique la quantité de mémoire RAM actuellement utilisée alors que l'historique affiche une courbe d'utilisation créée à partir des dernières valeurs.

La section **Mémoire physique (Mo)** affiche dans **Totale** la mémoire RAM, dans **Cache** la mémoire utilisée par le cache système et dans **Libre** la mémoire libre et totalement utilisable.

La section **Mémoire pour le noyau (Mo)** affiche dans **Totale** la mémoire totale utilisée par le noyau du système d'exploitation qui se divise entre la mémoire qui peut être **Paginée** et celle qui ne peut pas être paginée. La mémoire non paginée ne peut être déplacée sur le fichier de pagination, comme la mémoire utilisée par le gestionnaire de mémoire.

La section **Système** affiche le nombre d'identificateurs (**Handles**) actuellement créés et utilisés par le système d'exploitation. Plus ce nombre est élevé, plus les accès sur le disque peuvent être fréquents.

Un **processus** représente une instance de fonctionnement d'une application et dispose de son propre espace d'adresses et d'environnement. Il contient au moins un thread qui représente une unité de traitement. Généralement, une application contenant plusieurs threads est plus rapide que la même application utilisant des processus à la place des threads. En revanche, une application qui utilise des processus est plus robuste qu'une application qui utilise des threads.

**Fonctionnement** représente le temps écoulé depuis le démarrage du système. Enfin, **Pagination** affiche l'espace de pagination actuellement utilisé par rapport à l'espace total utilisable.

Le menu **Affichage** propose les options :

**Historique du processeur** : permet d'afficher soit un seul graphique par processeur, soit un graphique pour tous les processeurs.

**Afficher les temps du noyau** : superpose une seconde courbe qui représente le temps de processeur utilisé par le noyau au lieu du temps total.

Vous pouvez afficher le **Moniteur de ressources** (détalé dans la section suivante) en cliquant sur le bouton correspondant.

### Onglet Mise en réseau

Cet onglet permet de visualiser rapidement la charge réseau, exprimée en pourcentage par carte réseau.

Le graphique **Connexion au réseau local** affiche soit le nombre d'**octets total** (défaut), soit le nombre d'**octets reçus**, soit le nombre d'**octets envoyés**. Pour modifier l'affichage, cliquez sur le menu **Affichage - Historique** de la carte réseau puis sélectionnez l'affichage voulu.

La liste des cartes réseau ne permet aucune action, seul l'affichage peut être modifié.

Pour trier la liste dans un autre ordre, cliquez sur l'en-tête d'une autre colonne. L'ordre des colonnes est modifiable, ainsi que leur liste.

-  Une charge régulière de plus de 50 % d'utilisation sur une carte réseau peut indiquer une surcharge réseau sur cette carte.

### **Onglet Utilisateurs**

L'onglet **Utilisateurs** permet de visualiser toutes les sessions des utilisateurs connectés localement et à distance sur le serveur, que ce soit via Terminal Server ou le Bureau distant.

Il est possible de masquer les colonnes, sauf le nom de l'utilisateur. Pour trier la liste dans un autre ordre, cliquez sur l'en-tête d'une autre colonne. L'ordre des colonnes n'est pas modifiable.

Les actions possibles via le menu contextuel ou via les boutons sont :

**Envoyer un message** : envoie un message dans la session de l'utilisateur.

**Fermer la session** : ferme la session de l'utilisateur sélectionné sans fermer les fichiers. Le risque de perdre des données est important.

**Déconnexion ou Déconnecter** : ferme la session de l'utilisateur sélectionné de manière sécurisée. Le risque de perdre des données est faible.

**Connecter** : si l'on connaît le mot de passe de l'utilisateur sélectionné, il est possible de rediriger la session de l'utilisateur sur son ordinateur, alors que ce dernier est déconnecté. Attention, ce n'est pas un mode d'assistance à distance.

**Contrôle à distance** : configure les raccourcis-clavier pour les sessions distantes.

## Optimisation et performances

Toute procédure d'optimisation commence par l'étude de l'existant après avoir déterminé le cadre de l'étude dans le but de proposer des recommandations.

Bien que tout administrateur ait une idée plus ou moins précise du problème, il faut des éléments objectifs permettant de confirmer ou non son idée. Il n'est pas acceptable de rester sur une impression car elle peut être faussée par un élément auquel on ne pense pas.

Le cadre de l'étude dépasse toujours le simple cadre d'examen d'une application pour inclure également le système d'exploitation, le matériel et bien entendu, le réseau. Il faut donc commencer par déterminer correctement le cadre de l'étude afin de ne pas oublier un élément qui peut avoir son importance.



Une longue expérience et une parfaite connaissance de l'architecture matérielle peuvent vous aider pour proposer les meilleures recommandations.

Microsoft propose une solution basée sur des compteurs de performances. Un compteur mesure une valeur à un instant donné et une application se charge de fournir une représentation graphique de cette valeur en indiquant soit une valeur absolue, soit une valeur relative exprimée en pourcentage. La définition d'un compteur est accessible aux programmeurs qui peuvent les utiliser dans leurs applications, mais malheureusement à part les applications développées par Microsoft, peu nombreuses sont celles qui les mettent en œuvre.

**L'Analyseur de performances** est l'outil principal qui utilise ces compteurs et Microsoft recommande de toujours analyser les compteurs :

- Processeur,
- Mémoire,
- Disque,
- Réseau.

Ils sont suffisants pour déterminer s'il existe un problème provenant du matériel ou si l'on doit investiguer plus loin avec des compteurs applicatifs.

Une fois le cadre de l'étude défini, il faut déterminer quels outils sont appropriés. Heureusement Microsoft nous fournit une palette d'outils qui peuvent être plus ou moins utiles.

Le **Gestionnaire des tâches** est sûrement le premier outil que l'on peut citer, car il est très simple d'emploi et permet en un seul coup d'œil de se faire une idée des problèmes. Il ne permet pas d'établir des rapports, il n'est donc pas approprié pour une étude qui doit être objective ; dans ce cas, la collecte de compteurs est plus adaptée.

Concernant les recommandations, il faut être très prudent car si un goulet d'étranglement a été identifié et que la proposition consiste à modifier un élément pour le faire disparaître, vous pouvez être sûr que vous allez rencontrer un autre goulet d'étranglement. La question que vous devez vous poser est de prévoir le moment où vous allez le rencontrer. En fonction de l'utilisation de votre serveur, la réponse peut être tout de suite ou jamais.

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre les objectifs suivants décrits dans les sections suivantes :

### Configurer des paramètres serveur WSUS (**Windows Server Update Services**).

Cela inclut, sans s'y limiter :

- sélection du type de mise à jour ; paramètres du client ;
- utilisation de stratégie de groupe (GPO) ;
- création de groupe de clients ;
- mises à jour de logiciels ;
- test et approbation des mises à jour ;
- travailler en mode réseaux déconnectés.

### Collecter les données de performance.

Cela inclut, sans s'y limiter :

- gestion de collecteurs de données ;
- mise en œuvre de performances ;
- mise en œuvre de fiabilité ;
- interprétation de l'index de stabilité système ;

### Surveiller les journaux des événements.

Cela inclut, sans s'y limiter :

- affichages personnalisés des journaux ;
- gestion des journaux des applications et des services ;
- mise en œuvre des abonnements ;
- gestion du journal DNS.

### Collecter des données réseau.

Cela inclut, sans s'y limiter :

- mise en œuvre du protocole SNMP (*Simple Network Management Protocol*) ;
- mise en œuvre du MBSA (*Baseline Security Analyzer*) ;
- mise en œuvre du moniteur réseau.

## 2. Pré-requis matériel

Pour effectuer toutes les mises en pratique de ce chapitre vous allez utiliser les machines virtuelles suivantes :



### 3. Objectifs

Optimiser oui, mais encore faut-il savoir comment procéder. C'est sûrement l'opération la plus difficile à réaliser car elle ne dépend pas uniquement de la connaissance du système d'exploitation mais également des connaissances sur le matériel et elle fait appel à l'expérience.

Une autre difficulté que vous rencontrerez est que derrière toute action d'optimisation qui fait sauter un goulet, il existe un autre goulet ! L'expérience aide pour déterminer s'il est plus ou moins proche.

Dans ce chapitre, vous apprendrez quels composants sont importants pour améliorer les performances globales d'un système et les outils utiles pour identifier un goulet d'étranglement comme le **Gestionnaire des tâches**, le **Moniteur de fiabilité et de performances**.

Que faire lorsqu'un problème survient, comment l'identifier, comment dépanner le serveur sont des questions qui restent parfois sans réponse. Pour y répondre, ce chapitre passe en revue les utilitaires les plus courants fournis avec Windows Server 2008 qui sont une aide précieuse pour identifier un problème y compris l'étude exhaustive de l'observateur d'événements et de ses nouveautés.

La fin du chapitre montre les différents autres outils dont vous pourriez avoir besoin comme ceux de **Sysinternals** créés par Mark Russinovitch appartenant actuellement à Microsoft.

# Validation des acquis : questions/réponses

## 1. Questions

### Questions triviales

- 1 Quelle différence faites-vous entre un pare-feu réseau et un pare-feu d'hôte ?
- 2 Comment les règles du pare-feu sont-elles ajoutées ?
- 3 Quelle différence faites-vous entre **netsh firewall** et **netsh advfirewall** ?
- 4 Est-il possible de créer une règle pour le pare-feu concernant un service spécifique ?
- 5 À quoi sert le NAT ?
- 6 Citez trois protocoles VPN sécurisés inclus dans Windows Server 2008.
- 7 Citez un protocole VPN utilisant HTTPS comme couche de transport.
- 8 Citez au moins trois composants de contrainte d'un système NAP.
- 9 Dans quel cas devez-vous utiliser un serveur HRA ?
- 10 Citez au moins un élément de déclaration d'intégrité.

### Questions de compréhension

- 11 Votre collègue vous demande votre avis car il doit déployer six nouvelles règles sur le pare-feu des ordinateurs Windows Vista, il penche pour la création d'un script utilisant la commande **netsh advfirewall**. Qu'en pensez-vous et quelle est votre réponse ?
- 12 Un de vos collègues ne comprend pas pourquoi tout le monde dit que la configuration d'**IPSec** est simple alors qu'il trouve qu'elle n'a pas évolué depuis Windows 2000. Que lui répondez-vous ?
- 13 Votre collègue ne comprend pas pourquoi la configuration d'**IPSec** se trouve aujourd'hui placée dans la même console que le pare-feu, que pouvez-vous lui répondre ?
- 14 Vous demandez à votre collègue de configurer le **NAT** pour un site distant et il vous répond qu'il n'arrive pas à trouver l'onglet **Partage**, que lui répondez-vous ?
- 15 Un de vos collègues ne comprend pas la différence qui existe entre l'onglet **Services et ports** des propriétés du serveur NAT et les règles du pare-feu. Que lui répondez-vous ?
- 16 Un de vos collègues aimerait configurer toutes les authentifications possibles afin de garantir que tous les ordinateurs de l'entreprise puissent se connecter. Qu'en pensez-vous et que lui répondez-vous ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /16

Pour ce chapitre, votre score minimum doit être de 12 sur 16.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

## 3. Réponses

### Questions triviales

- 1 Quelle différence faites-vous entre un pare-feu réseau et un pare-feu d'hôte ?  
*Un pare-feu réseau protège un réseau entier contre des attaques externes au réseau de l'entreprise alors que le pare-feu d'hôte protège les ordinateurs contre des attaques internes.*
- 2 Comment les règles du pare-feu sont-elles ajoutées ?

Lorsque vous installez une application les règles nécessaires sont automatiquement ajoutées et configurées correctement.

**3** Quelle différence faites-vous entre **netsh firewall** et **netsh advfirewall** ?

**Netsh firewall** est l'ancienne méthode pour gérer le pare-feu. Il ne faudrait plus l'utiliser.

**4** Est-il possible de créer une règle pour le pare-feu concernant un service spécifique ?

Oui tout à fait.

**5** À quoi sert le NAT ?

Le NAT permet de n'utiliser qu'une adresse IP publique pour aller sur Internet quel que soit le nombre d'ordinateurs internes qui utilisent généralement des adresses privées provenant de la RFC 1918.

**6** Citez trois protocoles VPN sécurisés inclus dans Windows Server 2008.

Vous pouvez citer :

- PPTP
- L2TP/IPSec
- SSTP

**7** Citez un protocole VPN utilisant HTTPS comme couche de transport.

Bien entendu, il s'agit du protocole SSTP.

**8** Citez au moins trois composants de contrainte d'un système NAP.

Vous pouvez citer :

- **Serveur DHCP** de Windows Server 2008 pour recevoir une adresse IP provenant d'un serveur DHCP.
- **Serveur de routage et d'accès à distance** de Windows Server 2008 pour des accès VPN.
- **Autorité de certification NAP HRA** (Health Registration Authority) qui gère les demandes de certificats auprès d'une autorité de certification existante au nom du client NAP. Actuellement, la contrainte de mise en conformité NAP IPSec exige ce composant. Dans Windows Server 2008, il s'installe sur le même ordinateur que le serveur NPS et les services IIS doivent être également installés.
- **Serveur Terminal Services Gateway** de Windows Server 2008 pour des accès à Terminal Server.
- **Périphérique 802.1X**, il peut être utilisé aussi bien pour gérer des accès sans fil que des accès filaires.

**9** Dans quel cas devez-vous utiliser un serveur HRA ?

**L'autorité de certification NAP HRA** (Health Registration Authority) gère les demandes de certificats auprès d'une autorité de certification existante au nom du client NAP. Actuellement, la contrainte de mise en conformité NAP IPSec exige ce composant.

**10** Citez au moins un élément de déclaration d'intégrité.

Vous pouvez citer :

- Un logiciel pare-feu est **installé et activé**.
- Un logiciel antivirus est **installé et exécuté**.
- Les dernières mises à jour antivirus sont **installées**.
- Un logiciel anti-espion est **installé et exécuté**.
- Les dernières mises à jour anti-espionnes sont **installées**.
- Microsoft Update est **activé** sur l'ordinateur client.

## Questions de compréhension

- 
- 11** Votre collègue vous demande votre avis car il doit déployer six nouvelles règles sur le pare-feu des ordinateurs Windows Vista, il penche pour la création d'un script utilisant la commande **netsh advfirewall**. Qu'en pensez-vous et quelle est votre réponse ?

*Sa solution est possible mais il est préférable d'utiliser les stratégies de groupe pour les déployer. C'est plus efficace et cela garantit qu'un utilisateur ne peut les modifier.*

- 12** Un de vos collègues ne comprend pas pourquoi tout le monde dit que la configuration d'**IPSec** est simple alors qu'il trouve qu'elle n'a pas évolué depuis Windows 2000. Que lui répondez-vous ?

*Il utilise sûrement l'ancien outil soit la console **Stratégies de sécurité IP** qui n'est fournie que pour la compatibilité. Il faut lui préférer le **Pare-feu avec les fonctions avancées de sécurité**.*

- 13** Votre collègue ne comprend pas pourquoi la configuration d'IPSec se trouve aujourd'hui placée dans la même console que le pare-feu, que pouvez-vous lui répondre ?

*En réalité le pare-feu utilise des règles comme pour IPSec. Microsoft a jugé intéressant de les placer dans la même console.*

- 14** Vous demandez à votre collègue de configurer le **NAT** pour un site distant et il vous répond qu'il n'arrive pas à trouver l'onglet **Partage**, que lui répondez-vous ?

*L'onglet **Partage** est utilisé pour configurer le Partage de connexion Internet. Lorsque NAT est activé sur un serveur ce dernier est caché.*

- 15** Un de vos collègues ne comprend pas la différence qui existe entre l'onglet **Services et ports** des propriétés du serveur NAT et les règles du pare-feu. Que lui répondez-vous ?

*Il s'agit de règles qui pour le pare-feu ont une portée limitée à l'hôte alors que pour le NAT la portée est le réseau interne. Enfin pour le NAT, le trafic entrant peut également être redirigé vers un hôte particulier.*

- 16** Un de vos collègues aimerait configurer toutes les authentifications possibles afin de garantir que tous les ordinateurs de l'entreprise puissent se connecter. Qu'en pensez-vous et que lui répondez-vous ?

*C'est inutile, voire une mauvaise pratique, car des utilisateurs pourraient se connecter en utilisant des protocoles d'authentification pas ou peu sécurisés comme PAP ou CHAP.*

## Résumé du chapitre

Dans ce chapitre, vous avez appris à configurer des règles dans le pare-feu aussi bien pour protéger l'ordinateur contre des accès malveillants que pour sécuriser des connexions à l'aide d'IPSec. Ensuite, vous avez vu les différentes possibilités offertes par le service Routage et accès distant et surtout les possibilités de création des VPN ou d'installation et de configuration du service NAT. Enfin, NAP vous a été présenté de manière détaillée afin de comprendre son fonctionnement.

## Travaux pratiques

Dans les travaux pratiques pour les exercices 6, 7, 8, 9 et 10, vous devrez effectuer les opérations suivantes :

- Configurer et modifier des règles du pare-feu (Exercice 6).
- Implémenter IPSec pour sécuriser un serveur (Exercice 6).
- Mettre en œuvre une connexion VPN simple (Exercice 7).
- Mettre en œuvre une connexion VPN utilisant SSTP et un serveur Radius (Exercice 9).
- Implémenter NAT (Exercice 8).
- Implémenter la protection réseau NAP pour l'attribution d'adresses IP (Exercice 10).

## Accès réseau sans fil

Un des objectifs de l'examen 70-642 indique qu'il est nécessaire de connaître les réseaux sans fil. Bien que cet objectif ne touche pas directement un serveur ou en tout cas pas un serveur dans une grande entreprise car il est très peu probable qu'un serveur utilise une connexion sans fil, l'objectif ici est de comprendre les accès réseau sans fil pour créer des stratégies permettant à des ordinateurs clients de se connecter.

Les réseaux sans fil se démocratise et l'on trouve de plus en plus de points d'accès appelés également *hot spot* à travers le monde. Certains opérateurs de téléphonie proposent également des offres d'abonnement permettant à l'utilisateur nomade de se déplacer tout en utilisant différentes technologies, dont les réseaux sans fil. Au sein de l'entreprise, les réseaux sans fil peuvent rendre d'énormes services dans les cas où les collaborateurs doivent se déplacer d'un bureau à un autre, dans les salles de réunion et bien entendu dans les bâtiments dans lesquels il n'est pas possible d'installer des réseaux filaires comme par exemple dans des bâtiments classés.

Les principaux reproches adressés aux réseaux sans fil concernent l'utilisation d'une bande passante limitée et partagée entre tous les ordinateurs d'un point d'accès ainsi qu'une carence de sécurité au niveau de la couche transport.

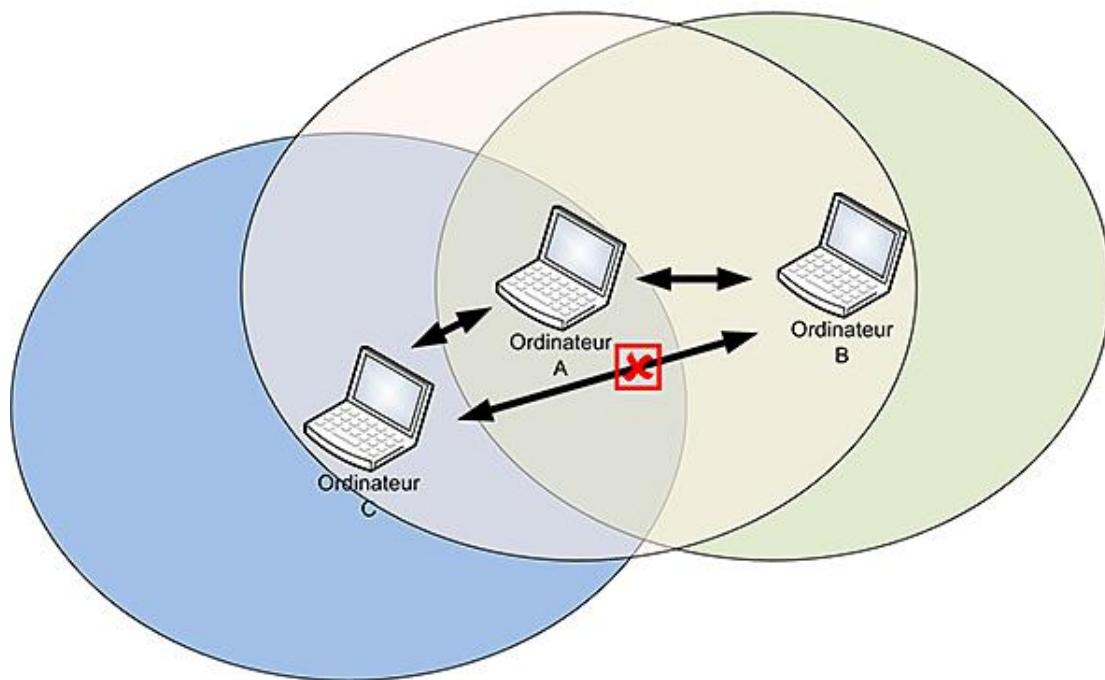
L'un des travaux de l'administrateur réseau consiste à limiter correctement le cadre d'utilisation des réseaux sans fil pour les utilisateurs nomades. Un autre travail consiste à rendre l'utilisation des réseaux sans fil de l'entreprise transparente. Pour effectuer ces tâches, il est nécessaire de comprendre les réseaux sans fil.

### 1. Mode d'infrastructure versus mode ad hoc

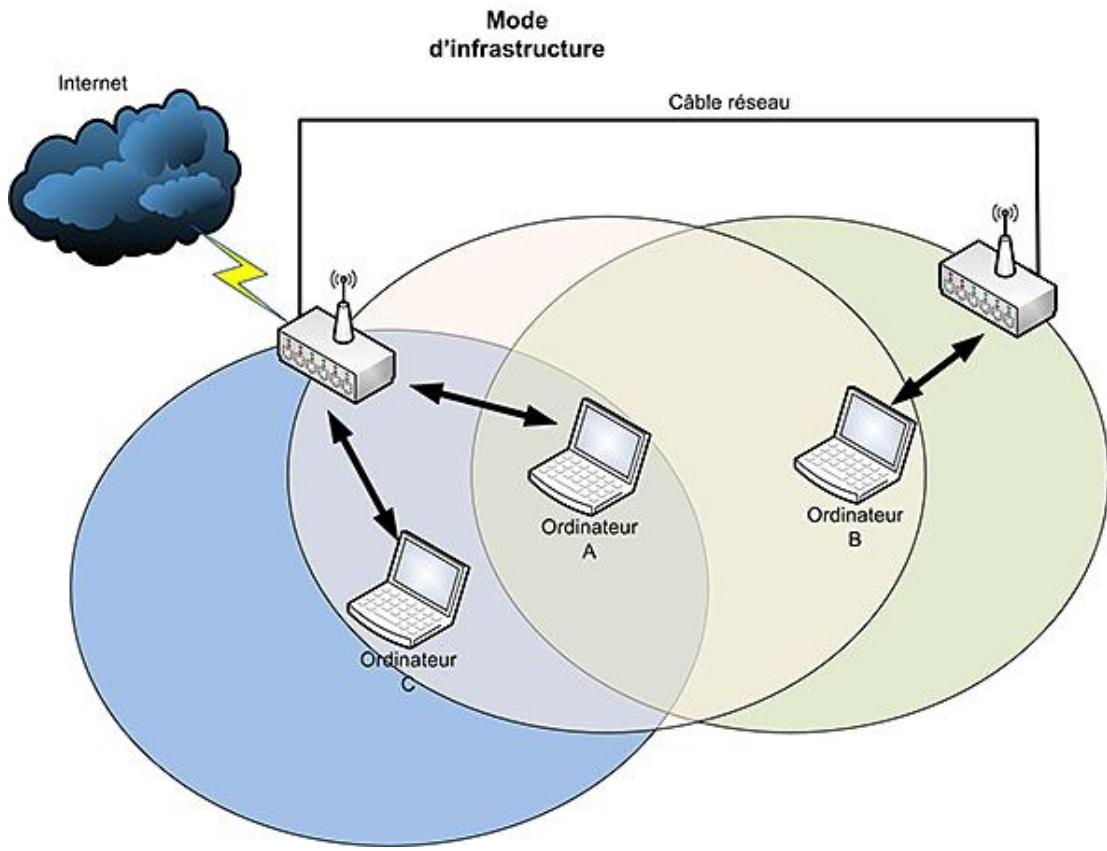
Dans le mode ad hoc, les ordinateurs peuvent communiquer entre eux sans passer par une infrastructure, en d'autres termes, ils peuvent communiquer directement avec leurs voisins situés dans leur espace de communication. Dans le mode d'infrastructure, toutes les communications passent obligatoirement par un périphérique d'infrastructure qui est généralement appelé un point d'accès.

La figure suivante montre le mode ad hoc dans lequel l'ordinateur A peut dialoguer avec ses pairs, soient l'ordinateur B et l'ordinateur C. Les disques représentent la zone de communication possible pour chaque ordinateur. Comme l'ordinateur B est hors de portée de l'ordinateur C il ne peut y avoir de communication entre eux.

Réseau ad-hoc



La figure suivante montre les mêmes ordinateurs reliés via un point d'accès distant. Cette fois tous les ordinateurs peuvent communiquer ensemble, voire aller sur Internet grâce aux éléments d'infrastructure.



Pour des raisons de sécurité évidentes, il est recommandé de désactiver les communications ad hoc sur les ordinateurs portables des utilisateurs.

## 2. Le point d'accès

Le point d'accès est identifié par son SSID (*Service Set Identifier*) qui est le nom du point d'accès. Il se compose d'une suite de 1 à 32 caractères alphanumériques. Généralement le point d'accès diffuse son SSID en utilisant des messages de diffusion (Broadcast). Bien qu'il soit possible de désactiver les messages de diffusion, c'est une méthode de protection totalement inefficace du réseau car chaque fois qu'un utilisateur se connecte, l'ordinateur client envoie le SSID du réseau en clair. D'autre part, cela complique la connexion pour les utilisateurs car ils doivent saisir manuellement le SSID du réseau pour pouvoir se connecter.

## 3. Les différentes normes Wi-Fi

Les réseaux sans fil sont réunis dans la norme IEEE 802.11. Bien qu'il existe un nombre important de normes Wi-Fi, seules les normes présentées dans le tableau suivant sont utilisées pour le transport.

Norme	Débit	Fréquence	Commentaire
802.11a	54Mb/s théorique 27Mb/s réel	5GHz	Peu utilisée actuellement. Portée limitée à un rayon d'environ 10 m.
802.11b	11Mb/s théorique 6Mb/s réel	2,4GHz	Largement utilisée Portée limitée à 300m
802.11g	54Mb/s théorique 25Mb/s réel	2,4GHz	Très largement répandue actuellement
802.11n	600Mb/s théorique	2,4GHz	Normalisation attendue pour le second

100Mb/s réel	5GHz	semestre 2009. Reste compatible avec les matériels existants 802.11b et 802.11g.
--------------	------	---

 Attention, la norme 802.1X est un standard de sécurité pour les réseaux sans fil et filaires permettant au matériel de s'authentifier pour avoir accès au réseau. 802.1X s'appuie sur EAP (Extensible Authentication Protocol) pour le transport des informations d'identification et un serveur d'identification comme par exemple l'utilisation d'un serveur Radius.

### a. Limitations

Parmi les limitations, il est possible de citer :

- Un réseau Wi-Fi par sa nature limite le nombre d'ordinateurs pouvant se connecter au même instant sur un point d'accès car la bande passante est partagée entre tous les ordinateurs connectés à ce point d'accès.
- Par défaut les signaux ne sont pas chiffrés et sont de ce fait facilement écoutables à l'aide d'outils appropriés.
- Les murs et éventuellement les matériaux les composant peuvent limiter la portée d'un point d'accès voire limiter l'utilisation d'un réseau Wi-Fi.

## 4. Sécurisation

Pour sécuriser une connexion Wi-Fi, il est nécessaire de sécuriser les communications en utilisant le chiffrage et éventuellement l'authentification. Pour cela, il est possible d'utiliser les protocoles ci-dessous.

### a. WEP (Wired Equivalent Privacy)

WEP définit un algorithme de chiffrement pour garantir un niveau de confidentialité équivalent à un réseau filaire. WEP utilise le protocole RC4 pour le chiffrement. La taille de la clé varie en fonction de son implémentation soit 40 bits pour WEP 64, 104 bits pour WEP 128 et 240 bits pour WEP 256.

Sous Windows Server 2008, la clé WEP doit comporter 26 caractères hexadécimaux (0-9 et lettres a-f).

Il s'agit de la plus mauvaise des méthodes de chiffrement car aujourd'hui il est possible de pénétrer un réseau protégé par une clé WEP en quelques secondes. Il est dès lors conseillé d'utiliser une autre méthode ou si ce n'est pas possible de remplacer le matériel du point d'accès, voire d'utiliser le protocole IPSec pour les communications Wi-Fi.

### b. WPA (Wi-Fi Protected Access) et WPA2

WPA est un programme de certification créé par la Wi-Fi alliance pour pallier les problèmes de sécurité de WEP.

WPA ajoute des fonctionnalités de sécurité à WEP et à l'authentification 802.11 comme :

- L'utilisation d'un mécanisme d'authentification amélioré.
- Des algorithmes de gestion de clés.
- Création de clés cryptographiques.
- Une amélioration pour l'encapsulation des données.

Le composant d'authentification est basé sur l'authentification 802.1X ce qui nécessite la mise en place d'une infrastructure pouvant être complexe (serveur Radius, gestion des certificats, voire mise en place d'une infrastructure de clés publiques). Heureusement, il est possible d'utiliser une version simplifiée appelée WPA-Personal qui permet l'utilisation de clés pré-partagées pouvant contenir de 8 à 63 caractères ASCII ou 64 caractères hexadécimaux au lieu d'une infrastructure 802.1X.

WPA fait référence aux ébauches de la norme 802.11i alors que WPA2 en est la version normalisée. WPA2 implémente tous les éléments obligatoires de la norme 802.11i et utilise AES comme algorithme de chiffrement au lieu de RC4.

La plupart des cartes réseaux compatibles WEP ont juste besoin d'être mises à jour pour supporter WPA.

Concernant la sécurité, elle est meilleure que celle de WEP, néanmoins WPA-Personal est plus vulnérable que WPA.

## 5. Gestion des réseaux sans fil à l'aide des stratégies de groupe



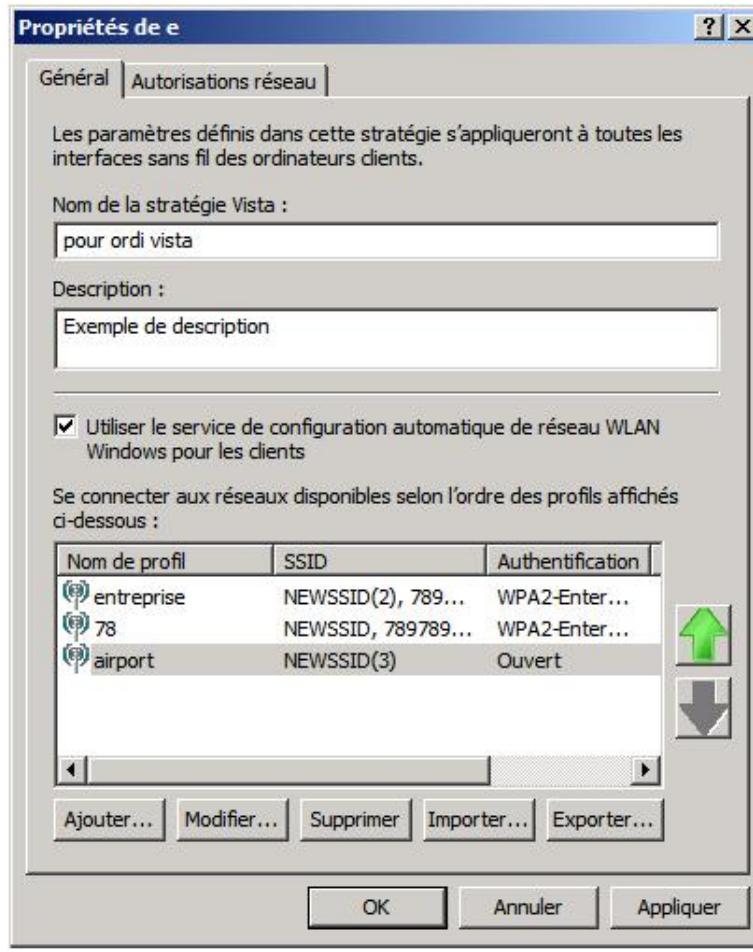
Dans une entreprise, il est plus simple de gérer les réseaux sans fil en utilisant les stratégies de groupe comme le montre la procédure suivante.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration et Gestion des stratégies de groupe**. Il faut être dans un domaine.
- Par exemple, développez l'arborescence jusqu'au domaine puis cliquez avec le bouton droit de la souris sur le nom du domaine puis sur **Créer un objet GPO dans ce domaine, et le lier ici**.
- Dans la boîte de dialogue, saisissez **wifi** pour le **Nom** puis cliquez sur **OK**.
- Dans l'arborescence, cliquez avec le bouton droit de la souris sur **wifi** puis sur **Modifier**.
- Dans l'éditeur de gestion des stratégies de groupe, développez l'arborescence suivante : **Stratégie wifi - Stratégies - Paramètres Windows - Paramètres de sécurité - Stratégies de réseau sans fil (IEEE 802.11)**.

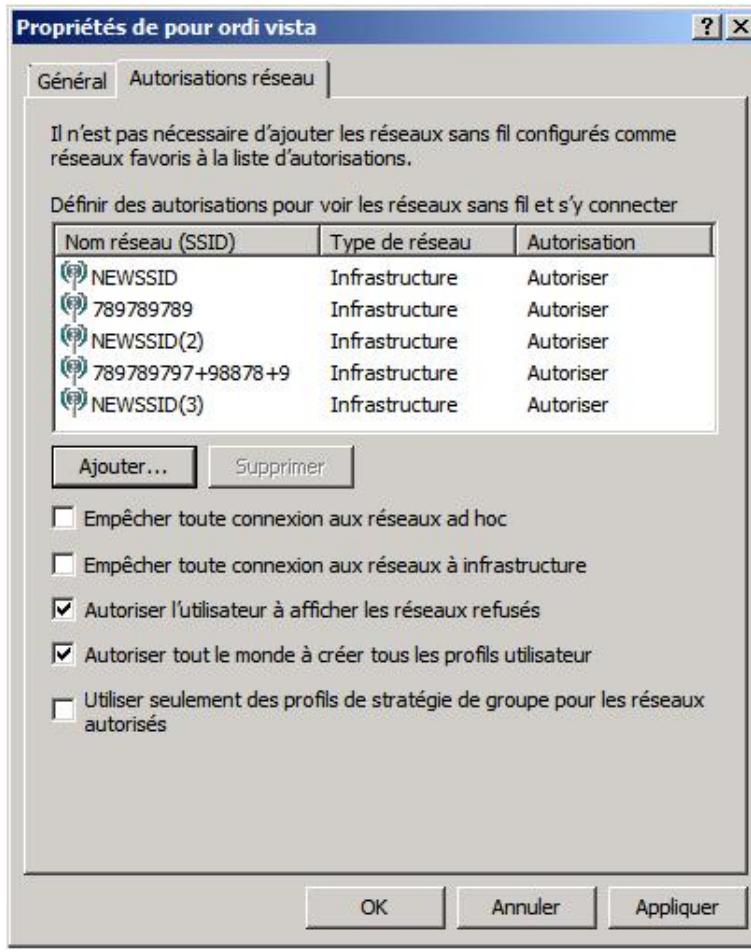
Vous pouvez créer des stratégies adaptées pour Windows Vista et Windows XP.

- Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Stratégies de réseau sans fil (IEEE 802.11)** puis sur **Créer une stratégie de réseau sans fil Vista**.
- Dans la boîte de dialogue **Propriétés de Nouvelle stratégie de réseau sans fil Vista** sous l'onglet **Général** saisissez un nom pour la stratégie et éventuellement une description. Ne désactivez pas la case à cocher **Utiliser le service de configuration automatique de réseau WLAN Windows pour les clients** sinon le service ne configurera plus les réseaux sans fil.

Dans la liste, vous pouvez gérer des réseaux sans fil auquel l'utilisateur peut se connecter. Vous pouvez définir pour chaque connexion une liste des SSID utilisables, et une méthode d'authentification et de chiffrement appropriée comme le montre l'image suivante.



L'onglet **Autorisations réseau** permet de gérer pour chaque nom réseau (SSID) des profils définis sous l'onglet **Général** une autorisation ou un refus comme le montre l'image suivante.



La case à cocher **Empêcher toute connexion aux réseaux ad hoc** permet d'empêcher l'utilisateur de créer de nouveaux profils et d'utiliser les profils ad-hoc définis.

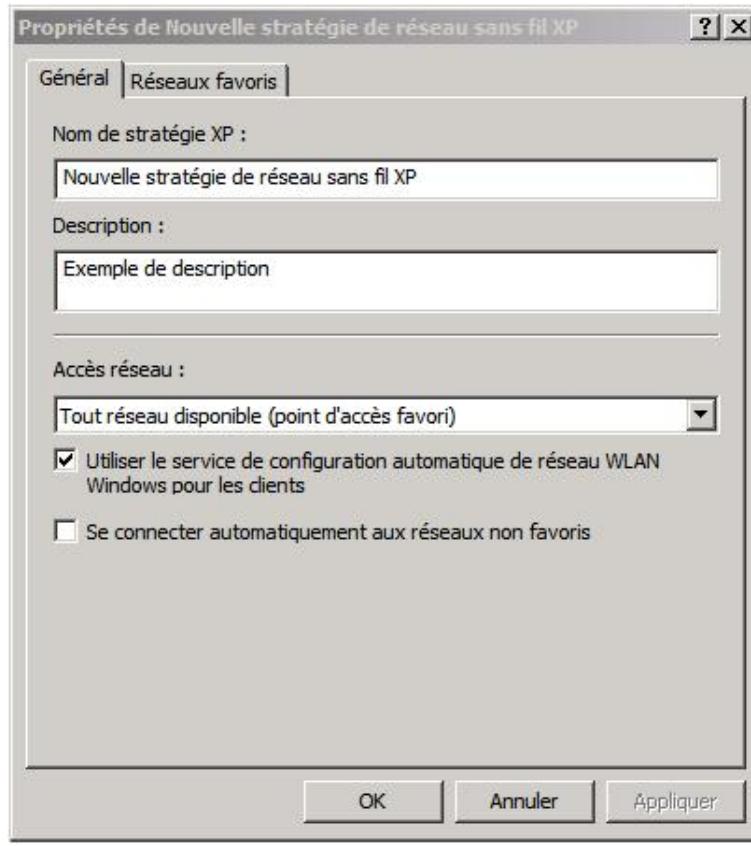
La case à cocher **Empêcher toute connexion aux réseaux à infrastructure** permet d'empêcher la connexion à la liste des réseaux d'infrastructure.

La case à cocher **Autoriser l'utilisateur à afficher les réseaux refusés** permet à l'utilisateur de voir également les réseaux sans fil qui sont définis comme **Refuser**.

La case à cocher **Autoriser tout le monde à créer tous les profils utilisateur** permet de spécifier si l'utilisateur peut créer de nouveaux profils sinon seuls les membres du groupe **Administrateurs** et **Opérateurs de réseaux** peuvent en créer.

La case à cocher **Utiliser seulement des profils de stratégie de groupe pour les réseaux autorisés** permet de limiter les réseaux auxquels l'utilisateur peut se connecter.

- Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Stratégies de réseau sans fil (IEEE 802.11)** puis sur **Créer une stratégie Windows XP**.
- Dans la boîte de dialogue **Propriétés de Nouvelle stratégie de réseau sans fil XP** sous l'onglet **Général** saisissez un nom pour la stratégie et éventuellement une description comme le montre l'image suivante.



La liste déroulante permet de spécifier la méthodologie d'accès réseau selon les valeurs suivantes **Tout réseau disponible (point d'accès favori)**, c'est-à-dire qui est défini sous l'onglet **Réseaux favoris** donc très restrictif, **Réseaux avec point d'accès uniquement (infrastructure)** ou **Réseau d'égal à égal (ad hoc) uniquement**.

Ne désactivez pas la case à cocher **Utiliser le service de configuration automatique de réseau WLAN Windows pour les clients** sinon le service ne configurera plus les réseaux sans fil.

Vous pouvez également spécifier qu'il est possible de se connecter automatiquement aux réseaux non favoris en activant la case à cocher correspondante.

Sous l'onglet **Réseaux favoris**, vous pouvez gérer la liste des réseaux favoris.

# Présentation de la protection d'accès réseau (NAP)

Du temps où Windows Server 2008 s'appelait encore Longhorn, une des nouveautés qui nous a tenu en haleine a été NAP (*Network Access Protection*) et la manière dont il allait être implémenté dans Windows Server 2008. Dans Windows Server 2003, il existe déjà une fonctionnalité similaire appelée **Network Access Quarantaine** qui permet de limiter l'accès aux clients VPN et aux connexions à distance si leur ordinateur n'est pas conforme à la sécurité demandée, en se basant sur l'exécution de scripts.

NAP reprend le concept de la quarantaine de Windows 2003 et l'étend à d'autres méthodes d'accès ou de communication réseau pour aider les administrateurs à garantir que les ordinateurs du réseau de l'entreprise soient conformes à la politique d'intégrité de sécurité.

- NAP n'a pas été conçu pour garantir la sécurité contre des accès non autorisés mais pour garantir l'intégrité de la sécurité.

Il faut garder à l'esprit que NAP n'interdit pas les utilisateurs de télécharger, d'installer ou d'exécuter des logiciels non autorisés sur leur ordinateur.

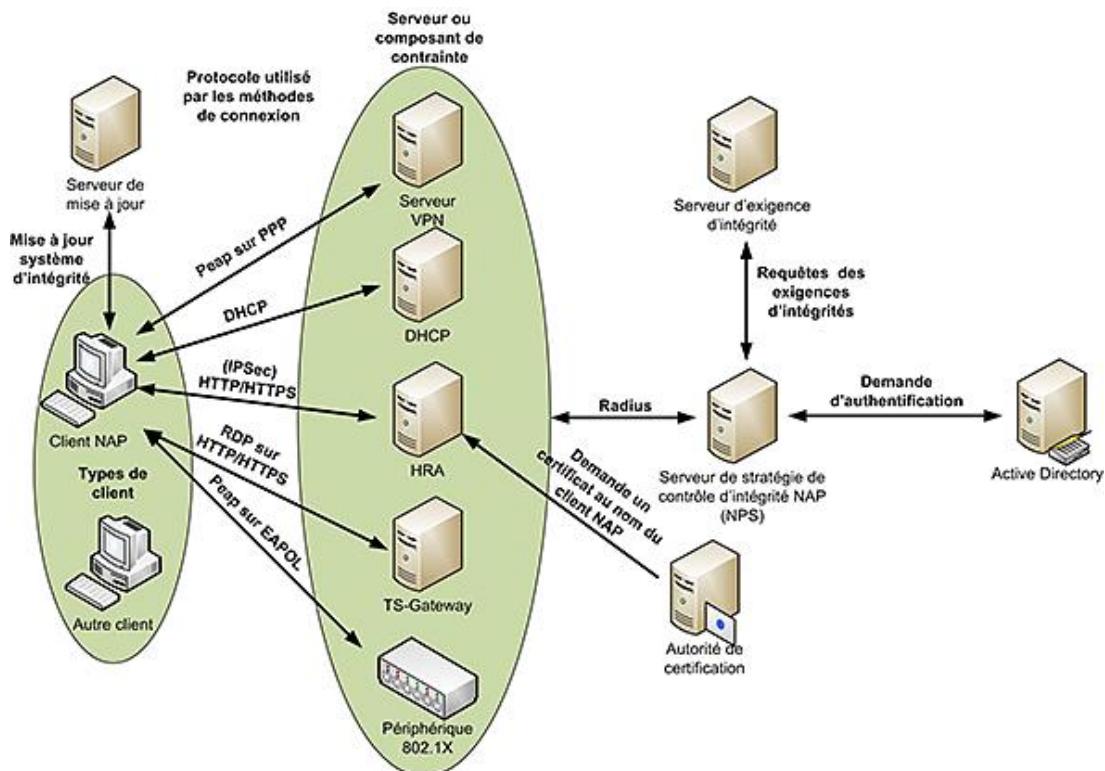
Actuellement, il devient de plus en plus difficile de garantir que tous les ordinateurs de l'entreprise sont intègres car certains utilisateurs mobiles peuvent être absents du réseau de l'entreprise pendant des jours, voire des semaines, ce qui les rend à terme plus vulnérables puisqu'ils ne reçoivent pas forcément les mises à jour de sécurité, les mises à jour applicatives ou les signatures des anti-virus et autres anti-spywares exigés par l'administrateur.

Dans un cadre traditionnel, l'ordinateur mobile qui rentre sur le réseau dispose d'un accès illimité aux ressources, et seulement ensuite il reçoit automatiquement les mises à jour. Il est clair qu'un risque de contaminer les autres ordinateurs du réseau existe dès le moment où l'ordinateur mobile entre sur le réseau et ce jusqu'au moment où toutes ces mises à jour sont appliquées. Fort d'une alliance avec de nombreux partenaires de renom, Microsoft propose une solution de mise en quarantaine de réseau nommée NAP (*Network Access Protection*).

Concernant les ordinateurs clients, il faut disposer d'un client NAP ; actuellement Windows Server 2008, Windows Server Vista et Windows XP SP3 disposent d'un client NAP. Une société partenaire a créé un client NAP pour des ordinateurs Linux et Macintosh.

## 1. Architecture et terminologie d'un système NAP

L'architecture d'un système NAP demande les composants suivants :



- **Client NAP**, soit un ordinateur supportant NAP et disposant des éléments nécessaires pour envoyer une

déclaration d'intégrité qui décrit son état d'intégrité. Au moins un client est requis.

- **Autre client**, soit un ordinateur qui ne supporte pas NAP. On parle également de **client non compatible NAP**.
- **Elément de contrainte** correspond à un serveur applicatif ou à un périphérique réseau qui est utilisé pour échanger les informations ou aider à la validation de celles-ci auprès du serveur de stratégie de contrôle d'intégrité. Au moins un élément est requis. Dans Windows Server 2008, il s'agit de :
  - **Serveur DHCP** de Windows Server 2008 pour recevoir une adresse IP provenant d'un serveur DHCP.
  - **Serveur de routage et d'accès à distance** de Windows Server 2008 pour des accès VPN.
  - **Autorité de certification NAP HRA** (*Health Registration Authority*) qui gère les demandes de certificats auprès d'une autorité de certification existante au nom du client NAP. Actuellement, la contrainte de mise en conformité NAP IPSec exige ce composant. Dans Windows Server 2008, il s'installe sur le même ordinateur que le serveur NPS et les services IIS doivent être également installés.
  - **Serveur Terminal Services Gateway** de Windows Server 2008 pour des accès à Terminal Server.
  - **Périphérique 802.1X** qui peut être utilisé aussi bien pour gérer des accès sans fil que des accès filaires.
- **Serveur de stratégie HPS** (*Health Policy Server*) correspond au rôle joué par le serveur NPS pour gérer les stratégies et valider la conformité du client NAP. Ce serveur est requis dans tous les cas.
- **Serveur d'exigence d'intégrité** (*Health Requirement Server*) correspond à un serveur qui sert de référence pour déterminer l'état de conformité d'une mesure et fournit cette information au serveur de stratégie, comme par exemple un serveur d'antivirus qui fournit au serveur **NPS** la dernière version du fichier de signatures. Ce type de serveur est optionnel et dépend des mesures à effectuer pour garantir l'intégrité. Bien entendu le serveur fournisseur d'intégrité doit supporter NAP.
- **Serveur Active Directory** permet au serveur Radius d'authentifier les clients dans un domaine. Ce serveur est requis pour les méthodes de contrainte de mise en conformité NAP IPSec, VPN et 802.1X.
- **Autorité de certification** est le serveur qui émet les certificats pour la méthode de contrainte de mise en conformité NAP IPSec. Et il peut également être utilisé pour l'authentification qui utilise des certificats comme les cartes à puces dans les méthodes de contrainte de mise en conformité NAP VPN et 802.1X.
- **Réseau illimité** correspond au réseau de l'entreprise auquel a accès le client NAP conforme aux exigences d'intégrité.
- **Réseau restreint** fait référence à un réseau logique ou physique sur lequel sont placés les :
  - **Serveurs de mise à jour** correspondant à un ou plusieurs serveurs se trouvant sur le réseau restreint qui fournissent les ressources requises au client NAP pour devenir conforme avec la stratégie de contrôle d'intégrité. Par exemple, il peut s'agir d'un serveur permettant de télécharger les dernières signatures de l'antivirus ou d'un serveur WSUS pour recevoir les mises à jour de sécurité. À installer et à configurer en fonction des mesures d'intégrité voulues.
  - **Clients non conforme**, jusqu'à ce qu'ils deviennent conformes en téléchargeant les mises à jour auprès des serveurs de mise à jour.
  - **Clients non compatible NAP**.

## 2. Fonctionnalités de NAP

### a. Déclaration d'intégrité

NAP permet de créer des stratégies d'intégrité de la sécurité basées sur des déclarations d'intégrités. Les

déclarations d'intégrités suivantes sont disponibles sur Windows Server 2008 à l'installation du serveur NPS :

- Un logiciel pare-feu est **installé et activé**.
- Un logiciel antivirus est **installé et exécuté**.
- Les dernières mises à jour antivirus sont **installées**.
- Un logiciel anti-espion est **installé et exécuté**.
- Les dernières mises à jour anti-espionnes sont **installées**.
- Microsoft Update est **activé** sur l'ordinateur client.

Il est possible de créer d'autres déclarations d'intégrité en développant les parties serveur et cliente.

## b. Méthodes de contrainte

Le tableau suivant présente les méthodes de contrainte de mise en conformité NAP actuelles ainsi que le résultat attendu si le client est conforme ou non :

Conformité	Client conforme	Client non conforme
<b>DHCP</b>	Reçoit une adresse IP non restreinte. Accède au réseau illimité.	Reçoit une adresse IP restreinte au niveau des routes. Accès au réseau restreint.
<b>VPN</b>	Accède au réseau illimité.	Accès au réseau restreint.
<b>802.1X</b>	Accède au réseau illimité.	Est placé dans un VLAN limité.
<b>IPSec</b>	Peut communiquer avec ses pairs.  Protection complémentaire à la couche 2. Fonctionne avec l'infrastructure et les serveurs existants. Isolation flexible.	Les pairs conformes rejettent les connexions des pairs non conformes. Se trouve dans un réseau restreint.
<b>TS-Gateway</b>	Fonctionne avec <b>Terminal Services Gateway</b> .	
<b>NAP-NAC</b>	Permet d'intégrer l'équivalent du NAP Cisco appelé <b>NAC</b> ( <i>Network Access Control</i> ) en utilisant le protocole HCAP ( <i>Host Credential Authorization Protocol</i> ).	

 Un des grands avantages de NAP est d'intégrer des technologies existantes de connexion au réseau en créant une solution unique de protection évolutive.

## c. Processus d'un système NAP

Les processus d'un système NAP sont :

- **La validation de la stratégie** qui permet d'interroger un ordinateur se connectant au réseau afin de connaître sa conformité par rapport aux stratégies définies par l'administrateur. Un ordinateur conforme a un accès illimité au réseau tandis qu'un ordinateur non conforme est placé sur le réseau restreint.
- **La contrainte de mise en conformité NAP assortie de restrictions réseau** qui permet de garantir la

conformité par rapport aux stratégies en proposant le téléchargement (automatique), comme avec l'utilisation d'un serveur **WSUS**, aux ordinateurs non-conformes des mises à jour manquantes, ou de modifier leur configuration en utilisant des logiciels de surveillance et de gestion comme **SCMM** (*System Center Management Server*). Un ordinateur non conforme est placé dans le réseau restreint pendant toute la durée de la mise en conformité. Ensuite, soit automatiquement, soit manuellement par une demande de l'utilisateur, il peut relancer le processus de validation.

- **Suivi de la conformité** qui permet de protéger un réseau en continu en contrôlant régulièrement que l'état d'intégrité ne change pas. Par exemple, si l'utilisateur arrête le pare-feu local et que dans la stratégie il est spécifié qu'il doit être exécuté, alors l'ordinateur peut relancer automatiquement le pare-feu. L'utilisateur devrait voir apparaître brièvement le changement d'état de conforme à non conforme, puis de nouveau conforme.

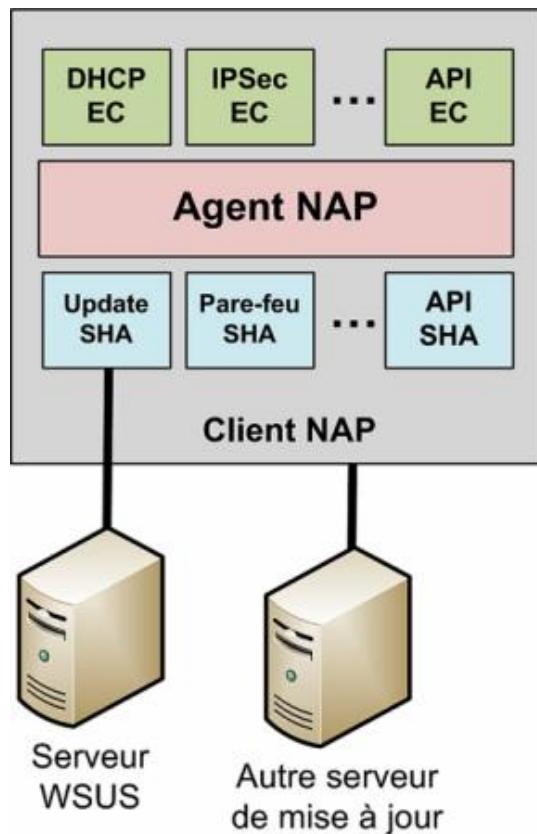
#### d. Scénarios communs pour implémenter NAP

Voici quelques scénarios d'implémentation de NAP :

- Vérification de l'état de santé des ordinateurs portables.
- Vérification de l'état de santé des ordinateurs de bureau.
- Vérification de l'état de santé des ordinateurs portables des visiteurs.
- Vérification de la santé des ordinateurs personnels des collaborateurs.

### 3. Architecture au niveau du client NAP

L'ordinateur client doit disposer d'un client NAP dont la responsabilité est la communication avec le type de demande de conformité en lui passant les informations de conformité récoltées. La figure suivante montre ces éléments :



#### a. L'agent d'intégrité système (SHA)

L'agent d'intégrité système maintient et rapporte l'état d'une ou plusieurs déclarations d'intégrité comme par exemple l'existence du pare-feu ou s'il est exécuté. L'agent d'intégrité système dialogue indirectement avec son homologue serveur appelé **Programmes de validation d'intégrité système (SHV)**, soit le composant de validation système de santé. Le SHV renvoie une réponse appelée **SoHR** (Réponse de l'état de santé) qui indique à l'agent d'intégrité système les opérations à entreprendre si le client n'est pas conforme.

Il est possible d'associer un serveur de mise à jour à une déclaration d'intégrité par exemple pour permettre le téléchargement des dernières signatures d'anti-virus.

Il est possible d'étendre les SHA existants en créant de nouveau à l'aide des **API** fournies et d'un langage de programmation.

Dans Windows Vista et Windows XP SP3, c'est l'application Windows Security Center qui fonctionne en tant qu'agent d'intégrité système.

Par contre, il n'existe pas d'agent d'intégrité système dans Windows Server 2008. Cela peut paraître un choix étrange et aucune information n'est disponible sur la raison de cette absence. D'un côté, le fait qu'un serveur non conforme soit placé sur le réseau restreint pourrait poser des problèmes de disponibilité auprès des utilisateurs, donc c'est une excellente raison de ne pas fournir un agent d'intégrité système. D'autre part, si la méthode de contrainte de mise en conformité NAP IPSec est choisie pour les clients, ils ne pourront pas communiquer avec le serveur Windows Server 2008 !

Une stratégie différente peut être créée pour des ordinateurs fonctionnant sous Windows XP et Windows Vista.

- 
-  La création d'une nouvelle déclaration d'intégrité demande la création d'un composant agent d'intégrité système pour la partie cliente, voire d'un composant par système d'exploitation supporté, et d'un programme de validation d'intégrité système qui valide la déclaration d'intégrité sur le serveur NPS.
- 

## b. Client de contrainte (EC)

Le composant client de conformité est un composant spécifique pour chaque type d'accès réseau ou de communication. Il envoie les déclarations d'intégrités appelés SSoHs (*System State of Health*) obtenues par l'agent NAP vers son homologue serveur appelé **serveur de contrainte (ES)** en utilisant un protocole de communication propre à la méthode de contrainte de mise en conformité NAP du composant.

Par défaut, Microsoft fournit les composants clients de contrainte pour les méthodes de contrainte suivantes :

- **Configuration d'adresses IPv4 DHCP.**
- **Connexion à distance VPN.**
- **Communication protégée IPSec.**
- **Connexion authentifiée 802.1X.**
- **Connexion Terminal Server par l'intermédiaire d'une passerelle TS Gateway.**

Il est possible de créer ses propres composants de contrainte en utilisant les **API** fournies. Microsoft a donc modifié les différentes applications clientes afin d'y intégrer les clients de contrainte EC.

## c. Agent NAP

L'agent NAP sert d'intermédiaire entre l'agent d'intégrité système et le client de contrainte. Ses tâches sont :

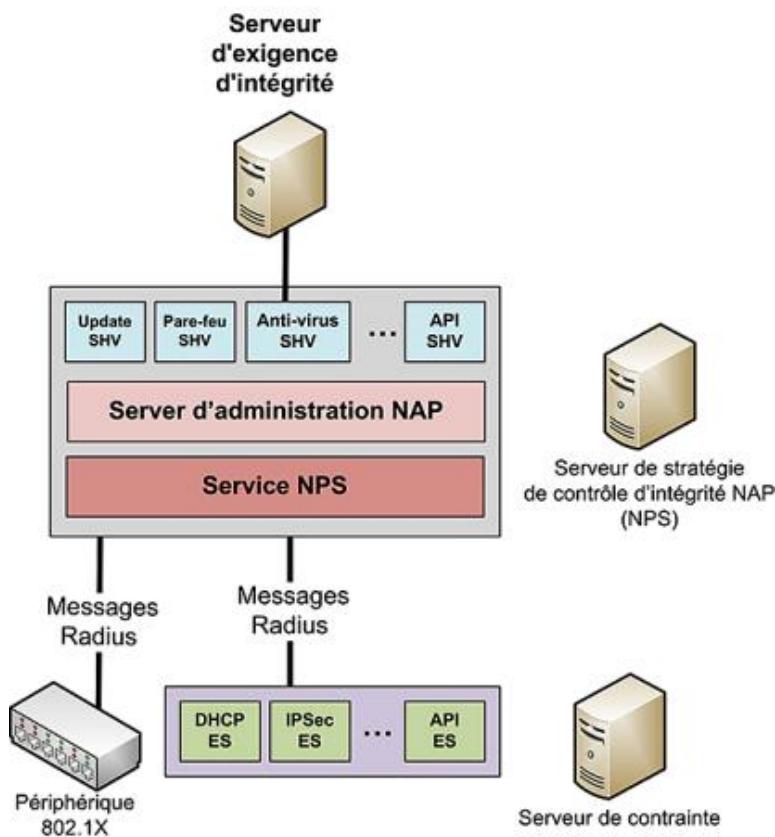
- Collecter, mettre en cache, voire mettre à jour, la déclaration d'intégrité (SoH) fournie par chaque agent d'intégrité système.
- Créer les déclarations d'intégrités (SSoH) de l'ordinateur et les passer au composant client de contrainte.
- Notifier les agents d'intégrité système lorsque la connexion réseau change.
- Passer les SoHRs à l'agent d'intégrité système approprié.



Concrètement, le client NAP est un service qu'il faut démarrer. Ensuite, il est nécessaire de le configurer afin qu'il réagisse en activant les composants clients de contrainte appropriés.

## 4. Architecture du côté serveur NAP

Du côté serveur, certains composants peuvent être placés sur d'autres ordinateurs mais vous retrouvez la notion de modularité présentée du côté client. En fait la majorité des composants sont l'équivalent serveur des composants clients.



### a. Serveur de stratégie de contrôle d'intégrité

Sur ce serveur, vous trouvez les composants suivants :

- **Service NPS** : correspond au service Radius Server ou Radius Proxy qui reçoit les messages SSoH provenant des éléments **ES** du serveur de contrainte et les passe au composant Serveur d'administration NAP. Ce mécanisme permet de placer les éléments de contrainte sur des éléments physiques différents.
- **Server d'administration NAP** : est l'équivalent serveur de l'agent NAP. Il est prévu pour effectuer les travaux suivants :
  - Récupérer les SSoHs de l'élément de contrainte à travers le service NPS.
  - Distribuer les SSoHs vers le programme de validation d'intégrité système approprié.
  - Collecter les SoHRs provenant des SHVs et les envoyer à l'élément de contrainte et de mise en conformité NAP approprié à travers le service NPS.
- **Programme de validation d'intégrité système SHV (System Health Validator)** : est l'équivalent serveur de l'agent d'intégrité système. Son objectif est de déterminer si le client NAP est conforme ou non et de renvoyer la réponse. Pour cela, il peut être aidé en fonction du validateur d'un serveur d'exigence de conformité qui lui fournit les informations pour être à jour.

Il reçoit un SoH du serveur d'administration NAP puis détermine son statut et renvoie une réponse SoHR contenant éventuellement les actions à entreprendre si le client n'est pas conforme.

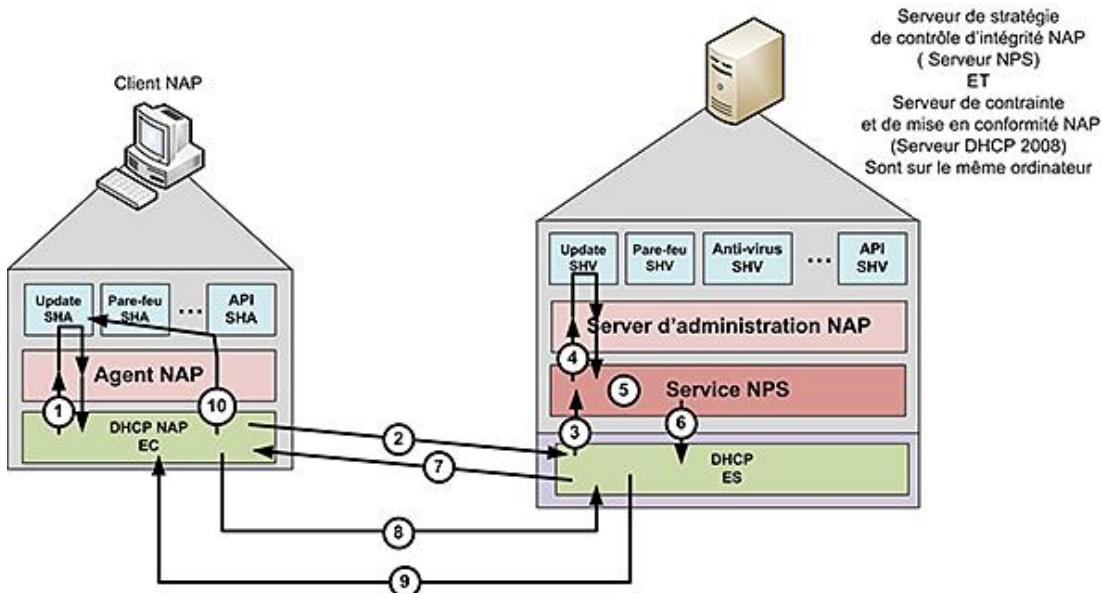
## b. Élément de contrainte de mise en conformité NAP

Il s'agit de l'équivalent serveur du composant client de conformité. Il reçoit les SSoHs provenant du client NAP via le protocole de communication utilisé par la méthode de contrainte de mise en conformité NAP, puis le passe à l'administrateur NAP en l'encapsulant dans un message Radius.

## 5. Étude détaillée du fonctionnement de NAP au travers de la méthode de contrainte de mise en conformité pour DHCP

Le client DHCP du client NAP a été modifié pour inclure le composant **DHCP NAP EC**. Il rajoute les informations SSoH aux messages DHCP en les encapsulant dans le paramètre d'option 43 **Information spécifique vendeur**.

La figure suivante montre les composants nécessaires pour réaliser la conformité DHCP :



1. Sur le client, le DHCP NAP EC interroge l'agent NAP afin d'obtenir une déclaration d'intégrité SSoH. Bien entendu, l'agent NAP passe la demande au SHA qui répond à l'agent NAP et ce dernier passe la réponse au DHCP NAP EC.

2. Le service **client DHCP** crée un message DHCP DISCOVER qui contient le SSoH et envoie le message DHCP.

3. Sur un serveur DHCP dont l'option NAP est activée, le SSoH est extrait par le composant DHCP NAP ES et envoyé au serveur de stratégie de contrôle d'intégrité NAP en l'encapsulant dans un message Radius.

4. Le **service NPS** reçoit le message Radius et passe les SoHs au SHVs appropriés qui retournent des SoHRs après analyse auprès du **serveur d'administration NAP** qui les réunit dans des SSoHRs.

5. Le **service NPS** compare les réponses SSoRHs avec les stratégies de conformité configurées pour préparer la réponse SSoHR.

6. La réponse **SSoHR** est envoyée dans un message Radius vers le serveur DHCP.

7. Le serveur DHCP envoie la réponse SSoHR en l'encapsulant dans le message DHCP OFFER.

8. Le client envoie le message DHCP REQUEST.

9. Le serveur DHCP envoie le message DHCP ACK contenant les informations d'adressage et de configuration en fonction du SSoHR. En d'autres mots, certaines options peuvent être modifiées comme le masque de sous-réseau, la passerelle par défaut, etc.

10. Le DHCP NAP EC passe le SSoHR à l'agent NAP qui le passe aux SHA appropriés. En fonction de la réponse, le client peut demander à un serveur de conformité comment se mettre en conformité.

Si le client n'est pas compatible NAP ou non conforme, il reçoit avec le message DHCP ACK, un masque de 255.255.255.255 et 0.0.0.0 pour le routeur. Il reçoit seulement une option DHCP de route statique sans classe pour lui permettre de communiquer avec les serveurs de mise à jour sur le réseau restreint.

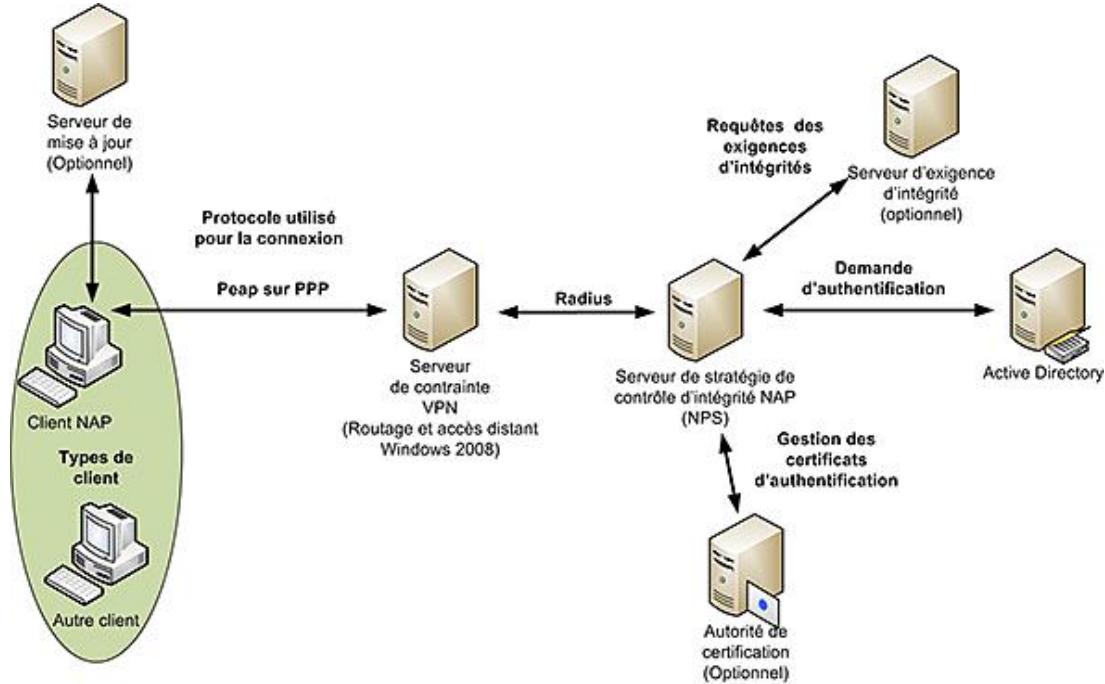
Actuellement, seule la conformité au protocole **IPv4** est prise en charge. Dans des environnements mixtes, il faut

prêter une attention particulière aux utilisateurs qui sont administrateurs, car ils peuvent modifier leurs paramètres IPv4 et obtenir un accès complet. C'est un point faible de la méthode de contrainte de mise en conformité par DHCP pour la protection d'accès réseau (NAP).

## 6. Contrainte de mise en conformité NAP pour les connexions VPN

La méthode de contrainte pour les connexions VPN permet de garantir que les ordinateurs clients sont conformes par rapport aux stratégies d'intégrité définies.

La figure suivante montre la topologie d'un tel système.

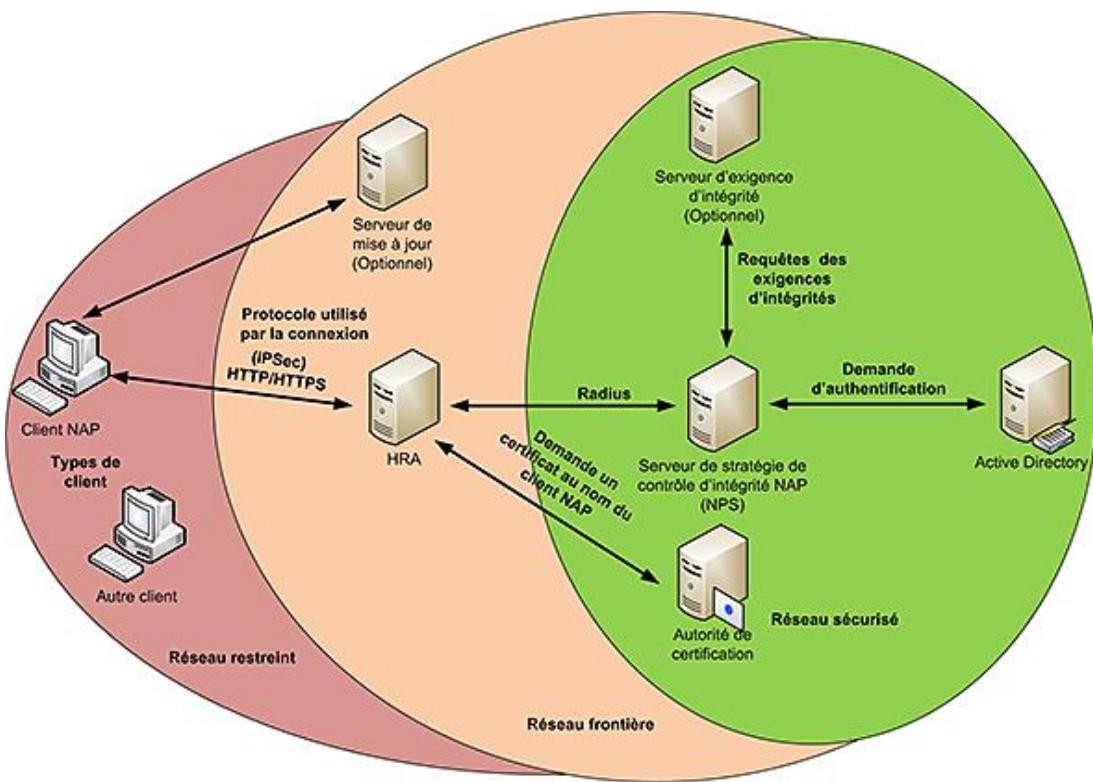


Les clients conformes ont accès à la totalité du réseau alors que les ordinateurs non conformes ou non compatibles NAP n'ont accès qu'à un réseau restreint car le serveur VPN filtre et détruit les paquets de manière silencieuse.

## 7. Contrainte de mise en conformité NAP pour les communications IPSec

La méthode de contrainte pour les communications IPSec permet de garantir que les ordinateurs clients qui sont conformes par rapport aux stratégies d'intégrité définies peuvent communiquer dans un réseau sécurisé. Cela permet de créer des domaines d'isolation.

La figure suivante montre la topologie d'un tel système.



IPSec divise le réseau physique de l'entreprise en trois sous réseaux appelés réseau restreint, réseau frontière et réseau sécurisé. Un client est toujours membre d'un seul et unique réseau.

#### a. Réseau restreint

Sur le réseau restreint, vous trouvez des clients non conformes ou qui n'ont pas reçu de certificats d'intégrité et bien entendu tous les clients non compatibles avec NAP.

Un ordinateur sur ce réseau peut communiquer avec d'autres ordinateurs se trouvant sur le réseau restreint, voire sur le réseau frontière, mais pas sur le réseau sécurisé. Par contre, ils acceptent des communications provenant de n'importe quel réseau.

#### b. Réseau frontière

Sur le réseau frontière, vous trouvez des ordinateurs qui disposent d'un certificat d'intégrité valide mais qui ne demandent pas l'utilisation du certificat d'intégrité pour des communications IPSec. Ce sont généralement les serveurs HRA et de mise à jour qui sont placés dans ce réseau.

Les ordinateurs placés sur ce réseau peuvent communiquer avec tous les ordinateurs quel que soit leur réseau, aussi bien en initiant la communication qu'en la recevant.

#### c. Réseau sécurisé

Sur le réseau sécurisé vous trouvez des ordinateurs conformes qui ont reçu un certificat valide en conséquence, ils peuvent communiquer en utilisant IPSec.

Les ordinateurs placés dans ce réseau peuvent initier des communications avec les ordinateurs des trois réseaux mais ne peuvent pas répondre à des communications provenant du réseau restreint. S'ils communiquent avec un ordinateur du réseau restreint, la communication n'est pas sécurisée.

#### d. Durée de vie du certificat d'intégrité

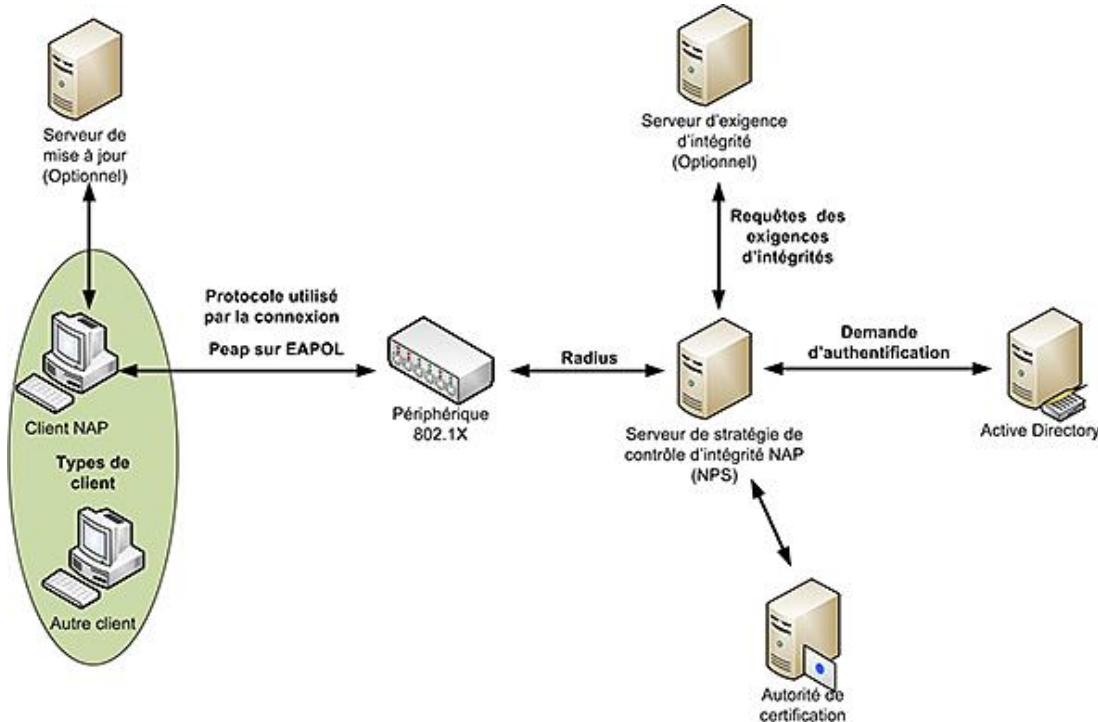
Pour une raison de sécurité, il faut que la durée de vie se compte en heures et pas en mois ou en années. Lorsque le certificat arrive à expiration, le client NAP redemande un certificat auprès du serveur HRA.

## 8. Contrainte de mise en conformité NAP pour les connexions 802.1X

La méthode de contrainte pour les connexions 802.1X fonctionne aussi bien pour Ethernet que pour des accès sans fil. Elle permet de garantir que les ordinateurs clients non conformes par rapport aux stratégies d'intégrité définies sont :

- Placés dans un VLAN spécifique.
- Leurs paquets IP sont filtrés et tout paquet n'ayant pas de correspondance avec le filtre est détruit.

La figure suivante montre la topologie d'un tel système.



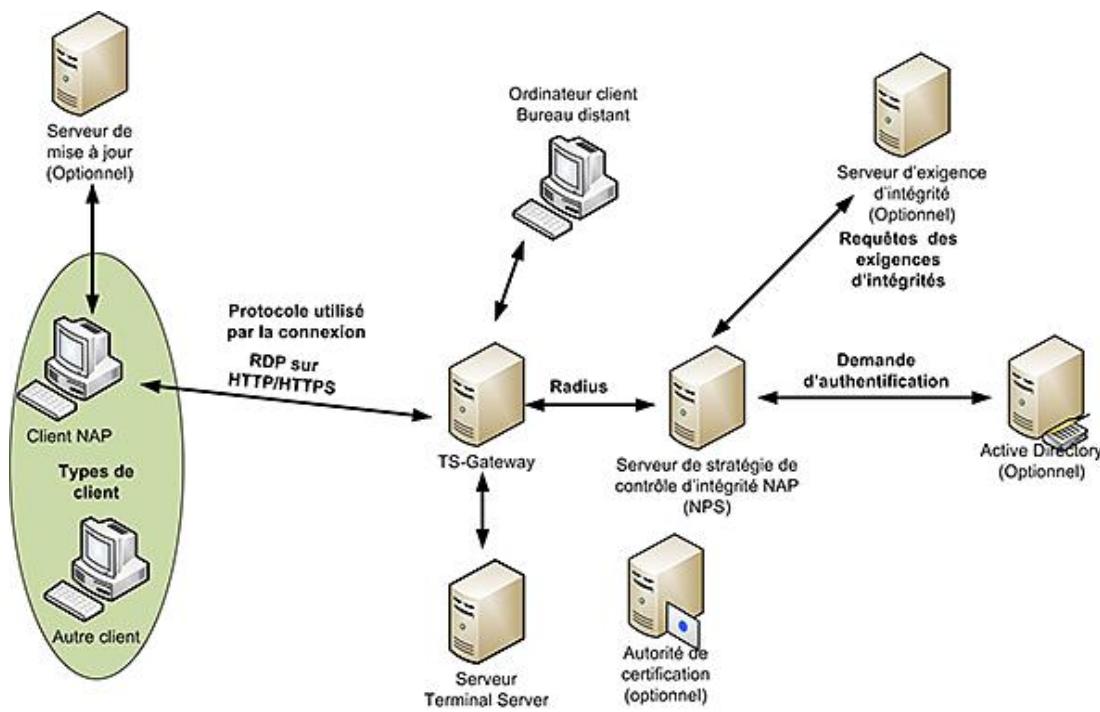
Cette topologie exige des périphériques prenant en charge la norme 802.1X, comme par exemple des commutateurs. Il faut également activer la prise en charge du protocole 802.1X au niveau des cartes réseaux des clients NAP.

Dans des réseaux de moyenne importance c'est-à-dire disposant de plusieurs commutateurs, il est nécessaire d'envisager l'utilisation de commutateurs pouvant être gérés à distance et de manière centralisée.

## 9. Contrainte de mise en conformité NAP pour les connexions TS-Gateway

La méthode de contrainte pour les connexions TS-Gateway permet de garantir que les ordinateurs clients conformes par rapport aux stratégies d'intégrité définies peuvent se connecter à un ordinateur :

- Client, appelé également Bureau distant.
- Serveur Terminal Server.



Un certificat doit exister sur le serveur passerelle mais il n'est pas nécessaire de disposer d'une autorité de certification.

Les ordinateurs clients NAP sont obligatoirement un ordinateur Windows XP SP3 ou Windows Vista alors que les ressources internes peuvent être un ordinateur client Windows XP à partir du SP2, Windows Vista dès le SP1, Windows Server 2003 dès le SP1 et Windows Server 2008.

## 10. Stratégies

Une stratégie définit une condition pour la déclencher et un comportement pour celui qui la subit. Sur un serveur NPS, il existe trois types de stratégies définies ci-dessous.

### a. Stratégie de demande de connexion

Elle permet de créer des stratégies de connexion pour indiquer si le traitement s'effectue localement ou si la demande de connexion est transférée vers des serveurs Radius.

Vous pouvez également spécifier l'authentification des demandes de connexion.

**La stratégie de demande de connexion comprend :**

- **Une vue d'ensemble**, soit des informations qui indiquent si la stratégie est active et la méthode de connexion réseau.
- **Des conditions** pour préciser le cadre de déclenchement de la stratégie (horaire, groupes, utilisateurs, système d'exploitation, etc.).
- **Des paramètres** pour définir des paramètres de connexion spécifiques aux protocoles utilisés.

### b. Stratégie réseau

La stratégie réseau permet d'indiquer qui peut se connecter et sous quelles conditions. Si vous utilisez NAP, vous pouvez inclure comme condition une stratégie de contrôle d'identité.

**La stratégie réseau comprend :**

- **Une vue d'ensemble**, soit des informations qui indiquent si la stratégie est active et si elle autorise ou bloque l'accès, et la méthode de connexion réseau.

- **Des conditions** pour préciser le cadre de déclenchement de la stratégie (horaire, groupes, utilisateurs, système d'exploitation, etc.).
- **Des contraintes** pour préciser les méthodes d'authentification, le délai d'inactivité et d'expiration, des restrictions horaires et le type de port NAS, soit le type de média d'accès (Ethernet, FDDI, VPN, etc.), l'ID de la station appelée.
- **Des paramètres** pour définir des paramètres de connexion spécifiques aux protocoles utilisés.

### c. Stratégie de contrôle d'intégrité

Elle permet de définir uniquement pour la protection d'accès réseau un comportement spécifique utilisé dans les stratégies réseau pour accorder ou refuser l'accès après avoir reçu une réponse du programme de validation d'intégrité système utilisé. Il est possible d'utiliser plusieurs programmes de validation d'intégrité système et les comportements sont :

- Réussite de tous les contrôles SHV pour le client.
- Échec de tous les contrôles SHV pour le client.
- Réussite d'un ou plusieurs contrôles SHV pour le client.
- Échec d'un ou plusieurs contrôles SHV pour le client.
- Client signalé en transition par un ou plusieurs programmes SHV.
- Client signalé infecté par un ou plusieurs programmes SHV.
- Client signalé inconnu par un ou plusieurs programmes SHV.

Grâce à ces stratégies, il est possible de déterminer différents types d'accès ou de refus dans les stratégies réseau.

## 11. Avantages et inconvénients

Comme inconvénient principal, on peut noter qu'il s'agit de la version 1 et que les procédures de configuration sont longues. Néanmoins le concept est des plus intéressants pour un administrateur en lui fournissant un niveau d'abstraction par rapport aux composants de conformité.

Enfin il peut paraître paradoxal que Windows Server 2003 et Windows Server 2008 ne soient pas (encore) supportés comme clients même si certains de ces serveurs disposeraient d'une exemption de conformité.

---

 Si l'on implémente NAP, il faut le faire pour tous les ordinateurs du réseau ou aucun.

---

Le tableau suivant résume les différentes méthodes d'accès, l'infrastructure nécessaire, et indique des avantages et des inconvénients :

Méthode d'accès	Infrastructure requise au niveau du serveur	Infrastructure requise au niveau du client	Avantages	Inconvénients
DHCP	NPS DHCP	Client NAP	Mise en œuvre simple.	Ne protège pas contre des accès non autorisés.
VPN	Active Directory NPS Routage et accès distant Autorité de certification	Client NAP	Garantit l'intégrité des clients distants.	Suivant la taille des mises à jour, la durée de mise à jour peut être importante.

IPSec	Active Directory NPS HRA IIS Autorité de certification	Client NAP	Granularité de la protection s'applique à l'ordinateur.  Hautement sécurisé.	Difficulté de mise en œuvre.  Requiert un serveur de certificat.
802.1X	Active Directory NPS Périphériques 802.1X	Client NAPActivation protocole 802.1X sur le client	Permet d'isoler facilement les clients non compatibles.  Pour client Ethernet ou sans fil.	Difficulté de mise en œuvre.  Requiert du matériel 802.1X.
TS-Gateway	NPS Terminal Server IIS	Client NAP Client TS		Difficulté de mise en œuvre.

Le tableau suivant montre quel composant peut résider sur quel système d'exploitation :

Composant	Windows Server 2008	Windows Server 2003	Windows Vista	Windows XP
Client NAP	Oui	Non	Oui	Dès le SP3
NPS	Oui	Non	Non	Non
DHCP	Oui	Non	Non	Non
Routage et accès distant	Oui	Non	Non	Non
HRA (IPSec)	Oui	Non	Non	Non
TS-Gateway	Oui	Non	Non	Non
802.1X	Oui	Non	Client uniquement	Client uniquement
Serveur de mise à jour WSUS	Oui	Oui	Non	Non
Server de mise à jour SCCM 2007	Oui	Oui	Non	Non
Serveur de mise à jour d'anti-virus	Oui	Oui	Non	Non

# Présentation de l'accès distant et des réseaux privés virtuels VPN

L'accès au réseau de l'entreprise depuis l'extérieur a toujours été une option très prisée que ce soit pour des informaticiens ou des utilisateurs. Lorsque les connexions à la demande transitaient par le réseau téléphonique, les protocoles utilisés n'étaient pas sécurisés. Par la suite la sécurité est devenue de mise et les protocoles ont évolué pour supporter la notion de réseau privé virtuel dont il est possible de simplifier la définition comme étant un accès distant sécurisé dont l'objectif principal est d'inclure l'ordinateur distant comme faisant partie du réseau de l'entreprise en créant un tunnel pour faire passer toutes les communications de l'ordinateur vers l'entreprise y compris les requêtes Internet.

## 1. Connexion réseau à distance

Dans Windows Server 2008, la notion de connexion réseau à distance comprend sans distinction l'accès réseau via une connexion à la demande et la connexion VPN présentée plus loin. Dans le livre, la connexion réseau à distance fait référence à une connexion utilisant simplement le protocole **PPP** (*Point to Point*) sinon le terme de connexion **VPN** est utilisé. Dans notre scénario, le client se connecte au serveur via un modem en utilisant le protocole d'accès distant **PPP**, les clients **SLIP** n'étant plus supportés.

Le protocole **PPP** encapsule les paquets IP pour circuler sur un réseau téléphonique. Ce protocole n'est donc pas sécurisé. Pour l'authentification de l'utilisateur, il existe plusieurs méthodes qui peuvent être utilisées pour améliorer la sécurité. Les méthodes d'authentification seront présentées plus loin. Pour le serveur il est possible d'améliorer la sécurité en utilisant un serveur Radius ainsi qu'un serveur de stratégie.

- 
- Vu l'engouement pour Internet et grâce aux nombreux points de connexion existant à travers le monde, la simple connexion réseau à distance en utilisant une liaison téléphonique a un intérêt limité.

---

  - Il est nécessaire d'avoir des modems et les avoir configuré afin qu'ils soient reconnus par le système d'accès distant.
- 

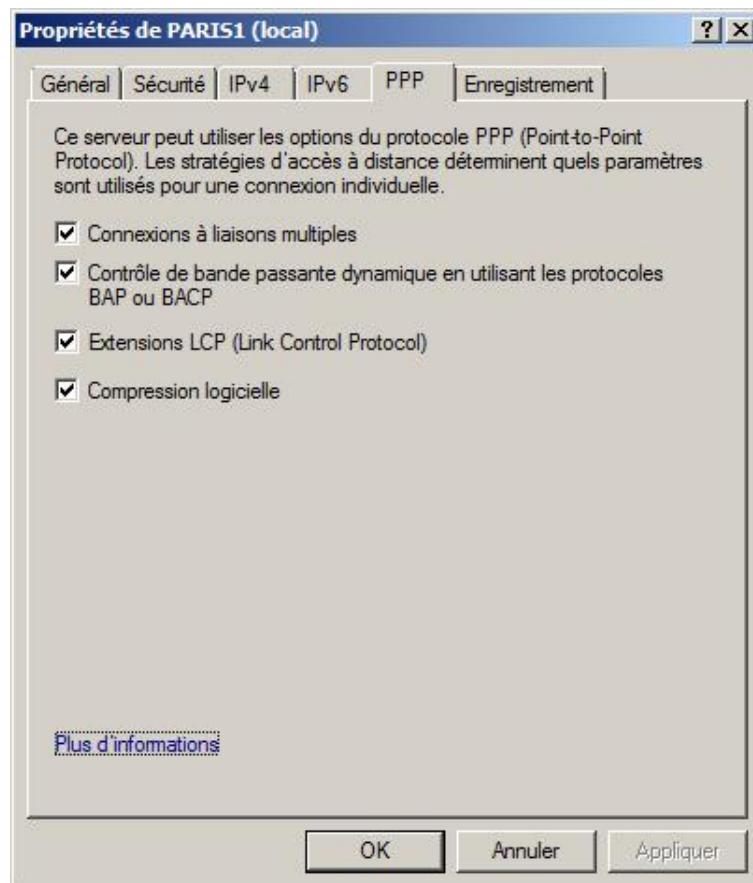
### a. Activation de l'accès à distance

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestionnaire de Serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud de **Rôles**.
- Cliquez sur le nœud de **Services de stratégie et d'accès distant**.
- Cliquez avec le bouton droit de la souris sur **Routage et accès distant** puis cliquez sur **Configurer et activer le routage et l'accès distant**.
- Sur la page **Bienvenue de l'assistant**, cliquez sur **Suivant**.
- Sur la page **Configuration**, cliquez sur **Accès à distance (Connexion à distance ou VPN)**.
- Sur la page **Accès à distance**, cochez la case **Accès à distance** puis cliquez sur **Suivant**.
- Sur la page **Sélection du réseau**, sélectionnez l'interface réseau du réseau interne puis cliquez sur **Suivant**.
- Sur la page **Attribution d'adresses IP**, vous pouvez choisir entre utiliser le serveur DHCP d'entreprise, sur lequel vous pourriez configurer des options spécifiques aux utilisateurs distants, ou à partir d'une plage d'adresses IP que vous spécifiez sur le serveur d'accès distant. Si vous utilisez un serveur DHCP distant, l'agent serveur DHCP sera ajouté et il faudra le configurer. Ensuite, cliquez sur **Suivant**.
- Si vous avez indiqué une plage d'adresses spécifiées, alors la page suivante vous demande de spécifier ces adresses.

- Sur la page **Gestion d'accès à distance multiples**, vous pouvez indiquer que le serveur d'accès distant gère également l'authentification, ou qu'il devienne un client Radius ce qui améliore la sécurité.
- Si vous avez indiqué de travailler en tant que client Radius, vous devez définir les paramètres Radius.
- Sur la page **Fin de l'assistant Installation d'un serveur de routage et d'accès distant**, lisez les informations de configuration avant de cliquer sur **Terminer**.

## b. Gestion de l'accès à distance

- Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur le nom du serveur puis cliquez sur **Propriétés**.
- Dans la boîte de dialogue, sur l'onglet **Général**, vous pouvez activer ou désactiver de manière indépendante l'accès à distance **IPv4** et **IPv6**.
- Sur l'onglet **Sécurité**, vous pouvez modifier la méthode d'authentification en utilisant soit l'authentification Windows, soit l'authentification Radius.
- Sur l'onglet **IPv4**, vous pouvez indiquer :
  - La méthode d'attribution des adresses IPv4 (DHCP ou en spécifiant une plage d'adresses).
  - Si le routage est activé, soit si les ordinateurs peuvent également se connecter au réseau de l'entreprise.
  - Si le serveur d'accès distant s'occupe de la résolution de noms NetBIOS et DNS sur le sous-réseau local.
  - La carte réseau à utiliser pour obtenir des informations DHCP, DNS et Wins.
- Sur l'onglet **IPv6**, vous pouvez indiquer :
  - L'activation du transfert IPv6 soit l'équivalent du routage IPv4.
  - L'activation des annonces de routage par défaut.
  - L'affectation d'un préfixe IPv6 pour les utilisateurs distants.
- Sur l'onglet **PPP** qui est en relation directe avec les connexions modem vous pouvez indiquer :
  - **Connexions à liaisons multiples** permet d'autoriser un utilisateur distant à utiliser plusieurs modems pour se connecter.
  - **Contrôle de la bande passante dynamique en utilisant les protocoles BAP ou BACP** soit si le serveur gère l'ajout et la suppression dynamique de modems en fonction des besoins.
  - **Extension LCP (Link Control Protocol)** à laisser activé.
  - **Compression logicielle** permet d'activer le protocole MPPC (*Microsoft Point to Point Compression*) entre l'ordinateur distant et le serveur.



- Sur l'onglet **Enregistrement**, vous définissez comment les enregistrements sont sauvegardés dans le journal. Vous pouvez également y inclure des informations de débogage dans un fichier appelé ppp.log situé dans %systemroot%\tracing.

Vous pouvez également configurer :

- Les ports pour l'accès distant (à voir plus loin).
- Visualiser les informations et statistiques sur les clients d'accès distants (à voir plus loin).
- Gérer les stratégies d'accès à distance (à voir plus loin).
- L'agent de relais DHCP (voir la section correspondante dans le chapitre Configuration de la résolution de noms).

## 2. Connexion VPN

La connexion VPN est une des méthodes les plus utilisées aujourd'hui pour se connecter depuis l'extérieur au réseau d'entreprise et fait souvent référence dans le langage populaire à une connexion sécurisée. Comme plusieurs concurrents, Microsoft possède sa propre solution qui est décrite ici. Tous les VPN utilisent les trames PPP puis les sécurisent avec leur technologie.

Les protocoles VPN supportés par Windows Server 2008 sont présentés dans le tableau suivant :

Protocole	Système d'exploitation supportant	Scénario	Méthode d'authentification	Ports utilisés
PPTP ( <i>Point to Point Tunneling Protocol</i> )	XP, 2003, Vista, WS08, W7, WS08 R2	Accès distant et site à site	Authentification de l'utilisateur en clair puis création du tunnel PPTP	TCP 1723 (Control), IP 47 (GRE - Data)

L2TP ( <i>Layer 2 Tunneling Protocol</i> )	XP, 2003, Vista, WS08, W7, WS08 R2	Accès distant et site à site	Authentification de l'ordinateur via IPSec puis de l'utilisateur dans le tunnel avec PPP	UDP Port 500 (IKE), IP 50 (ESP) éventuellement UDP port 4500 (NAT-T Data)
SSTP	Vista SP1, WS08, W7, WS08 R2	Accès distant	Création du tunnel SSL puis authentification de l'utilisateur avec PPP	TCP 443 (HTTPS)

### a. Point To Point tunneling Protocol PPTP

PPTP (*Point to Point Tunneling Protocol*) est un Protocole VPN qui authentifie l'utilisateur en clair puis crée le tunnel PPTP en utilisant le chiffrage MPPE (*Microsoft Point to Point Encryption*). PPTP est à l'heure actuelle le type de VPN le plus répandu car le client et le serveur sont inclus dans Windows. Son implémentation est très simple.

### b. Layer 2 Tunneling Protocol L2TP

L2TP est un protocole de VPN très sécurisé car il commence par créer un tunnel entre l'ordinateur distant et le serveur en les authentifiant mutuellement via IPSec puis dès que le tunnel est créé, l'utilisateur est authentifié. L2TP est le second type de VPN répandu mais son implémentation est assez complexe, surtout pour la partie gestion des certificats qui s'avère rapidement nécessaire. D'autre part, il faut garantir qu'entre le client distant et le serveur les matériels réseaux sont compatibles avec IPSec ce qui semble le cas partout actuellement.

Une des difficultés est le passage d'IPSec au travers de pare-feu, voire de proxy.

### c. Secure Socket Tunneling Protocol SSTP

SSTP est un protocole VPN apparu dans Windows Vista SP1 et Windows Server 2008. Il encapsule le protocole PPP dans HTTP sur SSL afin d'éviter les problèmes décrits précédemment. Il n'est pas nécessaire d'installer un serveur IIS sur le serveur d'accès distant. Les mécanismes nécessaires sont implémentés directement dans le serveur d'accès distant. Sa mise en œuvre est plus simple que L2TP mais plus complexe que PPTP.

## 3. Méthodes d'authentification

Les méthodes d'authentification indiquent la méthode utilisée pour transférer les informations d'identification de l'utilisateur entre l'ordinateur client et le serveur d'accès distant.

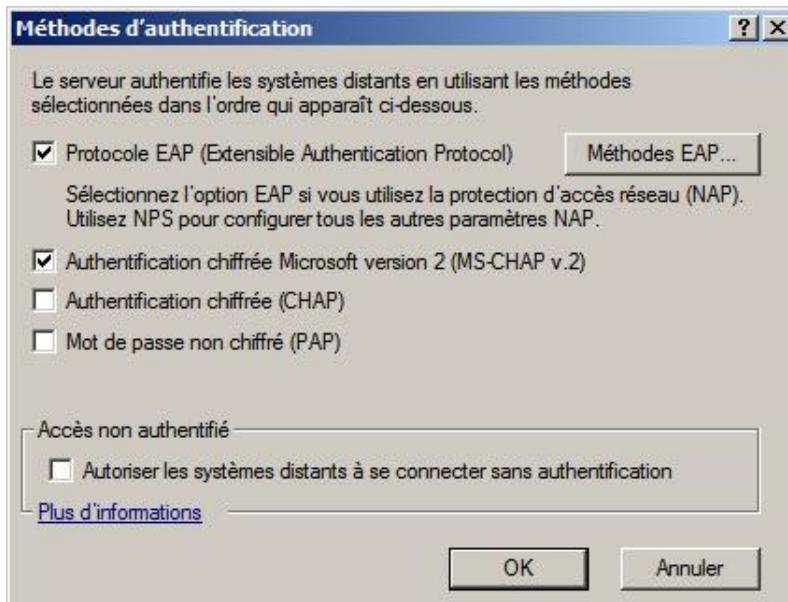
 Il ne faut pas confondre les méthodes d'authentification d'accès réseau distantes présentes ici avec l'authentification réseau NTLM (NT Lan Manager) et Kerberos. Kerberos est le protocole utilisé actuellement pour se connecter à des domaines Active Directory. NTLM est utilisé si l'ordinateur client est authentifié au niveau du serveur par son adresse IP, l'ordinateur client n'appartient à aucun domaine (groupe de travail), l'ordinateur client appartient à une forêt différente, des restrictions peuvent exister sur le pare-feu.

Les méthodes supportées dans Windows Server 2008 sont :

Méthode	Description
Accès non authentifié	<p>Indique si le serveur accepte des connexions non authentifiées, c'est-à-dire que ni le nom ni le mot de passe ne sont envoyés au serveur.</p> <p>Les scénarios suivants sont possibles :</p> <ul style="list-style-type: none"> <li>• <b>Autorisation DNIS</b> (<i>Dialed Number Identification Service</i>) basée sur le numéro de l'appelant.</li> <li>• <b>ANI/CLI</b> (<i>Automatic Number Identification/Calling Line Identification</i>) basée sur le numéro de l'appelant fourni par les opérateurs de téléphonie.</li> <li>• <b>Authentification invité</b> où l'appelant est mappé sur l'utilisateur Invité. Dans tous les cas, il faut activer et configurer une stratégie d'accès distant pour permettre cette méthode d'accès.</li> </ul>

	Elle est la méthode la moins sécurisée.
<b>PAP</b>	<p>PAP (<i>Password Authentication Protocol</i>). Les mots de passe sont en clair. PAP est surtout utilisé pour permettre l'accès soit à de vieux serveurs d'accès distants, soit à de vieux systèmes d'exploitation ne prenant pas en charge une autre méthode d'authentification.</p> <p>Cette méthode est fortement déconseillée.</p>
<b>CHAP</b>	<p>CHAP (<i>Challenge Handshake Authentication Protocol</i>) fonctionne en stimulation/réponse et utilise un protocole de hachage des mots de passe MD5 (<i>Message Digest 5</i>). MSCHAP est largement répandu et c'est souvent le choix à faire lorsqu'il faut être compatible avec un maximum de clients.</p> <p>Il faut noter que MSCHAP exige un mot de passe chiffré de manière réversible ce qui peut poser des problèmes de sécurité.</p>
<b>MS-CHAP-V2</b>	<p>MS-CHAP-V2 (<i>Microsoft PPP Chap Extensions</i>) (définition selon RFC 2759) fonctionne en authentification mutuelle à mot de passe unidirectionnel.</p> <p>Le serveur d'accès à distance ou le serveur NPS envoie un défi au client qui doit répondre en envoyant le nom de l'utilisateur, une chaîne de défi homologue arbitraire et un chiffrement unidirectionnel basé sur le défi envoyé, le défi homologue, la réponse chiffrée du client et le mot de passe utilisateur.</p> <p>Le serveur répond avec une indication du succès ou de l'échec de l'authentification ainsi qu'une réponse authentifiée basée sur le défi envoyé, le défi homologue, la réponse chiffrée du client et le mot de passe utilisateur.</p> <p>Le client vérifie la réponse d'authentification et en cas de succès se connecte.</p> <p>Il s'agit une des méthodes préférées.</p>
<b>EAP</b>	<p>EAP (<i>Extensible Authentication Protocol</i>) autorise l'authentification arbitraire d'une connexion d'accès à distance grâce à des modèles d'authentification appelés types EAP.</p> <p>Windows Server 2008 supporte :</p> <ul style="list-style-type: none"> <li>• EAP-TLS qui utilise des certificats et un chiffrement TLS comme par exemple avec les cartes à puce.</li> <li>• EAP-Radius utilisé pour une authentification sécurisée vers un serveur Radius.</li> <li>• PEAP pour une authentification de clients sans fil.</li> </ul> <p>EAP est considérée comme la méthode la plus sécurisée pour l'authentification.</p>

La figure suivante montre les méthodes d'authentification activées par défaut dans Windows Server 2008 pour un accès VPN.



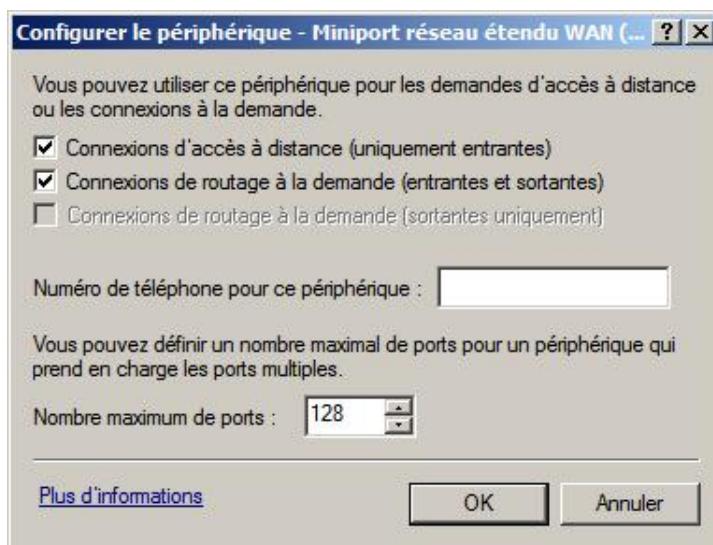
- Dans l'arborescence de la console, cliquez avec le bouton droit de la souris sur le nom du serveur puis cliquez sur **Propriétés**.
- Dans la boîte de dialogue, cliquez sur l'onglet **Sécurité**.
- Cliquez sur **Méthode d'authentification** et sélectionnez les méthodes dont vous avez besoin.
- Cliquez deux fois sur **OK** pour fermer la boîte de dialogue.

## 4. Configuration des ports

Un port correspond à un périphérique physique comme un modem ou virtuel comme les ports SSTP, PPTP ou L2TP pouvant prendre en charge une connexion point à point.

Le nombre de ports dépend du périphérique. Par exemple pour un modem il n'est pas possible de disposer de plus de connexions que physiquement permises par le périphérique. Pour les ports SSTP par exemple, vous êtes limités au nombre maximal de connexion RRAS de Windows (250 pour une édition Standard et illimité pour une édition Entreprise).

- Dans l'arborescence de **Routage et accès distant**, cliquez avec le bouton droit de la souris sur **Ports** puis sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés de Ports**, sélectionnez un périphérique puis cliquez sur **Configurer**.
- Les paramètres de configuration modifiables dépendent du périphérique sélectionné. Par exemple, pour SSTP vous ne pouvez qu'accepter des connexions entrantes, à l'inverse pour PPPoE vous ne pouvez que créer des connexions de routage à la demande en sortie. Généralement il est possible de modifier d'autres paramètres comme le montre l'image suivante :



Vous pouvez définir des connexions entrantes ou sortantes voire les deux, et éventuellement un nombre maximum de ports pour ce périphérique. Le numéro de téléphone pour ce périphérique est utilisé comme identificateur de station de la station appelée dans des connexions BAP. Pour L2TP et PPTP cela permet également de définir un port pour une adresse IP d'une interface spécifique.

- Si vous modifiez le nombre maximum de ports en configurant les propriétés du noeud **Ports** de **Routage et accès distant**, cela peut déconnecter des utilisateurs. Vous verrez également apparaître cette modification dans la section détail de la console.

---

 Vous pouvez utiliser le kit d'administration Connection Manager (CMAK) pour créer des profils de connexion VPN pour les utilisateurs.

---

## 5. Serveur Radius (*Remote Authentication Dial In User Service*) NPS

Suivant la taille de l'entreprise, la sécurité de l'accès distant peut être améliorée en déléguant la tâche d'authentification à un serveur Radius. Apparu avec Windows 2000 sous le nom de serveur IAS, il a été remplacé sous Windows Server 2008 par le serveur NPS (*Network Policy Server*). Radius est un protocole de délégation de l'authentification composé d'un client Radius et d'un serveur Radius. Généralement le client Radius, qui peut être un serveur Microsoft, un matériel Cisco ou autre, reçoit des demandes d'authentification. Au lieu de gérer la demande directement auprès du contrôleur de domaine, il passe la demande auprès du serveur Radius de manière sécurisée. Ce dernier commence par appliquer les stratégies définies, avant d'effectuer en cas de succès la demande d'authentification auprès d'un contrôleur de domaine, et il retourne la réponse auprès du client Radius. Vous pouvez remarquer que ce protocole permet de faire cohabiter des systèmes hétérogènes qui n'ont pas été conçus pour fonctionner ensemble. D'autre part, le fait d'y appliquer des stratégies permet d'étendre le service d'authentification offert par le contrôleur de domaine. Enfin le serveur Radius permet d'améliorer la sécurité car le client Radius peut se trouver en dehors d'une zone sécurisée, voire placé chez un fournisseur d'accès Internet, car plusieurs clients Radius peuvent communiquer avec un serveur Radius. Ce dernier peut être redondant pour améliorer la disponibilité.

Le serveur de stratégie réseau NPS permet la mise en œuvre de stratégies centralisée au niveau de l'entreprise pour :

- Le contrôle d'intégrité.
- L'authentification.
- L'autorisation des demandes de connexion des clients.

Il peut également agir en tant que proxy Radius qui reçoit des demandes provenant de clients Radius et les transfère vers d'autres serveurs Radius.

---

 Il peut paraître surprenant que lorsque vous installez le service de routage et d'accès distant, la console NPS soit disponible alors que son rôle n'est pas installé. En fait, la console permet uniquement de créer des stratégies locales.

---

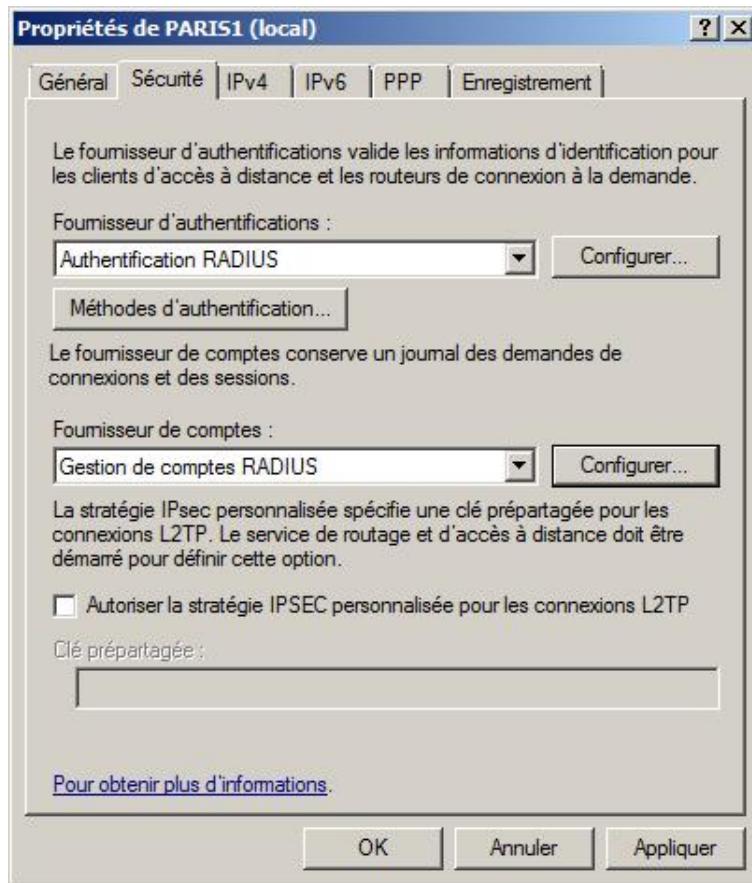
### a. Installation du serveur NPS

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestionnaire de Serveur**.
- Dans l'arborescence de la console, cliquez sur **Rôles**.
- Dans la fenêtre principale de **Rôles**, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez **Services de stratégie et d'accès réseau** puis cliquez sur **Suivant**.
- Sur la page **Stratégies et accès réseau**, cliquez sur **Suivant**.
- Sur la page **Services de rôle**, sélectionnez **Serveur NPS (Network Policy Server)**.
- Sur la page **Confirmation**, cliquez sur **Installer**.
- Dès que la page **Résultats** apparaît, contrôlez que le rôle est bien installé, puis cliquez sur **Fermer**.

### b. Configurer le client Radius

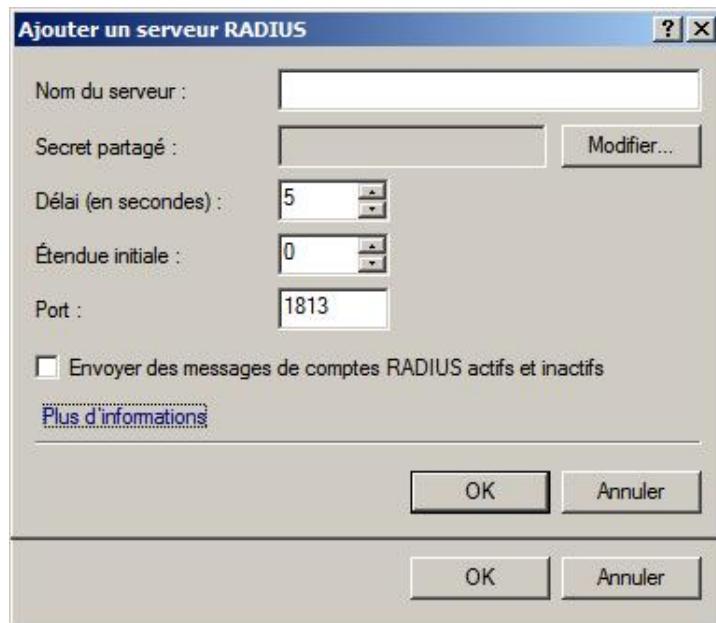
 Si le serveur NPS est installé sur le serveur d'accès à distance, cette procédure n'est pas possible. Il faut passer par le serveur NPS pour créer une stratégie d'accès.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Routage et accès distant**.
- Cliquez avec le bouton droit de la souris sur le nom du serveur puis sur **Propriétés**.



- Sur l'onglet **Sécurité**, vous pouvez modifier les éléments suivants :
  - **Fournisseur d'authentifications** : soit vous utilisez Windows et l'authentification peut utiliser la base SAM locale ou l'Active Directory, soit vous passez par un serveur Radius et configurez les informations du serveur.
  - **Méthodes d'authentification** indique celles qui sont prises en charge par ce serveur pour les connexions à la demande et l'accès distant.
  - **Fournisseur de comptes** propose de stocker les informations relatives aux connexions dans les journaux locaux pour la Gestion des comptes Windows ou sur le serveur Radius si la Gestion de comptes Radius est sélectionnée.
- En cliquant sur les boutons **Configurer**, vous afficherez la même boîte de dialogue, à savoir la liste des serveurs Radius ajoutés manuellement.
- En cliquant sur le bouton **Ajouter**, vous pouvez paramétrier les informations du serveur Radius à savoir le **Nom du serveur** (nom DNS ou adresse IP), le **Délai en secondes** qui correspond à la durée maximale pour que le client Radius reçoive une réponse avant de tenter d'appeler le suivant sur la liste, l'**Etendue initiale** ou la priorité (0 à 30), le port utilisé (1813) qui peut être 1812 (RFC2139) voire 1646 pour d'anciens serveurs Radius et vous pouvez **Envoyer des messages de comptes Radius actifs et inactifs** lors du démarrage et de l'arrêt du service Routage et accès distant, si le serveur Radius prend en charge cette fonctionnalité. Vous pouvez améliorer la

sécurité en saisissant un **Secret** soit l'équivalent d'une clé pré-partagée entre le client et le serveur Radius.



## 6. Les stratégies d'accès à distance

Depuis Windows Server 2000, les stratégies d'accès distantes se trouvaient sur le serveur local et pouvaient le cas échéant être déplacées vers le serveur IAS afin de distribuer les stratégies depuis un point central. Sous Windows Server 2008, les stratégies ne peuvent être gérées que via la console NPS. Si le serveur est local, seule une stratégie réseau est utile, sinon il faut créer en plus une stratégie de demande de connexion.

### a. Stratégie de demande de connexion

La stratégie de demande de connexion permet de créer des stratégies de connexion pour indiquer si le traitement s'effectue localement ou si la demande de connexion est transférée vers des serveurs Radius.

Vous pouvez également spécifier l'authentification des demandes de connexion.

**La stratégie de demande de connexion comprend :**

- **Une vue d'ensemble**, soit des informations qui indiquent si la stratégie est active et la méthode de connexion réseau.
- **Des conditions** pour préciser le cadre de déclenchement de la stratégie (horaire, groupes, utilisateurs, système d'exploitation, etc.).
- **Des paramètres** pour définir des paramètres de connexion spécifiques aux protocoles utilisés.

### b. Stratégie réseau

La stratégie réseau permet d'indiquer qui peut se connecter et sous quelles conditions. Si vous utilisez NAP, vous pouvez inclure comme condition une stratégie de contrôle d'identité.

**La stratégie réseau comprend :**

- **Une vue d'ensemble**, soit des informations qui indiquent si la stratégie est active et si elle autorise ou bloque l'accès, et la méthode de connexion réseau.
- **Des conditions** pour préciser le cadre de déclenchement de la stratégie (horaire, groupes, utilisateurs, système d'exploitation, etc.).

- **Des contraintes** pour préciser les méthodes d'authentification, le délai d'inactivité et d'expiration, des restrictions horaires et le type de port NAS, soit le type de média d'accès (Ethernet, FDDI, VPN, etc.), l'ID de la station appelée.
- **Des paramètres** pour définir des paramètres de connexion spécifiques aux protocoles utilisés.

### c. Lancement du serveur NPS et création d'une stratégie

Il est nécessaire que le serveur d'accès à distance soit configuré en tant que client Radius du serveur NPS considéré.

- Bien qu'il soit possible de lancer le serveur NPS à partir de la console Routage et accès distant, en développant le nom du serveur puis en cliquant avec le bouton droit de la souris sur **Connexion et stratégies d'accès à distance** puis sur **Lancer NPS**, il est préférable de la lancer directement depuis les Outils d'administration ; ainsi la console est en mode avancé.
- Dans **Serveur NPS**, cliquez sur **NPS (Local)** puis dans la section de détail, sélectionnez **Serveur Radius pour les connexions d'accès à distance ou VPN** dans la zone **Configuration standard** puis cliquez sur **Configurer une connexion VPN ou d'accès à distance**.
- Sur la page **Sélectionner le type de connexions d'accès à distance ou de réseau privé virtuel (VPN)**, sélectionnez le type de connexion pour lequel vous voulez créer une stratégie puis saisissez le nom de votre stratégie avant de cliquer sur **Suivant**.
- Sur la page **Spécifier un serveur d'accès à distance ou VPN**, si le serveur d'accès distant est également serveur NPS, vous pouvez cliquer sur **Suivant**, sinon ajoutez le nom du serveur d'accès distant qui doit être un client Radius.
- Sur la page **Configurer les méthodes d'authentification**, est sélectionné par défaut **MS-CHAPv2**, modifiez éventuellement ce choix puis cliquez sur **Suivant**.
- Sur la page **Spécifier des groupes d'utilisateurs**, restreignez éventuellement la stratégie à des groupes d'utilisateurs avant de cliquer sur **Suivant**.
- Sur la page **Spécifier des filtres IP**, vous pouvez éventuellement définir des filtres **IPv4** et/ou **IPv6** en entrée ou en sortie avant de cliquer sur **Suivant**. Ces filtres permettent d'autoriser ou de bloquer certains protocoles provenant d'un accès distant.
- Sur la page **Spécifier les paramètres de chiffrement**, modifiez éventuellement les choix d'amélioration de la sécurité avant de cliquer sur **Suivant**.
- Sur la page **Spécifier un nom de domaine**, saisissez éventuellement un nom de domaine pour les utilisateurs qui accèdent à distance, avant de cliquer sur **Suivant**.
- Sur la page **Fin de la configuration des nouvelles connexions d'accès à distance ou de réseau privé virtuel (VPN) et des clients Radius**, cliquez sur **Terminer**. Deux stratégies seront créées, soit une stratégie réseau et une stratégie de demande de connexion.

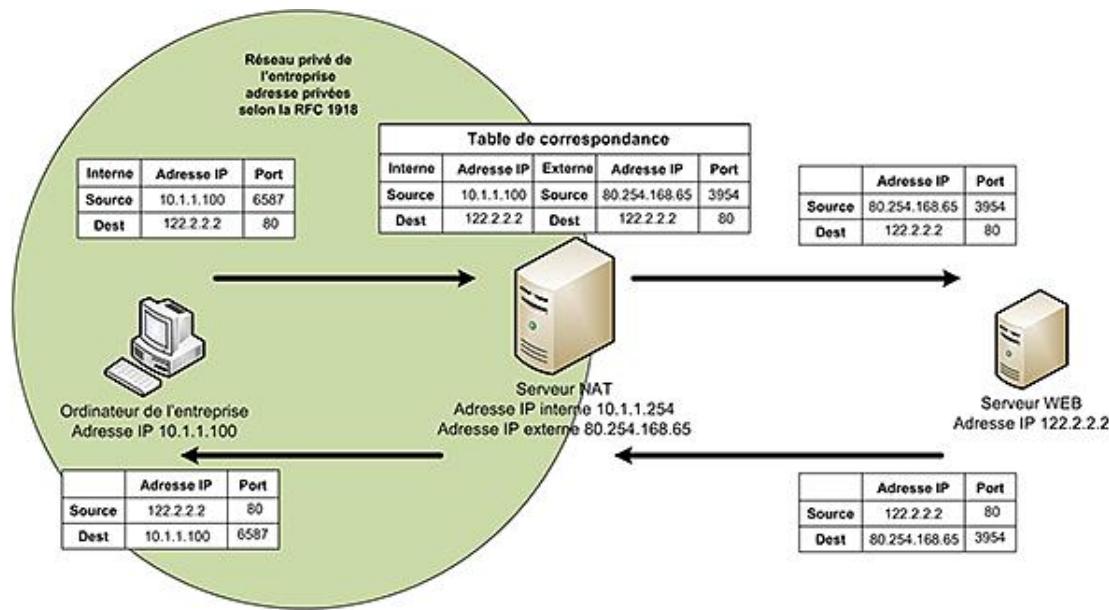
# Présentation de la traduction d'adresses réseau NAT



La traduction d'adresses réseau NAT permet à un réseau entier de partager une connexion Internet. Du côté Internet on ne voit qu'une seule adresse comme si ce n'était qu'un seul client. Le serveur NAT sert de passerelle entre le réseau interne et le réseau Internet. Son principal avantage est qu'il permet d'utiliser dans une entreprise des adresses privées et de n'utiliser qu'une adresse publique pour l'accès Internet.

Dans la terminologie utilisée par Cisco, cela correspond à la notion de PAT pour Port Address Translation, alors que le NAT Cisco demande une adresse IP externe par client interne. Le NAT décrit ici peut s'appeler également Hide-Mode NAT (Checkpoint), NATP pour Network Address Translation Port (RFC 3022), SNAT/MASQUERADE (LINUX Iptables), Static NAT, etc.

Lorsqu'un ordinateur interne doit avoir accès à l'Internet comme le montre la figure suivante, il crée des paquets dont l'en-tête contient son adresse source, le port source, l'adresse de destination qui correspond à l'ordinateur cible sur l'Internet et le port de destination qui correspond au protocole utilisé. Lors du passage dans le serveur NAT, ce dernier met en cache les informations source du paquet dans une table de correspondance et remplace l'adresse IP source par sa propre adresse IP externe (adresse IP publique), et éventuellement lui change le numéro de port source, puis envoie le paquet vers sa destination. Le serveur de destination reçoit le paquet dont il croit que l'émetteur est l'adresse IP publique du serveur NAT. Il renvoie sa réponse en plaçant dans la partie source son adresse IP et le port source et dans la destination l'adresse IP du serveur NAT et le numéro de port défini par le serveur NAT. Lorsque ce dernier reçoit le paquet, il cherche le destinataire réel dans sa table de correspondance puis modifie la destination en remplaçant l'adresse IP et le port. Enfin l'ordinateur reçoit la réponse.



Par défaut, il n'y a pas de règles de gestion des connexions entrantes et elles sont refusées. Dans Windows Server 2008, ce sont les règles du pare-feu qui sont utilisées comme filtre. D'autre part, il existe une fonctionnalité de redirection pour une connexion entrante vers un ordinateur particulier comme vous pouvez en trouver sur des pare-feu réseau avec fonctionnalités NAT de type Cisco, Checkpoint, Microsoft ISA Server, etc.

En fonction du nombre d'utilisateurs, il est possible d'utiliser un des services suivants pour la traduction d'adresses réseau :

- **Le partage de connexion Internet ICS** est prévu pour quelques utilisateurs. Il est également activable sur un serveur Windows Server 2008 si le service NAT n'est pas déjà activé. Son principal avantage est la simplicité car l'interface interne est automatiquement configurée avec l'adresse IP 192.168.0.1 et un mini serveur DHCP est configuré pour distribuer des adresses au sein du réseau interne. Il n'est donc pas nécessaire de configurer l'adressage IP d'une autre manière. La redirection d'adresses entrantes est également possible.
- **La traduction d'adresses réseau NAT** comme présenté dans cette section est prévue pour une vingtaine d'utilisateurs. La mise en œuvre est un peu plus complexe que pour un partage de connexion ICS.

- **Le pare-feu avec NAT** pour plus d'utilisateurs, certains pare-feu permettent la redondance pour une haute disponibilité, voire une répartition de la charge.

## 1. Ajout du service de routage et d'accès distant

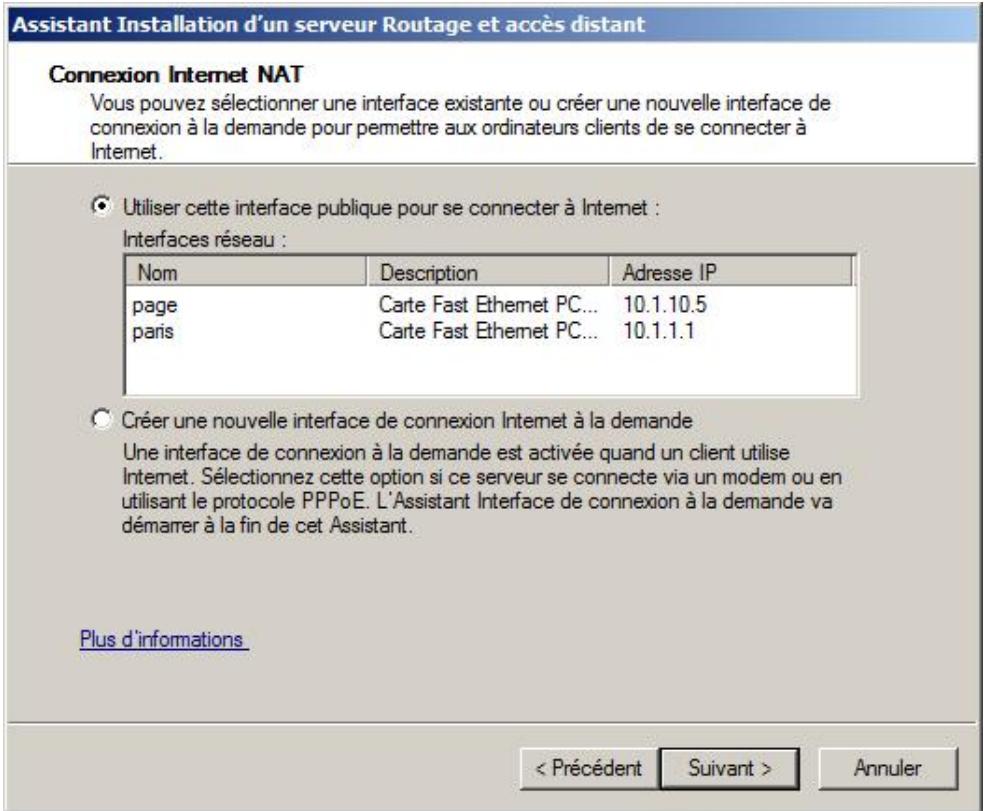
 Votre serveur doit disposer d'au moins deux cartes réseau.

Si le service de rôle n'est pas encore installé :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestionnaire de Serveur**.
- Dans l'arborescence de la console, cliquez sur **Rôles**.
- Dans la fenêtre principale de **Rôles**, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveurs**, sélectionnez **Services de stratégie et d'accès réseau** puis cliquez sur **Suivant**.
- Sur la page **Stratégies et accès réseau**, cliquez sur **Suivant**.
- Sur la page **Services de rôle**, sélectionnez **Routage**.
- Dans la boîte de dialogue **Assistant Ajout de rôles**, cliquez sur le bouton **Ajouter les services de rôle requis**.
- Sur la page **Service de rôle**, cliquez sur **Suivant**.
- Sur la page **confirmation**, cliquez sur **Installer**.
- Dès que la page **Résultats** apparaît, contrôlez que le rôle est bien installé, puis cliquez sur **Fermer**.

## 2. Activation de l'accès distant en NAT

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestionnaire de Serveur**.
- Dans l'arborescence de la console, cliquez sur le nœud de **Rôles**.
- Cliquez sur le nœud de **Services de stratégie et d'accès distant**.
- Cliquez avec le bouton droit de la souris sur **Routage et accès distant** puis cliquez sur **Configurer et activer le routage et l'accès distant**.
- Sur la page **Bienvenue** de l'assistant, cliquez sur **Suivant**.
- Sur la page **Configuration**, cliquez sur **NAT (Network Address Translation)** puis sur **Suivant**. Vous pouvez également cliquer sur l'option **Accès VPN (Virtual Private Network)** et **NAT**.
- Sur la page **Connexion Internet NAT**, sélectionnez l'interface réseau qui est sur le côté Internet, puis cliquez sur **Suivant**.

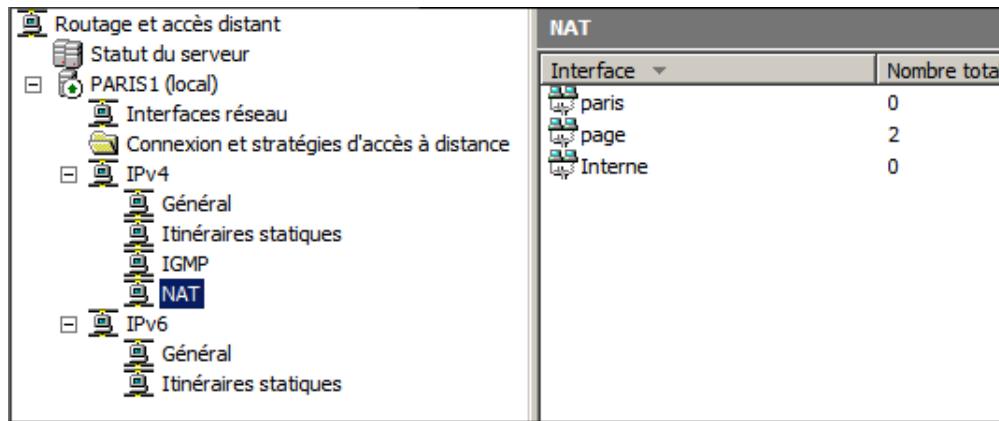


➤ Remarquez les noms des interfaces réseaux, ils ont été modifiés afin de simplifier la gestion du serveur.

➤ Il est également possible de définir une connexion Internet à la demande.

- Sur la page **Fin de l'Assistant Installation d'un serveur de routage et d'accès à distance**, cliquez sur **Terminer**.

Une fois l'installation terminée, la console ressemble à la figure suivante :



### 3. Propriétés du serveur NAT

- Dans l'arborescence de la console **Routage et Accès distant**, cliquez avec le bouton droit de la souris sur **NAT** puis sur **Propriétés**.
- Sur l'onglet **Général**, vous définissez comment les événements sont enregistrés dans le journal Système de l'observateur d'événements. Cela peut être :

**Enregistrer uniquement les erreurs dans le journal** (défaut).

**Enregistrer les erreurs et les avertissements.**

**Enregistrer tous les événements.**

**Désactiver l'enregistrement dans le journal des événements.**

- Sur l'onglet **Traduction**, vous définissez la durée de connexion des mappages dynamiques pour les connexions **TCP** (par défaut 1440 minutes) et **UDP** (1 minute). Un bouton vous permet de réinitialiser le cas échéant ces valeurs.
- Sur l'onglet **Attribution d'adresses**, vous pouvez activer un mini serveur DHCP, appelé également allocateur DHCP, pour distribuer des adresses sur le réseau privé. Pour cela vous devez indiquer l'adresse du réseau et son masque. Vous pouvez également exclure des adresses mais vous ne pouvez pas définir d'autres options DHCP.
- Sur l'onglet **Résolution de noms**, vous pouvez permettre au serveur NAT de relayer les demandes DNS des ordinateurs clients sur le réseau privé vers un serveur DNS, donc d'agir comme un proxy DNS. Le serveur DNS peut-être interne ou externe, voire utiliser une connexion à la demande.

---

 L'attribution d'adresses et la résolution de noms sont utilisables uniquement si le réseau interne se compose d'un seul sous-réseau IP.

---

## 4. Propriétés de l'interface interne

- Dans l'arborescence de la console **Routage et Accès distant**, développez le nœud **NAT**.
- Dans la section de détail, cliquez avec le bouton droit de la souris sur l'interface considérée puis sur **Propriétés**.
- Seul l'onglet **NAT** est visible, vous pouvez uniquement modifier le type d'interface de **Privé** à **Public**.

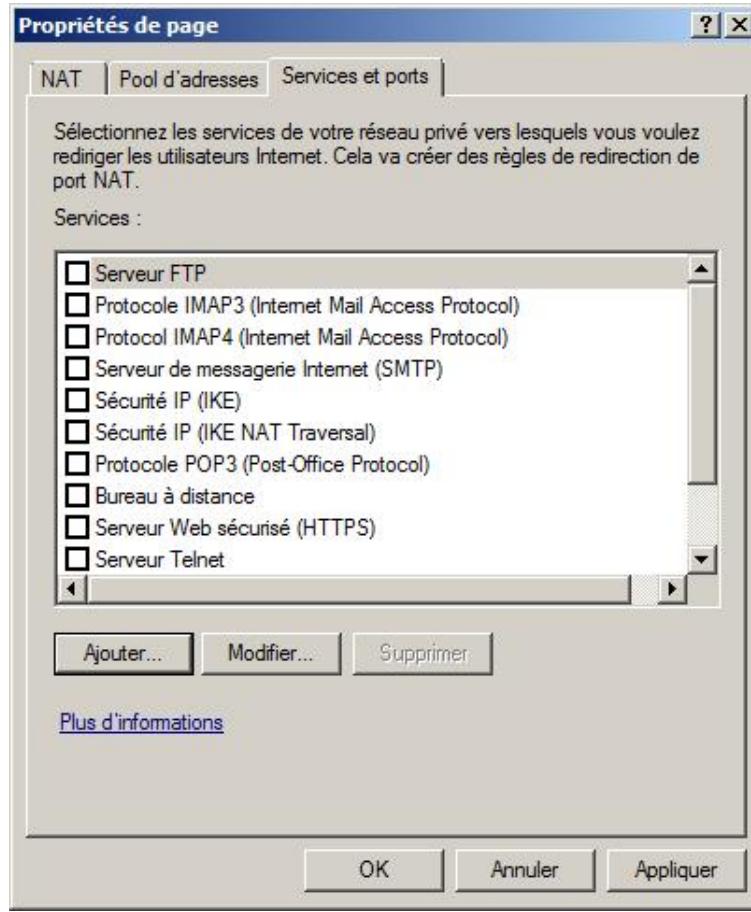
---

 Veuillez noter que la section de détail, vous indique des statistiques sur les résolutions y compris d'afficher les mappages en terme d'adresses IP.

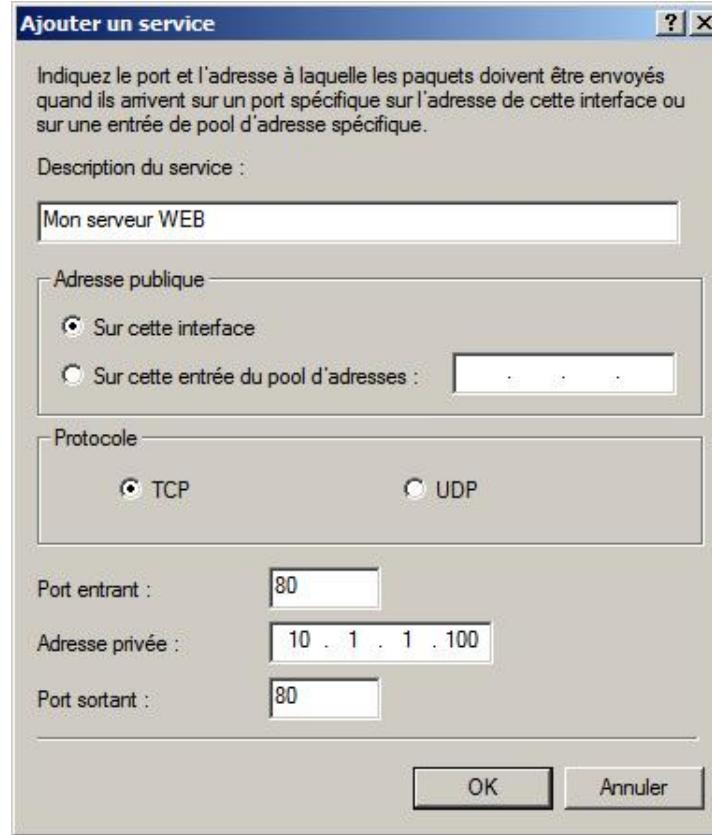
---

## 5. Propriétés de l'interface externe

- Effectuez la même procédure que pour l'interface interne.
- Sur l'onglet **NAT**, l'interface est publique et la case à cocher **Activer NAT sur cette interface** est activée. Notez qu'il est possible de disposer d'une interface publique mais sans activer de partage de connexion.
- Sur l'onglet **Pool d'adresses**, si vous avez demandé des adresses fixes, généralement des adresses publiques, auprès de votre fournisseur d'accès Internet, vous pouvez définir ces adresses ici. Elles seront utilisées pour la traduction d'adresses NAT sauf si vous cliquez sur **Réservations**. Dans ce cas vous pouvez créer un mappage spécifique entre une adresse IP publique et une adresse IP privée, soit en sortie uniquement voire en permettant une connexion entrante comme pour accéder à un serveur Web interne.
- Sur l'onglet **Services et ports**, vous pouvez définir quel service interne est disponible à partir d'Internet, soit en activant et configurant un service prédéfini, soit en en créant un. La figure suivante montre cet onglet.



- En cliquant sur **Ajouter**, vous pouvez ajouter un nouveau service comme le montre l'image suivante :



- Saisissez le nom du service dans la zone de texte **Description du service**. Puis soit vous utilisez l'adresse IP de

l'interface soit une adresse du pool d'adresse défini dans l'onglet **Pool d'adresses**. Ensuite sélectionnez le protocole utilisé par le service soit **TCP** ou **UDP**. Enfin vous devez indiquer le port utilisé par le service sur l'interface externe, l'adresse IP de l'ordinateur interne qui dispose du service et le port à utiliser en interne.

---

-  Pour une adresse IP publique, le port public doit également être unique pour le même protocole.
-

# Présentation d'IPSec (*IP Security*)

Le protocole **IPSec** permet de sécuriser tout ou une partie du trafic IP sur un réseau. Il protège de ce fait tous les protocoles se trouvant au-dessus de la couche 3 (réseau) du modèle OSI. Il permet le remplacement des protocoles de sécurisation applicatifs comme SSL ou TLS de la couche 6 (présentation) du modèle OSI, qui demandent une version spécifique du protocole applicatif utilisé, ainsi que les appareils de chiffrement existant au niveau de la couche 1 (physique) du modèle OSI exigeant d'utiliser à chaque extrémité (émetteur et récepteur) un appareil de chiffrement compatible.

Il a été conçu pour protéger le trafic de la manière suivante :

- **Confidentialité**, avec le chiffrement du trafic pour empêcher la visibilité du contenu aux personnes non autorisées.
- **Intégrité**, avec la garantie que le message n'a pas été altéré durant son transport.
- **Authentification** des pairs pour garantir que l'émetteur et le destinataire sont bien ceux qu'ils prétendent être.
- **Anti-replay** pour empêcher de rejouer les paquets.

Les deux modes utilisés sont le **mode transport** qui ne chiffre et/ou n'authentifie que le contenu du paquet sans modifier l'en-tête IP, et le **mode tunnel** qui chiffre et authentifie le paquet IP en modifiant l'en-tête IP.

Les protocoles suivants sont utilisés par IPsec pour assurer la sécurité au niveau du paquet.

L'**authentification de l'en-tête AH** garantit l'intégrité et l'authentification de l'en-tête IP, la charge n'est pas chiffrée. En d'autres termes, AH garantit que le paquet n'a pas été altéré durant le transport et que l'émetteur et le destinataire sont bien ceux qu'ils prétendent être. Le contrôle d'intégrité AH implique l'incompatibilité avec les mécanismes de translation d'adresses NAT.

---

 NAT-T ou NAT Traversal encapsule les données dans un tunnel UDP (défaut UDP 4500) afin de contourner cette contrainte liée à la modification de l'en-tête IP. Depuis Windows 2003 ou Windows XP SP2, le NAT Microsoft est compatible avec ce mécanisme.

---

L'**encapsulation de la charge ESP** utilise le protocole IP50 et garantit la confidentialité, éventuellement son intégrité et l'authentification de la charge du paquet. Ce mode ne garantit pas que le paquet provient d'une source sûre, c'est la raison pour laquelle il existe aujourd'hui un mode mixte appelé ESP +AH qui permet de garantir le meilleur des deux protocoles.

Depuis Windows Vista, Microsoft a revu les outils IPSec et les a intégrés avec le pare-feu car leurs similitudes sont grandes. En effet, chacun est utilisé pour sécuriser le système et les données et chacun utilise des règles qui indiquent comment se comporter.

## 1. Configurer les paramètres IPSec globalement

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.
- Sur la page principale **Pare-feu Windows avec fonctionnalités avancées de sécurité**, cliquez sur **Propriétés du Pare-feu Windows**.
- Cliquez sur l'onglet **Paramètres IPSec**.
- Cliquez sur le bouton **Personnaliser**.

La boîte de dialogue qui s'affiche permet de définir les paramètres IPSec utilisés par défaut.

---

 Il peut être utile dans une optique de dépannage d'exempter le protocole ICMP d'exigence IPSEC.

---

## a. Échange de clé (mode principal) personnalisé appelé IKE (*Internet Key Exchange*) ou phase 1

- Dans la section **Échange de clé (mode principal)**, activez l'option **Avancé**, cliquez sur **Personnaliser** puis sur **Ajouter**.

<p>Algorithme d'échange de clés</p> <p><input checked="" type="radio"/> <b>Diffie-Hellman à courbe elliptique P-384</b> La sécurité la plus élevée, l'utilisation la plus intense des ressources. Compatible uniquement avec Windows Vista ou une version plus récente</p> <p><input type="radio"/> <b>Diffie-Hellman à courbe elliptique P-256</b> Sécurité plus élevée, utilisation moyenne des ressources. Compatible uniquement avec Windows Vista ou une version plus récente de</p> <p><input type="radio"/> <b>Diffie-Hellman groupe 14</b> Plus puissant que DH groupe 2.</p> <p><input checked="" type="radio"/> <b>Diffie-Hellman groupe 2 (par défaut)</b> Plus puissant que DH groupe 1.</p> <p><input type="radio"/> <b>Diffie-Hellman groupe 1</b> Cet algorithme est fourni à des fins de compatibilité descendante uniquement.</p>	<p>Algorithme de chiffrement</p> <p><input checked="" type="radio"/> <b>AES-256</b> La sécurité la plus élevée, l'utilisation la plus intense des ressources. Compatible uniquement avec Windows Vista ou une version plus récente de</p> <p><input type="radio"/> <b>AES-192</b> Plus puissant que AES-128, utilisation moyenne des ressources. Compatible uniquement avec Windows Vista ou une version plus récente de Windows.</p> <p><input checked="" type="radio"/> <b>AES-128 (valeur par défaut)</b> Plus rapide et plus puissant que DES. Compatible uniquement avec Windows Vista ou une version</p> <p><input type="radio"/> <b>3DES</b> Utilisation de ressources supérieure à DES.</p> <p><input type="radio"/> <b>DES (non recommandé)</b> Cet algorithme est fourni à des fins de compatibilité descendante uniquement.</p>	<p>Algorithme d'intégrité</p> <p><input checked="" type="radio"/> <b>SHA1 (par défaut)</b> Considéré comme plus puissant que MD5, utilise un peu plus de ressources.</p> <p><input type="radio"/> <b>MD5 (non recommandé)</b> Cet algorithme est fourni à des fins de compatibilité descendante uniquement.</p>
--	--	---

Les boîtes de dialogue précédentes permettent de définir les 5 points qui doivent être compatibles entre l'émetteur et le destinataire, soit :

- L'algorithme utilisé pour échanger les clés ou comment initier le dialogue entre les deux pairs.
- L'algorithme de chiffrement ou comment conserver la confidentialité.
- L'algorithme d'intégrité ou comment garantir que le message n'a pas été altéré.



Il est possible de créer plusieurs méthodes de chiffrement et de confidentialité pour établir des dialogues avec différents systèmes.

- La durée de vie de la clé en minutes, cela veut dire que toutes les 480 minutes, les ordinateurs vont créer de nouvelles clés de session de manière transparente pour l'utilisateur.
- La durée de vie de la clé en session.



Une durée de vie de clé de session trop petite ralentit le système et ne protège pas forcément car un pirate pourrait, avec le temps, anticiper la prochaine clé utilisée.

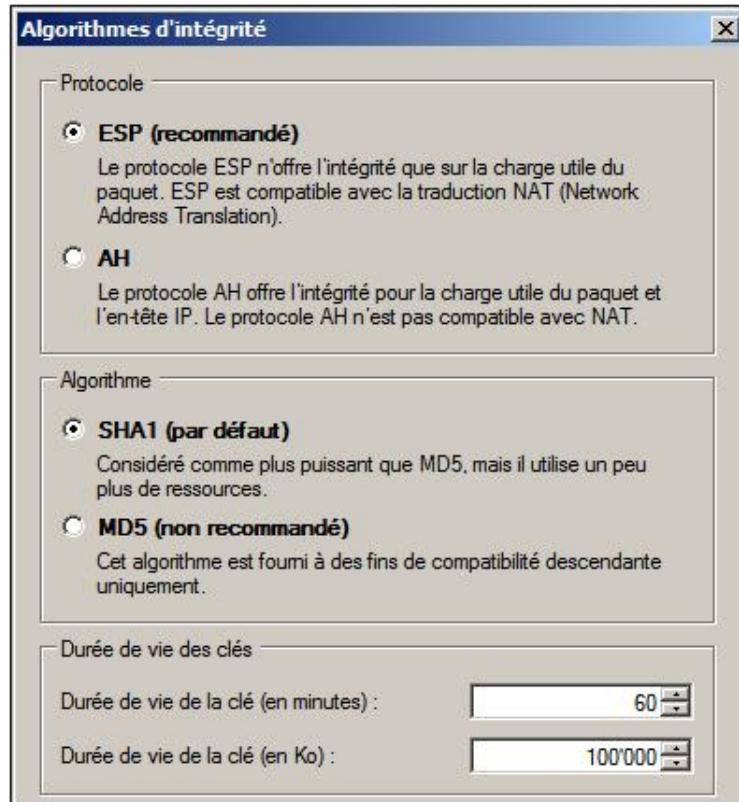
## b. Protection des données (mode rapide) personnalisée ou établissement d'IPsec en mode AH et/ou ESP

La boîte de dialogue suivante permet d'établir un tunnel IPsec en utilisant les protocoles AH ou ESP pour l'intégrité, ESP ou AH + ESP pour le chiffrement et l'intégrité des données.

Il est nécessaire de disposer à l'autre extrémité au moins un algorithme identique.

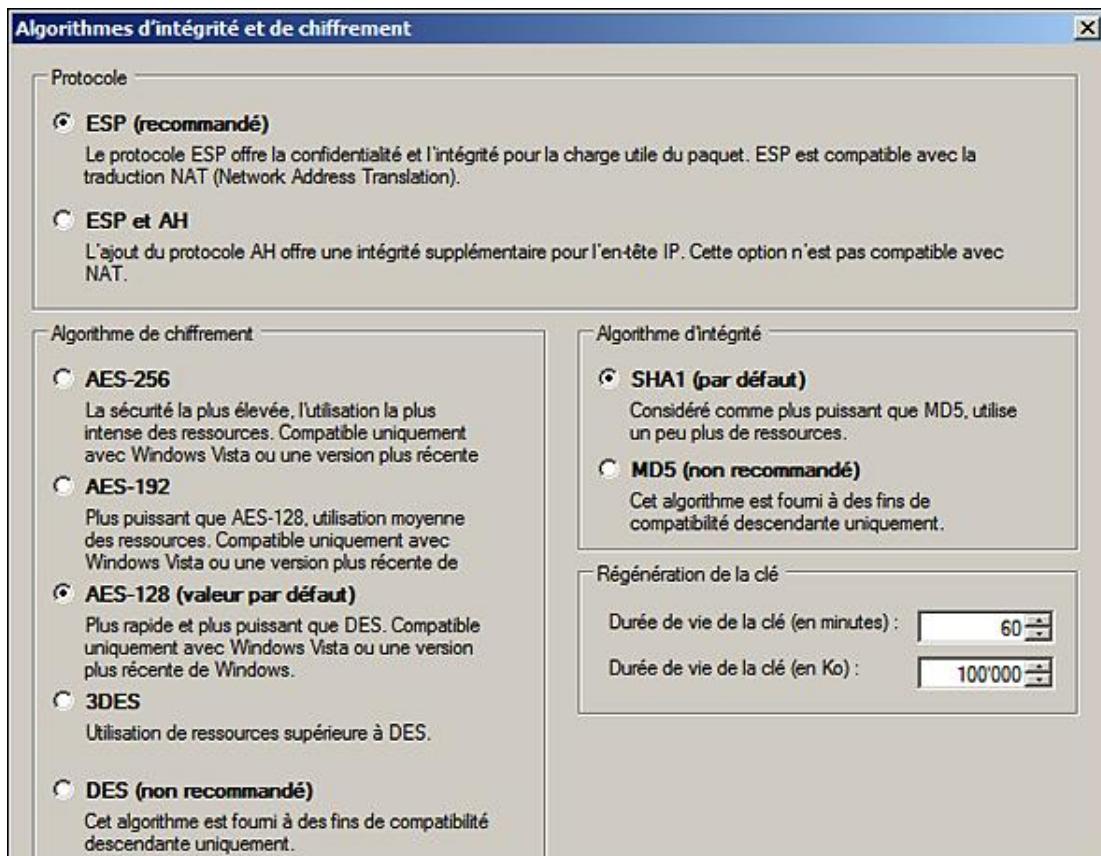
- Sur la boîte de dialogue **Personnaliser les paramètres IPSec**, dans la section **Protection des données (mode rapide)**, sélectionnez l'option **Avancé** puis cliquez sur **Personnaliser**.
- La sélection de la case à cocher **Demander le chiffrement de toutes les règles de sécurité de connexion** pour protéger le trafic réseau désactive la section **Algorithmes d'intégrité des données**.

Le bouton **Ajouter** pour les **Algorithmes d'intégrité des données** ouvre la boîte de dialogue suivante :



Le protocole utilisé est AH ou ESP et les algorithmes sont SHA+ ou MD5 ce qui donne quatre possibilités mais il faut également indiquer une durée de vie qui doit être identique à l'autre extrémité.

Le bouton **Ajouter** pour **Algorithmes d'intégrité et de chiffrement de données** ouvre la boîte de dialogue suivante :



Il permet en plus de sélectionner l'algorithme utilisé pour le chiffrement.

### c. Méthode d'authentification

La méthode d'authentification permet de sélectionner la méthode qui est utilisée par défaut pour authentifier l'autre extrémité. Cette méthode peut utiliser :

- Kerberos V5 pour l'utilisateur ;
- l'ordinateur ;
- les deux ;
- un certificat ;
- une clé pré-partagée et personnalisée ;
- la méthode par défaut, soit généralement Kerberos V5.

## 2. Créer une nouvelle règle de sécurité

L'outil pour créer des règles a été grandement amélioré et son usage est des plus aisés non seulement pour mettre en œuvre IPSec mais également pour créer des domaines serveurs ou d'isolation.

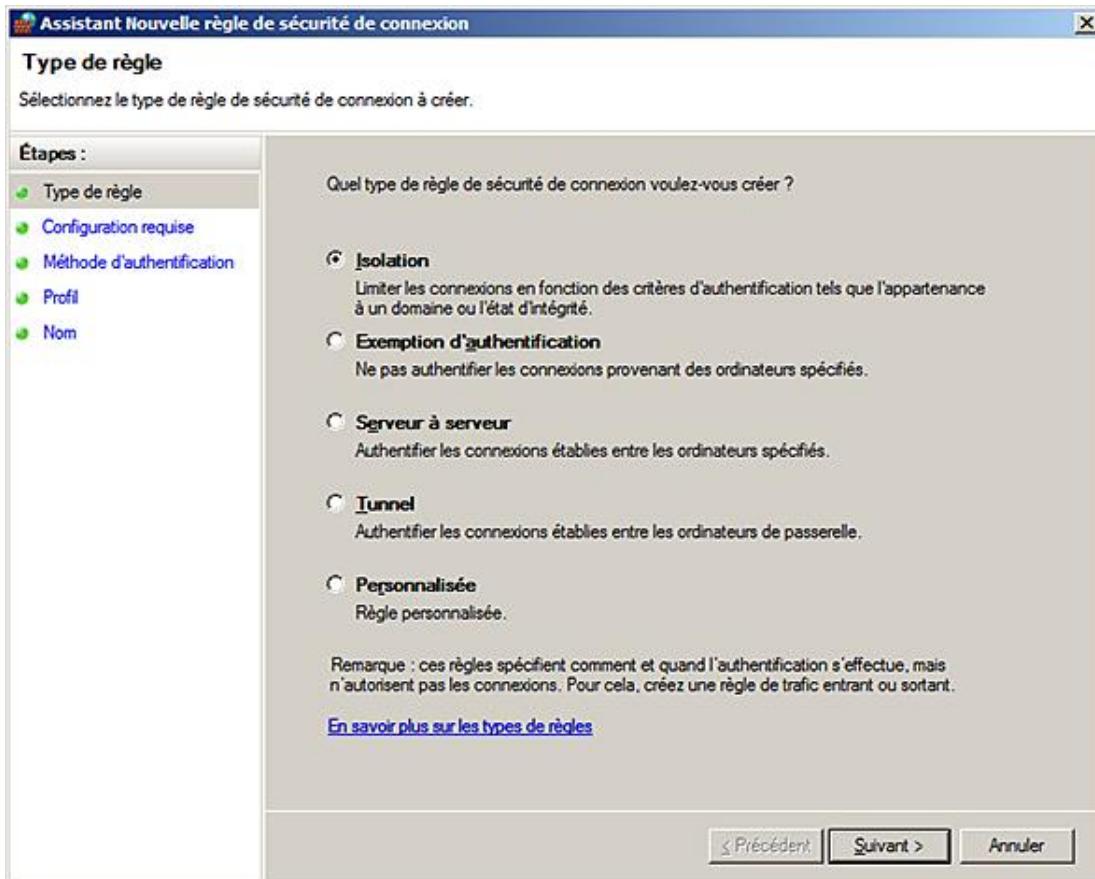
L'importation et l'exportation examinée avec le pare-feu tiennent également compte des paramètres IPSec.

 Bien que l'ancienne console soit toujours disponible, il faut utiliser le pare-feu pour créer et gérer les règles IPSec. L'ancienne console est valide si vous devez créer des règles pour des ordinateurs antérieurs à Windows Vista.

Toute la difficulté de configuration rencontrée avec l'ancienne console a disparu en augmentant le niveau

d'abstraction par rapport au protocole IPSec.

- Pour créer une nouvelle règle de sécurité, connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.
- Cliquez sur **Règles de sécurité de connexion**, puis sur **Nouvelle règle**.
- Sur la page **Type de règle**, vous pouvez sélectionner comment la règle va s'appliquer : en utilisant la notion d'isolation par rapport à un domaine, un tunnel de serveur à serveur, en n'utilisant pas l'authentification ou par une règle personnalisée.



**Isolation** permet de créer des emplacements sécurisés de communication.

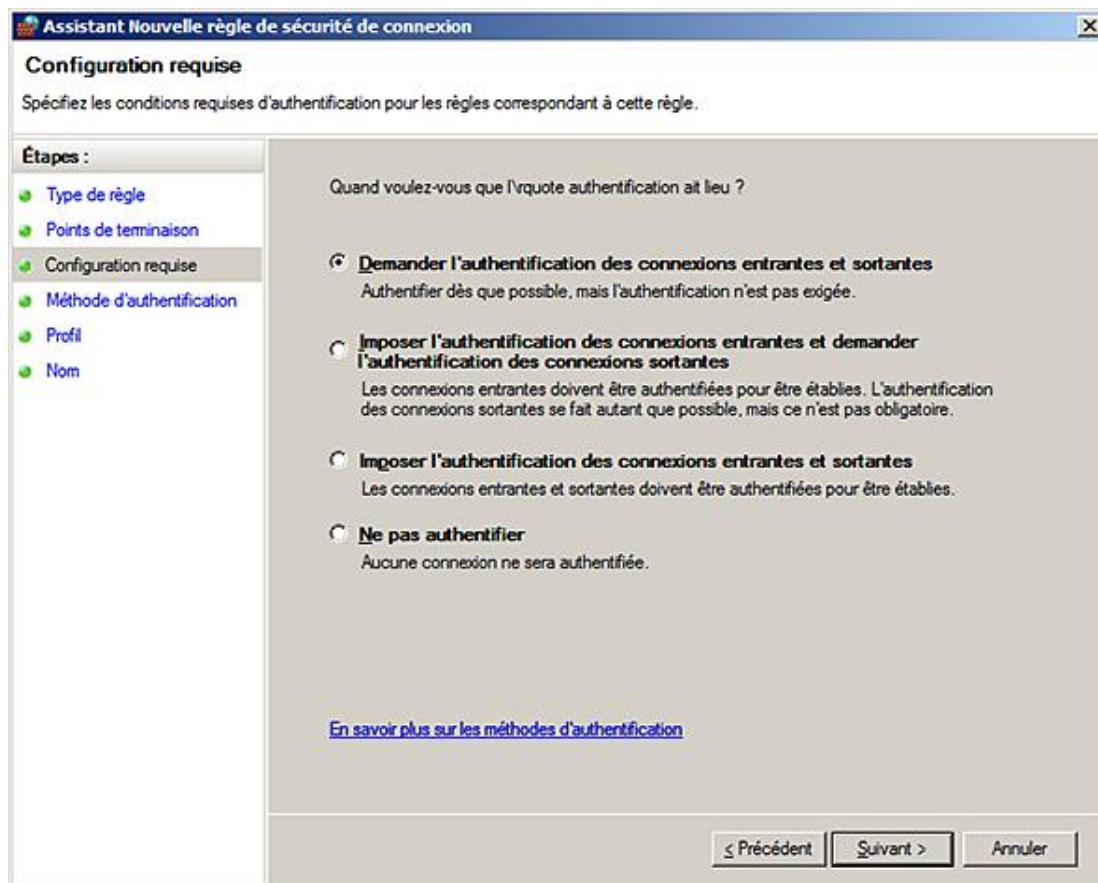
**Exemption d'authentification** permet de sécuriser une connexion mais sans garantir l'émetteur et le destinataire.

**Serveur à serveur** permet une communication sécurisée entre deux ordinateurs. Dans les anciennes versions de Windows, on utilisait le terme **Transport**.

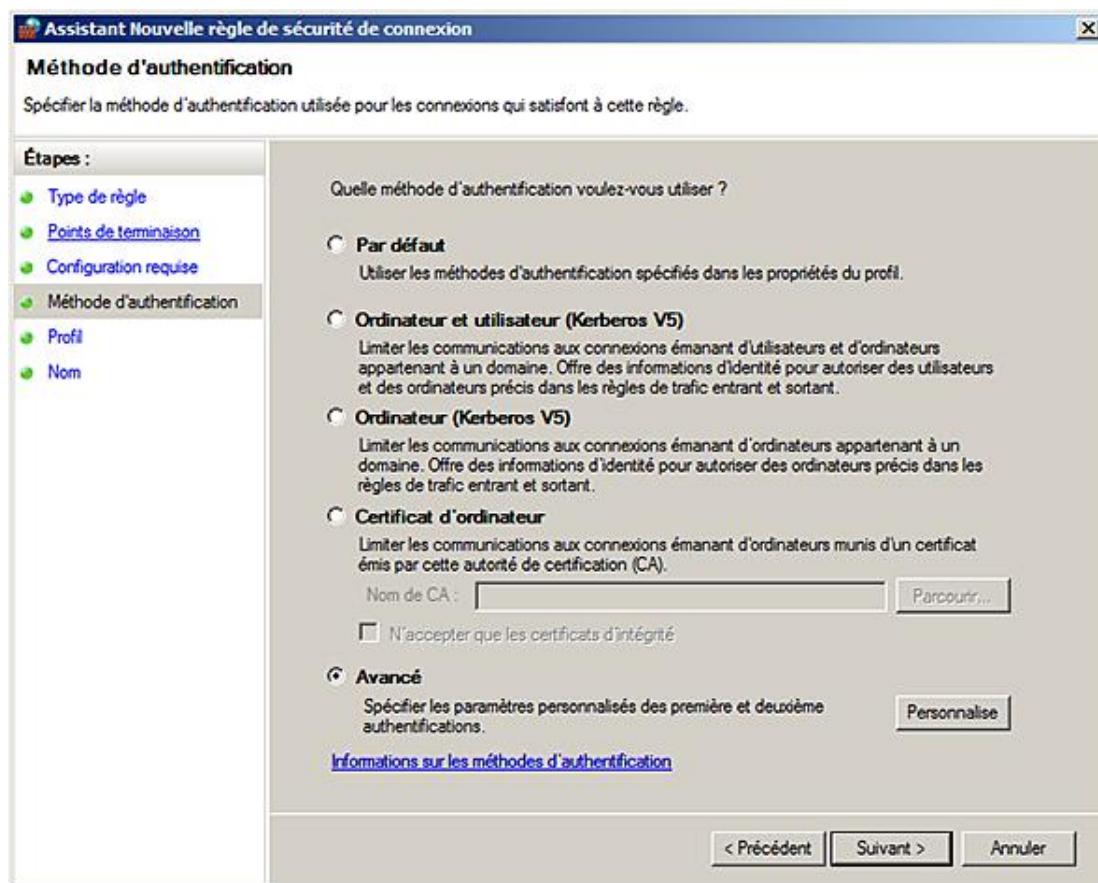
**Tunnel** permet de définir une communication sécurisée entre deux ordinateurs passant par un tunnel. Il ne définit pas le tunnel.

**Personnalisé** est un mode qui permet de définir les préférences manuellement. Cette option a été choisie pour la suite de la procédure.

- Sur la page **Points de terminaison**, vous pouvez sélectionner les deux points de terminaison pour créer une connexion sécurisée. Le point de connexion peut être une adresse IP, un sous-réseau IP, une plage d'adresses IP ou un groupe d'ordinateurs prédéfini comme les serveurs DHCP, WINS, DNS, passerelle par défaut ainsi que le sous-réseau local.
- Sur la page **Configuration requise**, vous pouvez définir comment authentifier l'ordinateur distant, soit en demandant, soit en exigeant une authentification.



- Sur la page **Méthode d'authentification** vous définissez les méthodes d'authentification comme le montre l'image suivante :



**Par défaut** selon ce qui a été spécifié dans les propriétés du profil IPSec.

**Ordinateur et utilisateur (Kerberos V5)** limite les connexions à des ordinateurs et des utilisateurs provenant du domaine.

**Ordinateur (Kerberos V5)** limite les connexions à des ordinateurs provenant du domaine.

**Certificat ordinateur** limite les communications aux ordinateurs munis d'un certificat adéquat.

**Avancé** permet de définir précisément comment authentifier y compris une authentification NTLMV2 ou l'utilisateur d'une clé pré-partagée.

- Sur la page **Méthode d'authentification**, vous pouvez sélectionner une méthode d'authentification différente de celle par défaut.
- Sur la page **Profil**, vous pouvez restreindre l'utilisation d'IPSec à un profil réseau (domaine privé publique).
- Sur la page **Nom**, indiquez le nom de la règle et sa description (facultative).

 Pour contrôler l'utilisation d'IPSec, le moniteur réseau peut vous montrer si les paquets utilisent IPSec.

 Pour dépanner IPSec, vous pouvez utiliser un ordinateur témoin qui fonctionne toujours sans IPSec. De cette manière, vous pouvez savoir si le problème provient de l'émetteur ou du destinataire.

### a. Analyse des règles de sécurité

Comme pour le pare-feu, il est possible de visualiser rapidement des informations sur l'état du pare-feu et recevoir des informations sur chaque règle activée.

De plus il est possible d'analyser les associations de sécurité créées que ce soit celles de la phase 1 appelée Mode principal (création du tunnel) ou de la phase 2 mode rapide (négociation des protocoles de sécurisation de la communication).

## 3. Utilisation de l'invite de commande

La commande **netsh** permet de gérer IPSec, y compris les règles, de manière efficace à l'aide de scripts. Bien qu'il existe deux contextes pour IPSec à savoir **ipsec** et **adfirewall**, c'est une bonne méthode de n'utiliser qu'adfirewall car le premier contexte est amené à disparaître dans une future version.

### Importation d'un fichier de stratégie

```
netsh advfirewall conSec import c:\MonRep\MonFichier.wfw
```

### Création d'une règle d'isolation de domaine

```
netsh advfirewall conSec add rule name="Règle d'isolation de Domaine"
"endpoint1=any endpoint2=any action=requireinrequestout
```

## 4. Isolation de domaine

De nos jours, la sécurité d'un réseau ne passe plus par une notion simpliste qui consiste à dire que soit l'on est à l'intérieur de l'entreprise (Intranet), donc sécurisé, soit on est à l'extérieur (Internet), donc dans un environnement peu sécurisé. Les utilisateurs veulent disposer d'une granularité plus fine sans pour autant augmenter le niveau de sécurité de tout le réseau d'entreprise.

Pour cela, il faudrait créer plusieurs réseaux internes disposant chacun d'un niveau de sécurité et de règles permettant la communication ou non vers d'autres ordinateurs sur intranet. Avant Windows 2008, il était possible de créer des réseaux virtuels (vlans) différents, d'exiger l'utilisation d'IPSec, voire même d'isoler des réseaux en utilisant des pare-feu réseaux. Windows 2008 introduit la notion d'isolation de domaine qui permet de configurer simplement les ordinateurs afin de bénéficier de la protection offerte par les technologies IPSec d'authentification, de certificats,

de chiffrage voire de l'intégration avec NAP. Dans un travail pratique, vous mettrez en œuvre une isolation de domaine.

# Présentation du pare-feu

## 1. Ce qu'il faut savoir

Un pare-feu permet de bloquer ou de laisser passer les paquets à l'aide de filtres agissant au niveau des couches 3, 4, et au-delà du modèle OSI.

Il existe des pare-feu de type réseau comme Microsoft ISA Server ou Cisco PIX/ASA se plaçant entre deux sous-réseaux et filtrant le flux de données, mais également des pare-feu de type hôte filtrant le flux de données entrant ou sortant de l'hôte.

- 
-  Un pare-feu d'hôte permet d'éviter que des ordinateurs malveillants situés sur le réseau interne attaquent les ordinateurs de l'entreprise.
- 

Le pare-feu de type hôte diminue la surface d'attaque de l'ordinateur protégé. Par défaut, les connexions sortantes sont permises alors que les connexions entrantes sont refusées.

Microsoft a introduit un pare-feu d'hôte très rudimentaire avec Windows NT4 puis en a ajouté un second, une version plus adaptée à l'hôte et activée par défaut avec Windows XP SP2 et Windows Server 2003 SP1. Il existait également depuis Windows Server 2000 un filtre permettant de configurer les connexions entrantes et sortantes d'une interface dont l'usage était tout sauf pratique.

Windows Vista et Windows Server 2008 remplacent ces trois pare-feu par un seul, plus simple à gérer et plus puissant, qui dispose notamment des caractéristiques suivantes :

- une nouvelle interface graphique intégrant le pare-feu avec la gestion d'IPSec,
- un filtrage complet des protocoles IPv4 et IPv6,
- le blocage de tout trafic entrant excepté s'il s'agit d'une réponse à une requête sortante,
- l'activation du pare-feu par défaut.

- 
-  Le pare-feu permet de définir des filtres au niveau de l'hôte ou de la carte réseau que ce soit pour les protocoles IP, TCP/UDP ou ICMP.
- 

## 2. Profil réseau

Dans Windows Server 2008, il existe trois profils réseau appelés **Domaine**, **Privé** et **Public**. Pour chaque profil, il est possible de définir des règles différentes pour le pare-feu.

Le profil **Domaine** est reconnu par Windows, lorsque le serveur se trouve dans son domaine Active Directory. Le profil **Public** s'applique pour tout réseau inconnu ou pas digne de confiance. Le profil **Privé** est un profil intermédiaire entre le profil **Public** et le profil de **Domaine**.

- 
-  Il peut être surprenant de créer des profils réseau différents pour un serveur. En fait, si le serveur peut être amené à quitter l'entreprise pour une exposition temporaire, le fait d'avoir au préalable créé des règles de connexion différentes évite des problèmes de sécurité et d'erreur de configuration.
- 

- 
-  Notez qu'un profil spécifique est associé à chaque interface réseau.
- 

Pour modifier le profil, il faut passer par le **Centre Réseau et partage**.

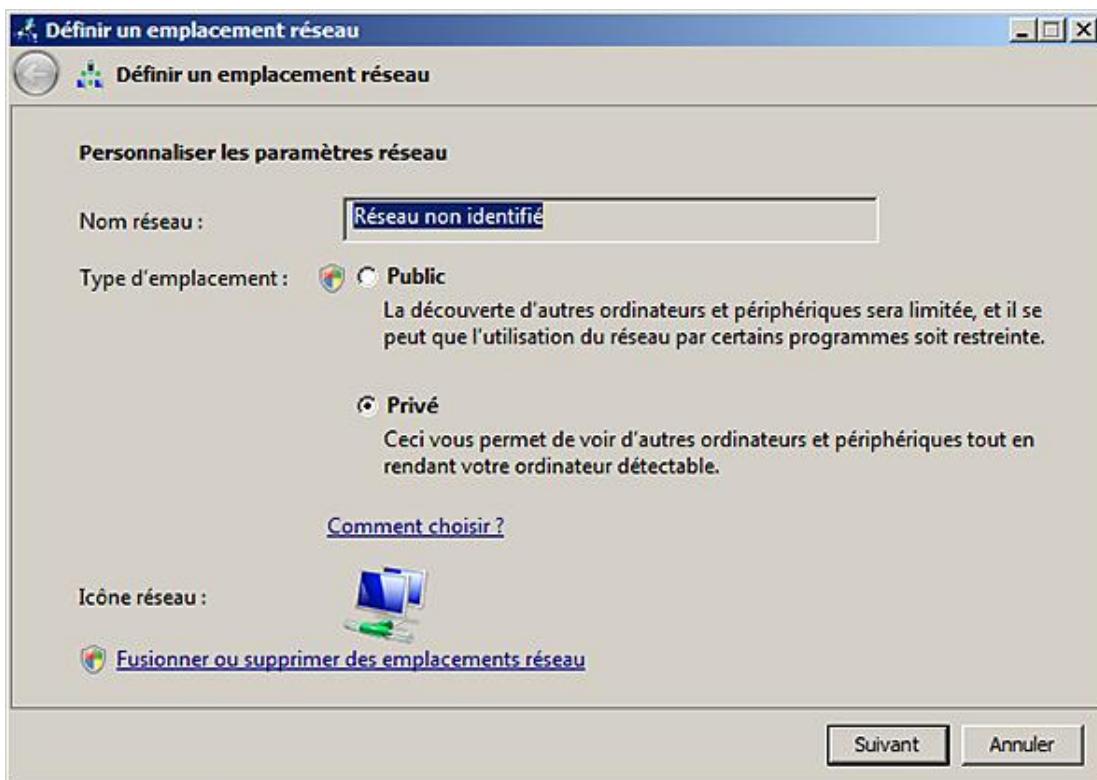
- Connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.
- Sur le **Bureau**, cliquez sur **Démarrer**, saisissez **Centre Réseau et partage** dans la zone **Rechercher** puis appuyez sur [Entrée].

- Dans la fenêtre **Centre Réseau et partage**, cliquez sur **Personnaliser**.
- Dans la boîte de dialogue **Définir un emplacement réseau**, sélectionnez le type d'emplacement puis cliquez sur **Suivant**.

 Si l'ordinateur n'est pas membre d'un domaine, le profil de domaine n'apparaît pas.

Le lien **Fusionner ou supprimer des emplacements réseau** permet de supprimer des emplacements déjà définis ou de diminuer le nombre d'emplacements en les fusionnant.

- Sur la page **Paramètres réseau définis correctement**, contrôlez les valeurs puis cliquez sur **Terminer**.



### 3. Le pare-feu standard

Le pare-feu standard est la vision simplifiée du pare-feu qui ne modifie que les paramètres du profil Public.

- Pour ouvrir le pare-feu, connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.
- Sur le **Bureau**, cliquez sur **Démarrer - Panneau de configuration** puis sur **Pare-feu Windows**.
- Cliquez sur **Activer ou désactiver le Pare-feu Windows** pour ouvrir la boîte de dialogue **Paramètres du Pare-feu Windows**.

#### Onglet Général

L'onglet **Général** permet d'activer ou de désactiver le pare-feu.

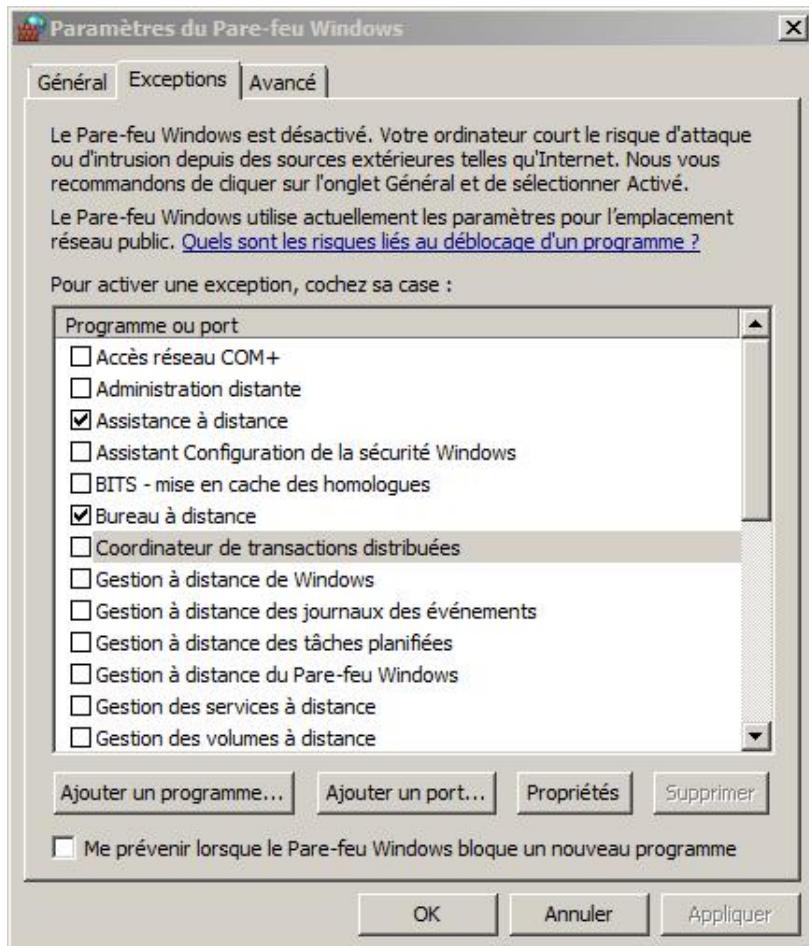
L'option **Activé** permet d'activer le pare-feu tout en permettant de filtrer et laisser rentrer des connexions entrantes faisant partie des exceptions. La case à cocher **Bloquer toutes les connexions entrantes** empêche toute exception.

L'option **Désactivé** désactive le pare-feu pour le réseau public.

 Il est déconseillé de désactiver le pare-feu, excepté pour effectuer du dépannage pendant de courts instants.

## Onglet Exceptions

L'onglet **Exceptions** permet de définir des exceptions pour les connexions entrantes ; celles-ci peuvent être définies par défaut, créées manuellement ou proposées par le pare-feu.



La liste indique les exceptions potentielles. Si la case à cocher correspondante est cochée, alors l'exception est activée.

 Il n'est plus possible de gérer les paramètres **ICMP** avec le pare-feu standard.

Le bouton **Ajouter un programme** permet d'ajouter une exception basée sur un fichier exécutable. Le bouton **Ajouter un port** permet d'ajouter une exception basée sur un port. Le bouton **Propriétés** affiche le nom, le chemin d'accès ou une description de l'exception sélectionnée. Le bouton **Supprimer** permet de supprimer une exception qui n'est pas une exception par défaut. La case à cocher **Me prévenir lorsque le Pare-feu Windows bloque un nouveau programme** permet d'afficher des avertissements lorsque le pare-feu bloque un nouveau programme.

## Onglet Avancé

L'onglet **Avancé** permet d'activer ou de désactiver le pare-feu sur chacune des cartes réseau. La liste des **Connexions réseau** permet d'activer ou de désactiver le pare-feu. Le bouton **Par défaut** permet de rétablir les valeurs par défaut du pare-feu et efface toutes les modifications apportées.

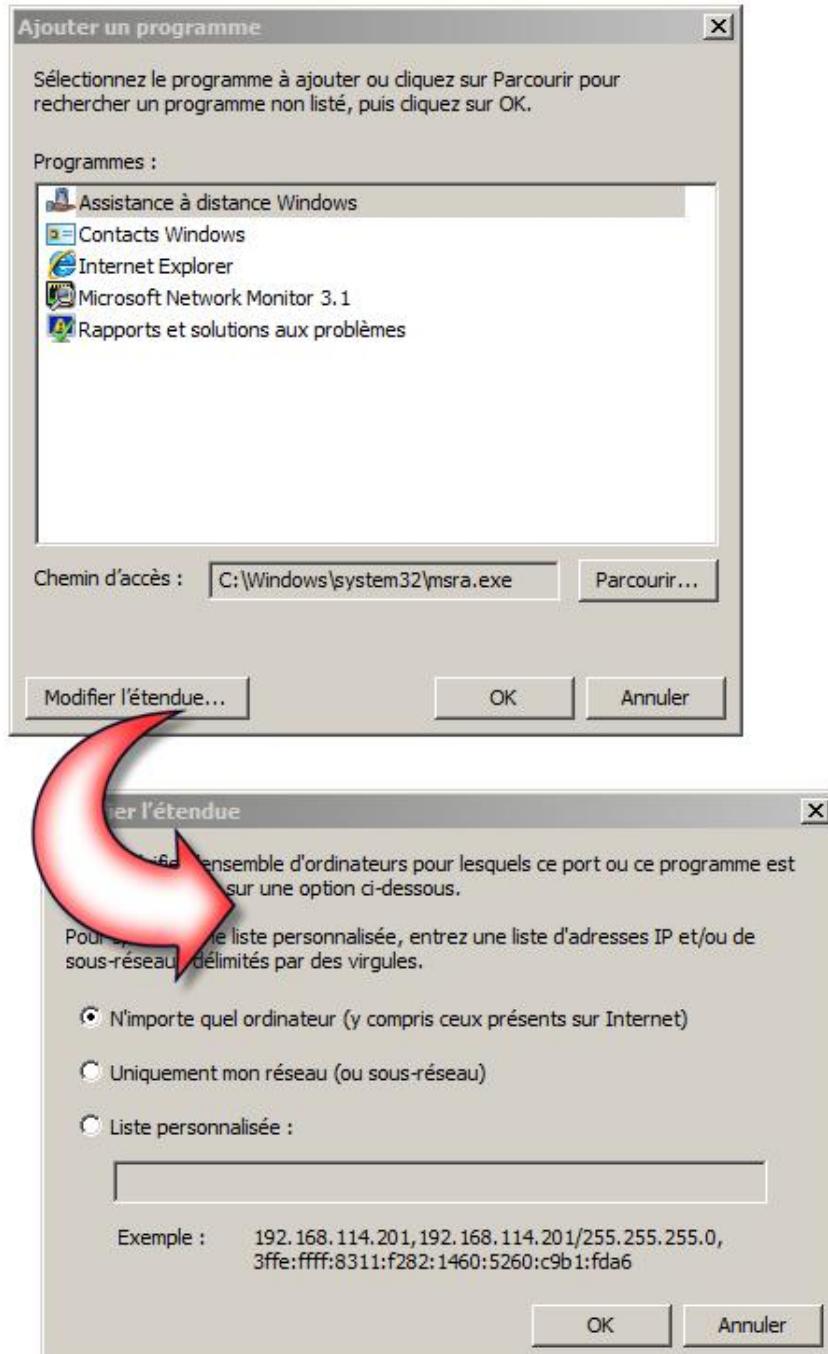
### a. Ajouter un programme

- Connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.
- Sur le **Bureau**, cliquez sur **Démarrer - Panneau de configuration** puis sur **Pare-feu Windows**.

- Cliquez sur **Autoriser un programme via le Pare-feu Windows**.

- Dans l'onglet **Exceptions**, cliquez sur **Ajouter un programme**.

La liste affiche les **Programmes** qui sont déjà dans la liste des exceptions.



- Cliquez sur **Parcourir** pour sélectionner le nom du fichier exécutable pour créer l'exception.
- Cliquez éventuellement sur **Modifier l'étendue** afin de limiter les ordinateurs qui ont accès au fichier exécutable. Par défaut, n'importe quel ordinateur peut se connecter, mais vous pouvez limiter l'accès soit à votre réseau ou sous-réseau, soit à une liste d'adresses IP.

## b. Ajouter un port

- Connectez-vous en tant qu'administrateur sur le serveur Windows Server 2008.

- Sur le **Bureau**, cliquez sur **Démarrer - Panneau de configuration** puis sur **Pare-feu Windows**.
- Cliquez sur **Autoriser un programme via le Pare-feu Windows**.
- Dans l'onglet **Exceptions**, cliquez sur **Ajouter un port**.
- Tapez le nom de l'exception, le numéro ou les numéros de port ainsi que le protocole utilisé (TCP ou UDP).
- Cliquez éventuellement sur **Modifier l'étendue** afin de limiter les ordinateurs qui ont accès. Par défaut, n'importe quel ordinateur peut se connecter, mais vous pouvez limiter l'accès soit à votre réseau ou sous-réseau, soit à une liste d'adresses IP.

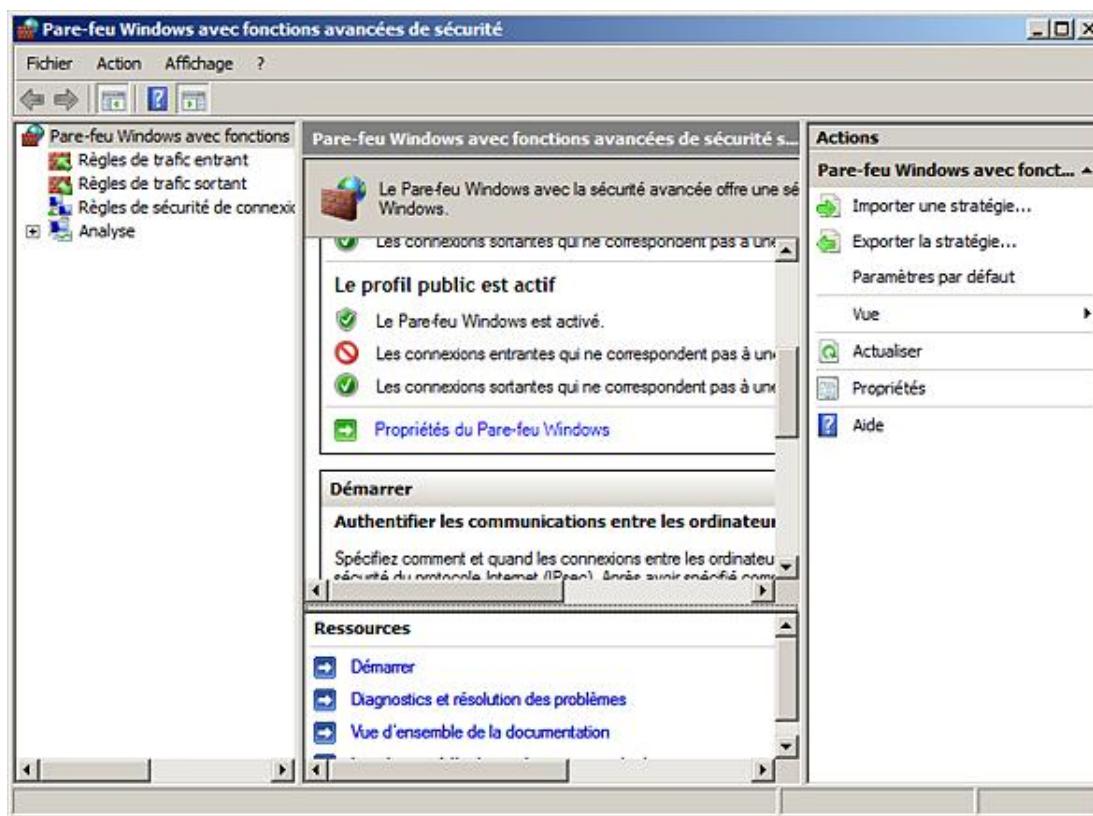
## 4. Le pare-feu Windows avec fonctions avancées de sécurité

Cette application permet de gérer l'intégralité du pare-feu de manière efficace. En exportant les stratégies définies, il sera non seulement possible de les importer dans un autre ordinateur exécutant au moins Windows Vista ou Windows Server 2008 mais également les placer dans une stratégie de groupe.

### a. Ouvrir le pare-feu Windows avec fonctions avancées de sécurité

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.

Votre console ressemble à la figure suivante :



#### Arborescence de la console

**Règles de trafic entrant** : contient toutes les règles définies pour le trafic entrant.

**Règles de trafic sortant** : contient toutes les règles définies pour le trafic sortant.

**Règles de sécurité de connexion** : règles utilisant IPSec.

**Analyse** : permet d'analyser les règles.

#### **Fenêtre principale** Section Vue d'ensemble

Il faut que dans l'arborescence de la console, le nœud **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local** soit sélectionné.

La vue d'ensemble affiche pour chaque profil, Domaine, Privé et Public, l'information indiquant si le pare-feu est activé ainsi que le comportement pour les connexions entrantes et sortantes.

#### **Section Démarrer (sous la section "Vue d'ensemble")**

Les liens renvoient au menu correspondant de l'arborescence de la console.

#### **Section Ressources**

Renvoie à la documentation en ligne.

#### **Actions**

**Importer une stratégie** : importe un fichier de stratégie de comportement du pare-feu (format wfw).

**Exporter la stratégie** : exporte un fichier de stratégie de comportement du pare-feu au format wfw.

**Paramètres par défaut** : réinitialise les valeurs par défaut ; toutes les modifications sont perdues, il est nécessaire d'effectuer une exportation de la stratégie avant.

**Vue** : permet de modifier l'affichage.

**Actualiser** : actualise immédiatement l'affichage.

**Propriétés** : affiche la boîte de dialogue **Propriétés de Pare-feu Windows avec fonctions avancées de sécurité** décrite plus haut.

**Aide** : affiche l'aide.

### **b. Restaurer les paramètres par défaut**

Une fonction intéressante a été implémentée afin de revenir à l'état initial, soit celui existant lorsque le serveur a été installé. Pour cela, effectuez la procédure suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Pare-feu Windows avec fonctions avancées de sécurité**.
- Dans l'arborescence, sélectionnez le nœud **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur Local**.
- Dans **Actions**, cliquez sur **Paramètres par défaut**.
- Lisez attentivement la mise en garde de la boîte de dialogue qui apparaît puis cliquez sur **Oui**.
- Cliquez sur **OK** dans la boîte de dialogue vous indiquant que les paramètres par défaut ont été réappliqués.

### **c. Propriétés du Pare-feu Windows**

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Pare-feu Windows avec fonctions avancées de sécurité**.

#### **Onglets Profil de domaine, Profil privé, Profil public**

## Pare-feu Windows avec fonctions avancées de sécurité sur Ordin...

Profil de domaine | Profil privé | Profil public | Paramètres IPsec |

Spécifiez le comportement lorsqu'un ordinateur est connecté à son domaine d'entreprise.

État :



État du pare-feu : Activé (recommandé)

Connexions entrantes : Bloquer (par défaut)

Connexions sortantes : Autoriser (par défaut)

Paramètres :



Spécifier les paramètres définissant le comportement du Pare-feu Windows.

Personnaliser...

Enregistrement :



Spécifier les paramètres de journalisation pour le dépannage.

Personnaliser...

[Informations sur ces paramètres](#)

OK

Annuler

Appliquer

Pour chaque profil, les valeurs sont les mêmes :

**État du pare-feu : Activé (recommandé) ou Inactif.**

**Connexions entrantes : Bloquer (par défaut), Bloquer toutes les connexions ou Autoriser.**

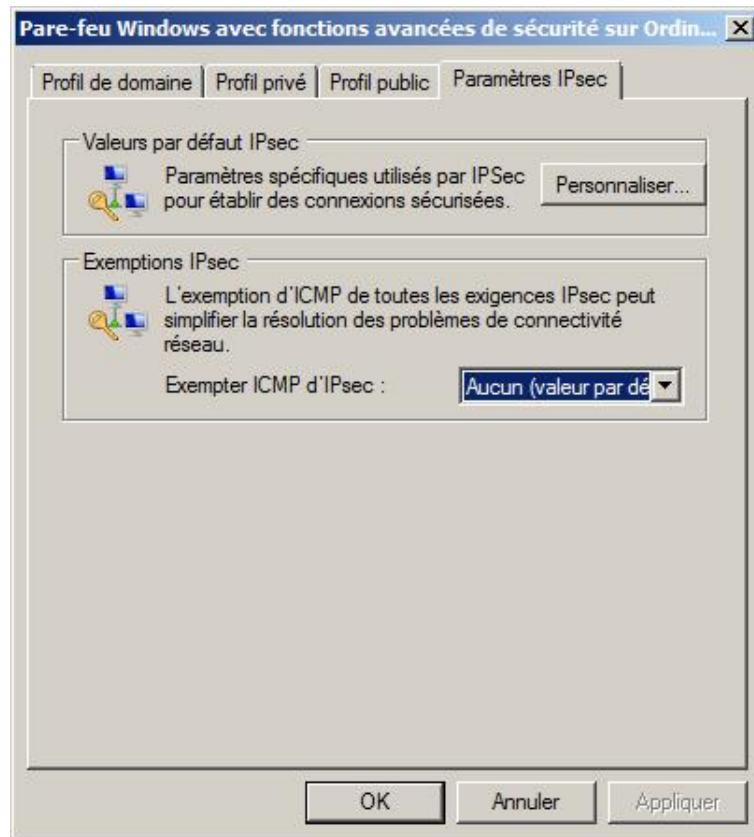
**Connexions sortantes : Autoriser (par défaut) ou Refuser.**

**Paramètres :** le bouton **Personnaliser** permet de paramétriser le comportement du pare-feu Windows :

- affiche une notification pour les connexions bloquées.
- permet une réponse de monodiffusion d'un message multidiffusion ou de diffusion.
- fusionne les règles locales de pare-feu avec les règles définies par stratégie de groupe.

**Enregistrement :** le bouton **Personnaliser** permet de spécifier les paramètres de journalisation : emplacement du fichier de journalisation (%systemroot%\system32\logfiles\firewall\pfirewall.log), taille maximale du fichier (4096 Ko par défaut), enregistrement des paquets ignorés (**Aucun** par défaut) et enregistrement des connexions réussies (**Aucun** par défaut).

### Onglet Paramètres IPsec



**Valeurs par défaut IPsec** : permet de définir le comportement par défaut lors de l'activation d'IPsec.

**Exemptions IPsec** : permet de ne pas utiliser IPsec pour ICMP, utile pour le dépannage.

#### d. Importer et exporter des stratégies de pare-feu

Un des grands avantages du nouveau pare-feu est qu'il est désormais possible d'exporter et d'importer des stratégies entre les différents ordinateurs qui composent le réseau de l'entreprise mais également d'importer ces stratégies dans une stratégie de groupes afin de la déployer efficacement.

Pour exporter une stratégie, effectuez les actions de la procédure suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Pare-feu Windows avec fonctions avancées de sécurité**.
- Dans l'arborescence, sélectionnez le nœud **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur Local**.
- Dans **Actions**, cliquez sur **Exporter la stratégie**.
- Dans la boîte de dialogue **Enregistrer sous**, sélectionnez un chemin et un nom pour enregistrer le fichier d'exportation de la stratégie, puis cliquez sur **Enregistrer**.
- Cliquez sur **OK** dans la boîte de dialogue vous notifiant que l'exportation de la stratégie est terminée.

Importer une stratégie peut avoir son importance dans un petit réseau n'utilisant pas l'Active Directory. Pour cette dernière, il est préférable d'utiliser les stratégies de groupe qui seront montrées plus loin. Pour importer une stratégie, effectuez les actions de la procédure suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Pare-feu Windows avec fonctions avancées de sécurité**.

- Dans l'arborescence, sélectionnez le nœud **Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur Local**.
- Dans **Actions**, cliquez sur **Importer la stratégie**.
- Dans la boîte de dialogue vous informant qu'importer une stratégie remplace tous les paramètres actuellement définis, cliquez sur **Oui**.
- Dans la boîte de dialogue **Ouvrir**, sélectionnez un chemin et un nom pour enregistrer le fichier d'exportation de la stratégie puis cliquez sur **Ouvrir**.
- Cliquez sur **OK** dans la boîte de dialogue vous notifiant que l'importation de la stratégie est terminée.

Pour déployer efficacement une stratégie de règles de pare-feu, il est possible d'importer une stratégie définie et testée préalablement en tant qu'élément d'une stratégie de groupe. Cette méthodologie permet de garantir une gestion centralisée.

Pour gérer les stratégies de pare-feu à l'aide des stratégies de groupe, effectuez les actions suivantes :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestion des stratégies de groupe**.
- Créez ou éditez une stratégie de groupe si possible au niveau du domaine.
- Dans l'**Éditeur de gestion des stratégies de groupe**, développez **Configuration Ordinateur, Stratégies, Paramètres Windows, Paramètres de sécurité, Pare-feu Windows avec fonctions avancées de sécurité**.
- Cliquez avec le bouton droit de la souris sur **Pare-feu Windows avec fonctions avancées de sécurité - LDAP: (//cn={....})**, puis sur **Importer une stratégie**.



- Dans la boîte de dialogue vous informant qu'importer une stratégie remplace tous les paramètres actuellement définis, cliquez sur **Oui**.

- Dans la boîte de dialogue **Ouvrir**, sélectionnez un chemin et un nom pour enregistrer le fichier d'exportation de la stratégie puis cliquez sur **Ouvrir**.
- Cliquez sur **OK** dans la boîte de dialogue vous notifiant que l'importation de la stratégie s'est terminée.

Dès lors, la stratégie définie pour le pare-feu s'appliquera pour les ordinateurs du domaine. Veuillez également noter qu'il est possible de gérer le comportement par défaut du pare-feu en cliquant sur **Propriétés** au lieu d'**importer une stratégie**. L'**export d'une stratégie** est également possible.

En cliquant sur **Propriétés du Pare-feu Windows**, il est possible de modifier le comportement pour chaque profil ainsi que les paramètres générateurs d'IPSec.

## e. Règles de trafic entrant ou sortant

Chaque règle de la liste peut être désactivée, activée, supprimée ou modifiée. Il est également possible d'ajouter une nouvelle règle.

Les actions possibles pour les règles de trafic entrant ou sortant sont :

**Nouvelle règle** : permet d'ajouter une nouvelle règle.

**Filtrer par profil** : permet de filtrer l'affichage par profil ou pour tous les profils.

**Filtrer par état** : permet de filtrer l'affichage pour tous les états ou par état activé ou désactivé.

**Filtrer par groupe** : permet de filtrer l'affichage en fonction du contenu de la colonne **Groupe**.

**Vue** : permet de personnaliser l'affichage des colonnes.

**Actualiser** : actualise immédiatement la liste.

**Exportation de la liste** : exporte la liste des règles dans un fichier texte ou tabulaire.

**Aide** : affiche l'aide.

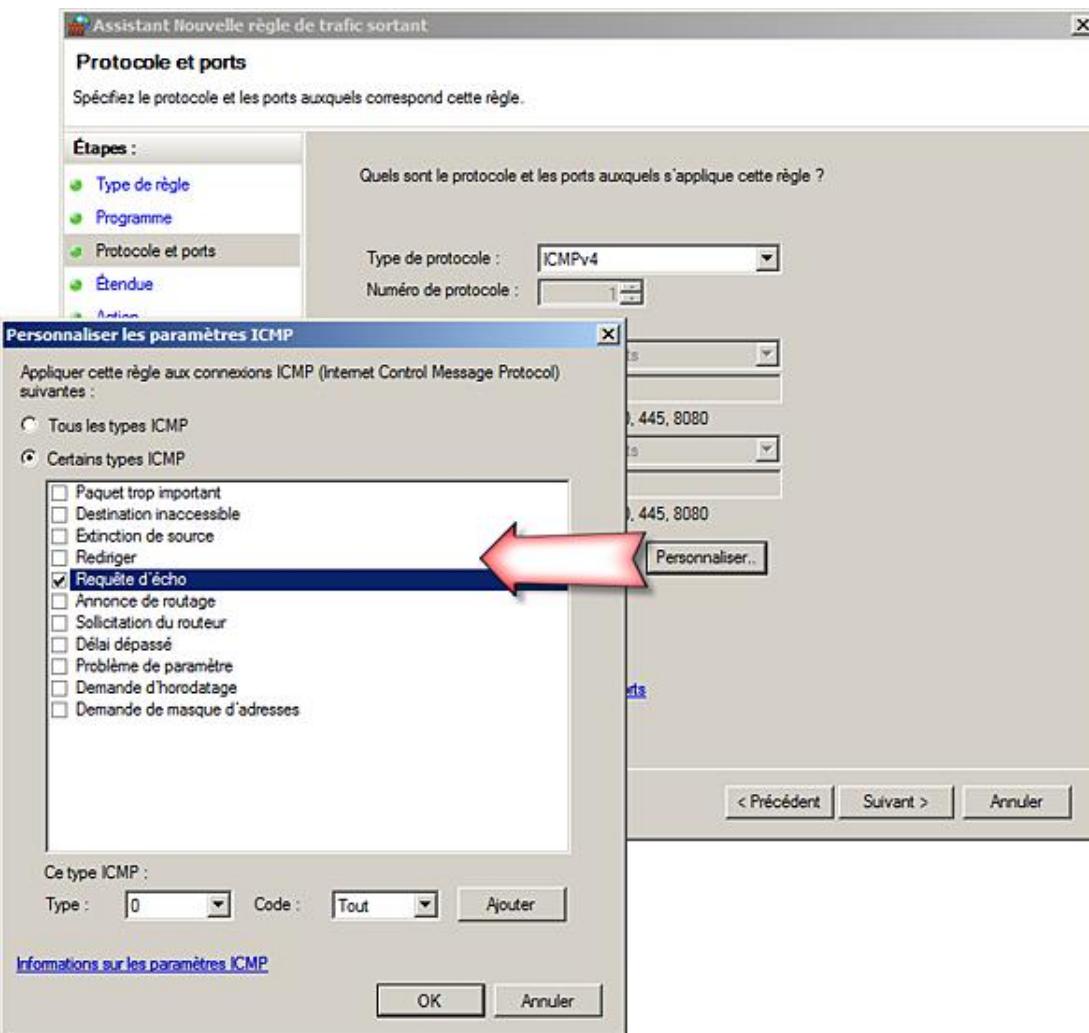
**Activer la règle ou Désactiver la règle** : active ou désactive la règle sélectionnée.

**Propriétés** : permet de modifier la règle sélectionnée.

**Aide** : affiche l'aide.

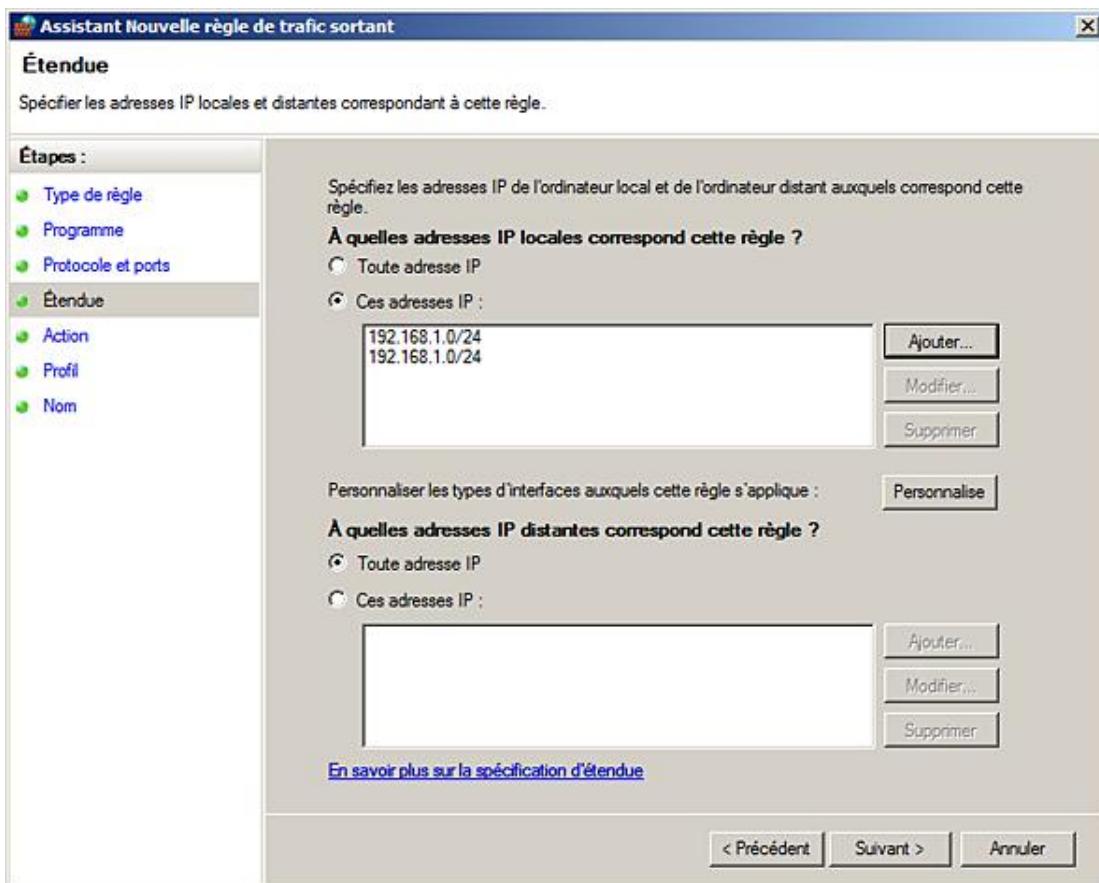
## f. Ajouter une règle

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.
- Cliquez soit sur **Règles de trafic entrant**, soit sur **Règles de trafic sortant** puis sur **Nouvelle règle**.
- Sur la page **Type de règle**, sélectionnez le type de règle : basé sur un programme, ou sur un port UDP ou TCP, une règle prédéfinie qui contrôle les connexions liées à Windows ou une règle personnalisée. En fonction du type de règle sélectionné, le nombre de pages de l'assistant varie.
- Si l'on choisit **Programme**, il est possible de sélectionner la règle pour un programme, ou tous les programmes. Puis cliquez sur **Suivant**.
- Sur la page **Protocole et ports**, il est possible de définir le type de protocole comme personnalisé c'est-à-dire avec le numéro attribué lors de sa normalisation ou en sélectionnant le nom des protocoles les plus utilisés comme IGMP, UDP, TCP, ICMP, L2TP, IPv4, IPv6... Il faut également définir les ports locaux et les ports distants qui doivent être utilisés. Enfin le bouton **Personnaliser** permet de définir les paramètres ICMP, comme le montrent les images suivantes.



➤ Certains administrateurs bloquent tout le trafic ICMP y compris les types ICMP **ECHO** et **ECHO REPLY** utilisés par la commande **PING**, ce que je déconseille pour les deux types ICMP cités.

- Sur la fenêtre étendue, il est possible de limiter l'application de la règle au niveau des adresses IP locales ou distantes :



Les plages d'adresses locales ou distantes peuvent aller d'une adresse spécifique à toutes les adresses. Une plage peut également s'appliquer à une interface spécifique.

- Sur la page **Action**, il est possible de définir si la connexion est autorisée ou bloquée , éventuellement autorisée si elle est sécurisée avec le protocole IPsec en mode intégrité (authentification) ou intégrité (authentification) + confidentialité (chiffrement).

L'ordre de priorité d'application des règles est la suivante : 1) Contournement authentifié (en d'autres mots, règles qui remplacent les règles de blocage). 2) Bloquer la connexion. 3) Autoriser la connexion. 4) Comportement de profil par défaut selon ce qui a été défini dans l'onglet **Profil** de la boîte de dialogue **Propriétés de Pare-feu Windows avec sécurité avancée**.

- Sur la page **Profil**, il faut indiquer le ou les profils subissant la règle.
- Enfin sur la page **Nom**, donnez un **Nom** à la règle et une **Description** (facultative).

La règle apparaît dans la liste et elle est activée.

## g.Modifier une règle

Les règles prédéfinies sont partiellement modifiables.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Pare-feu Windows avec fonctions avancées de sécurité**.
- Cliquez soit sur **Règles de trafic entrant**, soit sur **Règles de trafic sortant**.

- Dans la liste des règles, sélectionnez une règle puis cliquez sur **Propriétés**.
- Modifiez la règle selon les besoins. Pour plus d'informations sur les onglets, reportez-vous à la section précédente.

## **h. Filtrer les règles de trafic**

Il est possible et bien utile de pouvoir filtrer les règles de trafic que ce soit pour les trafics entrant ou sortant mais également en se basant sur d'autres critères comme :

- **Filtres par profil** : filtrer par profil de domaine, profil privé, profil public, ou tous les profils.
- **Filtres par état** : règles qui sont activées, règles désactivées ou toutes les règles.
- **Filtres par groupe** : afficher les stratégies prédéfinies en fonction des groupes auxquels elles appartiennent. Actuellement il n'est pas possible d'associer une règle à un groupe. Les nouvelles règles font automatiquement partie de Règles sans groupe.

La procédure pour activer une vue filtrée est :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Pare-feu Windows avec fonctions avancées de sécurité**.
- Dans l'arborescence, sélectionnez le nœud **Règles de trafic entrant** ou **Règles de trafic sortant**.
- Dans **Actions**, sélectionnez le filtre souhaité.

## **i. Analyse du Pare-feu**

Le nœud analyse permet de visualiser rapidement des informations sur l'état du pare-feu et donne des indications sur chaque règle activée.

Il est regrettable qu'aucune statistique ne soit disponible sur les paquets analysés par le pare-feu en fonction de la règle, car cela permettrait de créer des rapports intéressants.

## **j. Gestion du pare-feu à l'aide de l'invite de commande**

La commande **netsh** permet de gérer le pare-feu, y compris les règles, de manière efficace à l'aide de scripts. Bien qu'il existe deux contextes pour le pare-feu à savoir **firewall** et **advfirewall**, il est une bonne méthode de n'utiliser qu'**advfirewall**, car le premier contexte est amené à disparaître dans une future version.

- **Ajouter une règle pour une application :**

```
netsh advfirewall firewall add rule name="Mon Application" dir=in action=allow
program="C:\MonRep\MonApp.exe" enable=yes
```

- **Supprimer une règle :**

```
netsh advfirewall firewall delete rule name=rule name
program="C:\MonRep\MonApp.exe"
```

- **Restaurer les stratégies par défaut :**

```
netsh advfirewall reset
```

# Présentation

## 1. Correspondance avec l'examen

Ce chapitre couvre les objectifs suivants décrits dans les sections suivantes :

### Configuration de l'accès au réseau

#### Configurer l'accès à distance

Cela inclut, sans s'y limiter :

- gestion des connexions physiques ;
- gestion des stratégies d'accès à distance ;
- mise en œuvre du NAT (traduction des adresses réseau) ;
- mise en œuvre du partage de la connexion Internet ;
- mise en œuvre du réseau privé virtuel (VPN) ;
- mise en œuvre du service de routage et d'accès à distance (RRAS) ;
- mise en œuvre du filtrage entrant et sortant ;
- configuration d'un serveur RADIUS (*Remote Authentication Dial-In User Service*) ;
- configuration d'un proxy RADIUS ;
- gestion des protocoles d'accès distant ;
- utilisation du gestionnaire de connexion.

#### Configurer la protection d'accès réseau (NAP)

Cela inclut, sans s'y limiter :

- protection de la couche réseau ;
- mise en œuvre de la conformité en utilisant DHCP ;
- mise en œuvre de la conformité en utilisant VPN ;
- configuration des stratégies NAP ;
- mise en œuvre de la conformité en utilisant IPSec ;
- mise en œuvre de la conformité en utilisant 802.1x ;
- mise en œuvre de l'isolement d'un hôte.

#### Configurer l'authentification réseau

Cela inclut, sans s'y limiter d'être capable de décrire :

- l'authentification sur réseau local en utilisant NTLMv2 et Kerberos ;

- l'authentification WLAN en utilisant 802.1x ;
- l'authentification RAS en utilisant MS-CHAP, MS-CHAPv2 et EAP.

### **Configurer l'accès sans fil**

Cela inclut, sans s'y limiter :

- comprendre et configurer Set Service Identifier (SSID) ;
- comprendre et configurer Wired Equivalent Privacy (WEP) ;
- comprendre et configurer Wi-Fi Protected Access (WPA) ;
- comprendre et configurer Wi-Fi Protected Access 2 (WPA2) ;
- comprendre et configurer mode infrastructure ou ad hoc ;
- comprendre et configurer stratégie de groupe pour les liaisons sans fil.

### **Configurer les paramètres du pare-feu**

Cela inclut, sans s'y limiter :

- mise en œuvre du filtrage pour le trafic entrant et sortant ;
- gestion des règles en utilisant des stratégies de groupe ;
- identification des ports et des protocoles ;
- gestion du pare-feu Microsoft Windows ou Pare-feu Windows avec sécurité renforcée ;
- stratégie d'isolement des ordinateurs.

### **Configuration des services et de l'adressage IP**

#### **Configurer IPSec**

Cela inclut, sans s'y limiter :

- mise en œuvre des stratégies IPSec ;
- mise en œuvre de l'authentification AH (*Authentication Header*) ;
- mise en œuvre du chiffrage ESP (*Encapsulating Security Payload*).

## **2. Pré-requis matériel**

Pour effectuer toutes les mises en pratique de ce chapitre, vous allez utiliser les machines virtuelles suivantes :



## **3. Objectifs**

Ce chapitre s'intéresse aux éléments avancés pour la configuration réseau comme la mise en œuvre du pare-feu que ce soit en utilisant l'interface standard ou l'interface avancée, y compris l'utilisation du protocole IP sécurisé IPSec largement répandu et qui permet le chiffrement et garantit l'authentification de l'émetteur et du destinataire.

L'accès par des ordinateurs sans fil est également étudié. L'outil routage et accès distant est présenté avec ses trois éléments principaux que sont la translation d'adresses (NAT), les réseaux privés virtuels (VPN) et l'utilisation du protocole Radius. La fin du chapitre présente la Protection de l'Accès Réseau (NAP).

# Validation des acquis : questions/réponses

## 1. Questions

### Questions sans difficulté

- 1** Quelle est la différence entre imprimante et périphérique d'impression ?
- 2** Quel est le nom du répertoire qui contient les pilotes sur le serveur d'impression ?
- 3** Qu'est-ce qu'une visionneuse XPS ?
- 4** Citez au moins deux avantages du format XPS par rapport au format GDI.
- 5** Que signifie lister dans l'annuaire ?
- 6** Citez trois permissions DACLs applicables aux imprimantes.
- 7** Quel est l'emplacement par défaut du dossier de spool sur un serveur d'impression ?
- 8** Entre une priorité de 20 et une priorité de 45, laquelle est la plus élevée ?
- 9** Citez au moins trois types de ports possibles pour utiliser une imprimante.
- 10** Quelle URL par défaut doit-on utiliser pour accéder à un serveur d'impression IPP ?
- 11** Citez au moins deux pages de séparation disponibles par défaut.
- 12** Quelle différence essentielle existe-t-il entre les commandes **prnjobs** et **prnqctl** ?
- 13** Votre collègue veut exporter un serveur d'impression en utilisant la commande suivante : `printbrm -S \\Nom_du_serveur -E -F Nom_du_fichier` sans succès, pourquoi ?

### Questions de difficulté moyenne

- 14** Vous n'arrivez pas à supprimer un document à l'aide de la commande **Annuler**, quelle solution envisagez-vous pour y parvenir ?
- 15** Sur l'unique imprimante de votre entreprise, de nombreux documents sont dans la file d'attente et un de vos utilisateurs doit impérativement partir dans les dix minutes qui suivent avec un document imprimé qui se trouve en queue de peloton, comment pouvez-vous l'aider ?
- 16** Dans votre entreprise, vous gérez les 22 imprimantes à l'aide de l'utilitaire Gestion de l'impression installé sur votre ordinateur Windows Vista. Régulièrement vous rencontrez des problèmes de connexion, quelle peut en être l'origine ?
- 17** Plusieurs utilisateurs doivent utiliser le même périphérique d'impression. Actuellement, les utilisateurs se plaignent de devoir tout le temps définir leurs paramètres d'impression, comment pouvez-vous les aider ?
- 18** Des utilisateurs se plaignent que leurs documents n'arrivent pas à s'imprimer. Vous constatez qu'effectivement tout se passe bien excepté qu'aucun document ne s'imprime, quelle pourrait en être la cause ?
- 19** Vous devez installer une imprimante pour laquelle il n'existe pas de pilotes pour Windows Server 2008, que faites-vous ?
- 20** Selon vous, quel serait le moyen le plus facile pour se connecter à une imprimante ?
- 21** Comment faites-vous pour ajouter des pilotes supplémentaires ?
- 22** Votre entreprise ne dispose que de trois imprimantes. Un département qui imprime de gros volumes durant la journée pour préparer le travail du lendemain pénalise tous les utilisateurs, quelle serait la solution la plus économique à mettre en œuvre ?
- 23** Un utilisateur doit pouvoir modifier les propriétés de l'imprimante, quelle autorisation lui accordez-vous ?
- 24** Un utilisateur doit pouvoir supprimer une impression, quelle autorisation lui accordez-vous ?
- 25** Vous publiez les imprimantes à l'aide des stratégies de groupe, néanmoins certains utilisateurs se plaignent qu'ils ne voient pas les imprimantes. Après investigation vous vous apercevez que ces utilisateurs fonctionnent sous Windows XP, que faites-vous ?
- 26** Votre collègue ne peut pas créer d'imprimantes sur un Server Core, que lui dites-vous ?

### Questions très difficiles à aborder dès que vous aurez effectués les TP

- 27** Vous tentez de vous connecter à une imprimante, vous avez bien cliqué sur **Ajouter une imprimante réseau**,

**sans fil ou Bluetooth** malheureusement sans succès. Bien que l'imprimante soit partagée et opérationnelle, elle n'apparaît pas, pouvez-vous expliquer pourquoi ?

- 28** Votre entreprise utilise un immeuble entier, un de vos collègues veut améliorer la vitesse d'impression et propose d'utiliser la notion de pool d'imprimantes, que lui répondez-vous ?

## 2. Résultats

Référez-vous aux pages suivantes pour contrôler vos réponses. Pour chacune de vos bonnes réponses, comptez un point.

Nombre de points /28

Pour ce chapitre, votre score minimum doit être de 21 sur 28.

Si vous n'atteignez pas cette valeur, nous vous conseillons de reprendre l'étude de ce chapitre avant de passer au suivant.

## 3. Réponses

### Questions sans difficulté

- 1** Quelle est la différence entre imprimante et périphérique d'impression ?

*Une imprimante fait référence à une file d'attente alors que le périphérique d'impression fait référence à l'imprimante physique.*

- 2** Quel est le nom du répertoire qui contient les pilotes sur le serveur d'impression ?

*%systemroot%\system32\spool\drivers*

- 3** Qu'est-ce qu'une visionneuse XPS ?

*Une visionneuse XPS est un utilitaire qui permet de lire des documents au format XPS.*

- 4** Citez au moins deux avantages du format XPS par rapport au format GDI.

*Les avantages sont une meilleure qualité, une meilleure gestion de la couleur, des fichiers d'impression plus petits et une gestion administrative des imprimantes plus aisée.*

- 5** Que signifie lister dans l'annuaire ?

*Lister dans l'annuaire signifie publier une imprimante dans l'Active Directory.*

- 6** Citez trois permissions DACLs applicables aux imprimantes.

*Vous pouvez citer Imprimer, Gestion des documents, Gestion d'imprimantes mais également Autorisations en lecture, Modifier les autorisations et Appropriation.*

- 7** Quel est l'emplacement par défaut du dossier de spool sur un serveur d'impression ?

*%systemroot%\system32\spool\printers*

- 8** Entre une priorité de 20 et une priorité de 45, laquelle est la plus élevée ?

*20, les priorités varient entre 1 et 99 où 99 est la valeur la plus prioritaire, donc la réponse est 45.*

- 9** Citez au moins trois types de ports possibles pour utiliser une imprimante.

*Vous pouvez citer le port parallèle, le port série, le port File, le port local port TCP/IP et des ports spécifiques installés par les fabricants d'imprimantes.*

- 10** Quelle URL par défaut doit-on utiliser pour accéder à un serveur d'impression IPP ?

*http://server/printers où server est le nom du serveur.*

- 11** Citez au moins deux pages de séparation disponibles par défaut.

*Vous pouvez citer pcl.sep, pscript.sep et sysprint.sep.*

- 12** Quelle différence essentielle existe-t-il entre les commandes **prnjobs** et **prnqctl** ?

*Prnjobs gère des tâches comme prnqctl mais ce dernier permet de gérer toutes les tâches d'une imprimante à l'aide d'une seule commande.*

- 13** Votre collègue veut exporter un serveur d'impression en utilisant la commande suivante : printbrm -S \\Nom\_du\_serveur -E -F Nom\_du\_fichier sans succès, pourquoi ?

*Le paramètre d'exportation est -B et pas -E.*

### Questions de difficulté moyenne

- 14** Vous n'arrivez pas à supprimer un document à l'aide de la commande **Annuler**, quelle solution envisagez-vous pour y parvenir ?

*Il faut saisir les commandes **net stop spooler** et **net start spooler** dans une console.*

- 15** Sur l'unique imprimante de votre entreprise, de nombreux documents sont dans la file d'attente et un de vos utilisateurs doit impérativement partir dans les dix minutes qui suivent avec un document imprimé qui se trouve en queue de peloton, comment pouvez-vous l'aider ?

*La solution la plus simple est de modifier la priorité du document de l'utilisateur en lui donnant une valeur élevée proche de 99.*

- 16** Dans votre entreprise, vous gérez les 22 imprimantes à l'aide de l'utilitaire Gestion de l'impression installé sur votre ordinateur Windows Vista. Régulièrement vous rencontrez des problèmes de connexion, quelle peut en être l'origine ?

*Windows Vista ne peut gérer plus de 10 connexions. Dans ce cas, il semble plus facile de gérer les imprimantes via un serveur 2008.*

- 17** Plusieurs utilisateurs doivent utiliser le même périphérique d'impression. Actuellement, les utilisateurs se plaignent de devoir tout le temps définir leurs paramètres d'impression, comment pouvez-vous les aider ?

*La solution la plus simple consiste à identifier des groupes d'utilisateurs pour leur créer des imprimantes spécifiques.*

- 18** Des utilisateurs se plaignent que leurs documents n'arrivent pas à s'imprimer. Vous constatez qu'effectivement tout se passe bien excepté qu'aucun document ne s'imprime, quelle pourrait en être la cause ?

*Une des causes possibles pourrait être qu'il n'y a pas assez d'espace disque disponible.*

- 19** Vous devez installer une imprimante pour laquelle il n'existe pas de pilotes pour Windows Server 2008, que faites-vous ?

*Il faut chercher un pilote compatible basé sur une imprimante similaire.*

- 20** Selon vous, quel serait le moyen le plus facile pour se connecter à une imprimante ?

*Utiliser un chemin UNC (\\\Serveur\imprimante).*

- 21** Comment faites-vous pour ajouter des pilotes supplémentaires ?

*Il existe plusieurs méthodes, la première consiste à utiliser Windows Update, la seconde à cliquer sur **Nouveau pilote** dans l'onglet **Avancé** dans les propriétés de l'imprimante.*

- 22** Votre entreprise ne dispose que de trois imprimantes. Un département qui imprime de gros volumes durant la journée pour préparer le travail du lendemain pénalise tous les utilisateurs, quelle serait la solution la plus économique à mettre en œuvre ?

*Bien que l'on puisse acheter une nouvelle imprimante, la solution la plus économique semble être de créer une nouvelle imprimante pour les travaux volumineux et de la rendre disponible la nuit.*

- 23** Un utilisateur doit pouvoir modifier les propriétés de l'imprimante, quelle autorisation lui accordez-vous ?

*Gestion d'imprimantes.*

- 24** Un utilisateur doit pouvoir supprimer une impression, quelle autorisation lui accordez-vous ?

*Il est préférable de lui accorder Gestion des documents et pas Gestion d'imprimantes afin de lui limiter les autres droits.*

- 25** Vous publiez les imprimantes à l'aide des stratégies de groupe, néanmoins certains utilisateurs se plaignent qu'ils ne voient pas les imprimantes. Après investigation vous vous apercevez que ces utilisateurs fonctionnent sous Windows XP, que faites-vous ?

*Dans ce cas, il faut utiliser la commande **PushPrinterConnections** en la publiant également via un script et une stratégie de groupe.*

- 26** Votre collègue ne peut pas créer d'imprimantes sur un Server Core, que lui dites-vous ?

*Il faut d'abord installer le rôle Services d'impression.*

### **Questions très difficiles à aborder dès que vous aurez effectué les TP**

- 27** Vous tentez de vous connecter à une imprimante, vous avez bien cliqué sur **Ajouter une imprimante réseau, sans fil ou Bluetooth** malheureusement sans succès. Bien que l'imprimante soit partagée et opérationnelle, elle n'apparaît pas, pouvez-vous expliquer pourquoi ?

*Il se peut que le service d'exploration d'ordinateurs soit arrêté, donc aucune imprimante ne peut être recherchée.*

- 28** Votre entreprise utilise un immeuble entier, un de vos collègues veut améliorer la vitesse d'impression et propose d'utiliser la notion de pool d'imprimantes, que lui répondez-vous ?

*Si les conditions suivantes sont respectées il n'y a pas de problèmes, à savoir : il faut utiliser le même pilote et les imprimantes doivent être placées dans le même endroit, car on ne sait jamais quelle imprimante reçoit la tâche d'impression.*

## Résumé du chapitre

Vous avez appris le vocabulaire pour comprendre et gérer efficacement l'impression.

Vous avez appris à ajouter une imprimante locale ou réseau et à configurer ses paramètres.

Vous savez configurer le serveur d'impression et gérer les documents.

Vous pouvez mettre en œuvre le rôle Gestion de l'impression.

Vous avez appris à installer l'Impression Internet, à gérer une imprimante par l'intermédiaire de la console Web, comment ajouter une imprimante Internet et gérer les impressions.

Vous avez appris à mettre en œuvre le service LPD.

## Travaux pratiques

Dans les travaux pratiques dans l'exercice 11, vous devrez effectuer les opérations suivantes :

- Ajouter le rôle Service d'impression y compris sur un Server Core.
- Ajouter des imprimantes.
- Migrer des serveurs d'impression.
- Publier les imprimantes dans l'Active Directory.
- Création d'imprimantes en fonction des utilisateurs.
- Mise en œuvre de l'impression Internet.

## **Meilleures pratiques**

- N'utiliser que des périphériques d'impression qui disposent de pilotes signés.
- Créer plusieurs imprimantes par périphérique d'impression.
- Donner des priorités aux imprimantes.
- Limiter les utilisateurs ayant la permission Gestion des documents.
- Installer et utiliser l'utilitaire Gestion de l'impression.
- Déployer les imprimantes à l'aide des stratégies de groupe.

# Utilitaires ligne de commande



Dans le répertoire Printing\_Admin\_Scripts\fr-FR dont le chemin est %systemroot%\system32\ se trouvent 7 scripts vbs permettant de gérer des imprimantes en utilisant la ligne de commande ou des scripts.

- Ces commandes ne sont pas disponibles sur un Server Core tant que le service d'impression n'est pas installé.
- Forcez l'utilisation du moteur **cscript** en précisant **cscript** avant le nom de la commande.

## 1. Prncnfg.vbs

Cette commande permet de configurer ou d'afficher des informations concernant une imprimante ; la syntaxe complète est la suivante :

Administrator : Invite de commandes

```
C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript prncnfg.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : prncnfg [-gtx?][ -s serveur ][ -p imprimante ][ -u nouveau_nom_imprimante ]
               [ -u nom_utilisateur ][ -w mot_passe ][ -r nom_port ][ -l emplacement ]
               [ -m commentaire ][ -h nom_partage ][ -f fichier_sép ][ -y type_données ]
               [ -st temps_démarrage ][ -ut jusque-heure ][ -i priorité_défaut ]
               [ -o priorité ][ <+|->shared ][ <+|->direct ][ <+|->hidden ]
               [ <+|->published ][ <+|->readonly ][ <+|->queued ][ <+|->enablebidirectional ]
               [ <+|->keepprintedjobs ][ <+|->workoffline ][ <+|->enabledevq ]
               [ <+|->docompletefirst ]

Arguments :
-f   - nom du fichier contenant les séparateurs
-g   - lit la configuration
-h   - nom du partage
-i   - priorité par défaut
-l   - chaîne d'emplacement
-m   - chaîne de commentaire
-o   - priorité
-p   - nom de l'imprimante
-r   - nom du port
-s   - nom du serveur
-st  - heure de début
-t   - définit la configuration
-u   - nom_utilisateur
-ut  - heure de fin
-w   - mot_passe
-x   - change le nom de l'imprimante
-y   - chaîne de type de données
-u   - nouveau_nom_imprimante
```

- Pour afficher les informations d'une imprimante :

```
cscript prncnfg -g -s nom_du_serveur -p Nom_de_l'imprimante
```

- Pour modifier le nom d'une imprimante :

```
cscript prncnfg -x -s nom_du_serveur -p Nom_de_l'imprimante
-z Nouveau_Nom_de_l'imprimante
```

## 2. Prndrvr.vbs

Cette commande permet d'ajouter, de supprimer ou de lister les pilotes d'impressions ; la syntaxe complète est la suivante :

```

C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript prndrvr.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : prndrvr [-adlx?] [-m modèle][-v version][-e environnement] [-s serveur]
                  [-u nom_utilisateur][-w mot_passe][-h chemin_accès] [-i fichier_inf]
Arguments :
-a   - ajoute le pilote spécifié
-d   - supprime le pilote spécifié
-e   - environnement "Windows (NT x86 : X64 : IA64)"
-h   - chemin d'accès au pilote
-i   - nom pleinement qualifié du fichier inf
-l   - liste tous les pilotes
-m   - nom du modèle de pilote
-n   - nom du serveur
-u   - nom_utilisateur
-v   - version
-w   - mot_passe
-x   - supprime les pilotes non utilisés
-?   - affiche l'utilisation de la commande

```

- Pour afficher la liste de tous les pilotes :

```
cscript prndrvr.vbs -l
```

- Pour supprimer tous les pilotes supplémentaires :

```
cscript prndrvr.vbs -x -s Nom_de_l'imprimante
```

### 3. Prnjobs.vbs

Cette commande permet de mettre en pause, de reprendre, d'annuler ou d'afficher les tâches dans la file d'attente d'impression ; la syntaxe complète est la suivante :

```

C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript prnjobs.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : prnjobs [-znlx?] [-s serveur][-p imprimante][-j ID_tâche] [-u nom_utilisateur][-w mot_passe]
Arguments :
-j   - identificateur de la tâche
-l   - liste toutes les tâches
-n   - réactive la tâche interrompue
-p   - nom de l'imprimante
-s   - nom du serveur
-u   - nom_utilisateur
-w   - mot_passe
-x   - annule la tâche
-u   - interrompt la tâche
-?   - affiche l'utilisation de la commande

```

Avec cette commande, vous agissez au niveau de la tâche.

- Pour mettre en pause une tâche d'un serveur d'impression :

```
cscript prnjobs.vbs -z -s Nom_du_serveur -p Nom_de_l'imprimante
-j Numéro_du_job
```

### 4. Prnmngr.vbs

Cette commande permet d'ajouter, de supprimer et d'afficher des imprimantes. Il est également possible de gérer l'imprimante par défaut. La syntaxe complète est la suivante :

```

C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript prnmngr.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : prnmngr [-adxgtl?][cl [-s serveur][-p imprimante]
                         [-m modèle_pilote][-r port][-u nom_utilisateur][-w mot_passe]
Arguments :
-a   - ajoute une imprimante locale
-ac  - ajoute une connexion imprimante
-d   - supprime l'imprimante
-g   - recherche l'imprimante par défaut
-l   - liste toutes les imprimantes
-m   - modèle du pilote
-p   - nom de l'imprimante
-r   - nom du port
-s   - nom du serveur
-t   - définit l'imprimante par défaut
-u   - nom_utilisateur
-w   - mot_passe
-x   - supprime toutes les imprimantes
-xc  - supprimer toutes les connexions à l'imprimante
-xo  - supprimer toutes les imprimantes locales
-?   - affiche l'utilisation de la commande

```

- Afficher toutes les imprimantes du serveur :

```
cscript prnmngr.vbs -l -s Nom_du_serveur
```

- Ajouter une imprimante réseau :

```
cscript prnmngr.vbs -ac -p \\Nom_du_serveur\Nom_de_l'imprimante
```

## 5. Prnport.vbs

Cette commande permet de créer, de supprimer et d'afficher des ports d'impression TCP/IP. La syntaxe complète est la suivante :

```

C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript prnport.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : prnport [-adlg?][ -r port][-s serveur][-u nom_utilisateur][-w mot_passe]
                  [-o raw|lpr] [-h adresse_hôtel] [-q file_attente][-n nombre]
                  [-me : -md ] [-i index_SNMP] [-y communauté] [-2e : -2d]
Arguments :
-a   - ajouter un port
-d   - supprime le port spécifié
-g   - lit la configuration d'un port TCP
-h   - adresse IP du périphérique
-i   - index SNMP, si SNMP est activé
-l   - liste tous les ports TCP
-n   - type SNMP. [el] activé, [d] désactivé
-n   - numéro de port, s'applique à tous les ports TCP RAW
-o   - type de port, raw ou lpr
-q   - nom de la file d'attente, s'applique uniquement aux ports TCP LPR
-r   - nom du port
-s   - nom du serveur
-t   - définir la configuration d'un port TCP
-u   - nom_utilisateur
-w   - mot_passe
-y   - nom de la communauté, si SNMP est activé
-2   - spoule double, s'applique à tous les ports TCP LPR [el] activé, [d] désactivé
-?   - affiche l'utilisation de la commande

```

- Afficher tous les ports TCP/IP locaux :

```
Cscript prnport.vbs -l
```

- Ajouter un port TCP/IP sur un serveur :

```
Cscript prnport.vbs -a -s Nom_du_serveur -r Nom_du_port -h
AdresseIP_du_périphérique -o type_de_port -n Numéro_du_port
```

## 6. Prnqctl.vbs

Cette commande permet d'imprimer une page de test, de mettre en pause, de reprendre et d'annuler des documents en agissant au niveau de l'imprimante. Cette commande est semblable à prnjobs.

```
C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript prnqctl.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : prnqctl [-z[nex?]] [-s serveur][-p imprimante][-u nom_utilisateur][-w mot_passe]

Arguments :
-e   - imprime une page de test
-n   - réactive l'imprimante
-p   - nom de l'imprimante
-s   - nom du serveur
-u   - nom_utilisateur
-w   - mot_passe
-x   - annule toutes les tâches sur l'imprimante
-z   - met l'imprimante en pause
-?   - affiche l'utilisation de la commande
```

- Annuler toutes les tâches d'une imprimante :

```
cscript prnqctl.vbs -x -p Nom_de_l'imprimante
```

- Imprimer une page de test :

```
cscript prnqctl.vbs -e -p Nom_de_l'imprimante
```

## 7. Pubprn.vbs

Cet utilitaire en ligne de commande permet de publier une imprimante dans l'Active Directory ; la syntaxe complète est la suivante :

```
C:\Windows\System32\Printing_Admin_Scripts\fr-FR>cscript pubprn.vbs
Microsoft (R) Windows Script Host Version 5.7
Copyright (C) Microsoft Corporation 1996-2001. Tous droits réservés.

Utilisation : [cscript] pubprn.vbs Serveur "LDAP://OU=...,DC=...,"

    Serveur est un nom de serveur Windows (par exemple : Serveur\Imp) ou nom UNC de l'imprimante (\\\Serveur\Imp\Imprimante)
    "LDAP://CN=...,DC=..." est le chemin d'accès du service d'annuaire du conteneur destination

Exemple 1 : pubprn.vbs MonServeur "LDAP://CN=MonConteneur,DC=MonDomaine,DC=Societe,DC=Com"
Exemple 2 : pubprn.vbs \\MonServeur\Imprimante1 "LDAP://CN=MonConteneur,DC=MonDomaine,DC=Societe,DC=Com"
```

## 8. Printbrm.exe

L'utilitaire en ligne de commande printbrm.exe permet d'effectuer l'importation et l'exportation d'imprimantes ; la syntaxe complète est la suivante :

```
C:\>"C:\Windows\System32\spool\tools\PrintBrm.exe" /?
Erreur : un seul mode doit être sélectionné !

Accédez à l'outil de migration de la sauvegarde et de la récupération via une interface
de ligne de commande.

PrintBrm -B|R|Q -[S <serveur>] -F <fichier> [-O FORCE] [-P ALL|ORIG] [-NOBIN] [-LPR2TCP]
[-C <fichier de configuration>] [-?]

-B           Sauvegarder le serveur dans le fichier spécifié
-R           Restaurer le fichier de configuration dans le fichier sur le serveur
-Q           Interroger le serveur ou le fichier de sauvegarde
-S <nom de serveur> Serveur cible
-F <nom de fichier> Fichier de sauvegarde cible
-O FORCE     Forcer le remplacement des objets existants
-P ALL|ORIG   Publier toutes les imprimantes dans le répertoire ou publier les imprim
antes publiées initialement
-NOBIN      Omettre les fichiers binaires de la sauvegarde
-LPR2TCP    Convertir les ports LPR en ports TCP/IP standard lors de la restauratio
n
-C <nom de fichier> Utiliser le fichier de configuration spécifié pour BRM
-?          Afficher cette aide

C:\>
```

- Pour exporter un serveur d'impression :

```
printbrm -S \\<NomDuServeur> -B -F<NomDuFichier>
```

- Pour importer un serveur d'impression :

```
printbrm -S //<NomDuServeur> -R -F<NomDuFichier>
```

## Rôle Services d'impression sur un Server Core

Sur un Server Core, il n'est pas possible d'installer une imprimante tant que le rôle n'est pas installé. Dès son installation, le répertoire Printing\_Admin\_Scripts et les scripts vbs correspondants ont été ajoutés.

### Installation du rôle Services d'impression

- Dans l'invite de commande, saisissez `start /w ocsetup Printing-ServerCore-Role` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que le serveur d'impression est bien installé puis appuyez sur [Entrée].

### Désinstallation du rôle Services d'impression

- Dans l'invite de commande, saisissez `start /w ocsetup Printing-ServerCore-Role /uninstall` puis appuyez sur [Entrée].
- Saisissez ensuite `oclist` pour contrôler que le serveur d'impression est bien désinstallé puis appuyez sur [Entrée].

### Gestion du rôle Services d'impression

La gestion du rôle des services d'impression se fait à l'aide de la console Gestion d'impression à distance.



Il est possible de gérer le rôle Services d'impression sur un Server Core à partir d'un serveur Windows Server 2008, d'une station de travail Windows Vista ou par l'intermédiaire de scripts.

# Services LPD

## Installation du service de rôle Services LPD

Si le service d'impression Internet n'est pas encore installé, référez-vous à l'installation du rôle Services d'impression montré dans une section précédente.

Si ce service est installé, mais que les services LPD ne sont pas encore installés, procédez de la manière suivante :

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur le nœud **Rôles** pour développer l'arborescence.
- Cliquez sur **Services d'impression**.
- Dans la fenêtre principale **Services d'impression**, cliquez sur l'action **Ajouter des services de rôle**.
- Sur la page **Services de rôle**, sélectionnez **Services LPD** puis cliquez sur **Suivant**.
- Sur la page **Confirmation**, contrôlez vos informations puis cliquez sur **Installer**.
- Contrôlez le résultat de l'installation sur la page **Résultats** puis cliquez sur **Fermer**.

Le service Serveur d'impression TCP/IP est installé (LPDSVC).

Ce service ne se configure pas, il nagit que comme proxy entre les impressions LPR et l'impression Windows.

Sous Windows 2008, il est possible d'imprimer sur une imprimante LPR si la fonctionnalité moniteur de port LPR est installée.



Une règle ouvrant le port 515 est automatiquement créée pour le trafic entrant, appelée Serveur d'impression TCP/IP.

---

# Impression Internet IPP

L'impression Internet IPP est surtout utilisée par les administrateurs pour gérer les files d'attente d'une imprimante, ou un document sur un serveur d'impression, en utilisant le protocole HTTP/HTTPS au lieu du protocole RPC.

L'impression Internet peut également être utilisée pour ajouter une imprimante réseau en indiquant une URL plutôt qu'un chemin UNC.

Pour l'utilisateur, l'impression Internet peut être utilisée pour se connecter à une imprimante via Internet en utilisant un navigateur Web, ce qui installe automatiquement si nécessaire le pilote correspondant et ajoute une imprimante dont le protocole d'accès est HTTP/HTTPS.

Le protocole RPC est le premier choix pour imprimer à distance.

Si des restrictions empêchent son utilisation, par défaut il n'est pas possible d'imprimer jusqu'à ce que le client d'Impression Internet soit installé (Windows Vista et Windows 2008) pour utiliser le protocole HTTP/HTTPS à la place de RPC.

## 1. Installation du service de rôle Impression Internet



Impression Internet est un service de rôle qui dépend du serveur d'impression et du serveur Web IIS.

Si le service d'impression Internet n'est pas encore installé, référez-vous à l'installation du rôle Services d'impression montré dans la section précédente.

Si ce service est installé, mais que l'Impression Internet n'est pas encore installée, procédez ainsi :

- Connectez-vous en tant qu'administrateur sur le serveur d'impression.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur le nœud **Rôles** pour développer l'arborescence.
- Cliquez sur **Services d'impression**.
- Dans la fenêtre principale **Services d'impression**, cliquez sur l'action **Ajouter des services de rôle**.
- Sur la page **Services de rôle**, sélectionnez **Impression Internet** puis cliquez sur **Suivant**.
- Si la boîte de dialogue **Ajouter des services de rôle** apparaît, cliquez sur **Ajouter les services de rôle**.
- Sur la page **Serveur Web (IIS)**, cliquez sur **Suivant**.
- Sur la page **Services de rôle**, cliquez sur **Suivant**.
- Sur la page **Confirmation**, contrôlez vos informations puis cliquez sur **Installer**.
- Contrôlez le résultat de l'installation sur la page **Résultats** puis cliquez sur **Fermer**.

---

► Le répertoire virtuel **Printers** est ajouté au site par défaut du serveur Web. Sur le disque, il se trouve dans **%systemroot%\web\printers**. L'application **Impression Internet** utilise des pages **ASP**.

---

► Il peut s'avérer nécessaire de modifier sur le serveur Web la méthode d'authentification du répertoire virtuel.

---



Ajoutez un certificat SSL pour améliorer la sécurité en utilisant le protocole HTTPS et pas HTTP.

## 2. Connexion et installation d'une imprimante



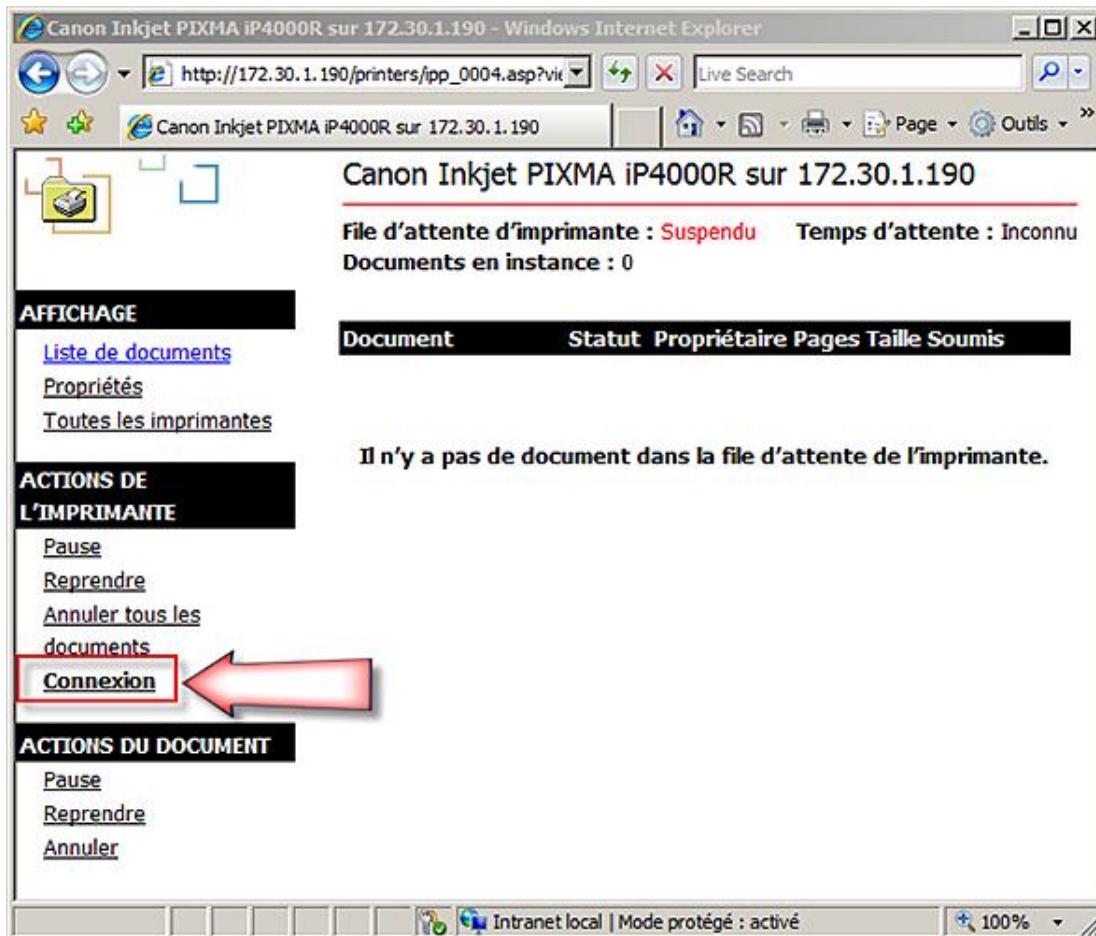
- Connectez-vous en tant qu'utilisateur sur une station de travail.
- Ouvrez Internet Explorer et saisissez l'URL suivante `http://NomServerIPP/printers`

L'utilisateur peut voir toutes les imprimantes du serveur d'impression sur lesquelles il a des droits.

- Cliquez sur le nom d'une des imprimantes affichées. Si c'est la première fois que vous vous connectez à cette imprimante, le volet de gauche affiche la commande **Connexion**.



Pour utiliser cette commande, il faut être membre du groupe **Administrateurs** ou **Utilisateurs avec pouvoir de l'ordinateur local**.



- Dans la boîte de dialogue **Ajouter une connexion d'imprimante Web**, cliquez sur **Oui** pour ajouter une connexion d'imprimante.

**►** Pour des clients Windows Vista et Windows Server 2008, les options de sécurité d'Internet Explorer, voire des stratégies de groupe, peuvent empêcher le téléchargement et l'installation du pilote. Une erreur de type **Le nom de l'imprimante est invalide** peut apparaître. Dans ce cas, il faut soit modifier les paramètres bloquants, soit installer l'imprimante par un autre moyen.

S'il n'est pas déjà installé, alors le pilote est installé et l'imprimante est ajoutée sur l'ordinateur local.

**►** Si l'impression Internet a été ajoutée au serveur d'impression, il est possible d'utiliser l'URL suivante pour ajouter une imprimante : **http://serveur/printers/NomImprimantePartagée/.printer**

L'imprimante Internet a été ajoutée comme on peut le voir dans la figure suivante :



Vous pouvez modifier les propriétés de l'imprimante. Vous pouvez configurer le port et modifier les options de sécurité

pour permettre une authentification différente. Il n'est pas possible de partager une imprimante Internet.

- Une imprimante réseau ne peut pas passer les pare-feu, excepté si un VPN est utilisé. Avec une imprimante Internet, les pare-feu ne sont pas un obstacle.

### 3. Gestion à l'aide de l'impression Internet



- Connectez-vous en tant qu'administrateur sur une station de travail.
- Ouvrez Internet Explorer et saisissez l'URL suivante : <http://NomServerIPP/printers>. La page s'ouvre et affiche toutes les imprimantes du serveur d'impression.
- Cliquez sur le lien correspondant au nom d'une imprimante.

The screenshot shows the printer management interface for a Canon Inkjet PIXMA iP4000R. At the top, it displays the printer's name and IP address: "Canon Inkjet PIXMA iP4000R sur 172.30.1.190". Below this, status information is shown: "File d'attente d'imprimante : Suspendu" (Print queue status: Suspended), "Temps d'attente : Inconnu" (Waiting time: Unknown), and "Documents en instance : 10 Taille moyenne : 1 pages" (Current documents: 10 Average size: 1 pages). The main area is a table listing the documents in the print queue:

Document	Statut	Propriétaire	Pages	Taille	Soumis
○ Sans titre - Bloc-notes	Administrateur 1		10.0 Ko	00:59:10	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		10.0 Ko	00:59:16	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		10.0 Ko	00:59:18	11.04.2008
○ Sans titre - Bloc-notes	testuser	1	996 octets	01:05:20	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		13.5 Ko	01:06:24	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		13.5 Ko	01:10:30	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		13.5 Ko	01:11:56	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		13.5 Ko	01:13:30	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		13.5 Ko	01:14:06	11.04.2008
○ Sans titre - Bloc-notes	Administrateur 1		10.6 Ko	01:34:40	11.04.2008

The left sidebar contains several sections: "AFFICHAGE" with links to "Liste de documents", "Propriétés", and "Toutes les imprimantes"; "ACTIONS DE L'IMPRIMANTE" with links to "Pause", "Reprendre", "Annuler tous les documents", and "Connexion"; and "ACTIONS DU DOCUMENT" with links to "Pause", "Reprendre", and "Annuler".

Le volet de gauche est séparé en plusieurs sections :

- **Affichage**

- **Liste de documents** affiche les documents en attente d'impression de la file d'attente de l'imprimante sélectionnée.

- **Propriétés** affiche les propriétés de l'imprimante.

- **Toutes les imprimantes** affiche toutes les imprimantes du serveur d'impression.

- **Actions de l'imprimante** agit sur l'imprimante sélectionnée.

- **Pause** met en pause l'impression au niveau de l'imprimante.

- **Reprendre** reprend l'impression au niveau de l'imprimante.

- **Annuler tous les documents** supprime de la file d'attente tous les documents de l'imprimante.

- **Connexion** ajoute une imprimante Internet à l'ordinateur local.
- **Actions du document** agit sur les documents sélectionnés.
  - **Pause** met en pause l'impression des documents sélectionnés.
  - **Reprendre** reprend l'impression des documents sélectionnés.
  - **Annuler** supprime de la file d'attente des documents sélectionnés.

# Rôle Services d'impression

Le rôle de serveur d'impression installe un utilitaire de gestion centralisée des imprimantes de l'entreprise. Apparu avec Windows Server 2003 R2, il est parfaitement bien conçu et se positionne au-dessus du gestionnaire d'impression local pour les ordinateurs fonctionnant sous Windows 2000, Windows XP, Windows Server 2003 et Windows Server 2008.

Vous devez être membre du groupe **Administrateurs** local du serveur ou membre des **Administrateurs de domaine**.

Cet utilitaire est automatiquement installé sur des ordinateurs exécutant Windows Vista et permet de gérer jusqu'à 10 ordinateurs.

## 1. Ajout du rôle Services d'impression



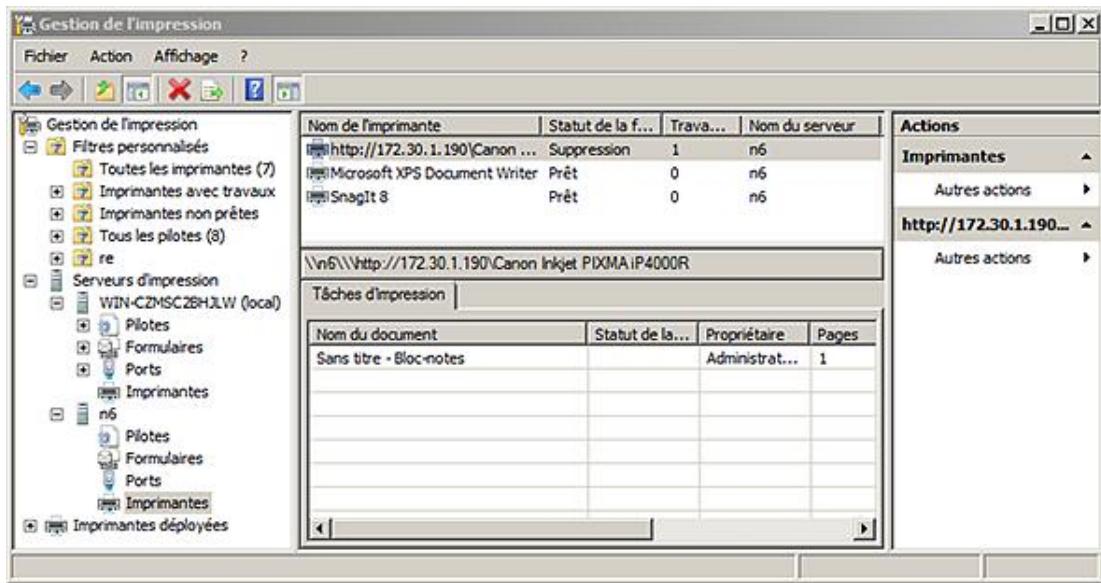
- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestionnaire de serveur**.
- Dans le volet de gauche, cliquez sur **Rôles**.
- Sur la page principale **Rôles**, cliquez sur **Ajouter des rôles**.
- Si la page **Avant de commencer** apparaît, cliquez sur **Suivant**.
- Sur la page **Rôles de serveur**, sélectionnez **Services d'impression** puis cliquez sur **Suivant**.
- Sur la page **Services d'impression**, lisez éventuellement les informations supplémentaires puis cliquez sur **Suivant**.
- Sur la page **Services de rôle**, le service **Serveur d'impression** est déjà sélectionné mais vous pouvez ajouter les services facultatifs **Services LPD** et **Impression Internet** examinés plus loin. Ensuite, cliquez sur **Suivant**.
- Sur la page **Confirmation**, contrôlez les informations puis cliquez sur **Installer**.
- Contrôlez le résultat de l'installation sur la page **Résultats** puis cliquez sur **Fermer**.

## 2. Gestion à l'aide du rôle Services d'impression



Il s'agit de démarrer une console MMC appelée **Printmanagement.msc**.

- Connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis **Gestion de l'impression**.



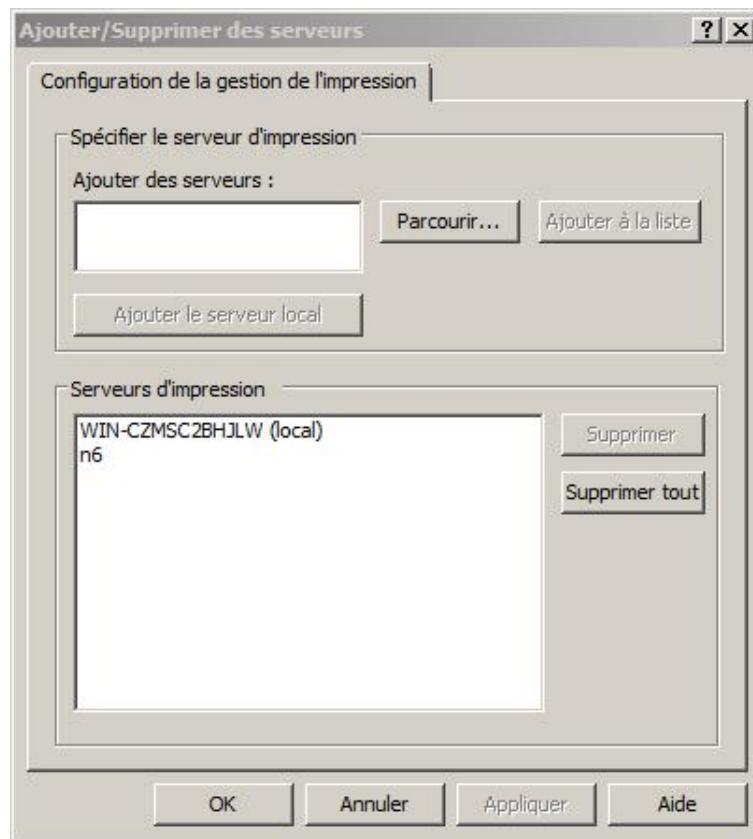
Le volet de gauche permet de se déplacer sur quatre niveaux, à savoir :

- Le gestionnaire d'impression.
- Le serveur d'impression.
- L'imprimante.
- Les imprimantes déployées.

Au niveau de la gestion de l'impression, les actions possibles sont :

- Ajouter/supprimer des serveurs.
- Migrer les imprimantes.
- Ajouter/supprimer des filtres.

#### a. Ajouter/supprimer des serveurs



Il est possible d'ajouter et de supprimer des serveurs pour les gérer à distance avec l'action **Ajouter/supprimer des serveurs** (pour que cette action soit disponible, sélectionnez **Gestion de l'impression** dans le volet de gauche). Vous pouvez les ajouter en saisissant le nom de l'ordinateur ou les rechercher à l'aide de la découverte réseau, si cette fonctionnalité est activée, via le bouton **Parcourir**. Pour ajouter l'ordinateur local, cliquez sur **Ajouter le serveur local**.

Pour supprimer un serveur, sélectionnez-le dans la boîte de dialogue puis cliquez sur **Supprimer**, sinon utilisez le bouton **Supprimer tout** pour supprimer tous les serveurs d'impression de la liste.

- Sur le serveur d'impression distant, il faut s'assurer que les règles entrantes suivantes du pare-feu sont activées : **Partage de fichiers et d'imprimantes (SMB-Entrée)** et **Partage de fichiers et d'imprimantes (service Spouleur - RPC)**.

## b. Migrer les imprimantes

La migration des imprimantes permet de déplacer des imprimantes et leurs pilotes d'un serveur d'impression à un autre en utilisant des fichiers.

L'assistant permet d'importer ou d'exporter des imprimantes.

### Exportation d'imprimantes

- Dans la console **Gestion de l'impression**, cliquez avec le bouton droit de la souris sur **Gestion de l'impression** dans le volet de gauche puis cliquez sur **Migrer les imprimantes**.
- Sur la page **Mise en route de la migration d'imprimante**, choisissez l'option d'exportation des files d'attentes d'impression, puis cliquez sur **Suivant**.
- Sur la page **Sélectionner le serveur d'impression**, sélectionnez le serveur actuel ou un autre serveur d'impression, puis cliquez sur **Suivant**.
- Sur la page **Vérifiez la liste des éléments à exporter**, vérifiez les imprimantes et les options qui seront exportées, puis cliquez sur **Suivant**. Notez que la granularité est toutes les imprimantes et objets du serveur d'impression.

- Sur la page **Sélectionner l'emplacement du fichier**, saisissez ou recherchez un chemin complet avec un nom de fichier d'exportation disposant d'une extension **printerExport**, puis cliquez sur **Suivant**.
- L'exportation peut durer plusieurs minutes avant que la page **Exportation** n'apparaisse. Ensuite, cliquez sur **Ouvrir l'observateur d'événements** pour vérifier que l'exportation s'est déroulée correctement, puis cliquez sur **Terminer**. La taille du fichier généré peut prendre plusieurs centaines de mégaoctets.



L'exportation d'imprimantes ne supprime pas les imprimantes du serveur d'exportation.

### **Importation d'imprimantes**

- Dans la console **Gestion de l'impression**, cliquez avec le bouton droit de la souris sur **Gestion de l'impression** dans le volet de gauche, puis cliquez sur **Migrer les imprimantes**.
- Sur la page **Mise en route de la migration d'imprimante**, choisissez l'option d'importation des files d'attente d'impression, puis cliquez sur **Suivant**.
- Sur la page **Sélectionner l'emplacement du fichier**, sélectionnez le fichier contenant les imprimantes à importer, puis cliquez sur **Suivant**.
- Sur la page **Vérifiez la liste des éléments à importer**, contrôlez les imprimantes et autres objets qui seront importés puis cliquez sur **Suivant**.
- Sur la page **Sélectionner le serveur d'impression**, sélectionnez le serveur actuel ou un autre serveur d'impression puis cliquez sur **Suivant**.
- Sur la page **Sélectionner les options d'importation**, dans la liste déroulante **Mode d'importation** vous pouvez choisir soit de remplacer les imprimantes existantes, soit de créer des copies si l'imprimante est déjà installée. La liste déroulante **Liste dans l'annuaire** permet de publier toutes les imprimantes, aucune ou seulement celles qui ne sont pas déjà publiées. Enfin il est possible de **Convertir les ports LPR en moniteurs de port standard** avant de cliquer sur **Suivant**.
- L'importation peut durer plusieurs minutes avant que la page **Importation** n'apparaisse. Ensuite, cliquez sur **Ouvrir l'observateur d'événements** pour vérifier que l'importation s'est déroulée correctement puis cliquez sur **Terminer**.

### **c. Les filtres**

Les filtres permettent d'afficher simplement des informations sur les imprimantes comme le statut, l'emplacement, le nom du partage, etc.

D'autre part, vous pouvez créer des filtres pour signaler le passage à un état spécifique dès que les conditions d'un filtre sont satisfaites, puis notifier le nouvel état par e-mail ou démarrer un script.

Des filtres prédéfinis permettent de visualiser :

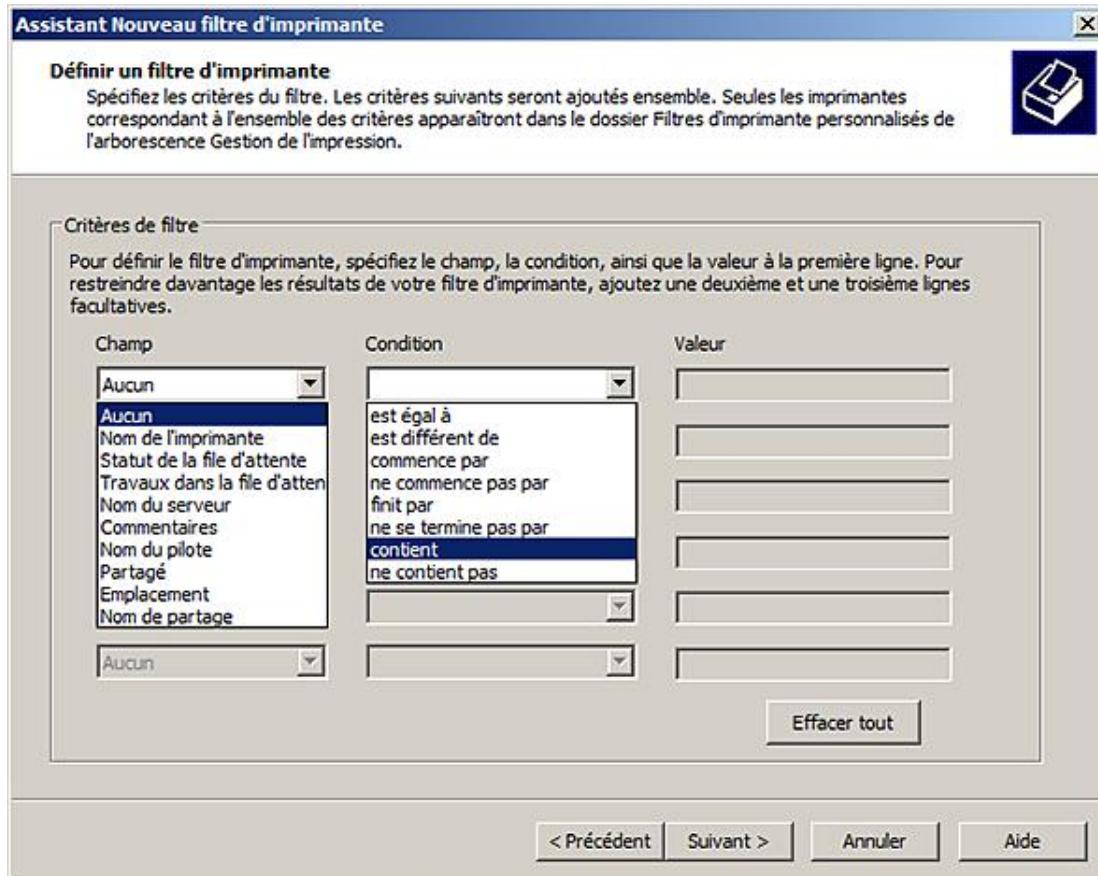
- **Toutes les imprimantes** : affiche toutes les imprimantes visibles depuis la console Gestion de l'impression.
- **Imprimantes avec travaux** : affiche toutes les imprimantes ayant au moins un travail en cours.
- **Imprimantes non prêtées** : affiche toutes les imprimantes dont le statut est différent de Prêt.
- **Tous les pilotes** : affiche tous les pilotes visibles depuis l'utilitaire Gestion de l'impression.



Il n'est pas possible de supprimer un filtre prédéfini.

### **Création d'un nouveau filtre**

- Dans la console **Gestion de l'impression**, cliquez avec le bouton droit de la souris sur **Filtres personnalisés** dans le volet de gauche puis cliquez sur **Ajouter un nouveau filtre d'imprimante**.
  - Sur la page **Nom et description du filtre d'imprimante** de l'Assistant Nouveau filtre d'imprimante, saisissez un nom pour le filtre qui soit explicite, éventuellement une description, et cochez la case **Afficher le nombre total d'imprimantes à côté du nom du filtre d'imprimante** si nécessaire avant de cliquer sur **Suivant**.
  - Sur la page **Définir un filtre d'imprimante**, indiquez un critère par ligne basé sur la notion de **Champ Condition Valeur**. L'opérateur logique **ET** est utilisé entre les critères. À la fin, cliquez sur **Suivant**.



- Sur la page **Définir des notifications (facultatif)**, vous pouvez choisir d'**Envoyer une notification par courrier électronique** en tapant l'adresse e-mail de l'expéditeur et du destinataire, le nom du serveur SMTP, et le message. Le bouton **Tester** permet de tester l'envoi du message. Vous pouvez également choisir d'**Exécuter le script** désigné par son chemin d'accès, ce script pouvant comprendre des arguments. Cela peut être utile dans le cas où l'imprimante se met en erreur, le script pouvant redémarrer le spouleur. Le bouton **Tester** permet d'exécuter le script. Ensuite, cliquez sur **Terminer**.

<input checked="" type="checkbox"/> Envoyer une notification par courrier électronique	
Adresse de messagerie des	printerAdmin@pffc.ch
Adresse de messagerie de l'expéditeur :	user@pffc.ch
Serveur SMTP :	mail.pffc.ch
Message :	Le spouleur a été redémarré sur le Serveur Ad3
<input type="button" value="Tester"/>	
<input checked="" type="checkbox"/> Exécuter le script	
Chemin d'accès :	c:\scripts\spool.vbs
Arguments supplémentaires :	
<input type="button" value="Tester"/>	

#### d. Gestion au niveau Serveurs d'impression

À ce niveau, il n'est possible que d'ajouter ou de supprimer un serveur d'impression comme montré dans les sections précédentes.

#### e. Gestion au niveau du serveur d'impression

Les actions possibles sont :

- **Ajouter une imprimante** à l'aide d'un assistant semblable à l'assistant d'ajout d'une imprimante sur le serveur.
- **Exporter les imprimantes vers un fichier**, qui permet d'exporter les imprimantes via l'assistant de migration.
- **Importer les imprimantes depuis un fichier**, qui permet d'importer les imprimantes via l'assistant de migration.
- **Définir des notifications** pour envoyer des messages électroniques.
- **Visualiser les propriétés** du serveur d'impression.

---

 Les actions sont identiques à une gestion locale du serveur.

---

Les quatre éléments d'un serveur d'impression permettent d'accéder rapidement aux onglets suivants :

- Pilotes
- Formulaires
- Ports
- Imprimantes

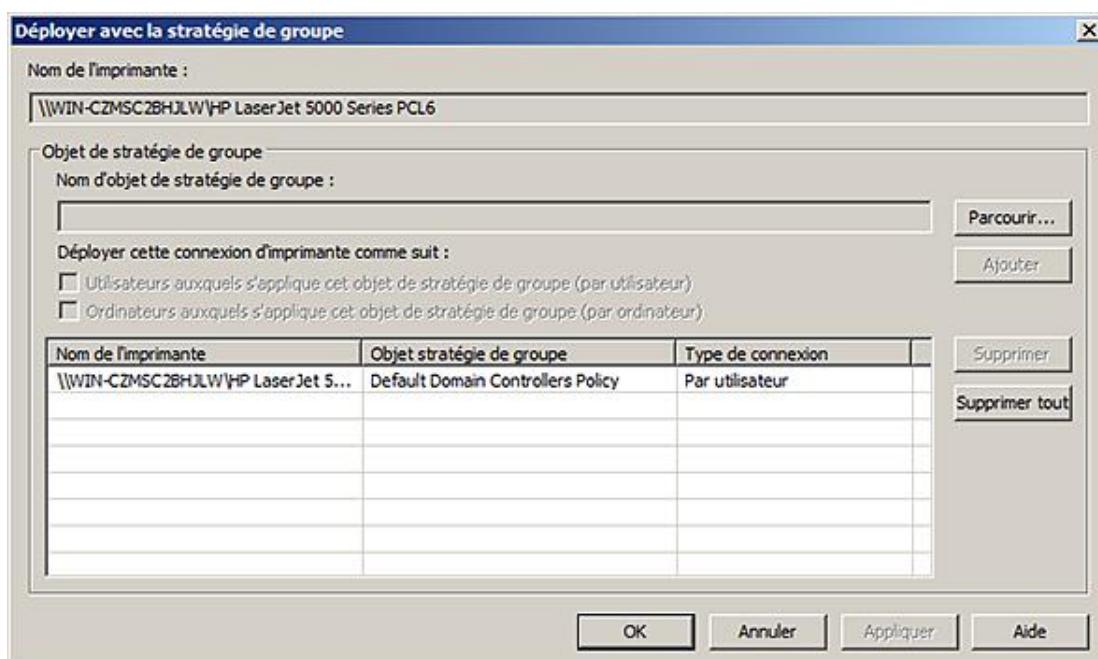
Au niveau **Imprimantes**, il est possible :

- d'**Ajouter une imprimante**,
  - d'afficher la file d'attente de l'imprimante dans la fenêtre principale : **Affichage étendu**.

#### **f. Gestion au niveau de l'imprimante**

Le niveau suivant est l'imprimante, les actions possibles sont :

- **Ouvrir la file d'attente de l'imprimante** : affiche la file d'attente dans une autre fenêtre.
  - **Répertorier dans l'annuaire** : publie l'imprimante dans l'Active Directory.
  - **Déployer avec la stratégie de groupe** : déploie automatiquement des connexions. Pour des ordinateurs antérieurs à Windows Vista, il faut utiliser l'utilitaire **PushPrinterConnections.exe**.



La procédure est la suivante :

- Cliquez sur **Parcourir** pour sélectionner une stratégie de groupe.
  - Indiquez si cette imprimante doit être déployée par utilisateur et/ou par ordinateur.
  - Si l'imprimante doit également être déployée pour d'autres stratégies de groupe, répétez l'opération, puis à la fin cliquez sur **OK**.

C'est la méthode recommandée pour installer des imprimantes. Son autre avantage est de pouvoir déployer ou mettre à jour des pilotes sans que l'utilisateur soit membre du groupe Administrateurs local.

 Dans un environnement d'entreprise, n'oubliez pas d'ajouter l'utilitaire PushPrinterConnections dans le script de GPO pour l'installer sur l'ordinateur client.

#### **g. Gestion des imprimantes déployées**

Après avoir déployé une imprimante avec une stratégie de groupe, il est possible de la gérer ici. En fait, il s'agit d'un filtre qui affiche toutes les imprimantes déployées avec la stratégie de groupe.

La seule opération possible est la modification de la stratégie définie.

# Gestion d'une imprimante

Les procédures pour ajouter et gérer une imprimante locale n'ont pas changé, seule l'interface a été un peu modifiée depuis Windows 2000.

## 1. Ajout d'une imprimante locale



Pour ajouter une imprimante locale, procédez comme suit :

- Connectez-vous en tant qu'administrateur sur l'ordinateur qui dispose d'un périphérique d'impression local.
- Cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage du panneau de configuration n'est pas classique, cliquez sur **Imprimantes** dans le groupe **Matériel et audio**, sinon cliquez directement sur **Imprimantes**.
- Dans la fenêtre **Imprimantes**, cliquez sur **Ajouter une imprimante**.
- Dans l'assistant **Ajouter une imprimante**, cliquez sur **Ajouter une imprimante locale**.
- Sur la page **Choisir un port d'imprimante**, sélectionnez **LPT1 : (Port imprimante)**, les autres choix vous permettent de choisir soit un port existant :
  - Un port parallèle **LPT**, trois ports parallèles sont définis par défaut.
  - Un port série **COM**, trois ports série sont définis par défaut.
  - Un port **File** pour imprimer dans un fichier.
  - Un port local pour le format **XPS**.

Soit un nouveau port :

- Un **port local** (mappage sur une connexion distante \\serveur\imprimante).
- Un **port TCP/IP**, décrit dans la prochaine section.

Puis cliquez sur **Suivant**.

---

► Certaines imprimantes installent un port spécifique, dans ce cas, installez au préalable le port spécifique de l'imprimante avant d'exécuter cet assistant.

---

- Sur la page **Installer le pilote d'imprimante**, sélectionnez d'abord Canon comme **Fabricant** puis Inkjet PIXMA IP3000 comme **Imprimante**, enfin cliquez sur **Suivant**.

Le bouton **Windows Update** réactualise la liste des imprimantes et des pilotes disponibles en téléchargeant la liste des imprimantes supplémentaires ne se trouvant pas dans la liste locale. Les deux listes ne fusionnent pas.

Le bouton **Disque fourni** vous permet de spécifier l'emplacement des pilotes de votre imprimante.

---

➤ Si aucun pilote ne semble exister, que ce soit dans la liste Windows Update ou sur le site Web du fabricant, essayez de trouver un pilote compatible avec une imprimante similaire.

---

➤ Un pilote signé numériquement offre une meilleure garantie contre les problèmes d'incompatibilité avec Windows. D'autre part, il offre la garantie que le pilote n'a pas été altéré depuis qu'il a reçu sa signature.

---

- Sur la page **Entrer un nom d'imprimante**, saisissez **MyPrinter** pour le nom explicite afin de reconnaître l'imprimante et activez la case à cocher **Définir en tant qu'imprimante par défaut** si elle doit être l'imprimante par défaut, puis cliquez sur **Suivant**.
- Sur la page **Partage d'imprimante**, le partage ainsi qu'un nom de partage vous sont proposés. Vous pouvez modifier le nom, indiquer un emplacement et placer un commentaire avant de cliquer sur **Suivant**.

➤ Si vous avez défini des sites dans l'Active Directory, il est possible d'associer l'emplacement au site Active Directory en fonction de l'adresse IP, ce qui facilite la gestion des emplacements.

---

- Sur la page **Vous avez ajouté**, vous pouvez imprimer une page de test pour contrôler si l'imprimante est bien installée. Cliquez ensuite sur **Terminer**.

➤ Les imprimantes USB s'installent automatiquement.

---

## 2. Création d'un port TCP/IP



- Cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage du panneau de configuration n'est pas classique, cliquez sur **Imprimantes** dans le groupe **Matériel et audio** sinon cliquez directement sur **Imprimantes**.
- Dans la fenêtre **Imprimantes**, cliquez sur **Ajouter une imprimante**.
- Dans l'assistant **Ajouter une imprimante**, cliquez sur **Ajouter une imprimante locale**.
- Sur la page **Choisir un port d'imprimante**, sélectionnez **Créer un nouveau port** puis le type de port **Standard TCP/IP Port**. Ensuite, cliquez sur **Suivant**.
- Sur la page **Entrer un nom d'hôte ou une adresse IP d'imprimante**, indiquez les paramètres permettant d'identifier l'imprimante comme affiché sur l'image ci-dessous puis cliquez sur **Suivant**.

**Entrer un nom d'hôte ou une adresse IP d'imprimante**

Type de périphérique :	Détection automatique
Nom d'hôte ou adresse IP :	172.30.1.252
Nom du port :	172.30.1.252
<input checked="" type="checkbox"/> Interroger l'imprimante et sélectionner automatiquement le pilote à utiliser	

**Type de périphérique** : vous pouvez choisir :

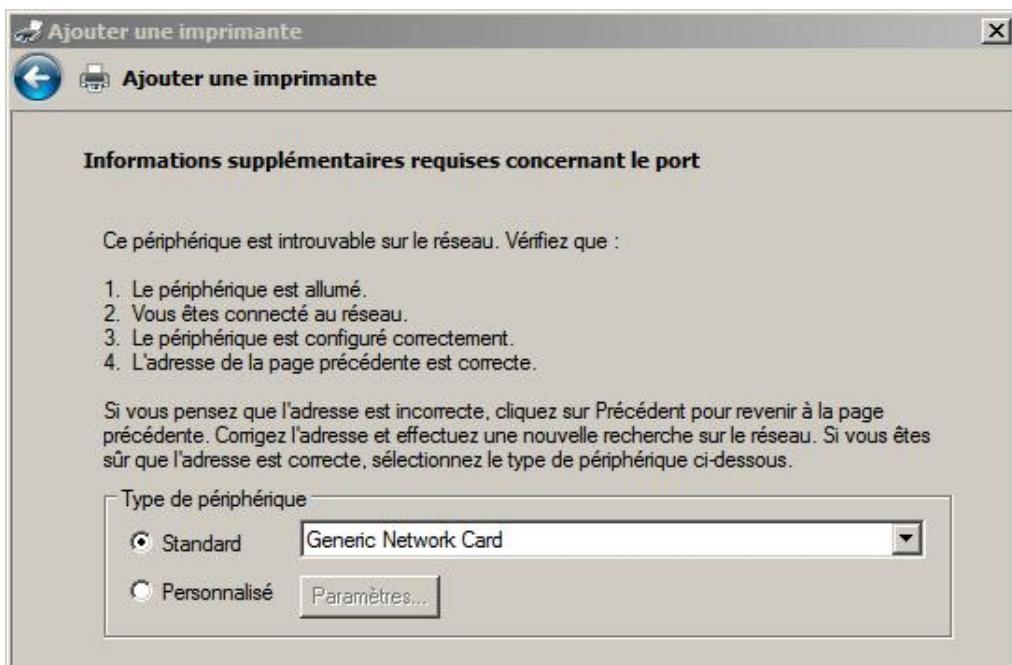
- **Détection automatique** pour essayer de retrouver automatiquement les paramètres de l'imprimante réseau.
- **Périphérique TCP/IP** si vous connaissez les paramètres IP de votre imprimante.
- **Périphérique de services Web** si l'imprimante est une imprimante Internet.

**Nom d'hôte ou adresse IP** : saisissez le nom DNS de l'imprimante ou son adresse IP.

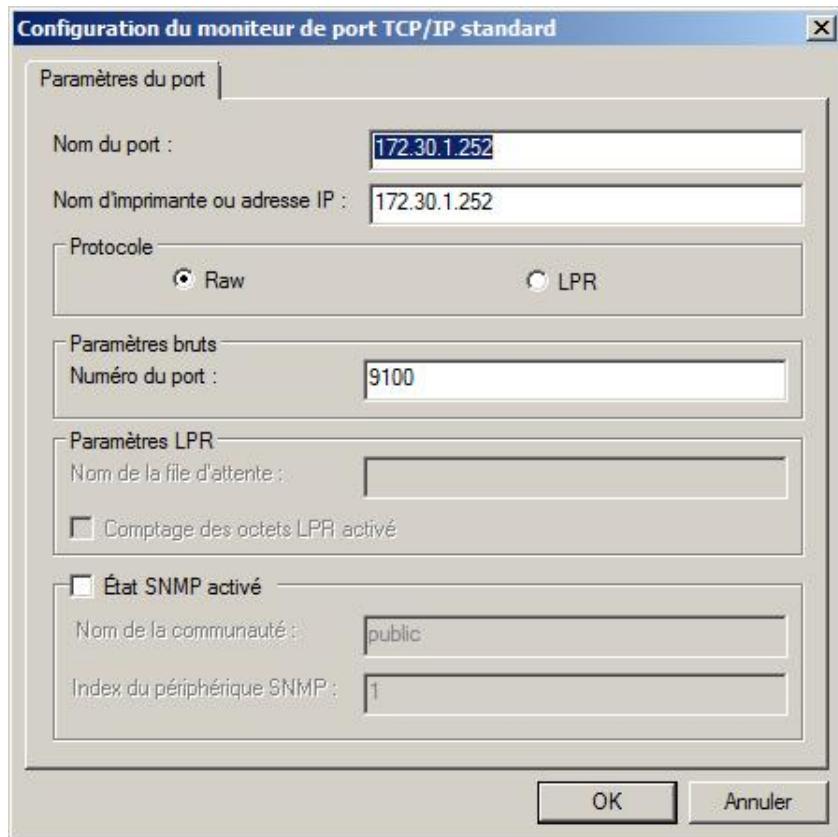
**Nom du port** : saisissez un nom explicite identifiant ce port. Il doit être unique sur le serveur d'impression.

La case à cocher **Interroger l'imprimante et sélectionner automatiquement le pilote à utiliser** permet de tenter de retrouver de manière transparente pour l'administrateur le meilleur pilote.

En cas d'erreur due à une mauvaise configuration, une imprimante non connectée, etc., la boîte de dialogue suivante apparaît :



Recherchez votre type d'imprimante dans la liste déroulante **Type de périphérique Standard** ou modifiez les paramètres en sélectionnant **Personnalisé** puis en cliquant sur **Paramètres**. Dans ce cas, il est nécessaire de connaître l'adresse IP utilisée par l'imprimante, le protocole Raw et son numéro de port ou LPR, et le nom de la file d'attente. Utilisez LPR uniquement si l'imprimante le requiert (anciens modèles).



Si aucune erreur n'a été détectée, continuez l'ajout de l'imprimante comme montré dans la section précédente.

### 3. Ajout d'une imprimante réseau



- Cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage du panneau de configuration n'est pas classique, cliquez sur **Imprimantes** dans le groupe **Matériel et audio** sinon cliquez directement sur **Imprimantes**.
- Dans la fenêtre **Imprimantes**, cliquez sur **Ajouter une imprimante**.
- Dans l'assistant **Ajouter une imprimante**, cliquez sur **Ajouter une imprimante réseau, sans fil ou Bluetooth**.
- Si aucune imprimante réseau n'a été trouvée, cliquez sur **L'imprimante que je veux n'est pas répertoriée**, sinon sélectionnez une imprimante de la liste puis cliquez sur **Suivant**.
- Si vous n'avez pas trouvé d'imprimante, vous pouvez :
  - **Rechercher une imprimante dans l'annuaire Active Directory** pour autant qu'elle soit publiée dans celui-ci.
  - **Sélectionner une imprimante partagée par nom**, en utilisant le bouton **Parcourir** si la découverte réseau est activée, sinon en saisissant le nom UNC (`\\\serveur\imprimante`) de l'imprimante, ou une imprimante Internet.
  - **Ajouter une imprimante à l'aide d'une adresse TCP/IP ou d'un nom d'hôte**, ce qui revient à créer un port standard TCP/IP.

- Sélectionnez l'option **Sélectionner une imprimante partagée par nom** et saisissez \\Win1\Canon Inkjet Pixma IP3000.

Si aucune erreur n'a été détectée, continuez l'ajout de l'imprimante comme montré dans la section précédente.

## 4. Configuration et gestion d'une imprimante



- Cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage du panneau de configuration n'est pas classique, cliquez sur **Imprimantes** dans le groupe **Matériel et audio** sinon cliquez directement sur **Imprimantes**.
- Dans la fenêtre **Imprimantes**, sélectionnez l'imprimante puis cliquez avec le bouton droit de la souris, enfin cliquez sur **Propriétés**.

### Onglet Général

La partie supérieure de cet onglet permet de donner un nom à l'imprimante, un emplacement et d'ajouter un commentaire. Soyez explicite !

Concernant l'emplacement, il est possible de le coupler avec l'Active Directory. Dans ce cas, la zone de texte se transforme en zone déroulante pour la sélection de l'emplacement et une petite zone de texte pour définir l'emplacement final de l'imprimante.

La seconde partie affiche les fonctionnalités propres à l'imprimante.

Le bouton **Options d'impression** permet de définir l'orientation de la feuille (portrait ou paysage), l'ordre des pages (première à dernière ou dernière à première), le nombre de feuilles par page, d'indiquer s'il faut tracer une bordure, de sélectionner l'alimentation du papier, de sélectionner le type de papier, d'indiquer une impression en couleur ou en noir et blanc ainsi que de fournir des paramètres propres à chaque périphérique d'impression.

- 
- Pour éviter de donner trop d'autorisations à l'utilisateur afin de personnaliser les paramètres de l'imprimante, il est préférable de créer plusieurs imprimantes disposant chacune de paramètres spécifiques.
- 

Le bouton **Imprimer une page de test** lance l'impression d'une page pour contrôler le fonctionnement de l'imprimante.

### Onglet Partage

La case à cocher **Partager cette imprimante** active le partage de l'imprimante avec les paramètres par défaut.

**Nom du partage** est le nom de l'imprimante partagée ; évitez les espaces dans le nom.

L'option **Rendu des travaux d'impression sur les ordinateurs client** indique si une partie du travail de préparation de l'impression se fait sur l'ordinateur client.

L'option **Lister dans l'annuaire** publie l'imprimante dans l'Active Directory. Il est possible de rechercher l'imprimante dans l'Active Directory.

Il faut être attentif au fait que le bouton de publication de l'imprimante dans l'Active Directory ne fait qu'enregistrer l'imprimante auprès du serveur dans l'Active Directory. Dès lors, il est possible de modifier son emplacement.

L'avantage principal de publier une imprimante dans l'Active Directory réside dans le fait qu'il est facile de modifier la visibilité de l'imprimante et d'autre part que l'on peut être certain que telle imprimante existe même si elle est temporairement hors ligne.

- 
- Il est recommandé de publier l'imprimante dans l'Active Directory.
- 

Le bouton **Pilotes supplémentaires** permet d'ajouter des pilotes pour les versions X86, X64 ou Itanium des autres systèmes d'exploitation Microsoft utilisés.

 Sur les clients antérieurs à Windows 2000, il faut installer une imprimante locale.

### Onglet Ports

Cet onglet affiche la liste des ports disponibles actuellement sur le serveur d'impression, leur description et s'ils sont rattachés à une imprimante.

Le bouton **Ajouter un port** permet d'ajouter un port **Local**, un port **Standard TCP/IP** ou un autre type de port si vous possédez une disquette.

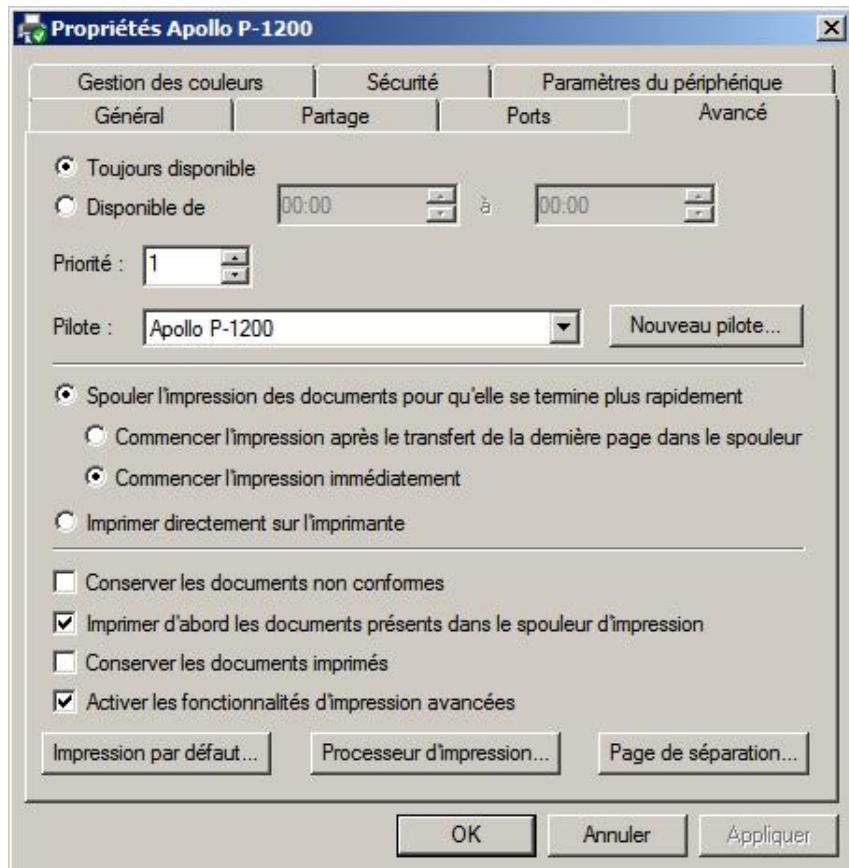
Le bouton **Supprimer le port** permet de supprimer le port sélectionné. Les ports définis par défaut ne peuvent être supprimés.

Le bouton **Configurer le port** permet éventuellement d'indiquer des paramètres pour le port sélectionné.

L'option **Activer la gestion du mode bidirectionnel** permet également au périphérique d'impression de communiquer avec l'imprimante.

L'option **Activer le pool d'imprimante** permet d'augmenter le débit d'impression en groupant plusieurs périphériques d'impression pour n'en faire plus qu'un. Il faut que tous les périphériques d'impression se situent au même emplacement, car l'utilisateur ne sait pas sur quel périphérique est envoyé son document, et qu'ils utilisent le même pilote, en d'autres termes que les périphériques d'impression soient identiques.

### Onglet Avancé



L'option **Toujours disponible** indique que l'imprimante est toujours prête pour imprimer des documents vers le périphérique d'impression. Pour une disponibilité moindre, il faut définir une fenêtre horaire journalière d'impression. Dans ce cas, les travaux d'impression sont toujours acceptés mais l'impression vers le périphérique d'impression se fait selon l'horaire défini.

 En production, certains départements comme la Comptabilité nécessitent d'imprimer de gros documents qui prennent du temps. Cette impression bloque généralement les autres utilisateurs. Une solution à ce problème consiste à créer deux imprimantes avec des disponibilités différentes.

La **Priorité** s'utilise lorsqu'il existe plusieurs imprimantes pour le même périphérique d'impression dans le but qu'une imprimante soit prioritaire par rapport aux autres. La valeur de 1 est la moins prioritaire et la valeur de 99 est la plus prioritaire.

 Certains utilisateurs exigent de pouvoir imprimer le plus rapidement possible. Il est possible de créer plusieurs imprimantes disposant de priorités différentes dont l'accessibilité est restreinte par des permissions afin de répondre à la demande.

La liste déroulante **Pilote** permet de sélectionner un pilote pour l'imprimante et le bouton **Nouveau pilote** d'ajouter un nouveau pilote pour l'imprimante.

Concernant le **Spouleur**, il est possible d'imprimer directement vers l'imprimante au lieu de stocker temporairement le document dans le répertoire de spool puis de l'imprimer. Cette méthode est utilisée principalement pour des périphériques d'impression non attachés.

Pour les options propres au spouleur, il est possible de choisir soit d'attendre que la dernière page du document soit placée dans le spool avant de lancer l'impression et de redonner la main à l'utilisateur, soit d'imprimer directement, ce qui permet de gagner du temps et de rendre la main à l'utilisateur rapidement.

La dernière section propose les options suivantes :

**Conserver les documents non conformes** permet d'éviter des erreurs causées par des documents disposant de tailles de papier différentes et de les imprimer.

**Imprimer d'abord les documents présents dans le spouleur d'impression** imprime en priorité les documents entièrement spoulés.

**Conserver les documents imprimés** n'efface pas les documents imprimés pour des raisons d'archivage ou dans le but d'imprimer plus rapidement d'autres exemplaires d'un même document.

**Activer les fonctionnalités d'impression avancées** utilise pour le rendu les données d'un métafichier EMF, l'ordre des pages, l'impression de livrets, etc.

Le bouton **Impression par défaut** permet de personnaliser certains paramètres propres au périphérique d'impression définis par son fabricant pour qu'ils soient utilisés par défaut.

Le bouton **Processeur d'impression** permet de sélectionner si nécessaire le moteur pour préparer la page.

Le bouton **Page de séparation** permet d'utiliser des pages de séparation pour imposer à l'imprimante un mode particulier. Il existe trois modes par défaut, à savoir :

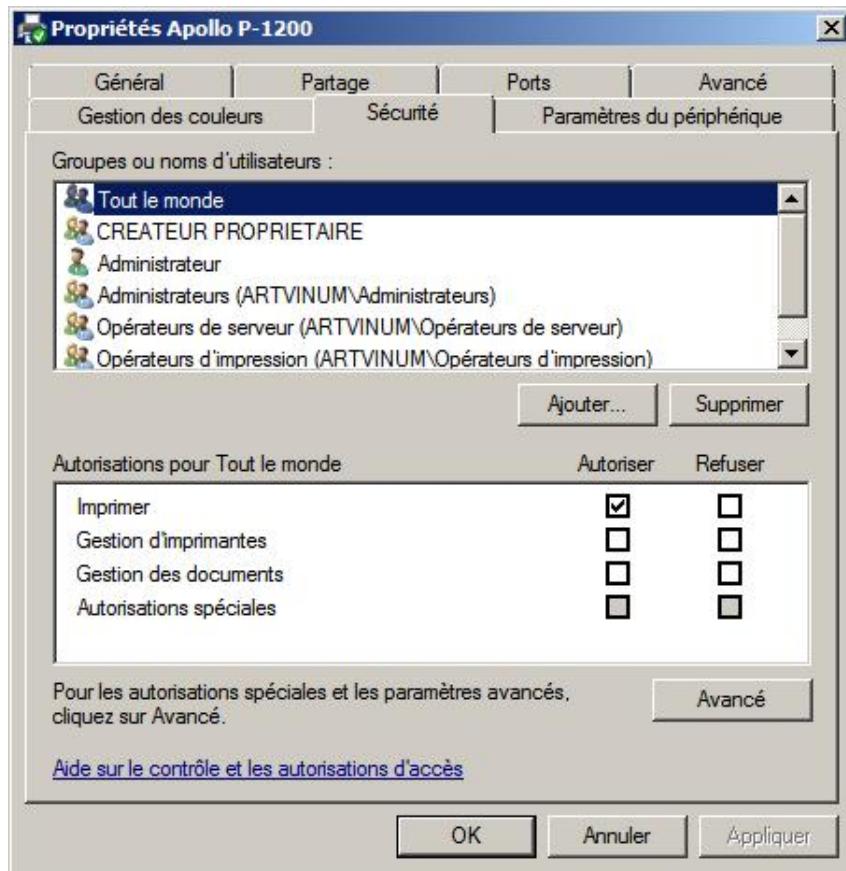
- **Pcl.sep** impose à l'imprimante le mode PCL et imprime une page de séparation avant chaque document. Non compatible avec le langage PJL.
- **Pscript.sep** impose à l'imprimante le mode PostScript sans imprimer de page de séparation.
- **Sysprint.sep** impose à l'imprimante le mode PostScript et imprime une page de séparation avant chaque document.

Par défaut, ces pages se trouvent dans le répertoire %systemroot%\system32.

### **Onglet Gestion des couleurs**

Le bouton **Gestion des couleurs** affiche une boîte de dialogue dans laquelle il est possible de définir, pour chaque périphérique d'impression, des profils pour gérer les couleurs et garantir le meilleur rendu possible, quel que soit le type de périphérique tel qu'un écran ou une imprimante.

### **Onglet Sécurité**



L'onglet **Sécurité** permet de gérer les permissions DACL applicables aux imprimantes. Chaque permission permet d'effectuer les opérations résumées dans le tableau suivant :

	<b>Imprimer</b>	<b>Gestion des documents</b>	<b>Gestion d'imprimantes</b>
Imprimer des documents	x	x	x
Connexion à des imprimantes	x	x	x
Suspendre, redémarrer ou annuler ses propres impressions	x	x	x
Gérer les paramètres pour les tâches d'impression		x	x
Suspendre, redémarrer et supprimer une impression		x	x
Partager une imprimante			x
Modifier les propriétés de l'imprimante			x
Modifier les permissions de l'imprimante			x
Supprimer des imprimantes			x

➤ Par défaut, le groupe **Tout le monde** a la permission **Imprimer**.

➤ Les administrateurs, les opérateurs de serveur et les opérateurs d'impression ont tous les droits sur le serveur d'impression.

Les autorisations spéciales (bouton **Avancé**) permettent également les opérations suivantes :

	<b>Imprimer</b>	<b>Gestion des documents</b>	<b>Gestion d'imprimantes</b>
Imprimer	x		x
Gestion d'imprimantes			x
Gestion des documents		x	
Autorisations de lecture	x	x	x
Modifier les autorisations		x	x
Appropriation		x	x

Dans la liste **Groupes ou noms d'utilisateurs**, vous trouvez les groupes ou les utilisateurs qui ont déjà reçu des permissions.

-  Pour simplifier la gestion des autorisations, il est conseillé d'assigner les permissions aux groupes et d'utiliser des groupes suffisamment génériques.

Les boutons **Ajouter** et **Supprimer** permettent d'ajouter des utilisateurs et des groupes pour leur assigner des permissions.

La liste **Autorisations** permet de définir les permissions pour le groupe ou l'utilisateur sélectionné. S'il faut utiliser des permissions spéciales, cliquez sur le bouton **Avancé**.

Ce bouton ouvre une boîte de dialogue identique à celle décrite pour les permissions **NTFS** dans le chapitre Mise en œuvre du serveur de fichiers qui permet de gérer les **autorisations spéciales**, de définir un **propriétaire** et de retrouver les **autorisations effectives**.

#### **Onglet Paramètres du périphérique**

Cet onglet est réservé pour configurer des paramètres propres à l'imprimante, définis par le fabricant. Pour éviter que les utilisateurs ne modifient ces paramètres, il est conseillé de créer plusieurs imprimantes, chacune étant spécifique à une catégorie d'utilisateurs.

## **5. Gestion des propriétés du serveur d'impression**



Win1

- Cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage du panneau de configuration n'est pas classique, cliquez sur **Imprimantes** dans le groupe **Matériel et audio** sinon cliquez directement sur **Imprimantes**.
- Dans la fenêtre **Imprimantes**, cliquez sur l'option **Propriétés du serveur** du menu **Fichier**.

#### **Onglet Formulaires**

Cet onglet permet d'ajouter, de modifier ou de supprimer des formulaires papiers adaptés aux besoins de votre entreprise.

Malheureusement, il n'est pas possible de supprimer les formulaires définis par défaut.

-  Il est conseillé de créer des formulaires qui peuvent être associés à une imprimante et de créer autant d'imprimantes que nécessaire.

## **Onglet Ports**

Cet onglet permet de définir des ports pour connecter logiquement une imprimante à un périphérique d'impression.

Dans les sections précédentes, il a été montré comment ajouter un port.

Cet onglet est identique à celui présenté pour les imprimantes. Il fait double emploi.

## **Onglet Pilotes**

L'onglet **Pilotes** permet de gérer les pilotes au niveau du serveur d'impression et de visualiser les propriétés des pilotes installés.

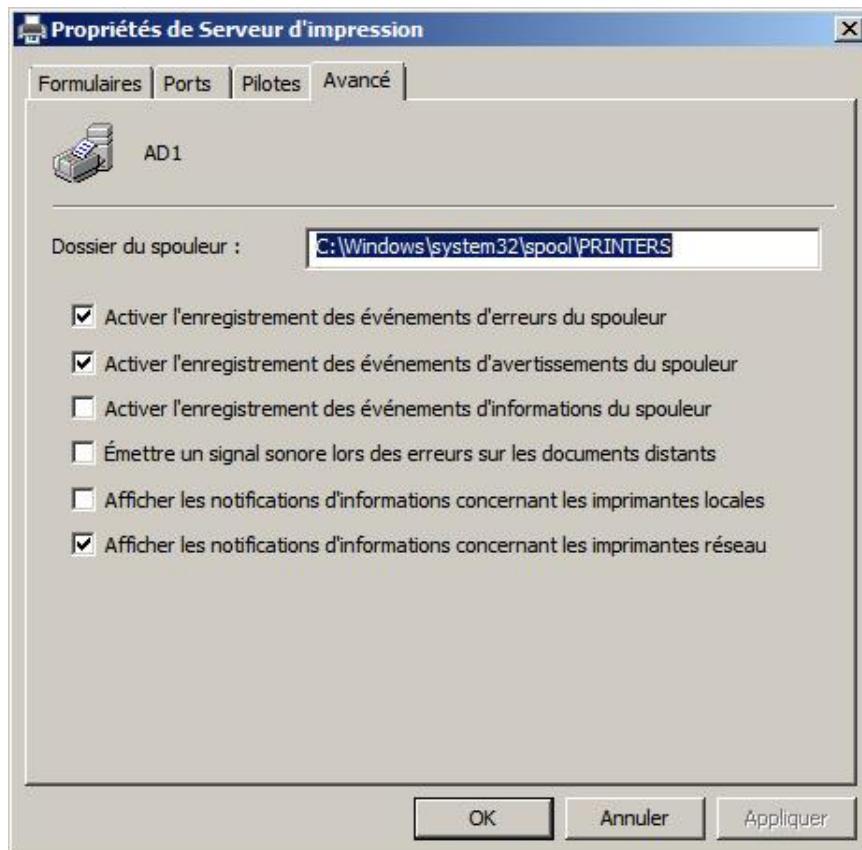
Le bouton **Ajouter** affiche l'assistant pour ajouter de nouveaux pilotes.

Le bouton **Supprimer** supprime le ou les pilotes sélectionnés.

Le bouton **Propriétés** affiche la liste des fichiers composant le pilote. Pour chaque fichier, il est possible de visualiser ses propriétés. Cette option est très utile pour le dépannage.

- Il faut ajouter les pilotes pour tous les systèmes d'exploitation à partir desquels les travaux d'impression sont lancés. Il faut également disposer de la bonne version du pilote en fonction du processeur.

## **Onglet Avancé**



Le **Dossier du spouleur** se trouve par défaut dans %systemroot%\system32\spool\printers ; il peut être déplacé sur un autre emplacement.

Il faut s'assurer que les utilisateurs qui peuvent imprimer disposent des droits de modification sur le dossier du spouleur.

S'il n'existe plus assez d'espace disque disponible dans le dossier de spool, l'impression ne peut s'effectuer et la demande dans la file d'impression est détruite sans que l'utilisateur en soit averti.

- Sur un serveur d'impression, il est conseillé de déplacer ce dossier sur un autre disque pour des raisons de performance.

- S'il n'est pas possible d'annuler des documents, il est possible d'arrêter le spouleur avec la commande **net**

stop spooler ; ensuite supprimez les documents dans le dossier du spouleur puis redémarrez les services avec net start spooler.

Les cases à cocher suivantes permettent de définir quels types d'événements seront enregistrés dans le journal d'événements Application :

- **Activer l'enregistrement des événements d'erreurs du spouleur**
- **Activer l'enregistrement des événements d'avertissements du spouleur**
- **Activer l'enregistrement des événements d'informations du spouleur**

Les autres cases à cocher concernent des notifications :

- **Émettre un signal sonore lors des erreurs sur les documents distants**
- **Afficher les notifications d'informations concernant les imprimantes locales**
- **Afficher les notifications d'informations concernant les imprimantes réseau**

## 6. Gestion des documents

Un utilisateur peut gérer ses propres documents dans la file d'attente avec la permission **Imprimer**. Les permissions **Gestion des documents** et **Gestion d'imprimantes** permettent de gérer tous les documents de l'imprimante.

La procédure suivante montre la gestion d'un document de la file d'attente :

- Connectez-vous en tant qu'administrateur sur le serveur d'impression.
- Cliquez sur **Démarrer** puis sur **Panneau de configuration**.
- Si l'affichage du panneau de configuration n'est pas classique, cliquez sur **Imprimantes** dans le groupe **Matériel et audio**, sinon cliquez directement sur **Imprimantes**. La liste des imprimantes s'affiche.
- Double cliquez sur l'imprimante dont vous voulez gérer un document. La liste d'attente des documents en cours s'affiche dans une fenêtre.

Nom du document	État	Propriétaire	Pages	Taille	Soumis	Port
Page de test	En attente	Administrateur	1	76.4 Ko	00:43:14 11.04.2008	
Sans titre - Bloc-notes	En attente	Administrateur	1	4.23 Ko	00:59:09 11.04.2008	
Sans titre - Bloc-notes	En attente	Administrateur	1	4.04 Ko	01:15:15 11.04.2008	
Sans titre - Bloc-notes	En attente	Administrateur	1	4.04 Ko	01:16:03 11.04.2008	
test.txt - Bloc-notes	En attente	testuser	1	1000 octets	22:45:38 16.04.2008	
monfichier.txt - Bloc-notes	En attente	testuser	1	1.90 Ko	22:46:07 16.04.2008	

6 document(s) dans la file

- Sélectionnez le document puis cliquez avec le bouton droit de la souris et sélectionnez une des actions suivantes :
  - **Suspendre** arrête l'impression du document en cours.
  - **Redémarrage** reprend l'impression d'un document suspendu.
  - **Annuler** supprime l'impression d'un document.

- **Propriétés** permet de visualiser et de modifier certaines propriétés du document à imprimer. Excepté l'onglet **Général**, les onglets de la boîte de dialogue **Propriétés** dépendent du fabricant du périphérique d'impression et il n'est pas toujours possible de modifier ces paramètres.

Pour mettre en pause, reprendre ou annuler tous les documents de l'imprimante, il faut utiliser les commandes du menu **Imprimante**.

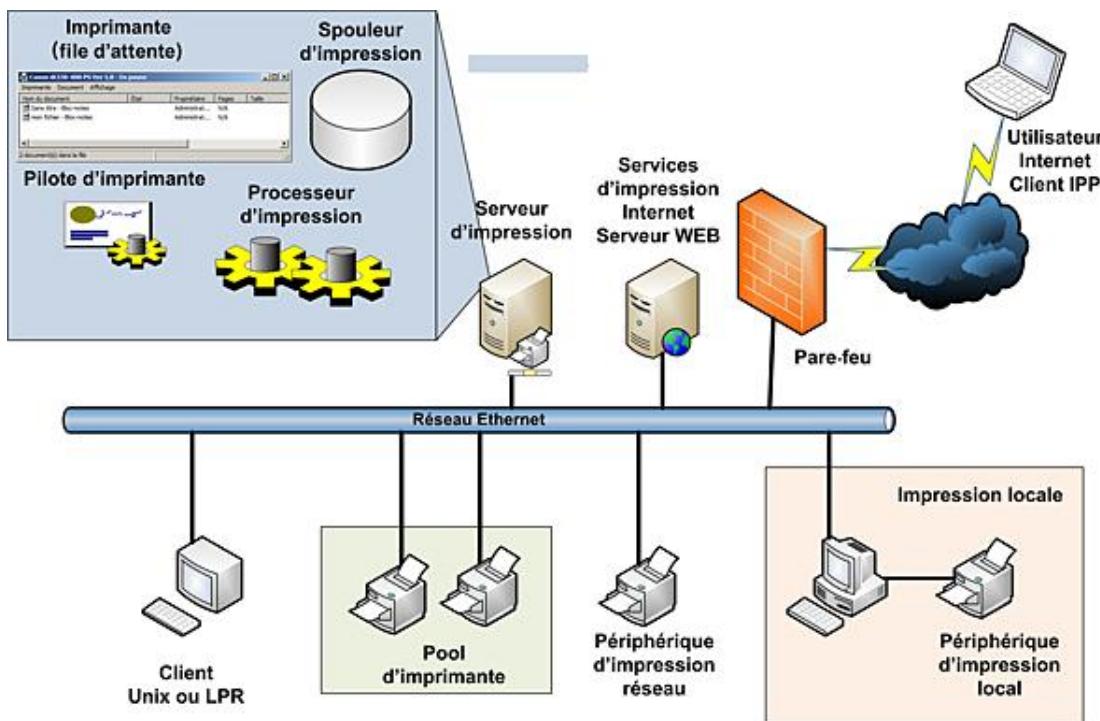
L'onglet **Général** affiche le nom du fichier, sa taille, le nombre de pages, le moteur utilisé et le format des données, le propriétaire et l'heure de soumission de l'impression.

Il est possible de modifier :

- l'utilisateur à notifier en modifiant le nom de l'utilisateur dans la zone de saisie **Avertir**.
- La **Priorité** du document dans la file d'attente de faible (1) à élevée (99).
- La **Planification** si une restriction d'horaire doit être appliquée.

# Terminologie

Bien que l'impression semble simple, les possibilités offertes à l'administrateur et aux utilisateurs sont nombreuses. Afin d'éviter toute ambiguïté, il est important de se familiariser avec la terminologie Microsoft concernant l'impression. La figure suivante résume les points essentiels.



## Imprimante

Une imprimante fait référence à une file d'attente, c'est-à-dire à une zone tampon sur disque servant de file d'attente pour l'impression sur le périphérique d'impression.

Une imprimante est la partie logique de la gestion du serveur d'impression et il est possible de créer plusieurs imprimantes ayant chacune des paramètres de gestion, ainsi que des options de sécurité, différents.

## Périphérique d'impression

Le périphérique d'impression fait référence à l'imprimante physique. Celle-ci peut être locale ou réseau.

## Impression locale

L'impression locale fait référence à une impression à partir d'un poste de travail sur un périphérique d'impression directement raccordé à cette station. Le raccordement peut se faire à l'aide d'un port parallèle, d'un port série ou d'un port USB. Généralement, il s'agit d'imprimantes bon marché dont le coût d'impression par page est assez élevé et dont la disponibilité n'est assurée que si la station de travail est allumée. Typiquement, elle n'est pas partagée.

## Impression réseau

L'impression réseau fait référence à une impression à partir d'un serveur d'impression dont le périphérique d'impression peut être raccordé localement ou via le réseau comme dans le cas d'une imprimante disposant d'une interface TCP/IP ou Bluetooth. Généralement, le serveur d'impression gère plusieurs imprimantes partagées dont le coût d'achat est plus élevé et la qualité d'impression meilleure qu'une imprimante locale mais dont le coût d'impression est plus faible. Sauf restrictions, la disponibilité est toujours assurée.

Dans l'architecture Microsoft, l'impression réseau gère la distribution des pilotes de l'imprimante.

Lorsqu'une station de travail se connecte à l'imprimante, elle contrôle qu'elle dispose de la version actuelle du pilote sinon elle le télécharge et l'installe de manière transparente pour l'utilisateur.

## Serveur d'impression

Le serveur d'impression fait référence à un serveur qui gère des imprimantes, les files d'attente et imprime sur plusieurs périphériques d'impression. Pour une station de travail, la notion de serveur d'impression est également valable car le concept et l'architecture sont les mêmes. Il se compose d'un spouleur d'impression, d'imprimantes, de

pilotes d'imprimantes et du processeur d'impression.

### **Pilote d'imprimante**

Le pilote d'imprimante est l'interface logicielle qui permet de gérer et d'imprimer sur un périphérique d'impression. Les pilotes sont prévus pour un système d'exploitation et une version X86, X64 ou Itanium. Dans la philosophie Microsoft, les pilotes sont gérés et distribués par le serveur d'impression lorsqu'un ordinateur client se connecte.

Si un pilote n'existe pas pour un périphérique d'impression particulier, il est toujours possible d'en installer un créé pour un périphérique similaire, mais il sera peut-être limité.

Lorsqu'une station de travail se connecte pour la première fois auprès d'une imprimante, la partie cliente du pilote est téléchargée sur la station de travail, elle contient entre autres le processeur d'impression.

Partage par défaut : "PRINT\$" = %systemroot%\system32\spool\drivers

### **Spouleur d'impression**

Le spouleur d'impression fait référence à la zone du disque dur où sont stockés les fichiers prêts à être imprimés. Par défaut, il s'agit du dossier %systemroot%\system32\spool\printers.

### **Document**

Le document est l'élément à imprimer. Une fois placé dans le spouleur, il est composé de deux fichiers : le premier est le rendu pour l'imprimante et porte l'extension SPL, le second contient des informations administratives et porte l'extension SHD.

### **Impression Internet IPP**

L'Impression Internet ou IPP fait référence à la possibilité de gérer et d'imprimer en utilisant le protocole de transport HTTP ou mieux, HTTPS. Pour l'utiliser, il faut installer un serveur Web (IIS) sur lequel l'application **Impression Internet** fonctionne.

L'avantage principal réside dans le fait que l'utilisateur peut imprimer en étant connecté sur un réseau externe à l'entreprise.

### **Client Impression Internet**

Le client Impression Internet est la partie qui s'installe sur le client afin d'imprimer sur une imprimante Internet.

### **Service d'impression LPD (Line Printer Daemon)**

Le service d'impression LPD permet aux utilisateurs UNIX ou utilisateur d'impression LPR d'imprimer sur les imprimantes Windows si le service LPD fonctionne.

### **Le moniteur de port LPR (Line Printer Remote)**

Le moniteur LPR permet à des ordinateurs Windows d'imprimer sur des imprimantes LPR.

### **Processeur d'impression**

Le processeur d'impression est un des éléments du processus de mise en file d'attente. Il gère la manière dont les documents sont envoyés à l'impression, dans quel ordre y compris l'ordre des pages, etc. Certains fabricants d'imprimantes créent leur propre processeur d'impression.

### **Gestion de l'impression**

La gestion de l'impression fait référence à l'application qui s'installe avec le rôle Services d'impression. Cette application permet de gérer de manière centralisée et efficace plusieurs serveurs d'impression.

### **XPS (XML Paper Specification)**

XPS est une spécification d'un langage de description de pages développé par Microsoft et basé sur XML. Il est indépendant du périphérique et de la résolution utilisée. Une imprimante XPS génère un fichier XPS lisible également sur l'ordinateur à l'aide d'une visionneuse XPS.

Depuis Windows Vista, l'impression est basée sur XPS et non plus sur la norme d'impression GDI. Une passerelle bidirectionnelle permet de passer du format XPS vers EMF généré par le moteur GDI.

Actuellement, ce sont surtout les applications WPF (*Windows Presentation Foundation*) du Framework 3 qui nécessitent l'utilisation d'une imprimante XPS.

Les avantages sont une meilleure qualité, une meilleure gestion de la couleur, des fichiers d'impression plus petits et

une gestion administrative des imprimantes plus aisée.

---



On "n'installe" pas une imprimante mais on "ajoute" une imprimante.

---

## Objectifs du chapitre

Dans ce chapitre, vous travaillez pour une entreprise fictive en tant qu'administrateur et votre direction vous demande d'implémenter les technologies étudiées dans les chapitres précédents. Bien entendu, certains choix ne correspondent pas forcément aux meilleures pratiques (Best practices).

# Sites WEB

## RFC (Request for Comments)

<http://www.rfc-editor.org>

## IANA (Internet Assigned Numbers Authority)

<http://www.iana.org>

## Calculateurs IP en ligne

<http://www.subnetmask.info>

<http://jodies.de/ipcalc>

<http://www.subnet-calculator.com/>

## Gestionnaire de noms de domaine Internet

[http://www\\_afnic.fr](http://www_afnic.fr)

<http://www.switch.ch>

<http://www.networksolutions.com>

## Repository du Script Center

<http://www.microsoft.com/technet/scriptcenter/scripts>

## Client Telnet

<http://ttssh2.sourceforge.jp>

## Framework pour Linux

<http://www.mono-project.com>

## Convertir Windows 2008 en Workstation!

<http://www.win2008workstation.com>

## Prochaine génération de la pile TCP/IP

[http://technet.microsoft.com/fr-ch/network/bb545475\(en-us\).aspx](http://technet.microsoft.com/fr-ch/network/bb545475(en-us).aspx)

## **Blogs**

Microsoft Entreprise Networking Team : <http://blogs.technet.com/networking/default.aspx>

Microsoft Technet Server Core : [http://blogs.technet.com/server\\_core/](http://blogs.technet.com/server_core/)

Microsoft Virtualization Team : <http://blogs.technet.com/virtualization/>

## Objectifs de l'examen 70-642

Tableau Microsoft des Compétences évaluées par l'examen 70-642 - MCTS : Configuration d'une Infrastructure réseau avec Windows Server 2008.

Compétences évaluées par l'examen 70-642	Chapitres	Travaux pratiques
<b>Configuration des services et de l'adressage IP (24 %)</b>		
Configurer l'adressage IPv4 et IPv6. Cela inclut, sans s'y limiter :		
configurer les options IP	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux Exercice 2 - Mise en œuvre de l'adressage IPv4 au niveau des sites de Paris et de Genève
sous-réseau	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux Exercice 2 - Mise en œuvre de l'adressage IPv4 au niveau des sites de Paris et de Genève
sur-réseau	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux Exercice 2 - Mise en œuvre de l'adressage IPv4 au niveau des sites de Paris et de Genève
autre configuration	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux Exercice 2 - Mise en œuvre de l'adressage IPv4 au niveau des sites de Paris et de Genève
Configurer DHCP ( <i>Dynamic Host Configuration Protocol</i> (DHCP)). Cela inclut, sans s'y limiter :		
options DHCP	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
création de nouvelles options	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
amorçage PXE	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
profils des utilisateurs par défaut		Exercice 3 - Mise en œuvre de l'adressage IPv6
agent relais DHCP	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
exclusions	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
autoriser un serveur dans Active Directory	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6

portée	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
bases du serveur	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6
Windows Server Hyper-V	Configuration autour du protocole DHCP	Exercice 3 - Mise en œuvre de l'adressage IPv6

Configurer le routage. Cela inclut, sans s'y limiter :

routage statique	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux
routage persistant	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux
RIP ( <i>Routing Internet Protocol</i> )	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux
OSPF ( <i>Open Shortest Path First</i> )	Configuration de base des services réseau	Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux

Configurer IPSec. Cela inclut, sans s'y limiter :

créer une stratégie IPSec	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms
AH ( <i>Authentication Header</i> ) IPSec	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms
ESP ( <i>Encapsulating Security Payload</i> ) IPsec	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms

### Configuration de la résolution de noms (27 %)

Configurer un serveur DNS (*Domain Name System*). Cela inclut, sans s'y limiter :

redirection conditionnelle	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
redirecteur externe	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
suggestion de serveurs racine	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
serveur de cache uniquement	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
bases de serveur	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
intégration entre WINS et DNS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
virtualisation Windows Server	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP

Configurer les zones DNS. Cela inclut, sans s'y limiter :

mise à jour DNS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
intervalles de mise à jour	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
adresses DNS listserv (nslookup)	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
zones primaires et secondaires	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
intégration Active Directory	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
DNS dynamique (DDNS)	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
GlobalNames	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
rafraîchissement du SOA	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP

Configurer les enregistrements DNS. Cela inclut, sans s'y limiter :

types d'enregistrement	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
host (hôte)	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
pointeur	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
MX	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
SRV	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
NS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
mises à jour dynamiques	Configuration de la résolution de noms  Configuration autour du protocole DHCP	Exercice 4 - Mise en œuvre d'un système DHCP
TTL ( <i>Time To Live</i> )	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP

Configurer la réPLICATION DNS. Cela inclut, sans s'y limiter :

zones DNS secondaires	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
zones stub DNS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP

intervalle de nettoyage DNS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
portée de la réPLICATION	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
Configurer la résolution de noms pour des ordinateurs clients. Cela inclut, sans s'y limiter :		
intégration DNS et WINS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
configurer le fichier HOSTS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
LMHOSTS	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
type de nœud	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
LLMNR ( <i>Link-Local Multicast Name Resolution</i> )	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
diffusion	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
cache du resolveur	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
liste des serveurs DNS	Configuration de base des services réseau Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
ordre de recherche des suffixes	Configuration de base des services réseau Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
gestion des paramètres du client via une stratégie de groupe	Configuration de la résolution de noms	Exercice 4 - Mise en œuvre d'un système DHCP
<b>Configuration de l'accès au réseau (22 %)</b>		
Configurer l'accès à distance. Cela inclut, sans s'y limiter :		
connexion physique	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite Exercice 7 - Sécurisation des liaisons intersites Exercice 8 - Accès à Internet et accès depuis Internet
stratégie d'accès à distance	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite Exercice 7 - Sécurisation des liaisons intersites Exercice 8 - Accès à Internet et accès depuis Internet

traduction des adresses réseau (NAT)	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
partage de la connexion Internet	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
réseau privé virtuel (VPN)	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
services de routage et d'accès à distance (RRAS)	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
filtrage entrant et sortant	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
configuration d'un serveur RADIUS ( <i>Remote Authentication Dial-In User Service</i> )	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
configuration d'un proxy RADIUS	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
protocoles d'accès distant	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite  Exercice 7 - Sécurisation des liaisons intersites  Exercice 8 - Accès à Internet et accès depuis Internet
gestionnaire de connexion	Configuration des services réseaux avancés	Exercice 6 - Sécurisation des liaisons intrasite

		Exercice 7 - Sécurisation des liaisons intersites Exercice 8 - Accès à Internet et accès depuis Internet
Configurer la protection d'accès réseau (NAP). Cela inclut, sans s'y limiter :		
protection de la couche réseau	Configuration des services réseaux avancés	Exercice 9 - VPN SSTP pour ordinateurs distants
application de DHCP	Configuration des services réseaux avancés	Exercice 9 - VPN SSTP pour ordinateurs distants
application de VPN	Configuration des services réseaux avancés	Exercice 9 - VPN SSTP pour ordinateurs distants
configuration des stratégies NAP	Configuration des services réseaux avancés	Exercice 9 - VPN SSTP pour ordinateurs distants
application d'IPSec ; 802.1x	Configuration des services réseaux avancés	Exercice 9 - VPN SSTP pour ordinateurs distants
isolement d'un hôte	Configuration des services réseaux avancés	Exercice 9 - VPN SSTP pour ordinateurs distants
Configurer l'authentification réseau. Cela inclut, sans s'y limiter :		
authentification sur réseau local en utilisant NTLMv2 et Kerberos	Configuration de base des service réseau	
authentification WLAN en utilisant 802.1x	Configuration de base des service réseau	
authentification RAS en utilisant MS-CHAP, MS-CHAPv2 et EAP	Configuration de base des service réseau	
Configurer l'accès sans fil. Cela inclut, sans s'y limiter :		
<i>Set Service Identifier (SSID)</i>	Configuration de base des service réseau	
<i>Wired Equivalent Privacy (WEP)</i>	Configuration de base des service réseau	
<i>Wi-Fi Protected Access (WPA)</i>	Configuration de base des service réseau	
<i>Wi-Fi Protected Access 2 (WPA2)</i>	Configuration de base des service réseau	
mode infrastructure ou ad hoc	Configuration de base des service réseau	
stratégie de groupe pour les liaisons sans fil	Configuration de base des service réseau	
Configurer les paramètres du pare-feu. Cela inclut, sans s'y limiter :		
filtrage du trafic entrant et sortant	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms
intégration de compte Active	Configuration des services réseaux	Exercice 5 - Mise en œuvre de la

Directory	avancés	résolution de noms
identification des ports et des protocoles	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms
Pare-feu Microsoft Windows ou Pare-feu Windows avec sécurité renforcée	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms
configurer un pare-feu via une stratégie de groupe	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms
stratégie d'isolement	Configuration des services réseaux avancés	Exercice 5 - Mise en œuvre de la résolution de noms

#### **Configuration des services fichiers et impression (13 %)**

Configurer un serveur de fichier. Cela inclut, sans s'y limiter :

publication des partages de fichiers	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
fichiers hors connexion	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
autorisations de partage	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
autorisations NTFS	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
EFS ( <i>Encrypting File System</i> )	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression

Configurer DFS (*Distributed File System*). Cela inclut, sans s'y limiter :

espace de noms DFS	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
configuration DFS et application	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
création et configuration de cibles	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
réplication DFS	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression

Configurer le service des clichés instantanés. Cela inclut, sans s'y limiter :

récupération de versions antérieures	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
planification	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
emplacements de stockage	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression

Configurer la sauvegarde et la restauration. Cela inclut, sans s'y limiter :

types de sauvegarde	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
---------------------	--------------------------------------	---

planification des sauvegardes	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
administration à distance	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
restauration des données	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression

Administrer les quotas sur les disques. Cela inclut, sans s'y limiter :

quota par volume ou par utilisateur	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
entrées de quotas	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression
modèles de quotas	Mise en œuvre du serveur de fichiers	Exercice 11 - Mise en œuvre du rôle de serveur d'impression

Configurer et surveiller les services d'impression. Cela inclut, sans s'y limiter :

partage d'une imprimante	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
publier les imprimantes dans Active Directory	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
autorisations d'imprimante	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
déployer une connexion d'imprimante	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
installer des pilotes d'impression	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
exporter et importer des files d'attente d'impression et des paramètres d'imprimante	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
ajouter des compteurs à l'Analyseur de performances et de fiabilité pour surveiller les serveurs d'impression	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
groupe d'impression	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP
priorité de l'impression	Mise en œuvre de l'impression	Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP

#### **Analyser et administrer une infrastructure réseau (14 %)**

Configurer des paramètres serveur WSUS (*Windows Server Update Services*). Cela inclut, sans s'y limiter :

sélection du type de mise à jour ; paramètres du client	Gestion et surveillance d'une infrastructure réseau	Exercice 13 - Optimisation et surveillance
objet de stratégie de groupe (GPO)	Gestion et surveillance d'une infrastructure réseau	Exercice 13 - Optimisation et surveillance
ciblage des clients	Gestion et surveillance d'une	Exercice 13 - Optimisation et

	infrastructure réseau	surveillance
mises à jour logiciels	Gestion et surveillance d'une infrastructure réseau	Exercice 13 - Optimisation et surveillance
test et approbation	Gestion et surveillance d'une infrastructure réseau	Exercice 13 - Optimisation et surveillance
réseaux déconnectés.	Gestion et surveillance d'une infrastructure réseau	Exercice 13 - Optimisation et surveillance
Collecter les données de performance. Cela inclut, sans s'y limiter :		
ensembles de collecteurs de données	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
analyseur de performances	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
analyseur de fiabilité	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
surveiller l'index de stabilité système	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
Surveiller les journaux des événements. Cela inclut, sans s'y limiter :		
affichages personnalisés	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
journaux des applications et des services	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
abonnements	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
journal DNS	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
Collecter des données réseau. Cela inclut, sans s'y limiter :		
<i>Simple Network Management Protocol (SNMP)</i>	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
Baseline Security Analyzer	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers
moniteur réseau	Gestion et surveillance d'une infrastructure réseau	Exercice 12 - Mise en œuvre d'un système de serveur de fichiers

# Exercice 14 - Mise en œuvre d'un serveur WSUS

## 1. Objectifs

Dans cet exercice vous allez installer et configurer un serveur WSUS pour distribuer les mises à jour sur le site de Paris.

## 2. Configuration de l'environnement

➤ Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

➤ Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

➤ Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt**, doit se trouver sur le Bureau). Après le redémarrage de **paris1**, vous pouvez continuer le lancement des scripts sur les autres ordinateurs.
- Sur **paris2**, après avoir placé le fichier **scriptParis2.bat**, exécutez-le
- Sur **geneve1**, après avoir placé le fichier **scriptgeneve1.bat**, exécutez-le.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt **mydom.eni** ainsi que serveur DNS. Il agit également en tant que routeur. Ses adresses IP sont 10.1.1.1/24 sur le segment paris et 172.30.1.1/24 sur le segment Internet.

**paris2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.1.1.2/24).

**geneve1** est membre du domaine **mydom.eni**. Il est également routeur et dispose d'adresses IP fixes soit 192.168.1.1/24 sur le segment geneve et 172.30.1.2/24 sur le segment Internet.

➤ La configuration proposée ne permet pas d'effectuer correctement l'exercice. Pour être optimum, il faut que la carte appelée Internet sur **paris1** et **geneve1** soit mappée sur la carte physique de l'ordinateur hôte et non plus sur local seul. Il est également probable de modifier l'adressage IPv4 de l'interface virtuelle appelée Internet pour accéder à Internet dans le monde réel.

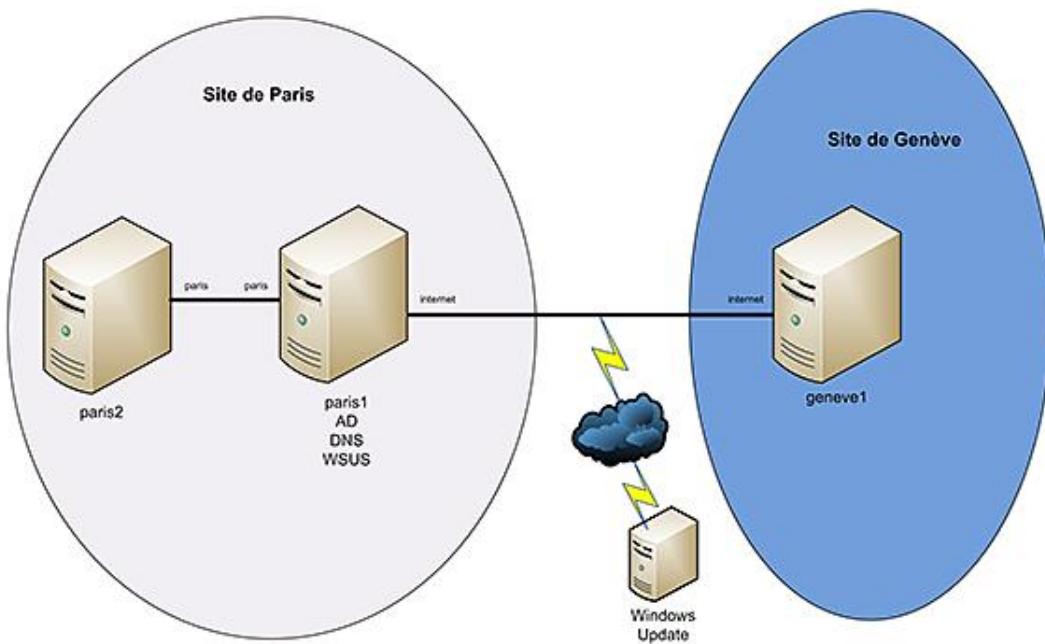
## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Gestion et surveillance d'une infrastructure réseau et plus particulièrement à la section consacrée à WSUS. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre de WSUS

Il a été décidé d'utiliser un serveur WSUS pour mettre à jour les différents ordinateurs de l'entreprise. À cet effet, un serveur WSUS est installé sur le site de Paris qui gère les ordinateurs de Paris.

La topologie est la suivante :



Les tâches à effectuer sont :

- Créer des sites Active Directory.
- Installer et configurer WSUS sur paris1.
- Définir quelles mises à jour approuver.
- Définir une stratégie de groupe pour que les ordinateurs du site de Paris reçoivent les mises à jour du serveur WSUS.

## 5. Création des sites Active Directory

Seul paris1 est requis.

Pour faciliter l'exercice, vous allez créer deux sites Active Directory soit un pour Genève et un pour Paris. Vous y déplacez les ordinateurs correspondants.

1. Connectez-vous en tant qu'administrateur sur paris1.
2. Démarrer **Sites et services Active Directory** des Outils d'administration.
3. Développez l'arborescence pour faire apparaître **Sites**.
4. Cliquez avec le bouton droit de la souris sur **Sites** puis sur **Nouveau site**.
5. Saisissez Geneve pour le nom puis sélectionnez **DefaultIPSITELINK** avant de cliquer sur **OK**.
6. Sur le message, cliquez sur **OK**.
7. Cliquez avec le bouton droit de la souris sur **Sites** puis sur **Nouveau site**.
8. Saisissez Paris pour le nom puis sélectionnez **DefaultIPSITELINK** avant de cliquer sur **OK**.

**OK.**

9. Sur le message, cliquez sur **OK**.
10. Cliquez avec le bouton droit de la souris sur **Subnets** puis sur **Nouveau Sous-réseau**.
11. Dans la boîte de dialogue, saisissez 192.168.1.0/24 et sélectionnez le site de Genève avant de cliquer sur **OK**.
12. Cliquez avec le bouton droit de la souris sur **Subnets** puis sur **Nouveau Sous-réseau**.
13. Dans la boîte de dialogue, saisissez 10.1.1.0/24 et sélectionnez le site de Paris avant de cliquer sur **OK**.
14. Déplacez l'ordinateur paris1 dans le site de Paris.

---

 Vous avez configuré deux sites Active Directory.

---

## 6. Installation et configuration d'un serveur WSUS sur paris1

---

 Seul paris1 est requis.

---

Il vous faut garantir que paris1 puisse accéder à Internet avant de pouvoir effectuer la suite de cette question.

Pour générer des rapports, il est nécessaire de télécharger et d'installer Microsoft Report Viewer Redistributable 2005. Celui-ci peut être installé avant ou après l'installation du serveur WSUS.

1. Connectez-vous en tant qu'administrateur sur paris1.
2. Lancez le Gestionnaire de Serveur.
3. Gardez le nœud **Gestionnaire de serveur (paris1)** sélectionné et dans la zone de détail, cliquez sur **Rechercher de nouveaux rôles**.
4. Après quelques instants, une boîte de dialogue vous indique qu'un ou plusieurs rôles sont disponibles. Cliquez sur **Ouvrir Windows Update**.
5. Dans la boîte de dialogue **Windows Update**, cliquez sur **Activer maintenant**.
6. Cliquez sur **Installer maintenant**. Et patientez jusqu'à ce que la nouvelle version de Windows Update soit installée et qu'elle ait recherché les nouvelles informations.
7. Cliquez sur **Afficher les mises à jour disponibles**.
8. Désélectionnez tous les produits (non recommandé en production) puis sélectionnez uniquement **Mise à jour pour le Gestionnaire de serveur Windows Server 2008 (KB940518)** avant de cliquer sur **Installer**.
9. Attendez que la mise à jour soit téléchargée et installée pour redémarrer l'ordinateur.
10. Après le redémarrage, connectez-vous en tant qu'administrateur puis lancez le **Gestionnaire de serveur** pour ajouter un nouveau rôle.
11. Un nouveau rôle est présent, soit Windows Server Update Services, que vous sélectionnez pour l'installer.
12. Lorsque l'assistant d'installation de **Windows Server Update Services 3.0 SP1** démarre, cliquez sur **Suivant**.
13. Sur la page **Contrat de licence**, sélectionnez **J'accepte les termes du contrat de licence** puis cliquez sur **Suivant**.
14. Sur la page **Composants nécessaires pour utiliser l'interface utilisateur d'administration**, cliquez sur **Suivant**.
15. Sur la page **Sélectionner la source des mises à jour**, désélectionnez la case à cocher

**Stocker les mises à jour localement** uniquement pour diminuer la durée de l'exercice, avant de cliquer sur **Suivant**.

16. Sur la page **Options de base de données**, laissez les valeurs par défaut, puis cliquez sur **Suivant**.
17. Sur la page **Sélection du site Web**, laissez les valeurs par défaut puis cliquez sur **Suivant**.
18. Sur la page **Prêt pour l'installation de Windows Server Update Services 3.0 SP1**, cliquez sur **Suivant**.
19. Après quelques minutes, cliquez sur **Terminer** pour finir l'installation.
20. L'assistant de configuration démarre automatiquement, sur la page **Avant de commencer** cliquez sur **Suivant**.
21. Sur la page **Programme d'amélioration de Microsoft Update**, éventuellement décochez la case avant de cliquer sur **Suivant**.
22. Sur la page **Choisir le serveur en amont**, laissez les valeurs par défaut et cliquez sur **Suivant**.
23. Sur la page **Définir le serveur Proxy**, laissez les valeurs par défaut et cliquez sur **Suivant**.
24. Sur la page **Se connecter au serveur en amont**, cliquez sur **Démarrer la connexion**. Il est nécessaire de disposer d'une connexion Internet. Attendez quelques minutes avant de cliquer sur **Suivant**.
25. Sur la page **Choisir les produits**, laissez les valeurs par défaut (Windows et Office sont sélectionnés) et cliquez sur **Suivant**.
26. Sur la page **Choisir les classifications**, cochez la case **Toutes les classifications** puis cliquez sur **Suivant**.
27. Sur la page **Définir la planification de la synchronisation**, sélectionnez l'option **Synchroniser manuellement** puis cliquez sur **Suivant**.
28. Sur la page **Terminé**, cliquez sur **Terminé**.
29. Avant de continuer, démarrez la console **Microsoft Windows Server Update Services 3.0 SP1** et dans la zone de détail attendez que la synchronisation soit terminée (elle peut prendre plusieurs heures).

---

 Le serveur WSUS est installé et configuré pour le site de Paris.

---

## 7. Approbation des mises à jour

---

 paris1 est requis.

---

Vous allez examiner comment vous pouvez approuver les mises à jour pour qu'elles puissent être distribuées au sein de votre entreprise en utilisant le serveur WSUS comme serveur de mise à jour.

1. Connectez-vous en tant qu'administrateur sur **paris1**.
2. Démarrez la console **Microsoft Windows Server Update Services 3.0 SP1 de groupe** des **Outils d'administration**.
3. Sélectionnez paris1 dans l'arborescence, la zone de détail ressemble à l'image suivante :



Ce composant logiciel enfichable permet de déployer de manière fiable et rapide les dernières mises à jour sur les ordinateurs.

#### Tâches à effectuer

- ⚠ 1861 mises à jour de sécurité sont en attente d'[approbation](#).
- ⚠ 284 mises à jour prioritaires en attente d'[approbation](#).
- ⚠ Votre serveur WSUS indique qu'aucun ordinateur n'est inscrit pour recevoir des mises à jour. Pour plus d'informations sur l'inscription des ordinateurs, voir [Pour configurer un ordinateur client](#).
- ⓘ 96 nouveaux produits et 9 nouvelles classifications ont été ajoutés au cours des 30 derniers jours. [Afficher les produits et les classifications](#)

#### Vue d'ensemble

##### État des ordinateurs



- |  |   |
|--|---|
| <span style="color: red;">■</span> Ordinateurs avec des erreurs :                | 0 |
| <span style="color: yellow;">■</span> Ordinateurs nécessitant des mises à jour : | 0 |
| <span style="color: green;">■</span> Ordinateurs installés/non applicables :     | 0 |

##### État de la synchronisation

- |                            |   |
|----------------------------|---|
| État :                     | En attente                              |
|                            | <a href="#">Synchroniser maintenant</a> |
| Dernière synchronisation : | 19.05.2009<br>03:46                     |

Résultat de la dernière synchronisation : [Réussie](#)

##### État des mises à jour



- |   |   |
|---|---|
| <span style="color: red;">■</span> Mises à jour avec des erreurs :                | 0 |
| <span style="color: yellow;">■</span> Mises à jour requises par des ordinateurs : | 0 |
| <span style="color: green;">■</span> Mises à jour installées/non applicables :    | 0 |

##### État de téléchargement

- |   |   |
|---|---|
| Mises à jour nécessitant des fichiers : | 0 |
|---|---|

##### Statistiques du serveur

- |                               |       |
|-------------------------------|-------|
| Mises à jour non approuvées : | 21682 |
| Mises à jour approuvées :     | 8     |
| Mises à jour refusées :       | 78    |
| Ordinateurs :                 | 0     |
| Groupes d'ordinateurs :       | 0     |

##### Connexion

- |                         |                |
|-------------------------|----------------|
| Type :                  | Local/SSL      |
| Port :                  | 80             |
| Rôle de l'utilisateur : | Administrateur |
| Version du serveur :    | 3.1.6001.65    |

#### Ressources

- ➡ [Page d'accueil WSUS](#)
- ➡ [Présentation technique WSUS](#)
- ➡ [Catalogue Microsoft Update](#)

- ➡ [Communauté WSUS](#)
- ➡ [Déclaration de confidentialité WSUS](#)

1. Dans l'arborescence cliquez sur **Toutes les mises à jour**, la zone de détail doit être vide mais le titre de la zone de détail indique qu'il y a plusieurs milliers de mises à jour disponibles qui sont non approuvées. Pour les faire apparaître, modifiez l'état de **Echec** ou **Nécessaire** à **Toutes**. Cette opération peut prendre plusieurs dizaines de secondes.
2. Sélectionnez une mise à jour disponible et cliquez avec le bouton droit de la souris, le menu contextuel apparaît et vous permet d'approuver ou de refuser la mise à jour. Néanmoins cette méthode d'approbation n'est pas très efficace car vous devez le faire pour chacune des mises à jour de la liste.
3. Une autre méthode consiste à sélectionner le nœud **Options** dans l'arborescence.
4. Dans la zone de détail, cliquez sur **Approbations automatiques**.
5. Dans la boîte de dialogue **Approbations automatiques** vous allez pouvoir créer des règles d'approbations basées soit sur la classification des mises à jour, soit sur un produit spécifique et des ordinateurs ou des groupes d'ordinateurs. Par défaut, une règle existe nommée **Règle d'approbation automatique par défaut** basée sur la classification (mise à jour critique et mise à jour de sécurité) qui s'applique à tous les ordinateurs ou des groupes d'ordinateurs si vous en avez créés. Activez-la en cochant son nom puis cliquez sur **OK**.
6. Cliquez sur **Exécuter la règle** pour qu'elle s'applique aux mises à jour sur le serveur WSUS.



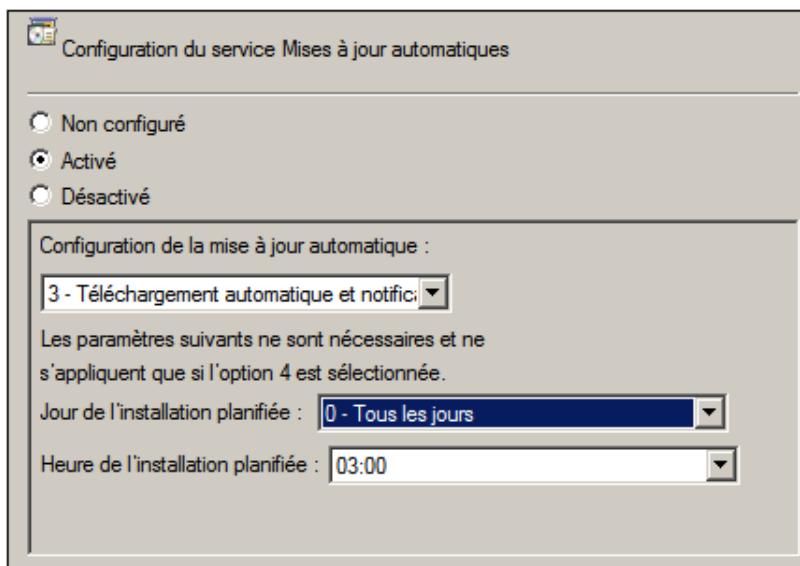
L'approbation est automatique et basée sur une règle.

## 8. Création d'une stratégie de groupes pour les mises à jour

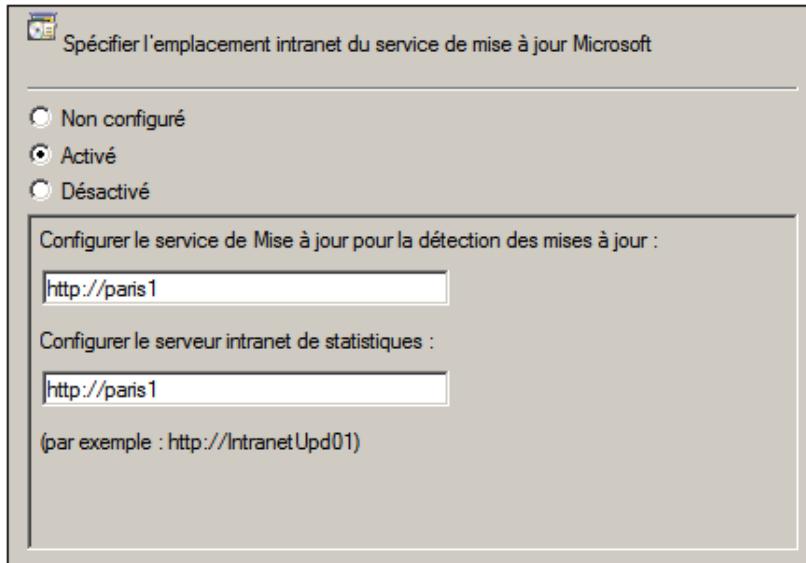
 paris1 est requis.

Vous allez créer une stratégie de groupe applicable uniquement aux ordinateurs du site de Paris afin qu'ils utilisent le serveur WSUS comme serveur de mise à jour.

1. Connectez-vous en tant qu'administrateur sur **paris1**.
2. Démarrez la console **Gestion des stratégies de groupe des Outils d'administration**.
3. Développez l'arborescence jusqu'à **Objets de stratégie de groupe**.
4. Cliquez avec le bouton droit de la souris sur **Objets de stratégie de groupe** puis cliquez sur **Nouveau**.
5. Dans la boîte de dialogue **Nouvel objet GPO**, saisissez **WSUSParis** pour le nom puis cliquez sur **OK**.
6. Dans la zone de détail, cliquez avec le bouton droit de la souris sur **WSUSPARIS** puis cliquez sur **Modifier**.
7. Dans l'**éditeur de gestion des stratégies de groupe**, développez **Configuration ordinateur - Modèles d'administration - Composants Windows - Windows Update**.
8. Modifiez les paramètres de stratégies suivants : Configuration du service Mises à jour automatiques comme le montre l'image suivante.



Spécifiez l'emplacement intranet du service de mise à jour Microsoft comme le montre l'image suivante :



1. Fermez l'**éditeur de gestion des stratégies de groupe**, vous pouvez également modifier d'autres paramètres mais ceux-ci ne sont pas utiles dans cet exercice.
2. Dans **Gestion de stratégie de groupe**, développez l'arborescence jusqu'au **Sites**.
3. Cliquez avec le bouton droit de la souris sur **Sites** puis cliquez sur **Afficher les sites**.
4. Dans la boîte de dialogue **Afficher les sites**, sélectionnez **Geneve** et **Paris**.
5. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Paris** puis cliquez sur **Lier un objet de stratégie de groupe existant**.
6. Dans la boîte de dialogue **Sélectionner un objet GPO**, sélectionnez **WSUSPARIS**.
7. Fermez la console **Gestion de stratégie de groupe**.

➤ La stratégie de groupe redirigeant les ordinateurs du site de Paris à utiliser le serveur WSUS est créée.

## 9. Déploiement de la stratégie de groupe

➤ paris1 et paris2 sont requis.

Vous allez déployer la stratégie de groupe applicable uniquement aux ordinateurs du site de Paris afin qu'ils utilisent le serveur WSUS comme serveur de mise à jour.

1. Connectez-vous en tant qu'administrateur sur **paris2**.
2. Dans une invite de commande, saisissez `gpupdate /force`.
3. Dans une invite de commande, saisissez `gpresult /v > t`.
4. Dans une invite de commande, saisissez `notepad t` et recherchez pour l'ordinateur si la stratégie WSUSPARIS est appliquée et si les paramètres du modèle d'administration sont également appliqués.
5. Pour forcer la mise à jour du serveur paris2 saisissez `wuauctl.exe /detectnow` dans une invite de commande sinon attendez au minimum 20 minutes. Généralement il faut quelques heures pour que l'ordinateur client soit synchronisé. En production, vous pouvez également ouvrir Windows Update et voir qu'il y a plusieurs mises à jour à installer. Dans cet exercice, vous ne pouvez pas ouvrir Windows Update car paris2 n'a pas accès à Internet.

➤ La stratégie est déployée.

## 10. Contrôle des mises à jour installées

- paris1 et paris2 sont requis.

Vous allez contrôler que paris2 est apte à recevoir les mises à jour approuvées sur le serveur WSUS.

1. Connectez-vous en tant qu'administrateur sur **paris1**.
2. Démarrer la console **Microsoft Windows Server Update Services 3.0 SP1 de groupe** des Outils d'administration.
3. Dans l'arborescence, développez **Ordinateurs** puis **Tous les ordinateurs** ; dans la zone de détail vous devrez voir quelque chose de similaire à l'image suivante. Il n'y a pas d'erreurs car les mises à jour sont bien visibles mais elles n'ont pas été installées.

Tous les ordinateurs (3 ordinateurs sur 3 affichés, 3 au total)				
État :	Toutes			
	Nom	Adresse IP	Système d'exploitation	Pourcentage mises à jour installée...
!	paris1.mydom.eni	fe80::8550:4055:3f34:4f6...	Windows Server 2008 Enterpr...	99% 1...
!	paris2.mydom.eni	10.1.1.2	Windows Server 2008 Enterpr...	99% 1...

- Si vous sélectionnez un ordinateur, vous pouvez afficher un rapport détaillé sur les mises à jour installées ou à installer pour cet ordinateur pour autant que Report Viewer Redistributable 2005 soit installé.

- Pour faciliter la gestion vous pouvez créer des groupes d'ordinateurs et déplacer les ordinateurs en modifiant leur appartenance. Les règles d'approbations automatiques permettent également de gérer ces groupes d'ordinateurs.

- Vous avez vu comment il est possible de visualiser les mises à jour installées sur les ordinateurs.

- Cet exercice vous a montré comment mettre en œuvre WSUS dans une entreprise.

- Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

# Exercice 13 - Optimisation et surveillance

## 1. Objectifs

Dans cet exercice vous allez rediriger les événements vers un serveur dans le but de disposer d'une gestion centralisée. Ensuite, lors de la réception d'un événement spécifique, vous allez configurer le gestionnaire des tâches pour déclencher une action. À l'aide de logiciels tiers, vous allez récupérer des informations à l'aide du protocole SNMP.

## 2. Configuration de l'environnement

- Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.
- Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.
- Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt**, doit se trouver sur le Bureau). Après le redémarrage de **paris1**, vous pouvez continuer le lancement des scripts sur les autres ordinateurs.
- Sur **paris2**, après avoir placé le fichier **scriptParis2.bat**, exécutez-le.
- Sur **geneve1**, après avoir placé le fichier **scriptgeneve1.bat**, exécutez-le.
- Sur **geneve2**, après avoir placé le fichier **scriptgeneve2.bat**, exécutez-le après le redémarrage de **geneve1**.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt mydom.eni ainsi que serveur DNS. Il agit également en tant que routeur. Ses adresses IP sont 10.1.1.1/24 sur le segment paris et 172.30.1.1/24 sur le segment Internet.

**paris2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.1.1.2/24).

**geneve1** est membre du domaine **mydom.eni**. Il est également routeur et dispose d'adresses IP fixes soit 192.168.1.1/24 sur le segment geneve et 172.30.1.2/24 sur le segment Internet.

**geneve2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe soit 192.168.1.2/24 sur le segment geneve.

## 3. Référence par rapport à la théorie

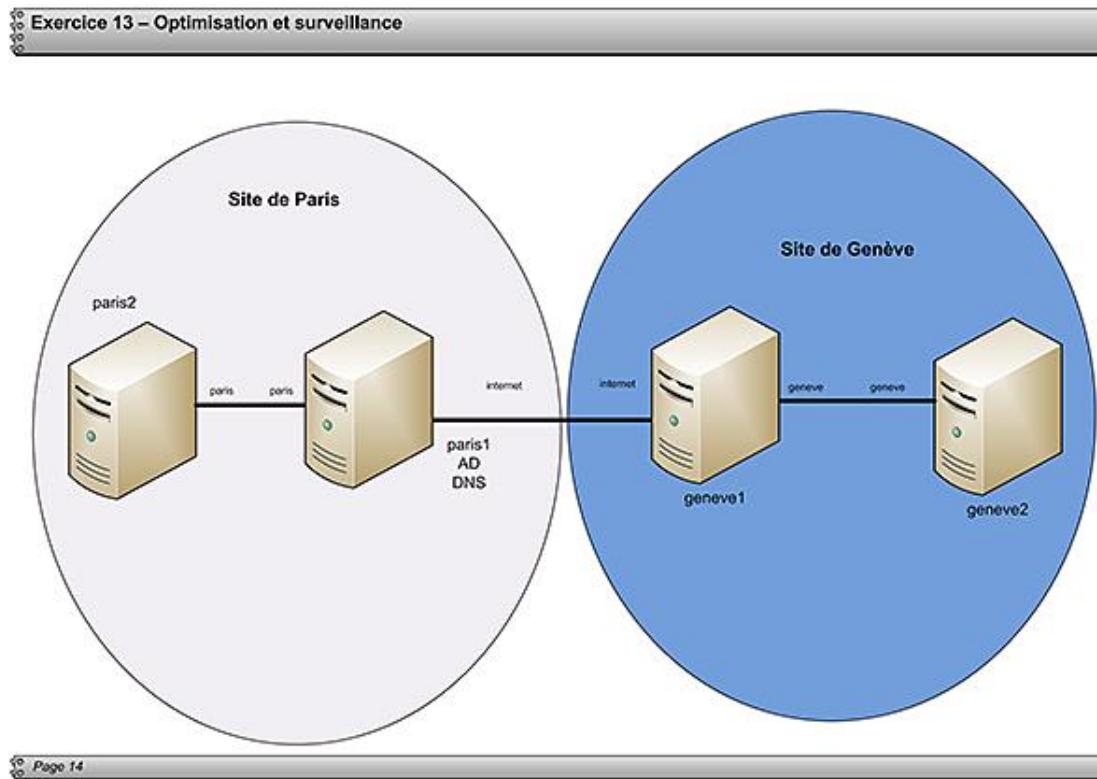
Vous pouvez vous référer au chapitre Gestion et surveillance d'une infrastructure réseau. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour l'optimisation et la surveillance

Il a été décidé de centraliser les événements de **paris2** et **geneve1** sur **paris1** puis de créer des vues sans l'observateur d'événements pour gérer ces différents ordinateurs. Afin d'être proactif, il faut démarrer une tâche planifiée lorsqu'une tentative de connexion échoue. Concernant la surveillance, plusieurs options doivent être

explorées dont la surveillance via SNMP. Pour cela, sur le site de Paris, il faut activer le protocole SNMP et utiliser un outil de gestion.

L'environnement est le suivant :



Les tâches à effectuer sont :

- Préparer paris1 à recevoir les événements.
- Rediriger les événements de paris2 vers paris1.
- Rediriger les événements de geneve1 vers paris1.
- Créer des vues personnalisées pour afficher les événements provenant de paris2 et geneve1.
- Créer une tâche planifiée déclenchée par un événement.
- Installer SNMP sur les ordinateurs du site de Paris.
- Installer un outil de gestion SNMP.
- Retrouver des informations via SNMP.

## 5. Configurer paris1 pour recevoir les événements

paris1 est requis.

1. Connectez-vous en tant qu'administrateur sur paris1.
2. Dans une invite de commande, saisissez wecutil qc.
3. Saisissez o pour Oui.



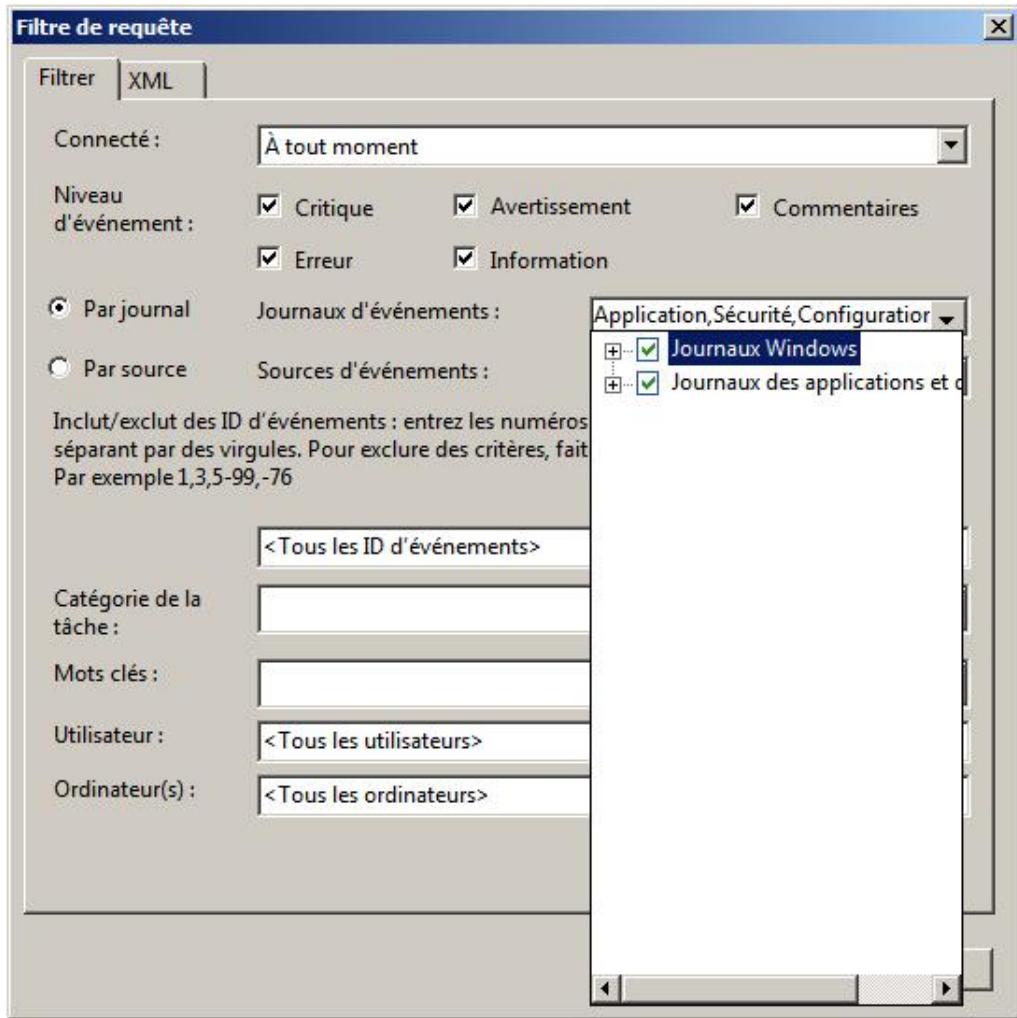
Le collecteur est configuré.

## 6. Rediriger les événements de paris2 vers paris1



paris1 et paris2 sont requis.

1. Connectez-vous en tant qu'administrateur sur paris2.
2. Dans une invite de commande saisissez `winrm quickconfig`.
3. Saisissez `y` pour Oui.
4. Ouvrez le **Gestionnaire de Serveur** puis développez **Configuration et Utilisateurs et groupes locaux**.
5. Ajoutez au groupe local **Administrateurs** l'ordinateur paris1. Pour cela, n'oubliez pas d'inclure **Ordinateurs** au type d'objets.
6. Connectez-vous en tant qu'administrateur sur paris1.
7. Ouvrez l'Observateur d'événements.
8. Cliquez avec le bouton droit de la souris sur **Abonnements** puis sur **Créer un abonnement**.
9. Dans la boîte de dialogue **Propriétés de l'abonnement**, saisissez Paris2Event pour le nom, le journal de destination doit être **Événements transmis**. Sélectionnez l'option **Initialisation par le collecteur**, puis cliquez sur **Sélectionner des ordinateurs**. Dans la boîte de dialogue, sélectionnez **paris2**. Sélectionnez les événements à recueillir en cliquant sur **Sélectionner des événements**.
10. Configurez la boîte de dialogue comme le montre l'image ci-dessous. Tous les événements seront récupérés puis cliquez sur **OK**.



1. Cliquez sur **OK**. La transmission des événements utilise les valeurs par défaut soit un délai de transmission de 15 minutes pour transmettre au maximum quinze événements.

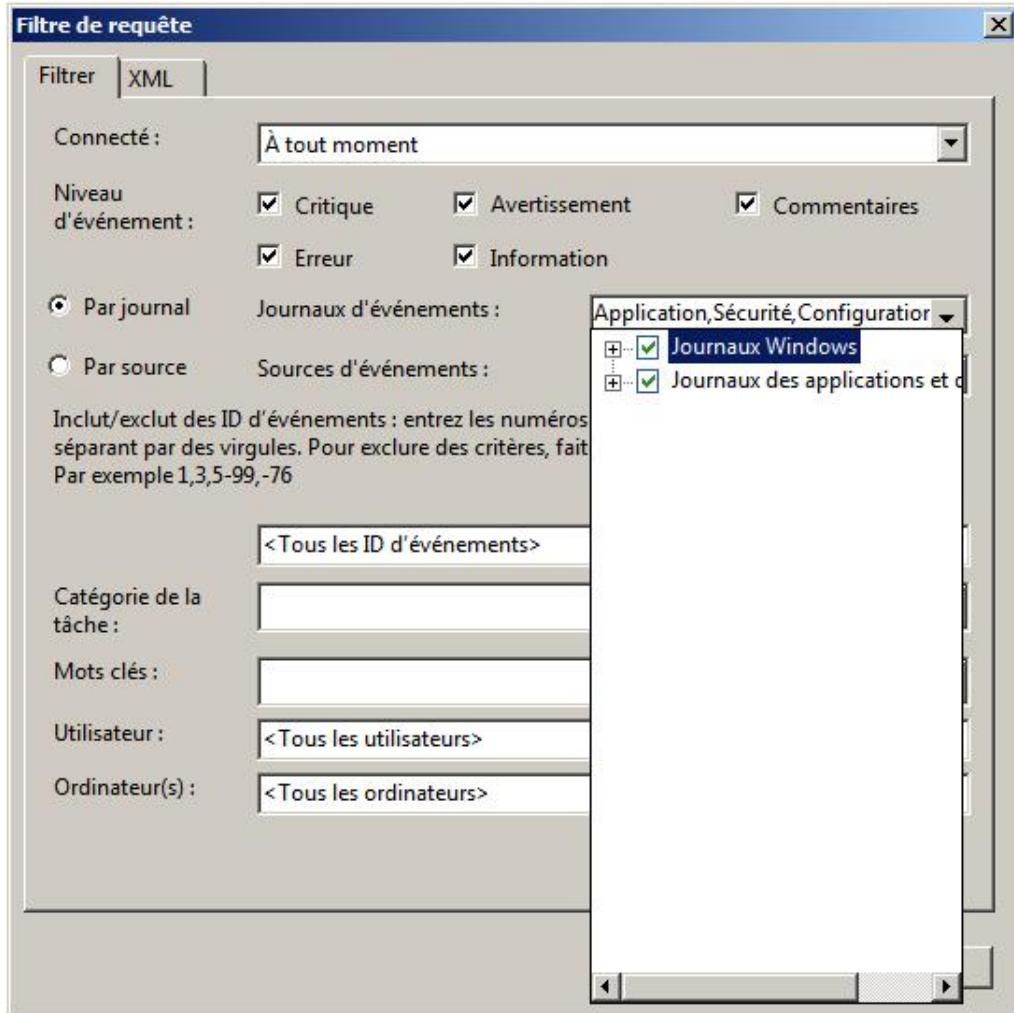
 Les événements de paris2 sont centralisés vers paris1. Le même événement existe maintenant sur les deux ordinateurs.

## 7. Rediriger les événements de geneve1 vers paris1

 paris1 et geneve1 sont requis.

1. Connectez-vous en tant qu'administrateur sur geneve1.
2. Dans une invite de commande saisissez `winrm quickconfig`.
3. Saisissez `y` pour Oui.
4. Ouvrez le **Gestionnaire de Serveur** puis développez **Configuration et Utilisateurs et groupes locaux**.
5. Ajoutez au groupe local **Administrateurs** l'ordinateur paris1. Pour cela, n'oubliez pas d'inclure **Ordinateurs** au type d'objets.
6. Connectez-vous en tant qu'administrateur sur paris1.
7. Ouvrez l'Observateur d'événements

8. Cliquez avec le bouton droit de la souris sur **Abonnements** puis sur **Créer un abonnement**.
9. Dans la boîte de dialogue **Propriétés de l'abonnement**, saisissez GeneveEvent pour le nom, le journal de destination doit être **Événements transmis**. Sélectionnez l'option **Initialisation par le collecteur** puis cliquez sur **Sélectionner des ordinateurs**. Dans la boîte de dialogue, sélectionnez **geneve1**. Sélectionnez les événements à recueillir en cliquant **Sélectionner des événements**,
10. Configurez la boîte de dialogue comme le montre l'image ci-dessous. Tous les événements seront récupérés puis cliquez sur **OK**.



1. Cliquez sur **Avancé** et sélectionnez **Minimiser la latence** puis cliquez sur **OK**.
2. Cliquez sur **OK**.

## 8. Crédit d'une tâche planifiée basée sur un événement

 paris1 est requis.

Vous allez rechercher un échec d'ouverture de session caractérisé par l'événement 4625 puis lancer un script qui va écrire un fichier sur le Bureau.

1. Si ce n'est pas déjà le cas, fermez votre session et tentez de vous connecter avec un nom d'utilisateur ou un mot de passe non reconnu.
2. Connectez-vous en tant qu'administrateur.

3. Ouvrez l'**observateur d'événements**.
4. Ouvrez le journal **Sécurité** sous **Journaux Windows**.
5. Recherchez et sélectionnez un événement portant l'ID 4625.
6. Cliquez avec le bouton droit de la souris sur cet événement puis cliquez sur **Joindre une tâche à cet événement**.
7. Dans l'assistant **Créer une tâche**, sur la page **Créer une tâche de base**, saisissez **Erreur 4625** pour le nom puis cliquez sur **Suivant**.
8. Sur la page **Lors de l'enregistrement d'un**, cliquez sur **Suivant**.
9. Sur la page **Action**, sélectionnez **Démarrer un programme** puis cliquez sur **Suivant**.
10. Sur la page **Démarrer un programme**, saisissez **c:\action.vbs** puis cliquez sur **Suivant**.
11. Sur la page **Terminer**, relisez vos paramètres puis cliquez sur **Terminer**.
12. Cliquez sur **OK** dans le message qui vous indique que pour toute modification vous devez passer par le planificateur de tâche.
13. Pour effectuer un test, verrouillez la session puis tentez de la rouvrir en utilisant un mauvais mot de passe puis ouvrez votre session, le fichier doit être créé.

---

 Une tâche planifiée répond à votre événement.

---

## 9. Gestion des événements

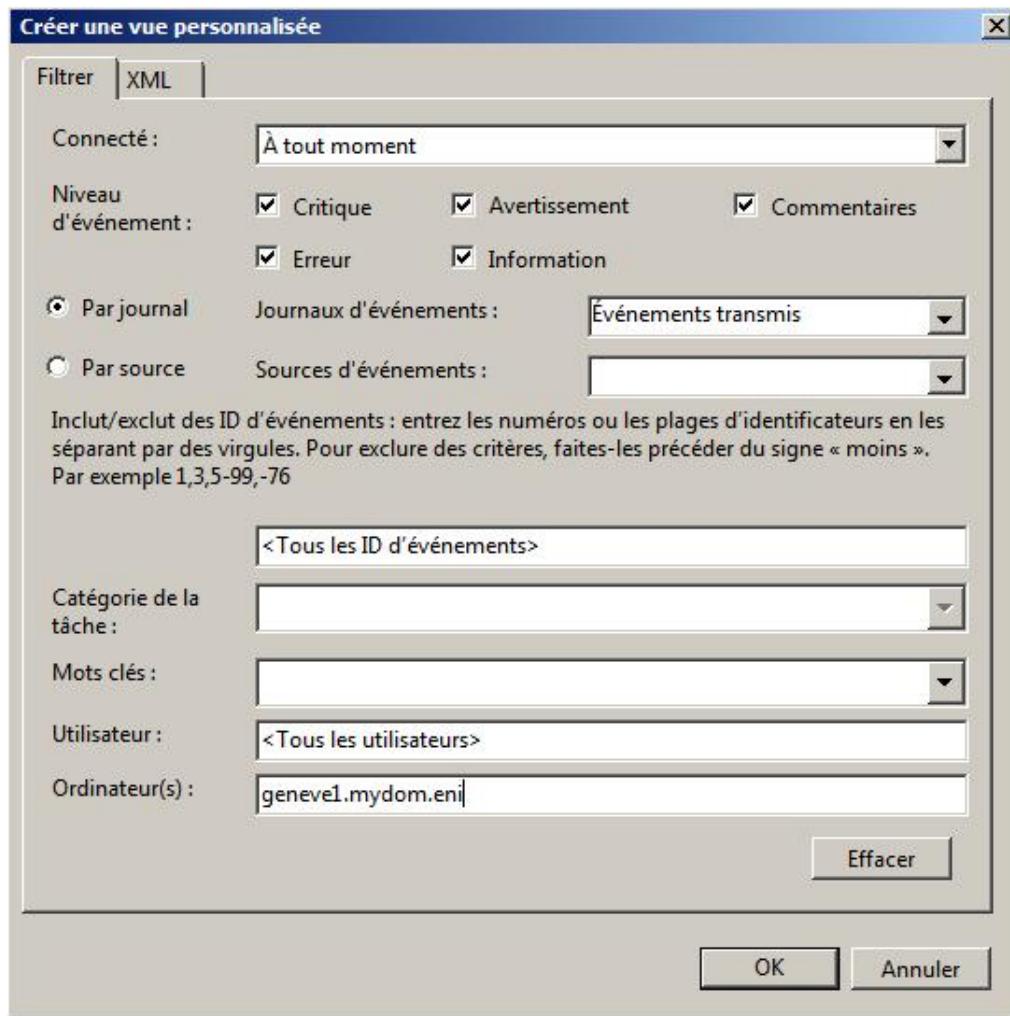
---

 paris1 et geneve1 sont requis.

---

Vous allez créer une vue personnalisée pour améliorer la lisibilité des événements du journal **Événements transmis** provenant de l'ordinateur geneve1.

1. Connectez-vous en tant qu'administrateur sur le serveur paris1.
2. Ouvrez la console **Observateur d'événements** des **Outils d'administration**.
3. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Affichages Personnalisés** puis cliquez sur **Créer une vue personnalisée**.
4. Dans la boîte de dialogue **Créer une vue personnalisée** modifiez les valeurs comme montré sur l'image suivante puis cliquez sur **OK**.



1. Saisissez **Événements de Genève1** pour le nom puis cliquez sur **OK**. La vue personnalisée s'ouvre et elle est filtrée comme définie.

➤ Vous venez de créer une vue personnalisée.

## 10. Installation de la fonctionnalité SNMP sur geneve1 et geneve2

➤ paris1, geneve1 et geneve2 sont requis.

La procédure suivante pour installer la fonctionnalité SNMP est à effectuer sur geneve1 et geneve2.

1. Connectez-vous en tant qu'administrateur sur le serveur considéré.
2. Démarrez le **Gestionnaire de serveur** des **Outils d'administration**.
3. Ajoutez le rôle **Services SNMP**.

➤ SNMP est installé sur geneve1 et geneve2.

## 11. Configuration du service SNMP

➤ paris1, geneve1 et geneve2 sont requis.

---

La procédure suivante pour configurer SNMP est à effectuer sur geneve1 et geneve2.

1. Connectez-vous en tant qu'administrateur sur le serveur considéré.
2. Démarrez la console **Services** des Outils d'administration.
3. Avec le bouton droit de la souris, cliquez sur **Service SNMP** puis sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés** sous l'onglet **Général**, garantissez que le type de démarrage est **Automatique** et que le service a démarré.
5. Dans la boîte de dialogue **Propriétés** sous l'onglet **Agent**, saisissez vos prénom et nom pour le contact puis indiquez un emplacement, enfin sélectionnez toutes les cases à cocher sous la zone **Service**.
6. Dans la boîte de dialogue **Propriétés** sous l'onglet **Interruptions**, saisissez **public** pour le nom de la communauté et cliquez sur **Ajouter à la liste**. Ensuite cliquez sur **Ajouter** pour ajouter l'adresse IP de paris1 soit 10.1.1.1.
7. Dans la boîte de dialogue **Propriétés**, sous l'onglet **Sécurité**, cliquez sur **Ajouter** dans la zone **Noms de communautés acceptées**. Puis ajoutez **public** comme nom de la communauté avec comme droit **LECTURE ECRITURE**.
8. Dans la boîte de dialogue **Propriétés** sous l'onglet **Sécurité**, cliquez sur **Ajouter** dans la zone **Accepter les paquets SNMP provenant de ces hôtes**. Puis ajoutez le nom paris1, et non pas son adresse IP.
9. Dans la boîte de dialogue **Propriétés**, cliquez sur **OK**.

- 
-  Le service SNMP est configuré sur geneve1 et geneve2.
- 

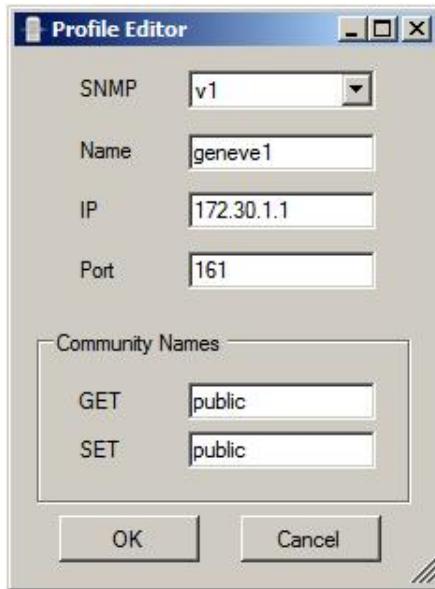
## 12. Utilisation d'un navigateur SNMP

---

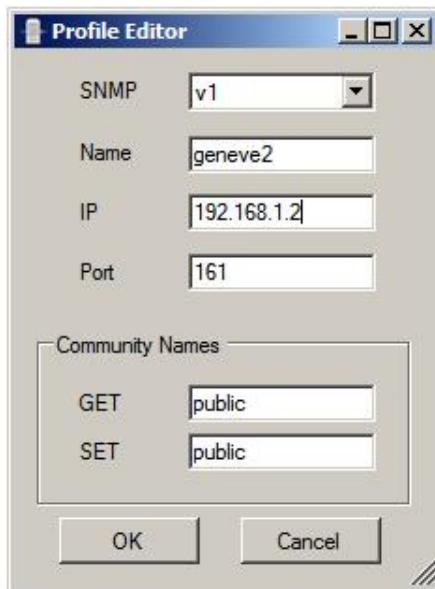
-  paris1, geneve1 et geneve2 sont requis.
- 

Pour consulter les informations provenant des ordinateurs en utilisant SNMP, il est nécessaire d'utiliser un outil comme snmputil. Malheureusement cet outil n'est pas très convivial. Il serait alors possible d'utiliser un outil tiers mais souvent ceux-ci sont payants et dépassent largement les fonctionnalités utilisées pour cet exercice. Vous allez donc télécharger depuis le site de Microsoft [www.codeplex.com](http://www.codeplex.com) l'outil crossroad qui est un explorateur SNMP, et l'utiliser pour explorer les informations contenues sur geneve1 et geneve2.

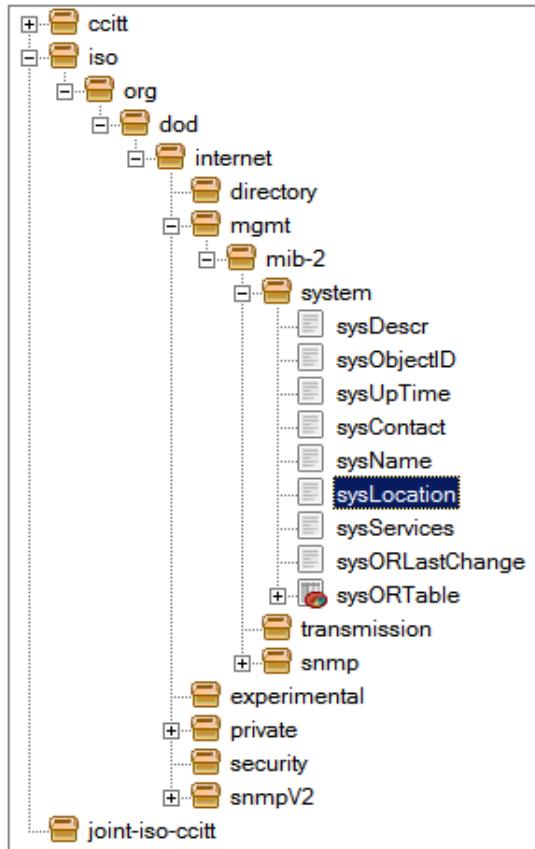
1. Téléchargez **crossroad** du site [www.codeplex.com](http://www.codeplex.com).
2. Connectez-vous en tant qu'administrateur sur paris1
3. Extrayez le contenu du fichier zip de crossroad sur le Bureau.
4. Dans le répertoire de **crossroad**, double cliquez sur **Browser**.
5. L'application se lance. Dans la zone de gauche, cliquez sur le bouton **Add**.
6. Modifiez la boîte de dialogue **Profile editor** comme le montre l'image suivante pour geneve1.



1. Faites de même pour geneve2.



1. Dans la liste de gauche, sélectionnez **geneve1** puis cliquez sur **Set Default**.
2. Dans la zone de détail, développez l'arborescence comme le montre l'image suivante.



1. Sélectionnez le nœud **sysName**, dans la zone **Output** vous devriez voir apparaître le nom **geneve1**.
2. Sélectionnez d'autres nœuds et regardez les valeurs trouvées.
3. Cliquez avec le bouton droit de la souris sur **Syslocation** puis cliquez sur **Set**.
4. Dans la boîte de dialogue **Set**, saisissez Bureau 15 de la rue des bains dans **New Value** puis cliquez sur **OK**.
5. Sur **geneve1**, ouvrez les propriétés du service du **service SNMP** puis sous l'onglet **Agent**, contrôlez que l'emplacement a changé.
6. Sur **paris1**, dans **crossroad**, dans la liste de gauche, sélectionnez **geneve2** puis cliquez sur **Set Default** et ensuite cliquez sur **Sysname** dans la zone de détail.

Vous avez utilisé un outil pour explorer, voire modifier la base MIB contenue sur geneve1 et geneve2.

Dans cet exercice vous avez vu comment centraliser des événements et gérer le protocole SNMP. Ces deux éléments vous permettent d'optimiser la gestion de vos ordinateurs sans utiliser d'outils plus complexes. Bien entendu, leur utilisation est idéale dans des environnements simples.

Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

# Exercice 12 - Mise en œuvre d'un système de serveur de fichiers

## 1. Objectifs

Dans cet exercice vous allez configurer, maintenir et utiliser un système de clichés instantanés. Ensuite, vous allez mettre en œuvre des fichiers hors connexion et gérer la synchronisation. La mise en œuvre des fichiers EFS concerne le point suivant. Enfin vous allez installer le rôle de serveur de fichiers pour gérer les permissions NTFS et de partage, les quotas et l'utilisation d'une racine DFS.

## 2. Configuration de l'environnement

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes.

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt** doit être placé sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres serveurs.
- Sur **paris2**, lancez le script **scriptParis2.bat**.
- Sur **paclient1**, lancez le script **paclient1.bat** (le fichier **joindom.vbs** doit être placé sur le Bureau).
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**.
- Sur **geneve2**, lancez le script **scriptGeneve2.bat** lorsque le serveur **geneve1** aura redémarré.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt mydom.eni ainsi que serveur DNS et routeur. Ses adresses sont 10.1.1.1/24 en interne et 172.30.1.1/24 pour le côté Internet.

**paris2** est membre du domaine mydom.eni et son adresse IP est 10.1.1.2/24.

**paclient1** est membre du domaine mydom.eni et son adresse IP est 10.1.1.3/24.

**geneve1** est membre du domaine mydom.eni, il est également routeur. Ses adresses sont 172.30.1.2/24 sur le côté Internet et 192.168.1.1/24 en interne.

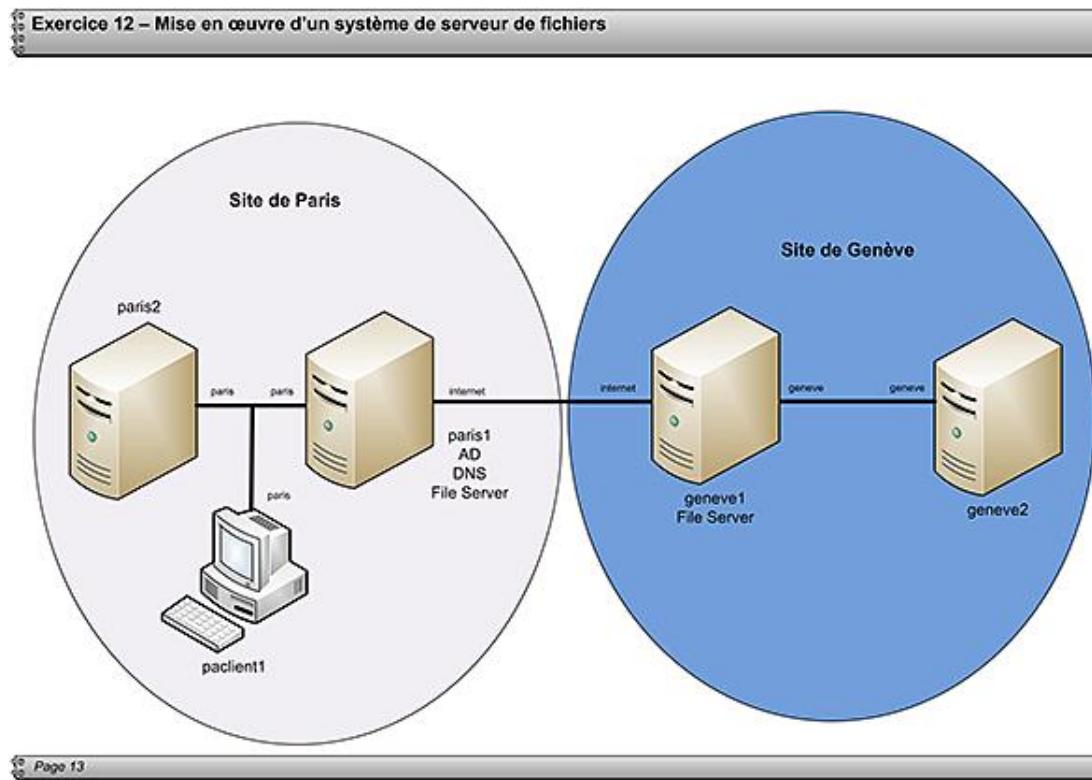
**geneve2** est membre du domaine mydom.eni et son adresse est 192.168.1.2/24.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer principalement au chapitre Mise en œuvre du serveur de fichiers. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre d'un système de serveur de fichiers

Il a été déterminé que les technologies utilisées pour gérer les fichiers ne sont pas optimales actuellement. Avant de prendre une décision sur l'implémentation de telle ou telle technologie, il vous est demandé d'effectuer un rapport sur les avantages et les désavantages pour l'implémentation des différentes technologies de gestion des fichiers. À cet égard, un bac à sable est créé dont la topologie est la suivante.



Les tâches suivantes sont à effectuer :

- Création de deux dossiers partagés appelés **Ventes** et **Marketing** sur **paris1**. Les utilisateurs du domaine doivent pouvoir effectuer des modifications.
- Mise en œuvre et test des clichés instantanés.
- Mise en œuvre et test des fichiers hors connexion.

## 5. Crédation et partage de deux dossiers en y appliquant des permissions

Seul paris1 est requis.

Vous allez créer deux répertoires appelés Ventes et Marketing qui seront partagés avec les mêmes noms. Il faut également modifier les permissions pour que les utilisateurs du domaine aient l'autorisation de modification à l'intérieur des dossiers.

### a. Crédation des dossiers

1. Sur **paris1**, créez les deux répertoires suivants :

- c:\Markteting
- c:\Ventes

### b. Partage des dossiers

1. Cliquez avec le bouton droit de la souris sur le dossier **Ventes** puis sur **Propriétés**.
2. Cliquez sur **Partage avancé** de l'onglet **Partage**.
3. Sur **Partage avancé**, cochez **Partager ce dossier** puis sur **Autorisations**.
4. Dans la boîte de dialogue **Autorisations** supprimez le groupe **Tout le monde** et ajoutez le groupe **Utilisateurs authentifiés** avec **Modifier comme autorisations**.
5. Fermez les boîtes de dialogue. Et refaites de même pour le dossier **Marketing**.

### c. Modifications des permissions NTFS

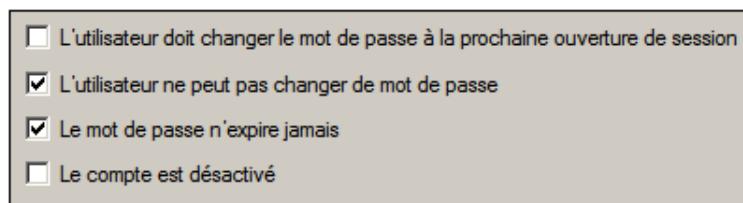
1. Cliquez avec le bouton droit de la souris sur le dossier **Ventes** puis sur **Propriétés**.
2. Cliquez sur **Partage avancé** de l'onglet **Sécurité**.
3. Cliquez sur **Modifier**.
4. Dans la boîte de dialogue **Autorisations pour Marketing**, sélectionnez le groupe **Utilisateurs (MYDOM\Utilisateurs)**, cochez **Modification (Autoriser)** puis cliquez sur **OK**.
5. Fermez les boîtes de dialogue. Et refaites de même pour le dossier **Marketing**.

 Vous venez de créer et de partager deux dossiers. Les permissions ont été mises à **Modifier** pour le groupe Utilisateurs au niveau NTFS et **Utilisateurs authentifiés** pour le partage.

## 6. Crédit d'utilisateurs

 Seul paris1 est requis.

- Connectez-vous en tant qu'**administrateur** sur **paris1**.
- Ouvrez la console **Utilisateurs et ordinateurs Active Directory** des Outils d'administration.
- Développez l'arborescence **mydom.eni**.
- Cliquez avec le bouton droit de la souris sur le conteneur **Users** puis sur **Nouveau-> Utilisateur**.
- Dans l'assistant **Nouvel objet - Utilisateur**, saisissez **toto** pour le Prénom, le nom, le Nom d'ouverture de session de l'utilisateur et le Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) puis cliquez sur **Suivant**.
- Sur la page suivante, saisissez **Pa\$\$word** pour le mot de passe et sa confirmation. Ensuite modifiez les cases à cocher comme montré sur l'image suivante.



- Enfin, cliquez sur **Suivant**, puis sur **Terminer**.

- Refaites la procédure pour l'utilisateur **titi**.

► Les utilisateurs toto et titi ont été créés.

## 7. Mise en œuvre des clichés instantanés pour le site de Paris

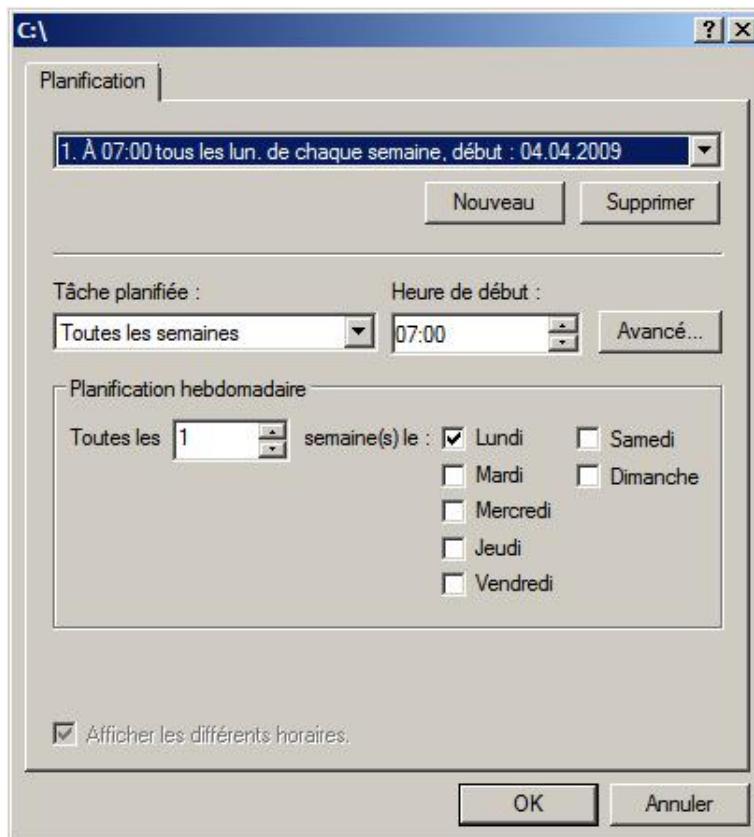
► Les ordinateurs **paris1** et **paris2** sont requis. La mise en œuvre se fait sur **paris1** et les tests à partir de **paris2**.

Dans ce scénario, vous allez mettre en œuvre les clichés instantanés pour le serveur **paris1**, et effectuer des tests avec le client **paris2**.

### a. Configuration des clichés instantanés

1. Sur **paris1**, lancez la console **Gestion de l'ordinateur**.
2. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Dossiers partagés** puis **Toutes les tâches - Configurer les clichés instantanés**.
3. Dans la boîte de dialogue **Clichés instantanés**, cliquez sur **Paramètres**.
4. Dans la boîte de dialogue **Paramètres**, cliquez sur **Planification**. C'est la seule modification qui va se faire car votre ordinateur ne dispose que d'un seul disque dur.
5. Dans la boîte de dialogue de **Planification**, modifiez les valeurs de manière à ce que la tâche planifiée démarre tous les jours exceptés le week-end à 6h00 et s'arrête à 21h00 en répétant la tâche toutes les heures.

Modifiez la boîte comme sur la figure suivante puis cliquez sur **Nouveau**.



1. Sélectionnez votre planification, normalement elle se trouve en troisième position dans la liste déroulante, puis cliquez sur **Avancé**.
2. Sur la boîte de dialogue **Options avancées de planification**, modifiez la boîte comme montré dans la figure suivante puis cliquez trois fois sur **OK**.



1. La tâche est planifiée et les clichés instantanés sont déjà activés. Vous allez créer manuellement le premier cliché instantané en cliquant sur **Créer**.
2. Laissez la console ouverte.

 Vous venez de configurer les clichés instantanés au niveau du serveur.

## b. Test de fonctionnement des clichés instantanés

En tant qu'utilisateur de l'ordinateur paris2, vous sauvegardez et modifiez des documents sur le répertoire Ventes. Régulièrement, vous allez démarrer la création des clichés instantanés afin de réduire la durée du scénario. Ensuite, vous verrez comment retrouver l'état d'un document ou d'un dossier selon l'état du cliché instantané.

1. Sur **paris2**, connectez-vous en tant qu'administrateur de domaine, puis saisissez \\paris1\Ventes dans la zone **Rechercher** du menu **Démarrer**.
2. Créez successivement les documents suivants :
  - **MonImage** de type Bitmap.
  - **MesVentes** de type document texte.
  - **Ventes2009** de type document texte.
3. Sur **paris1**, dans la boîte de dialogue **Clichés instantanés**, cliquez sur **Créer**.
4. Sur **paris2**, ouvrez **MesVentes** et modifiez le document, veillez à ce que la dernière ligne soit **Lundi, il faut que je recontacte le prospect X**. N'oubliez pas de sauvegarder le document.
5. Ajoutez de nouveaux documents selon vos envies.
6. Sur **paris1**, dans la boîte de dialogue **Clichés instantanés**, cliquez sur **Créer**.
7. Sur **paris2**, ouvrez **MesVentes** et modifiez le document après la dernière ligne créée. N'oubliez pas de sauvegarder le document.
8. Supprimez et créez également d'autres documents.

9. Sur **paris1**, dans la boîte de dialogue **Clichés instantanés**, cliquez sur **Créer**.
10. Sur **paris2**, supprimez le document **MesVentes**.

Votre document **MesVentes** n'est plus disponible. Comme le document n'est plus disponible, vous ne pouvez pas le sélectionner pour retrouver ses versions précédentes. En lieu et place, il faut le faire pour le dossier partagé.

  1. Sur **paris2**, dans le dossier \\paris1\Ventes, cliquez avec le bouton droit de la souris dans la zone libre puis sur **Propriétés**.
  2. Sélectionnez l'onglet **Version précédentes** puis la version la plus ancienne en se basant sur la date, et cliquez sur **Ouvrir**. Vous retrouvez l'état du dossier au moment de la création du premier cliché instantané.
  3. Recommez l'opération en utilisant la version actuelle du dossier pour faire apparaître l'état du dossier pour chaque cliché instantané.
  4. Pour chaque état du dossier, regardez l'évolution des documents ainsi que le contenu du document **MesVentes**.

Vous pouvez maintenant récupérer le document **MesVentes** à l'instant qui vous intéressait en utilisant le glissé-déplacé.

 Vous avez vu la mise en œuvre des clichés instantanés et une méthode pour retrouver un document effacé.

## 8. Mise en œuvre des fichiers hors connexion pour un utilisateur d'ordinateur portable du site de Paris

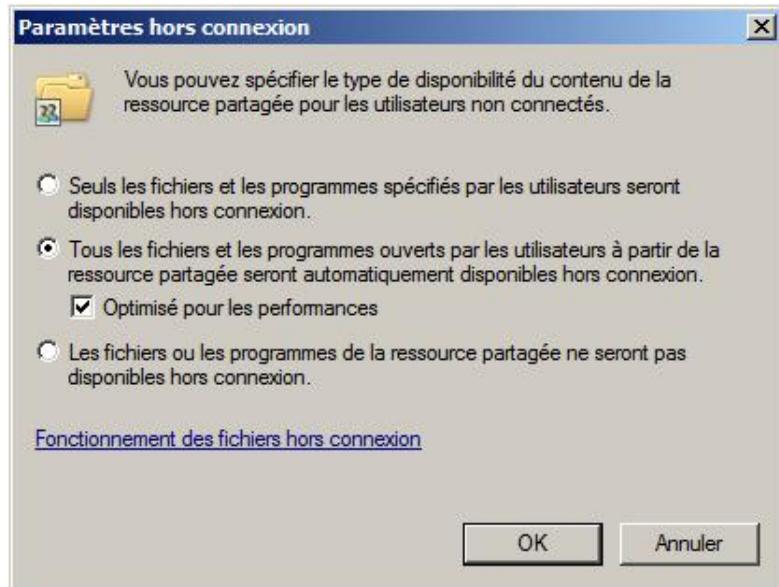
Dans ce scénario vous allez simuler le fonctionnement d'un ordinateur portable avec **paclient1** qui se connecte au partage **Marketing** de **paris1**. Il est nécessaire que les documents dudit dossier puissent être consultés et modifiés hors connexion. De plus, si certains documents sont modifiés sur le serveur et le client, il faut gérer manuellement les conflits.

### a. Mise en œuvre des fichiers hors connexion sur le serveur paris1

 Seul le serveur paris1 est requis.

Vous devez permettre la mise en cache automatique de tous les documents ouverts par l'utilisateur dans le dossier marketing.

- Connectez-vous en tant qu'administrateur sur **paris1**.
- Ouvrez l'explorateur pour faire apparaître le dossier **Marketing** (c:\Marketing).
- Cliquez avec le bouton droit de la souris sur le dossier **Marketing** pour faire apparaître le menu contextuel puis cliquez sur **Propriétés**.
- Dans la boîte de dialogue **Propriétés de marketing**, sélectionnez l'onglet **Partage** puis cliquez sur **Partage avancé**.
- Dans la boîte de dialogue **Partage avancé**, cliquez sur **Mise en cache**.
- Dans la boîte de dialogue **Paramètres hors connexion**, sélectionnez l'option comme indiqué sur l'image suivante.



- Cliquez deux fois sur **OK**.
- Cliquez sur **Fermer**.

► paris1 permet la mise en cache automatique des fichiers ouverts par les utilisateurs.

### b. Mise en œuvre des fichiers hors connexion sur le client paclient1

- Seul le serveur paclient1 est requis.
- Connectez-vous sur le serveur **paris2** en tant qu'utilisateur **toto**.
- Ouvrez le **Panneau de configuration** (mode classique).
- Dans le Panneau de configuration, double cliquez sur **Fichiers hors connexion**.
- Pour autoriser les fichiers hors connexion, il est nécessaire de disposer des droits d'administration, ce qui n'est pas le cas d'un utilisateur standard. Normalement, il serait préférable d'utiliser une stratégie de groupe, mais dans cet exercice, vous allez utiliser le compte d'utilisateur de l'administrateur. Si l'option n'est pas déjà activée, cliquez sur **Autoriser l'utilisation des fichiers hors connexion** et saisissez administrateur pour le nom de l'utilisateur et Pa\$\$word pour le mot de passe lorsqu'il vous sera demandé.
- Cliquez sur **OK**.
- Redémarrez **paclient1**.

► Les fichiers hors connexion sont activés pour l'utilisateur toto.

### c. Visualisation des fichiers hors connexion

► Les ordinateurs paris1 et paclient1 sont requis.

- Connectez-vous en tant que toto sur **paclient1**.
- Saisissez \\paris1\Marketing dans la zone **Rechercher** du menu **Démarrer**.
- Créez un nouveau document texte puis modifiez-le en ajoutant un texte que vous sauvegardez.
- Faites de même avec le dossier vente (\\paris1\Ventes).
- Connectez-vous en tant qu'administrateur sur **paris1**.
- Saisissez ncpa.cpl dans la zone **Rechercher** du menu **Démarrer**.
- Désactivez la carte réseau **paris**.
- Patientez quelques instants puis retournez sur l'ordinateur **paris2**.
- Pouvez-vous accéder au partage **Marketing** et éventuellement aux documents s'y trouvant ? Normalement vous pouvez accéder à tout document que vous avez ouvert au préalable et vous pouvez en créer d'autres.
- Faites de même avec le partage **Ventes**. Normalement vous ne pouvez pas y accéder.
- Sur **paris1**, réactivez la carte réseau et attendez quelques instants avant de continuer.

 Vous pouvez créer d'autres scénarios dans lesquels vous créez de nouveaux documents sur paris1 (à partir de paris1) puis désactiver la carte réseau ou supprimer voire modifier un document mais uniquement sur un des deux ordinateurs pour ne pas créer de conflit.

 Pour le dossier Ventes, vous pouvez utiliser le bouton droit de la souris sur un document pour le rendre toujours disponible hors connexion, et voir s'il l'est dès lors réellement ou s'il faut également l'ouvrir pour qu'il soit disponible hors connexion.

- Ouvrez le Panneau de configuration, puis double cliquez sur **Fichiers hors connexion**, enfin cliquez sur **Afficher vos fichiers hors connexion**.
- Développez **Ordinateur** pour voir les fichiers hors connexion.

 Vous avez examiné comment visualiser des documents.

#### d. Création et gestion d'un conflit

 Les ordinateurs paris1 et paclient1 sont requis.

Vous allez créer un document dans le dossier **Marketing** à partir de paclient1 puis vous allez couper la connexion entre paris1 et paclient1. Sur paris1 et paclient1 vous allez modifier le document, puis vous allez réactiver la connexion et synchroniser le dossier.

1. Connectez-vous en tant que toto sur **paclient1**.
2. Saisissez \\paris1\Marketing dans la zone **Rechercher** du menu **Démarrer**.
3. Créez un nouveau document texte puis modifiez-le en ajoutant un texte que vous sauvegardez.
4. Saisissez ncpa.cpl dans la zone **Rechercher** du menu **Démarrer**.

5. Désactivez la carte réseau **paris**.
6. Connectez-vous en tant qu'administrateur sur **paris1**.
7. Sur **paris1**, ouvrez et modifiez le document nouvellement créé.
8. Sur **paclient1**, ouvrez et modifiez le document nouvellement créé.
9. Sur **paris1**, réactivez la carte réseau **paris**. Attendez quelques instants.
10. Sur **paclient1**, dans la barre de notification, un message apparaît quelques instants pour vous signifier un conflit. Cliquez avec le bouton droit de la souris sur l'icône correspondante puis sur **Afficher les conflits**.
11. Dans la section de détail, sélectionnez le fichier puis cliquez sur le bouton **Résoudre**.
12. Dans la boîte de dialogue **Résoudre le conflit**, cliquez sur **Conserver les deux versions**. Au bout de quelques instants, vous verrez apparaître un nouveau document qui contient dans le nom (toto v1). Ce document est également répliqué sur le serveur **paris1**.

---

 Vous avez examiné comment résoudre un conflit avec les fichiers hors connexion.

---

## 9. Sécurisation des fichiers via EFS

 Les ordinateurs **paris1** et **paclient1** sont requis.

Dans ce scénario, vous allez examiner comment plusieurs personnes peuvent se partager un fichier. À partir de **paclient1**, vous allez créer un dossier appelé **Sécurité** sur le partage **Ventes**, puis le chiffrer. Vous allez également créer un dossier appelé **Dosefs** (`c:\Dosefs`) sur **paclient1** et le chiffrer. Sous le compte d'utilisateur titi vous allez tenter d'y accéder, puis sous toto vous aller autoriser titi à accéder aux fichiers chiffrés.

1. Connectez-vous en tant qu'utilisateur toto sur **paclient1**.
2. Sur **paclient1**, créez le dossier **c:\Dosefs** puis chiffrer-le.
3. Ajoutez deux fichiers.
4. À partir de **paclient1**, créez un dossier appelé **Sécurité** sur le partage **\paris1\Ventes** puis chiffrer-le.
5. Ajoutez deux fichiers.
6. Sur **paclient1**, changez d'utilisateur et connectez-vous en tant que titi.
7. Tentez d'accéder aux fichiers du dossier **c:\Dosefs** et **\paris1\Ventes\Sécurité**. Vous ne devriez pas pouvoir y accéder, même si vous les voyez.
8. Pour que titi dispose d'un certificat, il faut chiffrer un fichier car aucune stratégie de groupe n'a été configurée pour créer automatiquement ces certificats. Pour cela, créez un fichier dans **c:\Dosefs**.
9. Revenez sous l'utilisateur toto et sélectionnez un fichier créé par toto localement puis dans la boîte de dialogue **Attributs avancés** de propriétés du fichier, cliquez sur **Détails**.
10. Dans la boîte de dialogue **Accès utilisateur à Votre fichier**, ajoutez l'utilisateur titi ; remarquez que son certificat est un certificat de domaine.
11. Refaites la procédure pour un fichier se trouvant sur le serveur **paris1**.
12. Retournez sous titi et tentez d'y accéder. Cette fois-ci vous y avez accès.

---

 Vous avez vu comment chiffrer et accorder l'accès à un utilisateur.

---

## 10. Mise en œuvre de la sauvegarde et de la récupération d'urgence

---

-  Les ordinateurs paris1 et paris2 sont requis. La mise en œuvre se fait sur paris2.

Dans ce scénario, vous effectuez une sauvegarde du serveur **paris2** puis modifiez la configuration du serveur en ajoutant un rôle. Ensuite vous allez effectuer une récupération d'urgence pour revenir à l'état initial.

### a. Préparation de l'environnement

1. Sur **paris2**, installez la fonctionnalité **Outils d'administration distants**. Cela sert juste à personnaliser le serveur.
2. Sur **paris1**, créez un dossier appelé **Backup** (autorisation NTFS Modifier pour le groupe Utilisateurs). Partagez-le sous le nom Backup (autorisation de partage Modifier pour le groupe Tout le monde).

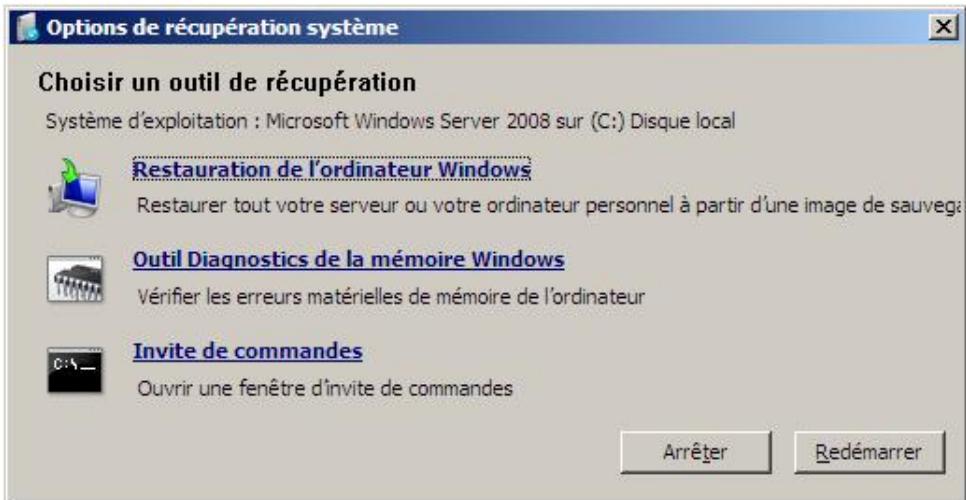
### b. Sauvegarde d'un serveur et modification de la configuration du serveur

1. Sur **paris2**, installez la fonctionnalité **Fonctionnalités de la sauvegarde de Windows Server**.
2. Lancez la **Sauvegarde de Windows Server**.
3. Cliquez sur **Sauvegarde unique** sous **Actions** dans **Sauvegarde de Windows Server**.
4. Dans l'assistant, sur la page **Options de sauvegarde**, sélectionnez **D'autres options**.
5. Sur la page **Sélectionnez la configuration de sauvegarde**, sélectionnez **Serveur Entier**.
6. Sur la page **Spécifiez le type de destination**, sélectionnez **Dossiers partagés distants**.
7. Sur la page **Spécifiez un dossier distant**, saisissez `\\\paris1\backup` et sélectionnez **Hériter** pour le contrôle d'accès.
8. Sur la page **Spécifiez une option avancée**, sélectionnez **Sauvegarde complète VSS**.
9. Sur la page **Confirmation**, contrôlez vos informations avant de démarrer la sauvegarde (prévoyez environ 6 Go d'espace disque).
10. À la fin de la sauvegarde, installez le rôle **Services DHCP**.

-  La sauvegarde complète de votre serveur a été effectuée et des modifications ont été réalisées après celle-ci.
- 

### c. Restauration d'urgence

1. Éteignez le serveur **paris2**. Ensuite démarrez sur l'image ISO ou le DVD de Windows Server 2008.
2. Après avoir entré vos informations linguistiques, cliquez sur **Suivant**.
3. Sur le masque **Suivant**, cliquez sur **Réparer l'ordinateur**.
4. Sur la boîte de dialogue **Options de récupération système**, cliquez sur **Suivant**.
5. Sur la boîte de dialogue suivante, cliquez sur **Invite de commande**. Il faut ajouter une adresse IP manuellement car il n'existe pas de serveur DHCP.



1. Laissez l'invite de commande ouverte puis dans la boîte de dialogue ci-dessus, cliquez sur **Restauration de l'ordinateur Windows**.
2. Sur la boîte de dialogue **Restauration de l'ordinateur Windows**, cliquez sur **Annuler**.
3. Sur la boîte de dialogue **Restaurez tout sur votre ordinateur à partir d'une sauvegarde**, cliquez sur **Suivant**.
4. Sur la page **Sélectionnez l'emplacement de la sauvegarde**, cliquez sur **Avancé**.
5. Sur la boîte de dialogue **Restauration de l'ordinateur Windows**, cliquez sur **Cherchez une sauvegarde réseau**.
6. Sur la boîte de dialogue **Voulez-vous vraiment vous connecter au réseau ?**, cliquez sur **Oui**.
7. Patientez quelques instants jusqu'à ce que la boîte de dialogue **Restauration de l'ordinateur Windows** apparaisse afin que les services réseaux soient démarrés.
8. Saisissez dans l'invite de commande netsh interface ipv4 set address name="Connexion au réseau local" source=static address=10.1.1.10 mask=255.255.255.0 puis netsh interface ipv4 add dnsserver name=" Connexion au réseau local " address=10.1.1.1 enfin net start dnscache.
9. Dans la boîte de dialogue **Restauration de l'ordinateur Windows**, saisissez \\paris1\Backup puis cliquez sur **OK**.
10. Indiquez administrateur pour le nom de l'utilisateur et Pa\$\$word pour le mot de passe, ensuite cliquez sur **OK**.
11. Dans **Sélectionnez l'emplacement de la sauvegarde**, cliquez sur la sauvegarde puis sur **Suivant**.
12. Sélectionnez la sauvegarde en fonction de la date et de l'heure puis cliquez sur **Suivant**.
13. Sur la page **Choisissez comment restaurer la sauvegarde**, cochez **Formater et repartitionner les disques** avant de cliquer sur **Suivant**.
14. Enfin sur la dernière page, prenez quelques instants pour lire les informations avant de cliquer sur **Terminer**.
15. Sur la boîte de dialogue qui apparaît, lisez le message et sélectionnez la case à cocher **Je confirme que je souhaite formater les disques et restaurer la sauvegarde** avant de cliquer sur **OK**.
16. Attendez la fin de la restauration et au redémarrage connectez-vous en tant qu'administrateur.
17. Contrôlez que les outils d'administration distants sont bien installés et que le service DHCP ne l'est pas.

## 11. Mise en œuvre du serveur de fichiers pour le site de Paris

-  Seul l'ordinateur paris1 est requis.
- 

Vous allez installer le rôle de services de fichiers sur paris1.

1. Connectez-vous en tant qu'administrateur.
  2. Ouvrez le **Gestionnaire de serveur**.
  3. Ajoutez le rôle de **Services de fichiers** y compris les rôles de services **Système de fichiers distribués**, l'espace de noms sera configuré ultérieurement et **Gestion de ressources du serveur de fichiers**.
- 

-  Le rôle de services de fichiers est installé.
- 

## 12. Mise en œuvre du serveur de fichiers pour le site de Genève

-  Seul l'ordinateur geneve1 est requis.
- 

Vous allez installer le rôle de services de fichiers sur geneve1.

1. Connectez-vous en tant qu'administrateur.
  2. Ouvrez le **Gestionnaire de serveur**.
  3. Ajoutez le rôle de **Services de fichiers** y compris les rôles de services **Système de fichiers distribués**, l'espace de noms sera configuré ultérieurement et **Gestion de ressources du serveur de fichiers**.
- 

-  Le rôle de services de fichiers est installé.
- 

## 13. Mise en œuvre des quotas à l'aide du serveur de fichiers

-  geneve1 et paris1 sont requis.
- 

Vous allez créer un nouveau modèle de quota qui sera utilisé plus loin.

1. Connectez-vous en tant qu'administrateur sur **geneve1**.
  2. Ouvrez la console **Gestionnaire de ressources du serveur de fichiers** des Outils d'administration.
  3. Développez l'arborescence **Gestion de quotas**.
  4. Cliquez avec le bouton droit de la souris sur **Modèles de quotas** puis sur **Créer un modèle de quota**.
  5. Dans la boîte de dialogue qui apparaît, saisissez `modèle de quota ENI` pour le nom du modèle. Limitez l'espace à **5 Mo** et indiquez qu'il s'agit d'un quota inconditionnel avant de cliquer sur **OK**.
-



Vous venez de créer un modèle de quota qui sera utilisé plus loin.

---

## 14. Mise en œuvre du filtrage de fichiers



geneve1 et paris1 sont requis.

---

Vous allez créer un nouveau modèle de filtre de fichiers qui sera utilisé plus loin. Vous ne devez permettre que le stockage de fichiers texte et office, images incluses.

1. Connectez-vous en tant qu'administrateur sur **geneve1**.
  2. Ouvrez la console **Gestionnaire de ressources du serveur de fichiers** des Outils d'administration.
  3. Développez l'arborescence **Gestion du filtrage des fichiers**.
  4. Cliquez avec le bouton droit de la souris sur **Modèles de filtres de fichiers** puis sur **Créer un modèle de filtre de fichiers**.
  5. Dans la boîte de dialogue qui apparaît, saisissez **modèle de filtre ENI** pour le nom du modèle. Sélectionnez le filtrage actif et cochez tous les groupes de fichiers exceptés **fichiers image, fichiers Office et fichiers texte** avant de cliquer sur **OK**.
- 



Vous venez de créer un modèle de filtre de fichiers qui sera utilisé plus loin.

---

## 15. Mise en œuvre de DFS à l'aide du serveur de fichiers



geneve1 et paris1 sont requis.

---

Vous allez créer un nouvel espace de noms qui sera utilisé plus loin.

1. Connectez-vous en tant qu'administrateur sur **geneve1**.
  2. Ouvrez la console **Gestion du système de fichiers distribués DFS** des Outils d'administration.
  3. Cliquez avec le bouton droit de la souris sur **Espace de noms** puis sur **Nouvel espace de noms**.
  4. Dans l'assistant, sur **Serveur d'espaces de noms**, saisissez geneve1 comme serveur puis cliquez sur **Suivant**. Si un éventuel message apparaît, cliquez sur **Oui**.
  5. Saisissez **Public** pour le nom sur la page **Noms et paramètres de l'espace de noms** avant de cliquer sur **Suivant**. Par défaut tous les utilisateurs ont un accès en lecture seule.
  6. Sur la page **Type d'espace de noms** cliquez sur **Suivant**. Par défaut il s'agit d'un espace de noms de domaine et le mode Windows Server 2008 est activé.
  7. Prenez quelques instants pour revoir vos choix puis cliquez sur **Créer**.
  8. Sur la page **Confirmation**, contrôlez que la création s'est bien déroulée puis cliquez sur **Fermer**.
- 



Vous venez de créer un nouvel espace de noms.

---

## 16. Gestion des permissions NTFS et des permissions de partage



Seul geneve1 est requis.

Vous allez créer un nouveau dossier partagé sur **geneve1** appelé **Recherches** en utilisant la console Gestion des partages ; il faut limiter les permissions NTFS aux seuls utilisateurs authentifiés pour pouvoir y accéder en modification. Concernant les quotas, les filtres de fichiers et les espaces de noms DFS, utilisez ceux que vous avez créés.

1. Connectez-vous en tant qu'administrateur sur **geneve1**.
2. Ouvrez la console **Gestion du partage et du stockage** des Outils d'administration.
3. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Gestion des partages et du stockage**, puis sur **Prévoir le partage**.
4. Dans l'assistant, sur la page **Emplacement du dossier partagé**, saisissez c:\Recherches dans **Emplacement** puis cliquez sur **Suivant**.
5. Dans la boîte de dialogue vous demandant de créer le dossier, cliquez sur **Oui**.
6. Sur la page **Autorisations NTFS**, sélectionnez l'option **Oui**, modifiez les autorisations NTFS puis cliquez sur **Modifier les autorisations**.
7. Dans la boîte de dialogue **Autorisations pour Recherches**, cliquez sur **Avancé**.
8. Dans la boîte de dialogue **Paramètres de sécurité avancés pour Recherches**, désélectionnez la case à cocher **Inclure les autorisations pouvant être héritées du parent de cet objet** car vous ne pouvez supprimer des autorisations héritées.
9. Dans la boîte de dialogue **Sécurité Windows**, cliquez sur **Copier**, puis cliquez sur **OK**.
10. Dans la boîte de dialogue **Autorisations pour Recherches**, sélectionnez le groupe **Utilisateurs** et cliquez sur **Supprimer**.
11. Dans la boîte de dialogue **Autorisations pour Recherches** cliquez sur **Ajouter**.
12. Dans la boîte de dialogue **Sélectionnez Utilisateurs, Ordinateurs ou Groupes**, saisissez Utilisateurs authentifiés puis cliquez sur **OK**.
13. Garantissez que **Utilisateurs authentifiés** est sélectionné puis dans la section des autorisations, cliquez sur **Modifier (Autoriser)**. Et enfin cliquez sur **OK**.
14. Sur la page **Autorisations NTFS**, cliquez sur **Suivant**.
15. Sur la page **Protocoles du partage**, cliquez sur **Suivant**.
16. Sur la page **Paramètres SMB**, cliquez sur **Suivant**.
17. Sur la page **Autorisations SMB**, sélectionnez l'option **Les administrateurs ont un contrôle total; tous les autres utilisateurs et groupes ont un accès en lecture et en écriture** puis cliquez sur **Suivant**.
18. Sur la page **Stratégie de quota**, cochez la case **Appliquer le quota** puis sélectionnez **Modèle de quota ENI** dans la liste déroulante **Dériver les propriétés de ce modèle de quota** enfin cliquez sur **Suivant**.
19. Sur la page **Stratégie de filtre de fichiers** cochez la case **Appliquer le filtre de fichiers** puis sélectionnez **Filtre de fichier ENI** dans la liste déroulante **Dériver les propriétés de ce modèle de filtre de fichiers**, enfin cliquez sur **Suivant**.
20. Sur la page **Publication de l'espace de nom DFS**, cochez la case **Publier le partage SMB sur un espace de noms DFS**, pour que le dossier parent soit **\mydom.eni\Public** et le nom de dossier soit **Recherches** puis sélectionnez **Modèle de quota ENI** dans la liste déroulante **Dériver les propriétés de ce modèle de quota**, enfin cliquez sur **Suivant**.
21. Sur la page **Revoir les paramètres et créer le partage**, prenez quelques instants pour revoir vos choix puis cliquez sur **Créer**.
22. Sur la page **Confirmation**, normalement le partage est créé sans erreur vous pouvez cliquer sur **Fermer**.

23. Vous pouvez maintenant tester le partage en y accédant directement via le chemin UNC `\Geneve1\recherches` ou `\mydom.eni\public\recherches` et en essayant de créer des fichiers textes, voire des fichiers compressés, d'ajouter des fichiers dont la taille totale excède 5 Mo.
- 

➤ Cet exercice montre les différentes méthodes pour gérer un serveur de fichiers. La gestion d'un serveur de fichiers à l'aide du rôle correspondant est une des méthodes les plus simples et les plus efficaces.

---

➤ Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 11 - Mise en œuvre du rôle de serveur d'impression

## 1. Objectifs

Dans cet exercice vous allez installer et configurer le rôle de serveur d'impression dans l'objectif de gérer efficacement des imprimantes. Pour l'impression Internet vous allez examiner en détail comment l'activer au niveau du client et quels ports ouvrir sur le pare-feu. Enfin vous verrez comment résoudre certains problèmes des utilisateurs et leur simplifier la vie afin qu'ils trouvent rapidement leurs imprimantes.

## 2. Configuration de l'environnement

➤ Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

➤ Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

➤ Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt** doit se trouver sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres ordinateurs.
- Sur **paris5**, lancez le script **scriptParis5.bat**.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**. Ensuite installez le moniteur réseau.
- Sur **geclient1**, placez les scripts **scriptGeclient1.bat** et **joindom.vbs** sur le Bureau puis lancez le script **scriptGeclient1.bat** après le redémarrage du serveur **geneve1** en utilisant les droits d'administration.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt **mydom.eni** ainsi que serveur **DNS** et routeur. Ses adresses IP sont 10.1.1.1/24 et 10.1.10.5/30.

**paris5** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.1.1.2/24).

**geneve1** est membre du domaine **mydom.eni** et routeur. Ses adresses IP fixes sont 10.1.10.6/30 et 10.2.1.17/30.

**geclient1** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.2.1.18/30).

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Mise en œuvre de l'impression consacré à la mise en œuvre du serveur d'impression. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre du rôle du serveur d'impression

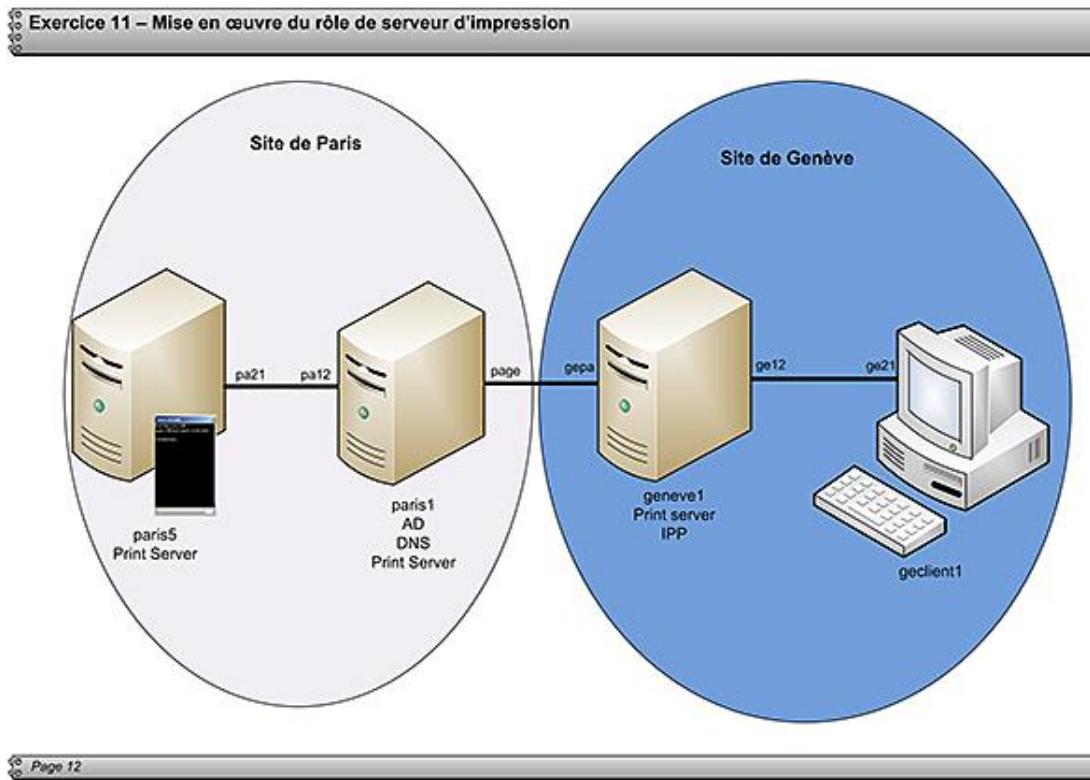
Les consultants ont déterminé qu'il est nécessaire d'installer deux serveurs d'impression sur le site de Paris afin de pouvoir imprimer dans toute l'entreprise. Le premier serveur désigné est **paris1** et le second est **paris5**. Vous allez devoir ajouter les imprimantes suivantes pour ces serveurs :

Serveur	Imprimante	Nom de partage	Port	Pool
paris1	HP Color LaserJet 2500PS	HP2500	10.2.2.1 Hewlett Packard Jet Direct	Non
paris1	Canon Inkjet PIXMA IP5000	CN5000	10.2.2.2 Generic Network Card	Non
paris5	Kyocera FS 1550+	KY1500	10.1.1.50 Kyocera Network Printer	Oui
paris5	Kyocera FS 1550+		10.1.1.51 Kyocera Network Printer	
paris5	Olivetti JP 370 (Color)	O370	10.1.1.52 Network Print Server (1 Port - USB)	Non

Il sera nécessaire de les publier dans l'Active Directory.

Par la suite vous avez déterminé qu'il est préférable de déplacer les imprimantes du serveur paris1 vers geneve1. Il vous faudra déplacer le serveur d'impression. Certains utilisateurs doivent imprimer en étant hors de l'entreprise. Il est nécessaire de leur permettre d'imprimer via l'impression Internet.

Un cadre se plaint que l'imprimante est toujours occupée entre autres par de longs travaux qui servent au service comptabilité pour le lendemain, il vous faut trouver une solution.



Les opérations à effectuer sont :

- 1) Configurer **paris5** de manière à ce que vous puissiez le gérer à distance.
- 2) Installer le rôle de serveur d'impression sur **paris1** et **paris5**.
- 3) Ajouter sur chaque serveur d'impression les imprimantes du tableau.
- 4) Vérifier, voire publier dans l'Active Directory les imprimantes.
- 5) Installer le rôle serveur d'impression sur **geneve1** puis migrer les imprimantes de **paris1** vers **geneve1**.
- 6) Permettre l'utilisation de l'impression Internet à partir de **geclient1**.
- 7) Créer une imprimante pour le cadre avec des droits spécifiques, une imprimante pour les utilisateurs, et modifier l'horaire d'impression pour le service de comptabilité.

## 5. Configuration de paris5 pour une gestion à distance



paris1 et paris5 doivent fonctionner, les opérations s'effectuent sur paris1 et paris5.

Il est nécessaire d'autoriser sur paris5 :

- Le Bureau distant.
  - La gestion du pare-feu.
  - La gestion à distance à l'aide de la console MMC.
1. Démarrer la machine virtuelle **paris5** et connectez-vous en tant qu'administrateur de domaine.
  2. Saisissez `cscript %windir%\system32\scregedit.wsf /ar 0`. Il n'y a pas besoin de permettre l'accès à des clients RDP 6.0.
  3. Saisissez `Netsh advfirewall set currentprofile settings remotemanagement enable`.
  4. Saisissez `Netsh advfirewall firewall set rule group="Administration distante" new enable=yes`.
  5. Sur **paris1**, contrôlez que vous pouvez accéder au Bureau distant, gérer le pare-feu et utiliser une console MMC à distance. Pensez à créer une MMC pour le test du pare-feu à distance.



paris5 peut être maintenant administré à distance.

## 6. Installation du serveur d'impression sur paris1 et paris5



paris1 et paris5 doivent fonctionner, les opérations s'effectuent sur paris1 et paris5.

1. Sur **paris1**, installez uniquement le rôle **Serveur d'impression**.
2. Sur **paris5**, installez uniquement le rôle **Serveur d'impression** (`start /w ocsetup Printing-ServerCore-Role`).
3. Après le redémarrage de **paris5**, dans la console **Gestion de l'impression** sur **paris1**, ajoutez **paris5** à la liste des serveurs gérés.



Vous avez installé le rôle de Serveur d'impression sur paris1 et paris5. De plus, vous pouvez administrer les deux serveurs à partir de paris1.

## 7. Ajout des imprimantes



paris1 et paris5 doivent fonctionner, les opérations s'effectuent sur paris1 et paris5.

1. À l'aide de l'assistant **Ajouter une imprimante** de la console **Gestion de l'impression**, ajoutez les imprimantes pour **paris1**.
2. La procédure est différente pour **paris5**. Le Server Core ne dispose pas de pilotes d'imprimantes et il n'est pas possible de les installer à distance à cause de messages dus à des problèmes de signature. Il faut donc ajouter ces pilotes manuellement. Commencez par partager sur paris1, le répertoire **FileRepository** du chemin `c:\windows\system32\driverstore` en utilisant les autorisations par défaut.

3. Sur **paris5**, saisissez la commande start /w rundll32 printui.dll,PrintUIEntry /id.
4. Sur la page **Assistant Ajout de pilote d'imprimante**, cliquez sur **Suivant**.
5. Sur la page **Sélection du processeur et du système d'exploitation**, vérifiez que **x86** est bien sélectionné puis cliquez sur **Suivant**.
6. Sur la page **Sélection du pilote d'imprimante**, cliquez sur **Disque Fourni**.
7. Dans la boîte de dialogue, saisissez \\paris1\FileRepository\prnky001.inf\_6388d9ad puis cliquez sur **OK**.
8. Sur la page **Sélection du pilote d'imprimante**, sélectionnez **Kyocera FS 1550+** puis cliquez sur **Suivant**.
9. Sur la page **Fin de l'assistant Ajout de pilote d'imprimante**, cliquez sur **Terminer**.
10. Répétez l'opération pour l'Olivetti JP 370 (Color) se trouvant dans le répertoire \\paris5\FileRepository\prnol001.inf\_eb42d9fe.
11. Maintenant, il est possible d'ajouter les imprimantes, alors en utilisant l'assistant **Ajouter une imprimante** de la console **Gestion de l'impression**, ajoutez les imprimantes pour **paris5**.
12. Activez le pool d'imprimante pour l'imprimante ky-1550.
13. Vous pouvez effectuer des tests d'impression.

 Vous avez ajouté les imprimantes comme demandé dans l'énoncé.

## 8. Vérification de la publication dans l'Active Directory des imprimantes

 paris1 et paris5 doivent fonctionner, les opérations s'effectuent sur paris1 et paris5.

1. Pour chaque imprimante, à l'aide de la console **Gestion de l'impression** contrôlez que la case à cocher **Lister dans l'annuaire** est cochée dans l'onglet **Partage des propriétés de l'imprimante**.
2. Sur **paris1**, démarrez **Utilisateurs et ordinateurs Active Directory** des Outils d'administration.
3. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Requêtes sauvegardées** puis sur **Nouveau - Requête**.
4. Saisissez un nom pour la requête puis cliquez sur **Définir la requête**.
5. Cliquez sur l'onglet **Ordinateurs** puis sélectionnez **Imprimantes** dans **Rechercher** et cliquez deux fois sur **OK**. Vous allez afficher toutes les imprimantes listées dans l'Active Directory.
6. Cliquez sur l'icône **Actualiser** pour faire apparaître le résultat, éventuellement cliquez sur votre requête au préalable. Vous pourriez rechercher un script VBS qui effectue le même type de recherche et comparer les résultats.

 Vos imprimantes sont maintenant publiées dans l'Active Directory.

## 9. Migration d'un serveur d'impression

 paris1 et geneve1 doivent fonctionner, les opérations s'effectuent sur paris1 et geneve1.

1. Sur **geneve1**, installez le rôle **Serveur d'impression**.
2. Sur **geneve1**, dans **Gestion de l'impression**, ajoutez le serveur **paris1**.
3. Dans **Gestion de l'impression** avec le bouton droit de la souris, cliquez sur **Exporter les imprimantes vers un fichier**.
4. Sur la page de l'assistant **Vérifiez la liste des éléments à exporter**, examinez les objets qui seront exportés puis cliquez sur **Suivant**.
5. Sur la page **Sélectionner l'emplacement du fichier**, saisissez un emplacement et un nom de fichier puis cliquez sur **Suivant**.
6. Attendez que l'exportation se termine et sur la page **Exportation** vérifiez qu'elle est réussie puis cliquez sur **Terminer**.
7. Dans **Gestion de l'impression** avec le bouton droit de la souris, cliquez sur **Importer les imprimantes depuis un fichier**.
8. Sur la page **Sélectionner l'emplacement du fichier**, saisissez l'emplacement et un nom du fichier sauvegardé puis cliquez sur **Suivant**.
9. Sur la page de l'assistant **Vérifiez la liste des éléments à importer**, examinez les objets qui seront exportés puis cliquez sur **Suivant**.
10. Sur la page **Sélectionner les options d'importation**, cliquez sur **Suivant**.
11. Sur la page **Sélectionner l'emplacement du fichier**, saisissez un emplacement et un nom de fichier puis cliquez sur **Suivant**.
12. Attendez que l'importation se termine et sur la page **Importation** vérifiez qu'elle est réussie puis cliquez sur **Terminer**.
13. Vérifiez que vous pouvez imprimer.
14. Supprimez le rôle **Serveur d'impression** sur **paris1**.

 Le serveur d'impression et ses imprimantes ont été déplacés depuis **paris1** vers **geneve1** et **paris1** n'est plus serveur d'impression.

## 10. L'impression Internet

 **paris1**, **geneve1** et **geclient1** doivent fonctionner, les opérations s'effectuent sur **geneve1** et **geclient1**.

1. Sur **geneve1**, installez le rôle de service d'**Impression Internet**.
2. Sur **geneve1**, testez l'URL <http://localhost/printers>.
3. Sur **geclient1**, dans un navigateur saisissez <http://geneve1/printers> puis effectuez une connexion pour l'imprimante HP Color LaserJet 2500 PS.
4. Faites de même en passant par `\geneve1` puis en vous connectant à l'imprimante HP2500. Vous devez avoir deux imprimantes sur **geclient1** comme montré dans l'image suivante :



Une imprimante utilise le protocole **RPC** et l'autre le protocole **HTTP** pour transmettre les documents à imprimer. Si vous effectuez cet atelier sur un serveur 2008, il faut ajouter la fonctionnalité client d'impression Internet à

l'ordinateur qui joue le rôle de client.

1. Lancez le **Moniteur réseau** puis cliquez sur **New Capture tab** et enfin cliquez sur l'icône **Start**.
2. Ouvrez le **Bloc-notes**, saisissez quelques lignes de texte avant d'imprimer votre document sur l'imprimante HP en utilisant les deux imprimantes ciblées.
3. Retournez dans le **Moniteur réseau** pour rechercher des trames RPC et HTTP.
4. Sur **geneve1**, lancez le Pare-feu Windows avec fonctions avancées de sécurité, puis activez et désactivez les règles suivantes pour le profil qui est actif normalement Domaine :
  - Partage de fichiers et d'imprimantes (service Spouleur - RPC)
  - Services World Wide Web (trafic HTTP)

Lorsqu'une règle est désactivée, tentez l'impression sur les deux imprimantes et observez le résultat.

- 
-  L'impression Internet est activée. Et vous avez pu examiner les ports à ouvrir lorsque vous utilisez les protocoles RPC et HTTP.
- 

## 11. Création d'imprimantes en fonction des utilisateurs

- 
-  paris1 et geneve1 doivent fonctionner, les opérations s'effectuent sur geneve1.
- 

La solution la plus simple consiste à rajouter des imprimantes disposant de paramètres adaptés aux différents utilisateurs. Dans notre cas, il est nécessaire de disposer de trois imprimantes à savoir :

- Une imprimante pour le cadre disposant d'une haute priorité.
  - Une imprimante pour les utilisateurs disposant d'une priorité standard.
  - Une imprimante pour les travaux de la comptabilité disposant d'heures d'impression durant la nuit.
1. Ajoutez deux imprimantes nommées respectivement **O370Cadre** et **O370Compta** basées sur les paramètres de l'imprimante O370.
  2. Pour l'imprimante **O370Cadre**, modifiez sa priorité afin qu'elle soit supérieure à l'imprimante **O370**.
  3. Pour l'imprimante **O370Compta**, modifiez sa disponibilité afin qu'elle devienne disponible de 20h00 à 6h00.
  4. Comme exercice supplémentaire, vous pourriez déployer ces imprimantes à l'aide des stratégies de groupe en créant une nouvelle stratégie appelée **GPOCadre** puis en déployant l'imprimante O370Cadre sur cette stratégie. Il faudrait filtrer la stratégie pour qu'elle ne soit reçue que par le cadre.

- 
-  Vous avez implémenté des imprimantes adaptées aux besoins des différents utilisateurs.
- 

-  Dans cet exercice vous avez examiné la méthode pour gérer des imprimantes à l'aide des outils les plus appropriés. Bien que d'apparence simpliste, la gestion efficace de l'impression requiert une attention particulière surtout lorsque vous avez des utilisateurs mobiles et un nombre important d'imprimantes de toutes sortes.
-



Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 10 - Mise en œuvre de la protection d'accès réseau NAP

## 1. Objectifs

Dans cet exercice vous allez installer et configurer NAP pour contrôler l'intégrité des ordinateurs clients qui demandent une adresse IP à un serveur DHCP. Plusieurs scénarios vont être joués afin de simuler différents clients possibles.

## 2. Configuration de l'environnement

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt** doit être placé sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres ordinateurs.
- Sur **paris2**, lancez le script **scriptParis2.bat** au redémarrage, connectez-vous en tant qu'administrateur de domaine puis lancez le script **AddDHCP.bat**. Installez également le moniteur réseau.
- Sur **paclient1**, aucun script n'est à exécuter.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt **mydom.eni** ainsi que serveur **DNS** et son adresse IP est **10.1.1.1/24**. **paris2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (**10.1.1.2/24**).

**paclient1** est simplement client DHCP et fait partie d'un groupe de travail.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Configuration des services réseaux avancés, principalement à la section consacrée à la protection de l'accès réseau. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre de la conformité DHCP

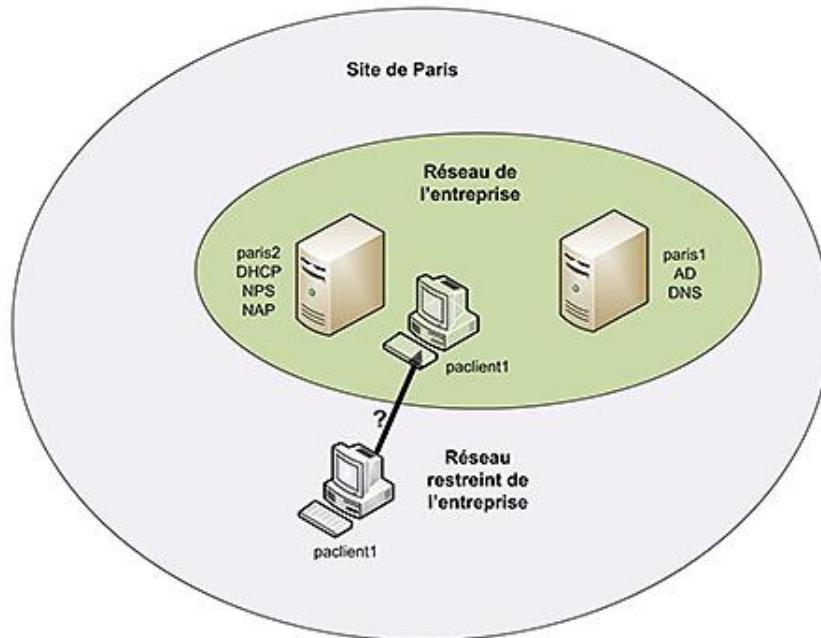
Il a été décidé de limiter l'accès au réseau de l'entreprise uniquement aux ordinateurs dont l'intégrité est conforme à la stratégie définie et de limiter l'accès aux autres ordinateurs en utilisant la protection de l'accès réseau NAP associée au serveur DHCP.

Il vous est demandé d'installer et configurer les serveurs NPS et NAP sur la même machine que le serveur DHCP. La stratégie consiste à vérifier que le pare-feu est bien activé. Enfin, vous devez tester la solution dans les cas suivants :

- Client hors domaine et agent NAP désactivé.

- Client hors domaine mais avec l'agent NAP activé.
- Client dans le domaine et agent NAP désactivé.
- Client dans le domaine, étude des paquets avec le moniteur réseau et activation manuelle de NAP et étude des paquets.
- Création et test d'une stratégie de groupe pour activer NAP sur le client.

#### Exercice 10 – Mise en œuvre de NAP-DHCP



Page 11

#### a. Réponse

Les tâches à effectuer sont :

- 1) Installer le rôle de serveur NPS.
- 2) Configurer le serveur NPS en tant que serveur de stratégie NAP.
- 3) Configurer le serveur DHCP pour gérer NAP sur l'étendue.
- 4) Tester le client hors domaine avec l'agent NAP désactivé.
- 5) Tester le client hors domaine mais avec l'agent NAP activé.
- 6) Tester le client dans le domaine avec l'agent NAP désactivé.
- 7) Tester le client dans le domaine, étudier les paquets avec le moniteur réseau et activer manuellement NAP et étudier les paquets.
- 8) Créer une stratégie de groupe pour activer NAP sur le client, puis la tester.

## 5. Installation du rôle de serveur NPS



paris1 et paris2 doivent fonctionner, les opérations s'effectuent sur paris2.

L'installation de ce rôle se fait sur le serveur DHCP. Bien qu'il soit possible d'utiliser deux serveurs distincts, cela permet de limiter le nombre de serveurs utilisés pour l'exercice.

1. Démarrez la machine virtuelle paris2 et connectez-vous en tant qu'administrateur de domaine.
2. Démarrez le Gestionnaire de serveur.
3. Ajoutez le service de rôle Serveur NPS (*Network Policy Server*) du rôle Services de stratégie et d'accès réseau.

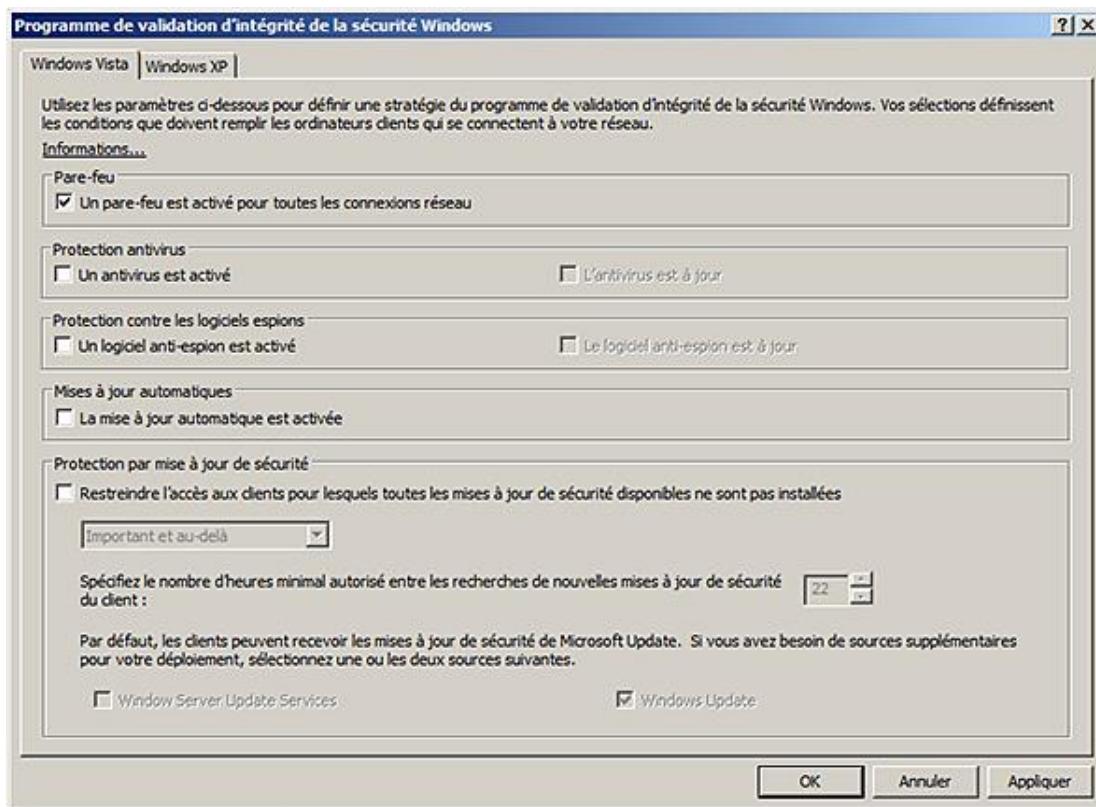
 Le rôle de serveur NAP est installé sur le serveur.

## 6. Configuration de NPS en tant que serveur de stratégie NAP

 paris1 et paris2 doivent fonctionner, les opérations s'effectuent sur paris2.

1. Lancez **Serveur NPS (Network Policy Server) (console nps.msc)** des Outils d'administration.
2. Dans la section de détail sous **Configuration standard** sélectionnez **Protection d'accès réseau (NAP)** dans la liste déroulante puis cliquez sur **Configurer la protection d'accès réseau (NAP)** pour démarrer l'assistant.
3. Dans l'assistant sur la page **Sélectionner la méthode de connexion réseau à utiliser avec la protection d'accès réseau (NAP)**, sélectionnez **Protocole DHCP (Dynamic Host Configuration Protocol)** pour la **Méthode de connexion réseau** et saisissez Stratégie NAP mydom.ini pour le **Nom de la stratégie**. Ensuite, cliquez sur **Suivant**.
4. Sur la page **Spécifiez les serveurs de contrainte de mise en conformité NAP exécutant Serveur DHCP**, cliquez sur **Suivant**, car l'ordinateur local est un serveur DHCP. Vous pourriez ajouter ici d'autres serveurs DHCP qui sont compatibles avec NAP.
5. Sur la page **Spécifier les étendues DHCP**, cliquez sur **Suivant**, car une seule étendue existe sur notre serveur DHCP. Vous pourriez limiter les étendues NAP en ajoutant le nom des étendues dont l'intégrité doit être contrôlée.
6. Sur la page **Configurer les groupes d'utilisateurs et les groupes d'ordinateurs**, cliquez sur **Suivant** car nous ne faisons pas d'exceptions. Vous pourriez limiter les groupes d'utilisateurs ou d'ordinateurs qui subissent la stratégie NAP en ajoutant leur nom dans la liste.
7. Sur la page **Spécifier un groupe de serveurs de mise à jour et une URL NAP**, cliquez sur **Suivant** car il n'est pas nécessaire dans cet exercice d'utiliser un groupe de serveurs de mise à jour.
8. Sur la page **Définir la stratégie de contrôle d'intégrité NAP**, vérifiez que **Validateur d'intégrité de la sécurité Windows** et **Activer la mise à jour automatique des ordinateurs clients** sont bien sélectionnées, ainsi que **Refuser l'accès réseau complet aux clients NAP non conformes**. N'autorisez qu'un accès restreint. Puis cliquez sur **Suivant**.
9. Sur la page **Fin de la configuration de la stratégie d'application du service NAP et des clients RADIUS**, prenez quelques instants pour examiner les stratégies qui vont être créées avant de cliquer sur **Terminer**.
10. Vous pouvez visualiser les stratégies créées sous **Stratégies** dans l'arborescence.
11. Maintenant, il faut encore définir quels paramètres doivent être validés par le validateur SHVs. Dans l'arborescence de la console, développez **Protection d'accès réseau** puis cliquez sur **Programme de validation d'intégrité système**, enfin dans la section de détail, double cliquez sur **Validateur d'intégrité de la sécurité Windows**.
12. Dans la boîte de dialogue **Propriétés de Validateur d'intégrité de la sécurité Windows**, cliquez sur **Configurer**. Nous ne modifions pas le comportement des codes d'erreurs.
13. Dans la boîte de dialogue **Programme de validation d'intégrité de la sécurité Windows**, cliquez sur l'onglet **Windows Vista** et modifiez les cases à cocher comme montré sur la

figure suivante :



1. Cliquez deux fois sur **OK**. La configuration du serveur NAP est terminée.

➤ Votre serveur est maintenant configuré en tant que serveur NAP pour le serveur DHCP local.

## 7. Configurer le serveur DHCP pour activer NAP sur l'étendue

➤ paris1 et paris2 doivent fonctionner, les opérations s'effectuent sur paris2.

1. Démarrez la console DHCP.
2. Dans l'arborescence, développez l'étendue existante puis cliquez avec le bouton droit de la souris pour faire apparaître les propriétés de l'étendue.
3. Cliquez sur l'onglet **Protection d'accès réseau**.
4. Sélectionnez l'option **Activer pour cette étendue** puis cliquez sur **OK**. La partie serveur de NAP est opérationnelle.
5. Ajoutez les options d'étendues suivantes pour les ordinateurs non conformes :

006 Serveur DNS 10.1.1.1

Classe de protection d'accès réseau par défaut.

015 Nom de domaine DNS restricted.mydom.eni

Classe de protection d'accès réseau par défaut.

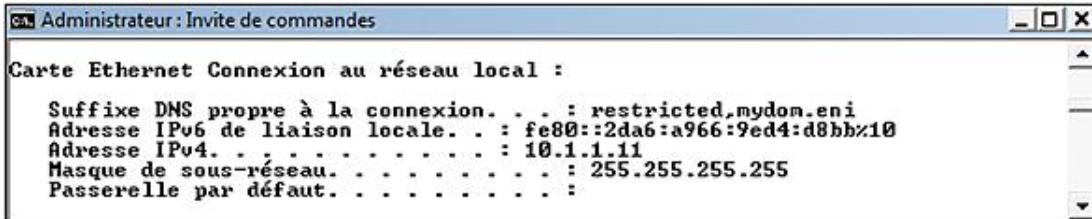
015 Nom de domaine DNS open.mydom.eni

Classe utilisateur par défaut.

## 8. Test du client hors domaine sans l'agent NAP activé

-  paris1, paris2 et paclient1 doivent fonctionner, les opérations s'effectuent sur paclient et paris2.

1. Démarrez la machine virtuelle **paclient1**.
2. Dans une invite de commande, saisissez ipconfig, le client doit avoir acquis une adresse IP et se trouve dans la zone restreinte comme le montre l'image suivante :



C'est normal, car l'ordinateur est considéré comme un client **Non compatible NAP** puisque par défaut le service **Agent de protection d'accès réseau** n'est pas démarré. Vous pouvez examiner l'observateur d'événements de **paris2** en filtrant sur **Services de stratégie et d'accès réseau** dans **Affichages personnalisés** pour voir les événements générés par la demande d'adresses IP. Vous pouvez également libérer et renouveler le bail pour **paclient1**.

-  Le client hors domaine sans agent NAP activé se trouve dans la zone restreinte.

## 9. Test du client hors domaine en activant l'agent NAP (paclient1)

-  paris1, paris2 et paclient1 doivent fonctionner, les opérations s'effectuent sur paclient1 et paris2.

Pour qu'un ordinateur client puisse envoyer son état d'intégrité au serveur NAP, il faut que les conditions suivantes soient réunies :

1 - Disposer d'un client NAP comme Windows XP SP3, Windows Vista et Windows Server 2008 ainsi que les futurs Windows 7 et Windows Server 2008 R2.

2 - Disposer du SHA correspondant à la stratégie appliquée. Par exemple Windows Server 2008 ne dispose pas des SHA et par conséquent ne peut envoyer son état d'intégrité au serveur NPS pour validation.

3 - Le service **Agent de protection d'accès réseau** doit être démarré.

4 - Activer le client de contrainte correspondant.

5 - Garantir que le service **Centre de sécurité** est démarré. Windows Server 2008 ne dispose pas de ce service.

Dès que toutes ces conditions sont réunies, alors l'ordinateur client devrait pouvoir être autorisé dans le réseau d'entreprise si les stratégies demandées sont validées.

1. Sur **paclient1**, libérez l'adresse IP avec la commande ipconfig /release.
2. En utilisant la commande net start, contrôlez que le service **Centre de sécurité** est démarré sinon faites le démarrer avec la commande net start wscsvc.
3. Faites de même avec le service **Agent de protection d'accès réseau** avec la commande net start napagent puis demandez une adresse IP avec la commande ipconfig /renew. Ensuite, sur **paris2**, examinez les événements correspondants si vous devez trouver deux événements d'abord un 6272 puis un 6276, indiquant que l'ordinateur est placé en quarantaine et la raison est toujours **client Non compatible NAP**.
4. Démarrez la console napclcfg.msc sur **paclient1**.

5. Dans l'arborescence cliquez sur **Clients de contrainte** puis dans la section de détail, activez **Client de contrainte de quarantaine DHCP**.
6. Libérez et renouvez l'adresse IP. Cette fois paclient1 est dans la zone non restreinte. Ensuite, sur **paris2**, examinez les événements correspondant si vous devez trouver deux événements, d'abord un 6272 puis un 6278 indiquant que l'ordinateur correspond aux critères définis dans la stratégie et par conséquent l'accès total est accordé. Prenez quelques secondes pour examiner le résultat de la commande `ipconfig /all`, une ligne supplémentaire vous indique que l'état de quarantaine du système est non restreint.
7. Désactivez le pare-feu sur **paclient1**, il se réactivera automatiquement car dans les stratégies réseau sur le serveur NPS vous avez précisé pour chaque stratégie que le client doit se mettre à jour automatiquement. Pour vous en convaincre, sur le serveur **paris2** modifiez chaque stratégie réseau NAP DHCP en double cliquant dessus puis en désactivant **Mise à jour automatique** du paramètre **Contrainte de mise en conformité NAP** de l'onglet **Paramètres**. Ensuite désactivez le pare-feu sur **paclient1**. Cette fois, rien ne se passe excepté une notification qui apparaît. Sur **paris2**, réactivez les mises à jour automatiques et vous verrez **paclient1** est de nouveau automatiquement conforme.

Vous pourriez encore effectuer d'autres tests comme par exemple désactiver le démarrage du **Centre de sécurité** et voir le résultat.

 Vous avez étudié le scénario dans lequel un ordinateur ne fait pas partie du domaine mais dispose d'un client NAP.

## 10. Test du client dans le domaine avec l'agent NAP désactivé

 paris1, paris2 et paclient1 doivent fonctionner, les opérations s'effectuent sur paclient1 et paris2.

1. Faites rentrer **paclient1** dans le domaine puis connectez-vous en utilisant l'administrateur de domaine.
2. Avec la commande `ipconfig` examinez si le serveur est dans la zone de quarantaine. Pourquoi ? Simplement parce que le service **Agent de protection d'accès réseau** n'est pas démarré, ensuite démarrez-le et renouvez votre adresse. Le serveur devrait se trouver maintenant dans la zone non restreinte.

 Vous avez étudié le scénario dans lequel un ordinateur fait partie du domaine mais le client NAP est désactivé.

## 11. Test du client dans le domaine en activant l'agent NAP

 paris1, paris2 et paclient1 doivent fonctionner, les opérations s'effectuent sur paclient1 et paris2.

1. Sur **paris2**, démarrez le moniteur réseau puis créez une nouvelle capture. Dans la section **Display Filter**, saisissez `dhcp` puis cliquez sur l'icône **Apply**.
2. Cliquez sur l'icône **Start** pour démarrer la capture.
3. Sur **paclient1** arrêtez le service **Agent de protection d'accès réseau** puis libérez et renouvez l'adresse IP. Ensuite examinez les trames réseaux capturées, principalement la trame **DHCP DISCOVER** : dans la section **Frame details** développez le nœud **Dhcp**, il n'y a pas d'envoi du paramètre **VendorSpecificInformation** : **-- Type 43** car l'agent NAP est arrêté.
4. Sur **paclient1** démarrez le service **Agent de protection d'accès réseau** puis libérez et renouvez l'adresse IP. Ensuite examinez les trames réseaux capturées, principalement la trame **DHCP DISCOVER** : dans la section **Frame details** développez le nœud **Dhcp**, puis le paramètre **VendorSpecificInformation** : **-- Type 43**. C'est bien dans le premier message DHCP que le client envoie les informations au serveur NAP sur son état

d'intégrité.

5. Saisissez la commande `netsh nap client show config` puis examinez et comparez le résultat avec les informations obtenues par `napclcfg.msc` et `ipconfig /all`. Faites de même avec la commande `netsh nap client show state`.
6. Enfin ouvrez l'observateur d'événements sur paclient1 en utilisant la commande `eventvwr.msc`.
7. Dans l'arborescence, développez **Journaux des applications et des services, Microsoft, Windows et Network Access Protection**. Vous pourrez y trouver des messages sur NAP.

 L'intérêt de ce scénario a été d'examiner comment l'état de santé est transmis auprès du serveur NAP.

## 12. Créez une stratégie de groupe pour activer NAP sur le client puis la tester

 paris1, paris2 et paclient1 doivent fonctionner, les opérations s'effectuent sur paclient1 et paris1.

1. Sur **paris1**, démarrez **Gestion des stratégies de groupe** des Outils d'administration.
2. Dans l'arborescence, développez **Forêt : mydom.eni, Domaines** et **mydom.eni**.
3. Cliquez avec le bouton droit de la souris sur **mydom.eni** puis sur **Créer un objet GPO dans ce domaine, et le lier ici**. Saisissez **NAPGPO** pour le nom.
4. Cliquez avec le bouton droit de la souris sur **NAPGPO** puis cliquez sur **Modifier**.
5. Dans l'éditeur de gestion des stratégies de groupes, modifiez les paramètres suivants :  
**Configuration ordinateur, Stratégies, Paramètres Windows, Paramètres de sécurité, Services Système**. Pour les propriétés d'**Agent de protection d'accès réseau**, cochez **Définir ce paramètre de stratégie** puis sélectionnez le mode de démarrage du service sur **Automatique**.

**Configuration ordinateur, Stratégies, Paramètres Windows, Paramètres de sécurité, Network Access Protection, Configuration du client NAP, Clients de contrainte**. Activez **Clients de contrainte de quarantaine DHCP**.

**Configuration ordinateur, Stratégies, Modèles d'administration, Composants Windows, Centre de sécurité**. Dans les propriétés d'**Activer le centre de sécurité (ordinateurs appartenant à un domaine uniquement)**, sélectionnez l'option **Activé**.

6. Fermez l'éditeur de gestion des stratégies de groupes et appliquez ces paramètres.
7. Dans **Gestion de la stratégie de groupe**, cliquez sur **NAPGPO**.
8. Dans la section détail dans **Filtrage de sécurité**, supprimez **Utilisateurs authentifiés** puis ajoutez **paclient1**, n'oubliez pas de modifier le type d'objet pour y inclure **ordinateurs**. Dans le monde réel, il faudrait utiliser des groupes.
9. Sur **paclient1**, saisissez `gpupdate /force`.
10. Saisissez `gpresult /v` et contrôlez que la stratégie NAPGPO a été appliquée ainsi que les paramètres.
11. Redémarrez **paclient1** puis contrôlez qu'il n'est pas restreint.

 Ce dernier scénario vous montre comment généraliser l'activation de NAP dans une entreprise en utilisant les stratégies de groupe.

 Cet exercice vous a montré comment mettre en œuvre NAP dans un environnement DHCP. Plusieurs scénarios ont été testés pour montrer le comportement des clients compatibles NAP. Les principaux moyens de configuration du client et des outils de dépannage vous ont également été montrés dans les réponses

proposées.

---



Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 9 - VPN SSTP pour ordinateurs distants

## 1. Objectifs

Dans cet exercice vous allez mettre en œuvre une solution VPN utilisant le protocole SSTP (*Secure Sockets Tunneling Protocol*) composée d'un serveur Active Directory, d'un serveur d'accès distant, d'un serveur de certificats et d'un ordinateur client désirant se connecter au serveur de l'entreprise à l'aide d'un VPN sécurisé.

## 2. Configuration de l'environnement

➤ Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

➤ Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

➤ Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris2**, lancez le script **scriptParis2.bat** (le fichier **WMyDomEni.txt** doit se trouver sur le Bureau). Attendez le redémarrage avant de poursuivre l'installation, ensuite installez le moniteur réseau.
- Sur **paris1**, lancez le script **scriptParis1.bat** et installez le moniteur réseau.
- Sur **paris3**, lancez le script **scriptParis3.bat**.
- Sur **geclient1**, placez les scripts **scriptGeclient1.bat** et **joindom.vbs** sur le Bureau puis lancez le script **scriptGeclient1.bat**. Attention, veillez à l'exécuter en mode administrateur !

Après le lancement des scripts, **paris2** est contrôleur de domaine pour la forêt **mydom.eni** ainsi que serveur **DNS**. Il dispose d'une adresse IP fixe (10.1.1.2/24).

**paris1** est membre du domaine **mydom.eni**. Ses adresses IP sont 10.1.1.1/24 en interne et 172.30.1.1/24 pour le côté Internet.

**paris3** est membre du domaine **mydom.eni**. Ses adresses IP sont 10.1.1.3/24 en interne et 172.30.1.3/24 pour le côté Internet.

**geclient1** est un ordinateur faisant partie du domaine pouvant se trouver sur Internet avec l'adresse IP fixe est 172.30.1.5/230 ou sur le domaine ave l'adresse IP 10.1.1.5/30.

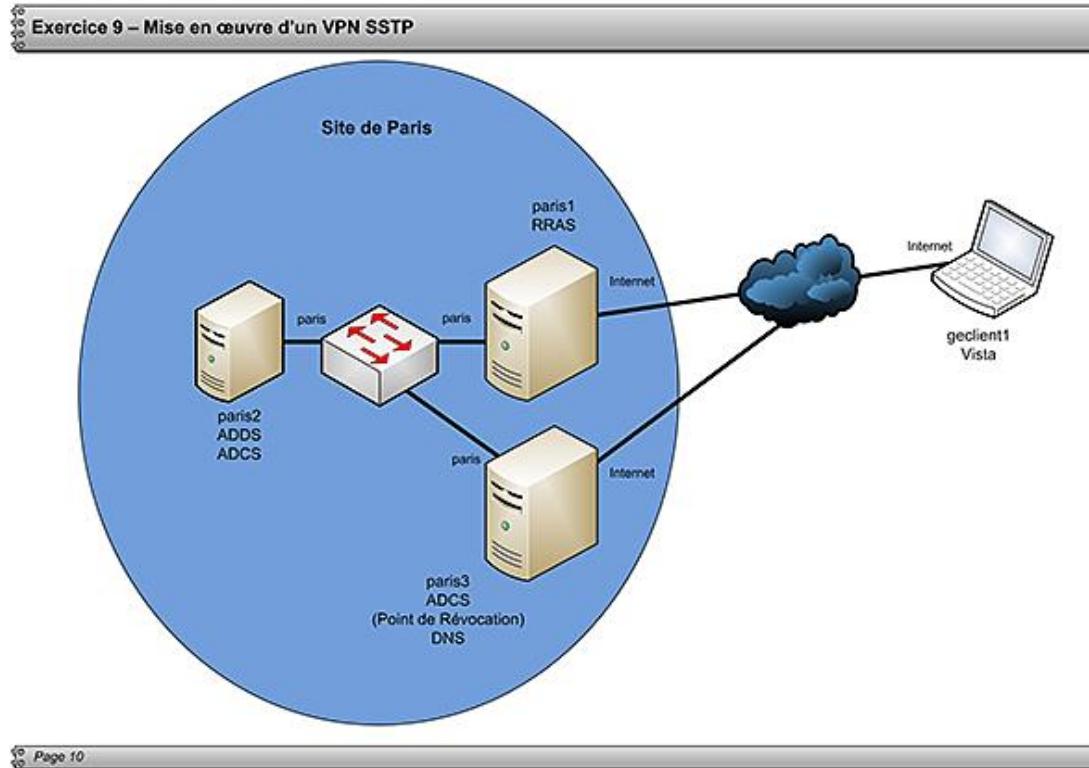
➤ Comme par défaut le protocole icmp est bloqué par le pare-feu, les scripts le modifient pour autoriser le protocole icmpv4 afin que vous puissiez effectuer des tests avec la commande ping.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Configuration des services réseaux avancés et plus particulièrement à la section consacrée aux **VPN**. Les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre d'un VPN SSTP

Avec vos collègues, vous savez déjà implémenter des **VPN** en utilisant diverses technologies y compris le serveur d'accès à distance de Windows pour les protocoles **PPTP** et **L2TP**. Vous voulez tester la mise en œuvre d'un **tunnel VPN SSTP**. Pour cela vous montez un bac à sable composé d'un serveur Active Directory qui servira de serveur de certificats, d'un serveur d'accès à distance et d'un serveur devant gérer la liste de révocation des certificats. Un ordinateur client fonctionnant sous Windows Vista simulera un utilisateur nomade. La difficulté réside dans le fait qu'il est nécessaire de disposer d'un serveur pour contrôler la liste de révocation des certificats. Pour faire simple il a été décidé que le serveur de certificat est un serveur de certificats d'entreprise et que le répondeur pour l'authentification des certificats est le service de rôle le plus simple à installer et à gérer.



Les tâches à effectuer sont :

- Configurer le **serveur DNS** sur **paris3** simulant un serveur DNS externe ne connaissant que les adresses de l'interface externe de **paris1** et **paris3**.
- Installer le service de certificats sur **paris2** pour mettre en place une infrastructure de **PKI**. Le serveur de certificat est de type **Entreprise** et n'est pas visible du côté Internet.
- Installer et configurer le sur **paris3** un répondeur en ligne permettant de valider un certificat et d'indiquer si le certificat est révoqué. Le répondeur en ligne est accessible aussi bien à partir du réseau de l'Entreprise qu'à partir d'Internet.
- Installer et configurer le rôle de serveur d'accès à distance
- Tester la connexion SSTP en créant un utilisateur.

**►** Il est important de suivre les procédures pas à pas et de les effectuer dans l'ordre car dans la version actuelle de Windows Server 2008, il est difficile de modifier le certificat utilisé pour la création du tunnel SSL sur le serveur d'accès à distance. Windows Server 2008 R2 offre des commandes supplémentaires permettant une gestion plus aisée.

## 5. Configurer le serveur simulant le serveur DNS externe sur paris3

**►** paris3 et geclient1 doivent fonctionner.

- 
1. Sur **paris3**, lancez la console DNS.
  2. Créez une nouvelle zone principale de recherche directe appelée mydom.eni qui n'accepte pas les mises à jour dynamiques.
  3. Dans la zone mydom.eni, créez un enregistrement DNS de **type A** pour Paris1.mydom.eni mappé sur l'adresse IP 172.30.1.1.
  4. Faites de même pour paris3.mydom.eni avec l'adresse 172.30.1.3.
  5. Sur geclient1, connectez-vous en tant qu'utilisateur de domaine, puis dans une invite de commande, saisissez ping paris1 et ping paris3. Normalement, vous êtes sur le réseau interne et les réponses proviennent du réseau 10.1.1.0/24.
  6. Ajoutez au **Bureau** les scripts **GotoInternet.bat** et **GotoDomaine.bat**. Ces scripts modifient l'adresse IP et l'adresse DNS de l'ordinateur geclient1 afin qu'il soit dans le domaine ou sur Internet.
  7. Lancez le script **GotoInternet.bat** puis saisissez ping paris1 et ping paris3 dans une invite de commande. Cette fois, les réponses proviennent du réseau 172.30.1.0/24. La connectivité est parfaite pour joindre les ordinateurs **paris1** et **paris3**.
  8. Lancez le script **GotoDomaine.bat**.
- 

 L'ordinateur client peut atteindre les ordinateurs paris1 et paris3 aussi bien depuis l'intérieur de l'entreprise que de l'extérieur.

---

## 6. Installation du rôle de serveur de certificats sur paris2

---

 paris2 est le seul ordinateur requis.

---

1. Sur **paris2**, lancez le **Gestionnaire de Serveur** pour ajouter le rôle de service **Autorité de Certification** du rôle **Services de certificats Active Directory**.
  2. Pour le **Type d'installation**, sélectionnez **Entreprise**.
  3. Pour le **Type d'autorité de certification**, sélectionnez **Autorité de certification racine**.
  4. Pour **Clé privée**, sélectionnez **Créer une nouvelle clé privée**.
  5. Pour **Chiffrement**, acceptez les valeurs proposées.
  6. Pour le **Nom de l'autorité de certification**, acceptez les valeurs proposées.
  7. Pour la **Période de validité**, acceptez les valeurs proposées.
  8. Pour la **Base de données de certificats**, acceptez les valeurs proposées.
  9. Sur la page **Confirmation**, cliquez sur **Installer** puis vérifiez que l'installation s'est bien déroulée.
- 

 Le serveur de certificat est installé. Il sert d'autorité principale de confiance. Néanmoins à ce stade, les autres ordinateurs n'ont pas encore reçu le certificat racine et ne peuvent par conséquent requérir un certificat. Pour l'ajout du certificat de l'autorité principale de confiance, il faudra redémarrer l'ordinateur comme indiqué dans les procédures. L'enrôlement automatique des certificats n'est pas activé afin de montrer quels types de certificats sont nécessaires et à quel moment il faut les demander.

---

## 7. Installation du répondeur en ligne

---

 paris2 et paris3 doivent fonctionner.

---

Comme il est nécessaire de disposer d'un serveur pour interroger l'état d'un certificat, vous allez installer uniquement le rôle de services **Répondeur en ligne** du rôle **Services de certificat Active Directory**.

1. Connectez-vous sur **paris3** en tant qu'administrateur de domaine, installez uniquement le rôle de services **Répondeur en ligne** du rôle **Services de certificat Active Directory**.

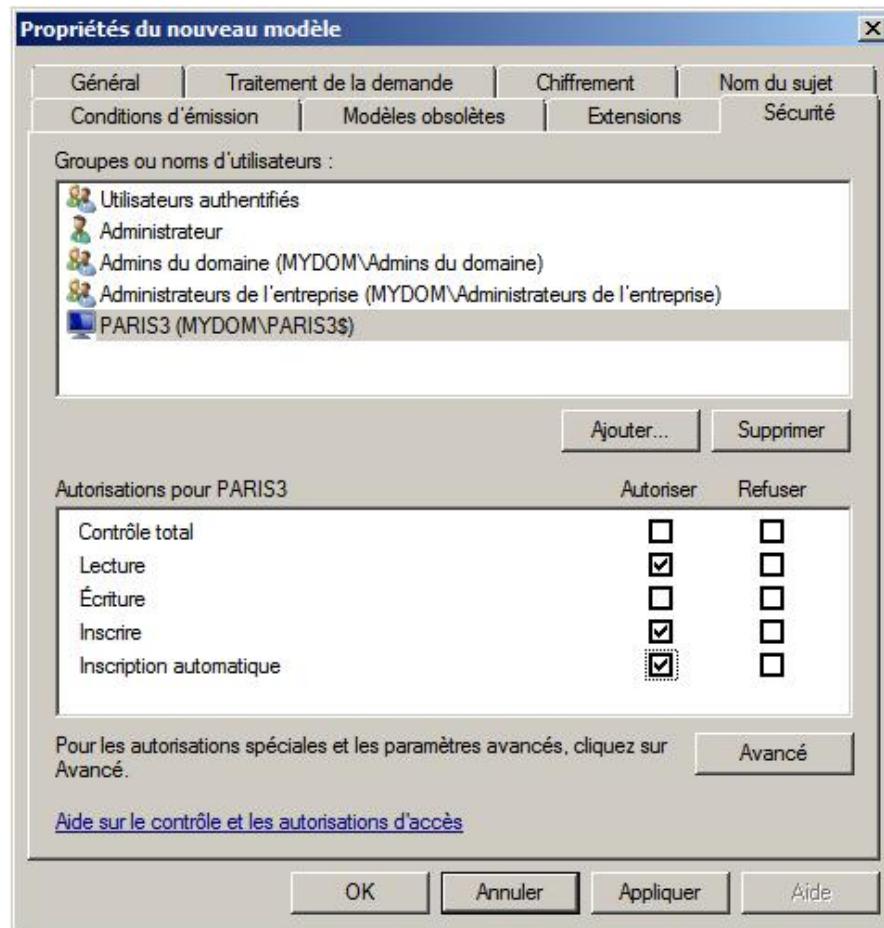
 Le répondeur en ligne est installé ainsi que le serveur IIS qui est nécessaire pour répondre aux demandes.

## 8. Configurer l'autorité de certification pour que le répondeur en ligne puisse répondre aux demandes de signature OCSP

 paris2 et paris3 doivent fonctionner.

paris3 doit disposer d'un certificat particulier lui permettant de pouvoir répondre aux demandes de signature OCSP. Par défaut, ce type de certificats n'est pas activé. Vous allez donc créer une copie du modèle puis permettre uniquement à paris3 de pouvoir demander un tel certificat pour des raisons évidentes de sécurité. D'autre part, vous allez indiquer à l'autorité de certification qu'il existe un répondeur en ligne accessible depuis une URL spécifique. Cette information sera par la suite incluse dans les certificats qui seront émis et permettra à l'ordinateur client d'interroger le répondeur en ligne pour obtenir le statut du certificat.

1. Sur **paris2**, dans une MMC vierge ajoutez le **snap-in Modèles de certificats**.
2. Dans la zone de détail pour le nœud **Modèles de certificats**, cliquez avec le bouton droit de la souris sur **Signature de la réponse OCSP** puis sur **Duplicer le modèle**.
3. Sur la boîte de message qui apparaît, sélectionnez **Windows Server 2008, Edition Enterprise** puis cliquez sur **OK**.
4. Sur la boîte de dialogue **Propriétés du nouveau modèle**, modifiez le **Nom complet du modèle** en **OCSP pour Paris3** sur l'onglet **Général** puis sur l'onglet **Sécurité**, cliquez sur **Ajouter**.
5. Dans la boîte de dialogue **Sélectionnez Utilisateurs, Ordinateurs ou Groupes**, cliquez sur **Types d'objets** pour inclure **Ordinateurs** puis saisissez paris3 dans la zone de texte **Entrez les noms d'objets à sélectionner** et cliquez sur **OK**.
6. Sur la boîte de dialogue **Propriétés du nouveau modèle**, sélectionnez **paris3** et modifiez ses permissions comme le montre la figure suivante puis cliquez sur **OK**.



1. Sur **paris2**, lancez la console **Autorité de certification**.
2. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **mydom-Paris2-CA** puis sur **Propriétés**.
3. Sélectionnez l'extension **Accès aux informations de l'autorité (AIA)** de l'onglet **Extensions**.
4. Ajoutez `http://paris3.mydom.eni/ocsp` comme emplacement.
5. Sélectionnez l'emplacement `http://paris3.mydom.eni/ocsp` puis cochez les cases **Inclure dans l'extension AIA des certificats émis** et **Inclure dans l'extension OCSP (Online Certificate Status Protocol)** et cliquez sur **OK**.
6. Sur le message qui apparaît vous demandant de redémarrer les services, cliquez sur **Oui**.
7. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Modèles de certificats** puis sur **Nouveau Modèle de certificat à délivrer**.
8. Dans la liste des modèles de certificats, sélectionnez **OCSP pour Paris3** puis cliquez sur **OK**.

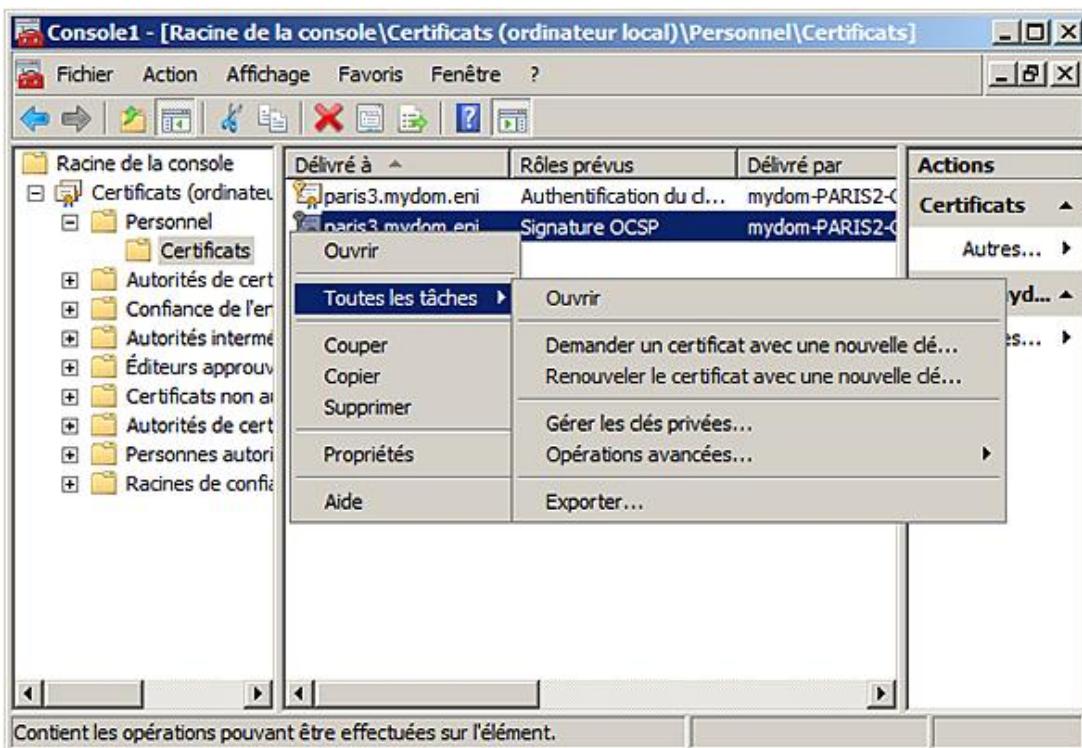
 Vous avez ajouté le modèle de certificat pour que **paris3** puisse l'utiliser afin de signer les réponses de demande pour connaître le statut d'un certificat. Vous avez également modifié la configuration de l'autorité de certification pour indiquer l'URL du répondre en ligne.

## 9. Configurer le répondre en ligne

 **paris2** et **paris3** doivent fonctionner.

La première étape consiste à requérir un certificat basé sur le modèle **OCSP pour Paris3**. Comme le certificat de l'autorité principale de confiance n'est pas dans le magasin, il est nécessaire de redémarrer l'ordinateur (Il est possible d'exporter et d'importer le certificat). Ensuite, il faut configurer le répondeur en ligne.

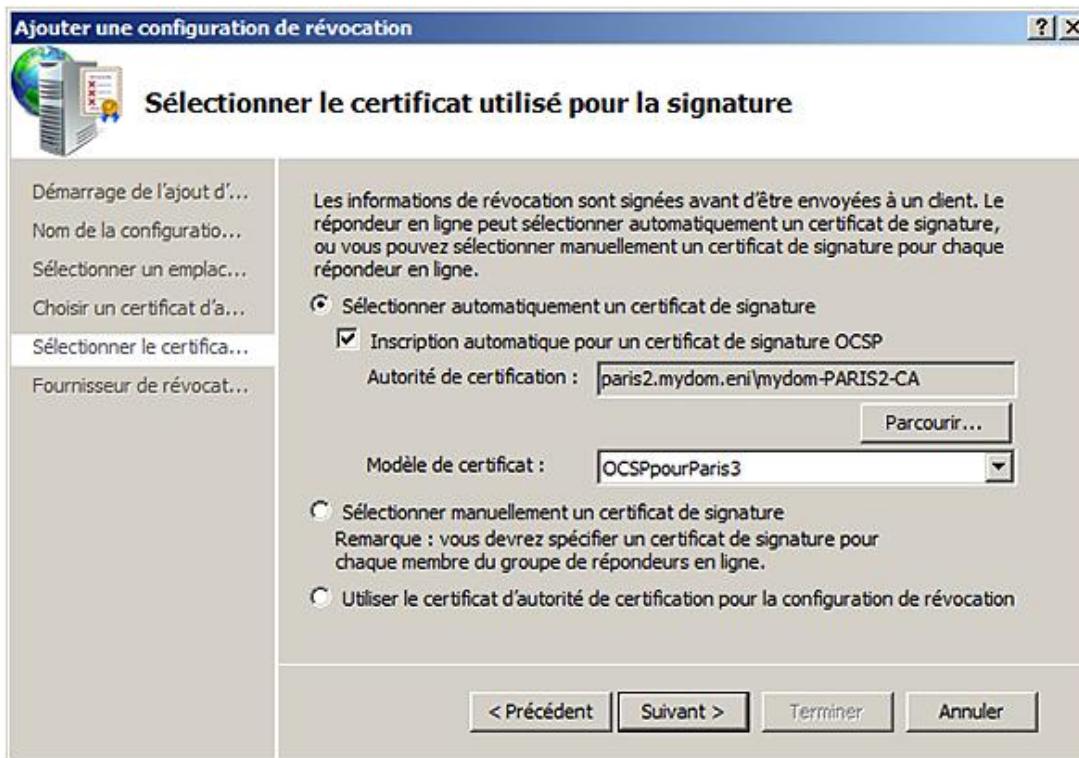
1. Redémarrez **paris3**.
2. Sur **paris3**, dans une console **MMC** vierge, ajoutez le **snap-in certificats** pour l'ordinateur local.
3. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Personnel** puis sur **Toutes les tâches - Demander un nouveau certificat**.
4. Dans l'assistant sur la page **Avant de commencer**, cliquez sur **Suivant**.
5. Sur la page **Demander des certificats**, sélectionnez **OCSP pour Paris3** et éventuellement **Ordinateur**, puis cliquez sur **Inscription**. Enfin cliquez sur **Terminer**.
6. Dans la zone de détail, cliquez avec le bouton droit de la souris sur le certificat nouvellement créé dont le rôle prévu est **Signature OCSP** puis sur **Toutes les tâches - Gérer les clés privées** comme le montre la figure suivante :



1. Dans la boîte de dialogue **Autorisations pour <Aucun> Private keys**, cliquez sur **Ajouter**.
2. Dans la boîte de dialogue **Sélectionnez Utilisateurs, Ordinateurs ou Groupes**, saisissez Service réseau dans la zone de texte **Entrez les noms d'objets à sélectionner** et cliquez sur **OK**.
3. Vérifiez que les autorisations sont **Contrôle total (Autoriser)** puis cliquez sur **OK**.
4. Sur **paris3**, démarrez la console **Gestion des répondeurs en ligne**.
5. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Configuration de révocation** puis sur **Ajouter une configuration de révocation**.
6. Dans l'assistant, sur la page **Démarrage de l'ajout d'une configuration de révocation**, cliquez sur **Suivant**.
7. Sur la page **Nom de la configuration de révocation**, saisissez **paris3\_RPL** puis cliquez sur **Suivant**.
8. Sur la page **Sélectionner un emplacement de certificat d'autorité de certification**, sélectionnez **Sélectionner un certificat pour une autorité de certification d'entreprise**.

**existante**, puis cliquez sur **Suivant**.

9. Sur la page **Choisir un certificat d'autorité de certification**, sélectionnez **Parcourir les certificats d'autorité de certification publiés dans Active Directory** puis cliquez sur **Parcourir**.
10. Dans la boîte de dialogue **Sélectionner une Autorité de certification**, sélectionnez **mydom-PARIS2-CA** puis cliquez sur **OK** et ensuite sur **Suivant**.
11. Sur la page **Sélectionner le certificat utilisé pour la signature**, sélectionnez les options comme le montre la figure suivante puis cliquez sur **Suivant**.



1. Sur la page **Fournisseur de révocation**, cliquez sur **Terminer**.

➤ Le répondre est maintenant configuré et opérationnel.

## 10. Installation et configuration du rôle de serveur d'accès à distance

➤ paris1, paris2 et paris3 doivent fonctionner, les opérations s'effectuent sur paris2

Pour démarrer, il est nécessaire de demander un certificat qui sera utilisé pour le tunnel SSL, puis d'installer le service de routage et d'accès à distance et enfin le configurer.

1. Redémarrez **paris1** pour ajouter l'autorité de certification racine.
2. Sur **paris1**, créez une console **MMC** pour le **Snap-In Certificats (ordinateur local)**.
3. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Personnel**, puis **Toutes les tâches - Demander un nouveau certificat**. Ce certificat sera utilisé par le client pour authentifier le serveur SSTP.
4. Sur la page **Demander des certificats**, cochez **Ordinateur**, puis cliquez sur **Inscription**.
5. Dans l'arborescence, vous pouvez visualiser votre certificat dans la section détail de Certificats (ordinateur local) | Personnel | Certificats. Si vous l'ouvrez, sur l'onglet **Détail** vous pouvez voir dans le champ **Accès aux informations de l'Autorité** le nom du serveur **paris3**.

6. Cliquez avec le bouton droit sur le certificat puis cliquez sur **Propriétés**.
7. Sur l'onglet **Général**, sélectionnez **N'activer que les rôles suivants** pour les rôles du certificat puis cliquez sur **OK**.
8. Installez **Services de routage et d'accès à distance** du rôle **Services de stratégie et d'accès réseau**.
9. Lancez la console **Routage et accès distant** et lancez l'assistant **Configurer et activer le routage et l'accès à distance**.
10. Sur la page **Configuration**, sélectionnez **Accès à distance (connexion à distance ou VPN)**.
11. Sur la page **Accès à distance**, sélectionnez **VPN**.
12. Sur la page **Connexion VPN**, sélectionnez **Internet** comme interface réseau.
13. Sur la page **Attribution d'adresses IP**, sélectionnez **A partir d'une plage d'adresses spécifiée**.
14. Sur la page **Assignment de plages d'adresses**, spécifiez de 10.100.1.1 à 10.100.1.10.
15. Sur la page **Gestion de serveurs d'accès à distance multiples**, sélectionnez **Non, utiliser Routage et accès distant pour authentifier les demandes de connexion**.

 Un certificat Ordinateur a été demandé qui sera utilisé pour le tunnel SSL et le serveur d'accès distant est installé et configuré.

## 11. Ajout d'un utilisateur dans l'Active Directory et configuration du compte pour être client d'accès distant

 paris2 est le seul ordinateur requis.

Vous allez créer un utilisateur et lui donner le droit de se connecter à distance.

1. Sur **paris2**, lancez **Utilisateurs et ordinateurs Active Directory**.
2. Dans l'arborescence, cliquez avec le bouton droit de la souris sur **Users** puis sur **Nouveau - Utilisateur**.
3. Saisissez **toto** pour le **Prénom** ainsi que le **Nom d'ouverture de session de l'utilisateur**. Ensuite, cliquez sur **Suivant**.
4. Saisissez **Pa\$\$word** pour le mot de passe et sa confirmation. Décochez **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**. Ensuite, cliquez sur **Suivant** puis sur **Terminer**.
5. Dans la section de détail du conteneur **Users**, cliquez avec le bouton droit de la souris sur **toto** puis sur **Propriétés**.
6. Sélectionnez **Autoriser l'accès** sur l'onglet **Appel entrant** puis cliquez sur **OK**.

 L'utilisateur **toto** est créé et peut utiliser l'accès à distance.

## 12. Test de connexion en créant une connexion VPN PPTP

 paris1, paris2 et geclient1 doivent fonctionner, les opérations s'effectuent sur geclient1.

1. Sur **geclient1**, lancez le script **GotoInternet.bat**.
2. Ouvrez le **Centre Réseau et partage**.
3. Dans les tâches, cliquez sur **Configurer une connexion ou un réseau**.
4. Dans l'assistant, sur la page **Choisir une option**, cliquez sur **Connexion à votre espace de travail**, puis cliquez sur **Suivant**.
5. Sur la page **Comment voulez-vous vous connecter?**, cliquez sur **Utiliser ma connexion Internet (VPN)**.
6. Sur la page **Voulez-vous configurer une connexion Internet avant de continuer?**, cliquez sur **Je configurerai une connexion Internet ultérieurement**.
7. Sur la page **Entrez l'adresse Internet à laquelle vous souhaitez vous connecter**, saisissez paris1.mydom.eni pour l'**Adresse Internet** et VPN PPTP Paris pour le **Nom de la destination**, enfin cliquez sur **Suivant**.
8. Sur la page **Entrez votre nom d'utilisateur et votre mot de passe**, saisissez toto pour le **Nom d'utilisateur**, Pa\$\$word pour le **Mot de passe** et mydom pour le **Domaine (facultatif)**. N'oubliez pas de cocher la case **Mémoriser ce mot de passe**. Enfin, cliquez sur **Créer**.
9. Dans **Tâches**, cliquez sur **Gérer les connexions réseau**.
10. Sur **paris2** et **paris1**, lancez le moniteur réseau puis démarrez une capture.
11. Sur la fenêtre **Connexions Réseau**, cliquez avec le bouton droit de la souris sur **VPN PPTP Paris**, puis sur **Connecter**.
12. Dans une invite de commande, saisissez ipconfig pour voir que la connexion VPN est active ainsi que ping 10.1.1.2 pour atteindre **paris2**. Cela prouve que la connexion VPN fonctionne.
13. Sur **paris2** et **paris1**, examinez les captures.

 La connexion VPN via PPTP fonctionne.

### 13. Test de connexion en créant une connexion VPN SSTP

 paris1, paris2, paris3 et geclient1 doivent fonctionner, les opérations s'effectuent sur geclient1.

1. Sur **geclient1**, lancez le script **GotoDomaine.bat**.
2. Redémarrez l'ordinateur.
3. Lancez le script **GotoInternet.bat**.
4. Ouvrez le **Centre Réseau et partage** et créez une nouvelle connexion VPN appelée **VPN SSTP Paris** en utilisant les mêmes paramètres que pour la connexion VPN PPTP Paris.
5. Sur la fenêtre **Connexions réseau**, cliquez avec le bouton droit de la souris sur **VPN SSTP Paris** puis sur **Propriétés**.
6. Sélectionnez **Protocole SSTP (Secure Socket Tunneling Protocol)** sous **Type de réseau VPN** dans l'onglet **Gestion de réseau** puis cliquez sur **OK**.
7. Sur **paris2** et **paris1**, lancez le moniteur réseau puis démarrez une capture.
8. Sur la fenêtre **Connexions Réseau**, cliquez avec le bouton droit de la souris sur **VPN SSTP Paris** puis sur **Connecter**.
9. Dans une invite de commande, saisissez ipconfig pour voir que la connexion VPN est active ainsi que ping 10.1.1.2 pour atteindre **paris2**. Cela prouve que la connexion **VPN** fonctionne.

10. Sur **paris2** et **paris1**, examinez les captures.
11. Fermez la connexion VPN.
12. Enfin sur **paris1**, désactivez la règle d'entrée **Routage et accès distant (GRE-Entrée)** sur le pare-feu avec fonctions avancées. Puis tentez successivement une connexion **VPN PPTP** et **VPN SSTP**.

---

➤ Dans cet exercice, vous avez vu comment mettre en œuvre un serveur d'accès distant qui accepte des connexions VPN SSTP. Il vous a fallu pour cela mettre en œuvre une infrastructure PKI pour gérer les certificats. Plusieurs aspects concernant les bonnes pratiques pour implémenter l'infrastructure PKI et la sécurité n'ont pas été abordés pour simplifier l'exercice.

---

➤ Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 8 - Accès à Internet et accès depuis Internet

## 1. Objectifs

Dans cet exercice vous allez installer et configurer la traduction d'adresses réseau NAT pour permettre aux utilisateurs de l'entreprise l'accès à Internet. Vous allez également permettre à des utilisateurs externes de pouvoir accéder à des ressources internes.

## 2. Configuration de l'environnement

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt** doit se trouver sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres ordinateurs.
- Sur **paris2**, lancez le script **scriptParis2.bat**.
- Sur **paris3**, lancez le script **scriptParis3.bat**.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**, ensuite installez le moniteur réseau.
- Sur **geneve2**, lancez le script **scriptGeneve2.bat**.

Après le lancement des scripts, paris1 est contrôleur de domaine pour la forêt mydom.eni ainsi que serveur DNS et routeur. Ses adresses IP sont 10.1.1.1/24 en interne et 172.30.1.1/24 pour le côté Internet.

**paris2** est membre du domaine mydom.eni et dispose d'une adresse IP fixe (10.1.1.2/24).

**paris3** est membre du domaine mydom.eni et dispose d'une adresse IP fixe (10.1.1.3 /24).

**geneve1** est un serveur Web se trouvant sur Internet. Il n'est pas membre du domaine mydom.eni. Son adresse IP fixe est 172.30.1.2/24. Il utilise pour le test le serveur DNS de mydom.eni.

**geneve2** est membre du domaine mydom.eni, il simule un client VPN. Il dispose d'une adresse IP fixe (172.30.1.3/24).

 Comme par défaut le protocole icmp est bloqué par le pare-feu, les scripts le réactivent pour que vous puissiez effectuer des tests avec la commande ping.

## 3. Référence par rapport à la théorie

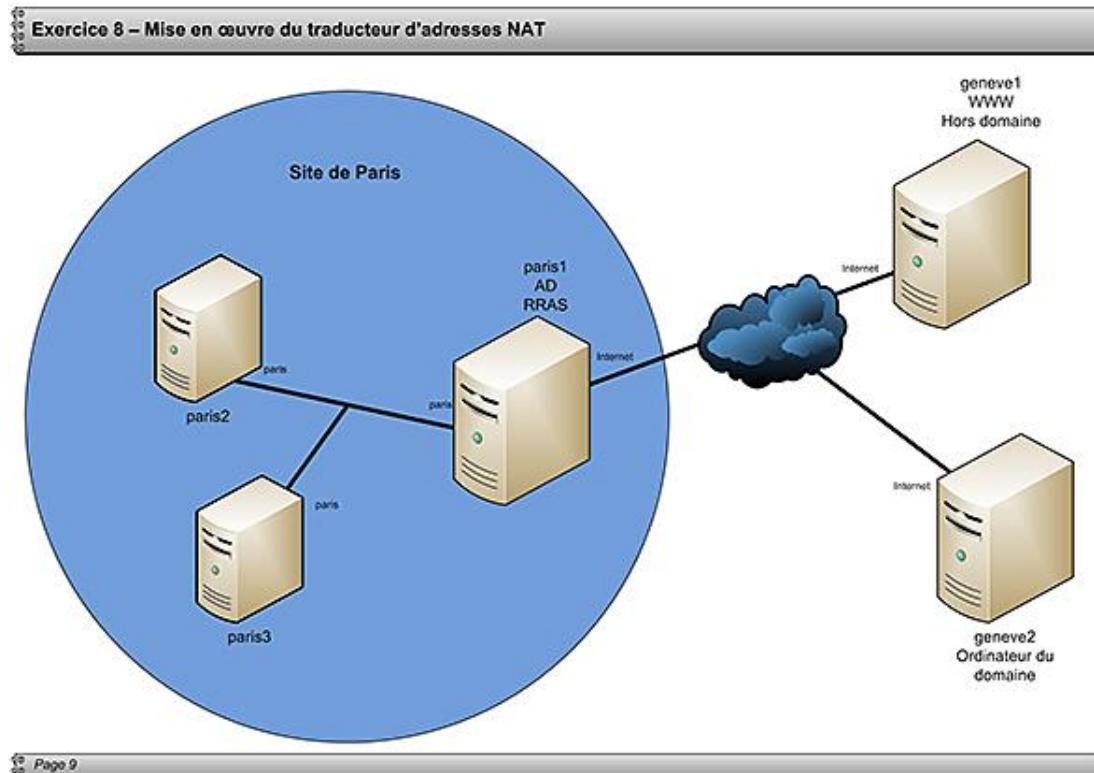
Vous pouvez vous référer au chapitre Configuration des services réseaux avancés et plus particulièrement à la section consacrée à NAT. Les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre du traducteur d'adresses NAT

Avec vos collègues, vous désirez vérifier la définition du **NAT** Microsoft. Pour certains NAT mappe chaque adresse **IPv4** interne vers son adresse IP externe correspondante (mappage 1:1). Pour d'autres, il s'agit uniquement d'une translation de ports et qui nécessite une seule adresse IP externe pour toutes les adresses du réseau interne.

Dans le second scénario, vous allez permettre à un utilisateur externe de pouvoir accéder au Bureau distant sur un ordinateur interne.

Dans cet exercice, les ordinateurs de Genève simulent des ordinateurs se situant directement sur Internet.



Les tâches à effectuer sont :

- Installation du routage et d'accès à distance sur **paris1**.
- Configuration du serveur d'accès à distance en tant que serveur **NAT**.
- Test de la configuration du **NAT** en se connectant sur le serveur **Web** depuis **paris2** et **paris3**. Les trames sont récupérées via le moniteur réseau.
- Test de la configuration du serveur **NAT** pour permettre à un utilisateur d'accéder au **Bureau distant** de **paris3**.
- Test de la configuration pour l'accès au **Bureau distant**.

## 5. Installation du serveur de routage et d'accès à distance

► Seul l'ordinateur **paris1** est requis.

1. Sur **paris1**, installez le service d'accès à distance. Il est indiqué ici la commande :  
`ServerManagerCmd -install NPAS-RRAS-SERVICES`

► Le service d'accès à distance est installé mais il n'est pas configuré.

## 6. Configuration du serveur d'accès à distance en tant que serveur NAT

 Seul l'ordinateur **paris1** est requis.

1. Sur **paris1**, lancez **Routage et accès distant**.
2. Dans l'arborescence, sur le nœud du serveur, cliquez avec le bouton droit de la souris puis sur **Configurer et activer le routage et l'accès à distance**.
3. Sur la page de bienvenue de l'assistant, cliquez sur **Suivant**.
4. Sur la page **Configuration**, sélectionnez **Configuration personnalisée** puis cliquez sur **Suivant**.
5. Sur la page **Configuration personnalisée**, sélectionnez **NAT** puis cliquez sur **Suivant**.
6. Sur la page **Fin de l'assistant**, cliquez sur **Terminer** et faites démarrer les services.
7. Dans l'arborescence, sur le nœud **NAT**, cliquez avec le bouton droit de la souris puis sur **Nouvelle interface**.
8. Dans la boîte de dialogue **Nouvelle interface pour IPNAT**, sélectionnez **Internet** puis cliquez sur **OK**.
9. Sur la boîte de dialogue **Propriétés de Propriétés de Traduction d'adresses réseau**, sélectionnez **Interface publique connectée à Internet** et cochez la case **Activer NAT sur cette interface**, enfin cliquez sur **OK**.
10. Dans l'arborescence, sur le nœud **NAT**, cliquez avec le bouton droit de la souris puis sur **Nouvelle interface**.
11. Dans la boîte de dialogue **Nouvelle interface pour IPNAT**, sélectionnez **paris** puis cliquez sur **OK**.
12. Sur la boîte de dialogue **Propriétés de Propriétés de Traduction d'adresses réseau**, sélectionnez **Interface privée connectée au réseau privé**, enfin cliquez sur **OK**.

 Votre serveur est configuré en tant que serveur NAT.

## 7. Test de la configuration du NAT

 Les ordinateurs **paris1**, **paris2**, **paris3** et **geneve1** sont requis.

1. Sur **geneve1** lancez le moniteur réseau et une capture en créant un filtre pour le protocole **HTTP**.
2. Sur **paris1**, contrôlez qu'un enregistrement existe pour **geneve1** sinon rajoutez-le avec l'adresse 172.30.1.2.
3. Sur **paris1**, lancez Internet Explorer pour atteindre <http://geneve1>, ensuite sur **geneve1**, examinez les trames capturées et surtout la source et la destination.
4. Sur **paris1**, en utilisant **Routage et accès distant**, développez l'arborescence jusqu'au nœud **NAT** puis examinez dans la fenêtre de détails les statistiques. Normalement il ne devrait pas encore y avoir de paquets entrants et sortants.
5. Dans la fenêtre de détails, cliquez avec le bouton droit de la souris sur l'interface **Internet** puis sur **Afficher les mappages**. La boîte de dialogue doit être vide.
6. Faites de même sur **paris2** et **paris3** tout en examinant les différents éléments

présentés.

- 
- Il peut être utile de garantir qu'**Internet Explorer** recharge chaque fois la page en cliquant sur l'option **A chaque visite de pages** de la boîte de dialogue **Paramètres des fichiers Internet temporaires et de l'historique** du bouton **Paramètres** de la zone **Historique de navigation** de l'onglet **Général** des **Options Internet**.
  
  - Les tests vous ont montré que les ordinateurs paris2 et paris3 sont vus comme étant paris1 sur l'interface externe du NAT. L'affichage des mappages montre également le mappage des ports.
- 

## 8. Configuration du NAT pour permettre l'accès depuis Internet au Bureau distant

- 
- Seul l'ordinateur **paris1** est requis.
  
    1. Sur **paris1**, dans l'arborescence, cliquez sur le nœud **NAT** pour faire apparaître la fenêtre de détail.
    2. Dans la fenêtre de détail, cliquez avec le bouton droit de la souris sur l'interface internet puis sur **Propriétés**.
    3. Sur l'onglet **Services et ports**, cliquez sur **Bureau à distance** dans la liste des services.
    4. Sur la boîte de dialogue **Modifier le service**, saisissez 10.1.1.3 dans la zone **Adresse privée** puis cliquez deux fois sur **OK**.  
  - La configuration est terminée.
- 

## 9. Test de la configuration d'accès depuis Internet

- 
- Les ordinateurs paris1, paris3, geneve1 et geneve2 sont requis.
  
    1. Tout d'abord, il faut activer le **Bureau distant** sur **paris2**.
    2. Sur **geneve1**, lancez **Connexion Bureau à distance** dans la boîte de dialogue saisissez 172.30.1.1 pour **Ordinateur** ce qui correspond à l'adresse visible par **geneve1** puis cliquez sur **Connexion**.
    3. Dans la boîte de dialogue **Sécurité de Windows**, saisissez administrateur pour le nom de l'utilisateur et Pa\$\$word pour le mot de passe. Au bout de quelques secondes, le **Bureau de paris3** se trouve sur **geneve1**.
    4. Faites de même avec **geneve2**. Il ne devrait pas y avoir de différence, que vous soyez sur un ordinateur du domaine ou non.  
  - Dans cet exercice vous avez configuré routage et accès à distance pour NAT que ce soit pour permettre un accès à Internet ou depuis Internet.
  
  - Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.
-

# Exercice 7 - Sécurisation des liaisons intersites

## 1. Objectifs

Dans cet exercice vous allez sécuriser l'environnement intersites en créant un tunnel VPN PPTP. Ensuite vous allez étudier les paquets qui circulent sur le réseau.

## 2. Configuration de l'environnement

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt** doit se trouver sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres ordinateurs. Ensuite installez le moniteur réseau.
- Sur **paris2**, lancez le script **scriptParis2.bat**. Ensuite installez le moniteur réseau.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**.
- Sur **geneve2**, placez les scripts **scriptGeneve2.bat**.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt mydom.eni ainsi que serveur **DNS**. Ses adresses IP sont 10.1.1.1/24 sur le segment paris et 172.30.1.1/24 sur le segment internet. Le moniteur réseau est installé.

**paris2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.1.1.2/24). Le moniteur réseau est installé.

**geneve1** est membre du domaine **mydom.eni**. Ses adresses IP fixes sont 172.30.1.2/24 sur le segment internet et 192.168.1.1/24 sur le segment geneve.

**geneve2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe 192.168.1.2/24.

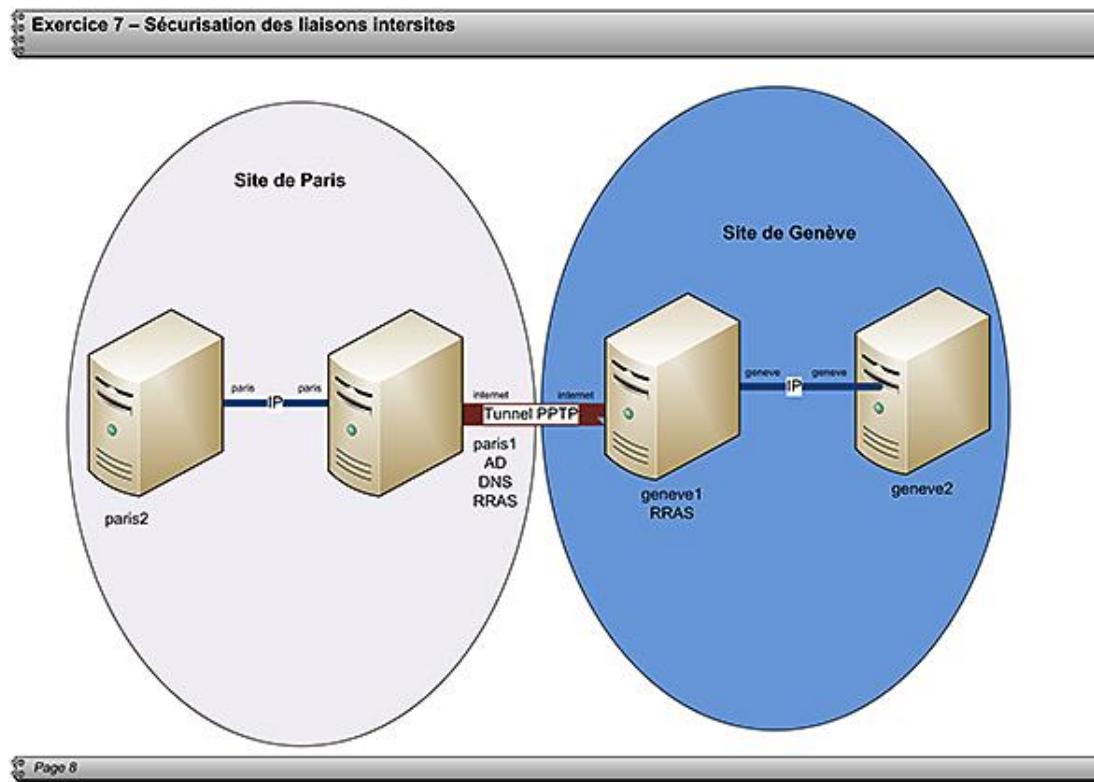
 Comme par défaut le protocole **icmp** est bloqué par le pare-feu, les scripts le réactivent pour que vous puissiez effectuer des tests avec la commande ping.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Configuration des services réseaux avancés et plus particulièrement à la section consacrée au VPN, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la sécurisation des liaisons intersites

Les consultants ont déterminé qu'il était de la responsabilité de l'entreprise de gérer la sécurité de la liaison intersite entre Genève et Paris. Pour cela, ils préconisent la mise en place d'un tunnel **L2TP/IPsec** ou **PPTP** entre les serveurs **paris1** et **geneve1** qui seront les points de terminaison du tunnel. Après étude, il s'avère qu'actuellement il n'est pas possible d'implémenter IPsec entre les serveurs **paris1** et **geneve1**. Il faut donc implémenter PPTP.



Les tâches à effectuer sont :

- Installation du service d'accès à distance sur **paris1** et **geneve1**.
- Configuration du service d'accès à distance sur **paris1** et **geneve1**.
- Création d'une connexion à la demande sur **paris1** et **geneve1**.
- Test de la connexion à l'aide de la commande **ping** et étude des paquets à l'aide du moniteur réseau.

## 5. Installation, configuration et création d'une connexion à la demande sur paris1 et geneve1

Les opérations se déroulent sur les ordinateurs **paris1** et **geneve1**.

1. Successivement sur **geneve1** et **paris1**, installez le **service d'accès à distance**. Le **routage** n'est pas requis. Vous pouvez également saisir `ServerManagerCmd -install NPAS-RRAS`.
2. Successivement sur **geneve1** et **paris1**, lancez **Routage et accès distant** puis cliquez avec le bouton droit de la souris sur le nom du serveur et ensuite sur **Configurer et activer le routage et l'accès à distance**.
3. Sur la page **Bienvenue!**, cliquez sur **Suivant**.
4. Sur la page **Configuration**, sélectionnez **Accès à distance (connexion à distance ou VPN)** puis cliquez sur **Suivant**.
5. Sur la page **Accès à distance**, cochez la case **VPN** puis cliquez sur **Suivant**. Vous

configurez le serveur afin qu'il puisse répondre à des demandes de connexion.

6. Sur la page **Connexion VPN**, cliquez sur l'interface réseau internet pour définir la carte qui est connectée à Internet puis cliquez sur **Suivant**.
7. Sur **geneve1** uniquement la page **Sélection du réseau** apparaît, sélectionnez **geneve** pour l'interface réseau puis cliquez sur **Suivant**.
8. Sur la page **Attribution d'adresses IP**, sélectionnez **A partir d'une plage d'adresses spécifiées** puis cliquez sur **Suivant**.
9. Sur la page **Assignation de plages d'adresses**, ajoutez pour :
  - **geneve1** de 10.100.1.1 à 10.100.1.6 (il nous faut au maximum deux adresses), les plages choisies sont arbitraires et seront utilisées pour faire passer les paquets dans le tunnel.
  - **paris1** de 10.200.1.1 à 10.200.1.6 (il nous faut au maximum deux adresses).

Enfin cliquez sur **Suivant**.

10. Sur la page **Gestion de serveurs d'accès à distance multiples**, sélectionnez **Non, utiliser Routage et accès distant pour authentifier les demandes de connexion** puis cliquez sur **Suivant**.
11. Sur la page **Fin de l'installation**, cliquez sur **Terminer**.
12. Cliquez **OK** sur la boîte de dialogue qui pourrait apparaître vous indiquant que **Windows n'a pas pu ajouter cet ordinateur à la liste des serveurs d'accès à distance valide dans l'Active Directory**.
13. Cliquez **OK** sur la boîte de dialogue qui pourrait apparaître vous indiquant **qu'il faudrait configurer le relais DHCP avec votre adresse IP**.
14. Le service **Routage et accès à distance doit avoir démarré**. Et votre serveur est configuré et opérationnel pour accepter des connexions entrantes (PPTP, L2TP et SSTP).
15. Sur **geneve1**, vous allez ajouter une nouvelle interface réseau pour pouvoir initier le cas échéant le tunnel, il sera défini comme étant bidirectionnel. Dans l'arborescence de la console **Routage et accès distant**, cliquez avec le bouton droit de la souris sur **Interfaces réseau** puis sur **Nouvelle interface de connexion à la demande**.
16. Sur la page **Bienvenue!**, cliquez sur **Suivant**.
17. Sur la page **Nom de l'interface**, saisissez **VPN\_PARIS** puis cliquez sur **Suivant**.
18. Sur la page **Type de connexion**, sélectionnez **Se connecter en utilisant un réseau privé virtuel (VPN)** puis cliquez sur **Suivant**.
19. Sur la page **Type de réseau privé virtuel**, sélectionnez **Protocole PPTP (Point To Point Tunneling Protocol)** puis cliquez sur **Suivant**.
20. Sur la page **Adresse de destination**, saisissez 172.30.1.1 soit l'adresse de **paris1** sur le segment Internet puis cliquez sur **Suivant**.
21. Sur la page **Protocoles et sécurité**, sélectionnez **Router les paquets IP sur cette interface** et **Ajouter un compte d'utilisateur pour qu'un routeur distant puisse effectuer un appel entrant** avant de cliquer sur **Suivant**.
22. Sur la page **Itinéraires statiques pour les réseaux distants**, ajoutez le réseau 10.1.1.0 avec le masque 255.255.255.0 et un métrique de 1 puis cliquez sur **Suivant**. Il s'agit du segment de réseau paris qui n'est pas encore accessible.
23. Sur la page **Informations d'identification des appels entrants**, saisissez **Pa\$\$word** pour le mot de passe. Notez le nom de l'utilisateur qui sera créé localement sur l'ordinateur.
24. Sur la page **Informations d'identification des appels sortants**, saisissez **VPN\_GENEVE** pour le nom de l'utilisateur, **mydom** pour le domaine et **Pa\$\$word** pour le mot de passe. Comme **paris1** est un contrôleur de domaine, le compte sera créé dans l'Active Directory.

25. Sur la page **Fin de l'installation**, cliquez sur **Terminer**. Vous pouvez voir votre nouvelle connexion à la demande et actuellement son état est déconnecté.
26. Sur **paris1**, vous allez effectuer la même opération mais en utilisant les valeurs indiquées. Dans l'arborescence de la console **Routage et accès distant**, cliquez avec le bouton droit de la souris sur **Interfaces réseau** puis sur **Nouvelle interface de connexion à la demande**.
27. Sur la page **Bienvenue!**, cliquez sur **Suivant**.
28. Sur la page **Nom de l'interface**, saisissez **VPN\_GENEVE** puis cliquez sur **Suivant**.
29. Sur la page **Type de connexion**, sélectionnez **Se connecter en utilisant un réseau privé virtuel (VPN)** puis cliquez sur **Suivant**.
30. Sur la page **Type de réseau privé virtuel**, sélectionnez **Protocole PPTP (Point To Point Tunneling Protocol)** puis cliquez sur **Suivant**.
31. Sur la page **Adresse de destination**, saisissez **172.30.1.2** soit l'adresse de **geneve1** sur le segment internet puis cliquez sur **Suivant**.
32. Sur la page **Protocoles et sécurité**, sélectionnez **Router les paquets IP sur cette interface** et **Ajouter un compte d'utilisateur pour qu'un routeur distant puisse effectuer un appel entrant** avant de cliquer sur **Suivant**.
33. Sur la page **Itinéraires statiques pour les réseaux distants**, ajoutez le réseau **192.168.1.0** avec le masque **255.255.255.0** et un métrique de **1** puis cliquez sur **Suivant**. Il s'agit du segment de réseau **geneve** qui n'est pas encore accessible.
34. Sur la page **Informations d'identification des appels entrants**, saisissez **Pa\$\$word** pour le mot de passe. Notez le nom de l'utilisateur qui sera créé localement sur l'ordinateur et dont vous avez déjà indiqué les informations d'authentification pour la connexion depuis **geneve1**.
35. Sur la page **Informations d'identification des appels sortants**, saisissez **VPN\_PARIS** pour le nom de l'utilisateur, **geneve1** pour le domaine et **Pa\$\$word** pour le mot de passe.
36. Sur la page **Fin de l'installation**, cliquez sur **Terminer**. Vous pouvez voir votre nouvelle connexion à la demande et actuellement son état est déconnecté.
37. Cliquez avec le bouton droit de la souris sur l'interface **VPN\_GENEVE** puis sur **Se connecter**. Votre tunnel doit être opérationnel.

 Normalement, la connexion devrait être établie en 10 secondes. En cas d'erreur, lisez attentivement le message et tentez un dépannage. Si l'erreur provient d'un mot de passe ou d'un nom erroné, contrôlez non seulement les éléments de connexion mais également les comptes qui ont été créés. Si les serveurs ne peuvent pas se contacter, il s'agit sûrement d'un problème de liaison existant entre les machines virtuelles, contrôlez le mappage voire arrêtez le service puis tentez un **ping**.

## 6. Test de connexion et analyse des paquets

 Les opérations se déroulent sur les ordinateurs **paris1**, **paris2**, **geneve1** et **geneve2**.

1. Lancez le moniteur réseau sur **paris1** et **paris2** et démarrez une capture. Vous allez capturer les trames d'un **ping** provenant de **geneve2**.
2. Sur **geneve2**, saisissez **ping paris2** puis arrêtez la capture sur **paris1** et **paris2**. Vous devriez voir les trames suivantes sur **paris2** :

Time Offset	F	Conv Id	Source	Destination	Protocol Name	Description
1.191713			10.1.1.2	10.1.1.1	ARP	ARP:Request, 10.1.1.2 asks for 10.1.1.1
1.201728			10.1.1.1	10.1.1.2	ARP	ARP:Response, 10.1.1.1 at 00-03-FF-D9-6A-CF
1.201728	{IPv4:6}		10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2
2.203168	{IPv4:6}	192.168.1.2	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2
2.203168	{IPv4:6}	10.1.1.2	192.168.1.2	10.1.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2
3.194593	{IPv4:6}	192.168.1.2	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2
3.194593	{IPv4:6}	10.1.1.2	192.168.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2
4.196033	{IPv4:6}	192.168.1.2	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2
4.196033	{IPv4:6}	10.1.1.2	192.168.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2

La commande ping est reconnaissable ainsi que l'émetteur réel.

Et sur paris1 :

Time Offset	Process Name	Conv Id	Source	Destination	Protocol Name	Description
1.652376	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
1.752520	{IPv4:7}	172.30.1.1	172.30.1.2	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0x1bb4	
1.862678		192.168.1.2	192.168.1.1	ARP	ARP:Request, 192.168.1.2 asks for 192.168.1.1	
1.892722		192.168.1.1	192.168.1.2	ARP	ARP:Request, 192.168.1.1 asks for 192.168.1.2	
1.862678		192.168.1.2	192.168.1.1	ARP	ARP:Request, 192.168.1.2 asks for 192.168.1.1	
1.872693	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
1.882707	{IPv4:7}	172.30.1.1	172.30.1.2	PPP	PPP:Compressed datagram	
1.892722		192.168.1.1	192.168.1.2	ARP	ARP:Request, 192.168.1.1 asks for 192.168.1.2	
1.982851	{IPv4:7}	172.30.1.2	172.30.1.1	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0xe573	
2.022909	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
2.022909		10.1.1.1	10.1.1.2	ARP	ARP:Request, 10.1.1.1 asks for 10.1.1.2	
2.022909		10.1.1.2	10.1.1.1	ARP	ARP:Request, 10.1.1.2 asks for 10.1.1.1	
2.022909	{IPv4:7}	172.30.1.1	172.30.1.2	PPP	PPP:Compressed datagram	
2.133067	{IPv4:7}	172.30.1.2	172.30.1.1	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0xe573	
2.022909		10.1.1.1	10.1.1.2	ARP	ARP:Request, 10.1.1.1 asks for 10.1.1.2	
2.022909		10.1.1.2	10.1.1.1	ARP	ARP:Response, 10.1.1.2 at 00-03-FF-01-E8-46	
2.022909	{IPv4:8}	192.168.1.2	10.1.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2	
2.022909		10.1.1.2	10.1.1.1	ARP	ARP:Request, 10.1.1.2 asks for 10.1.1.1	
2.022909	{IPv4:8}	10.1.1.1	10.1.1.2	ARP	ARP:Response, 10.1.1.1 at 00-03-FF-09-6A-CF	
2.022909	{IPv4:8}	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2	
2.653816	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
2.753960	{IPv4:7}	172.30.1.1	172.30.1.2	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0x1bb4	
3.024349	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
3.024349	{IPv4:7}	172.30.1.1	172.30.1.2	PPP	PPP:Compressed datagram	
3.194507	{IPv4:7}	172.30.1.2	172.30.1.1	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0xe573	
3.024349	{IPv4:8}	192.168.1.2	10.1.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2	
3.024349	{IPv4:8}	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2	
3.665270	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
3.765414	{IPv4:7}	172.30.1.1	172.30.1.2	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0x1bb4	
4.025789	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
4.025789	{IPv4:7}	172.30.1.1	172.30.1.2	PPP	PPP:Compressed datagram	
4.125933	{IPv4:7}	172.30.1.2	172.30.1.1	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0xe573	
4.025789	{IPv4:8}	192.168.1.2	10.1.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2	
4.025789	{IPv4:8}	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2	
5.027229	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	
5.027229	{IPv4:7}	172.30.1.1	172.30.1.2	PPP	PPP:Compressed datagram	
5.127373	{IPv4:7}	172.30.1.2	172.30.1.1	GRE	GRE:Protocol = PPP, Flags = ..K.....A..... Version 1 , Length = 0x0 , CallID = 0xe573	
5.027229	{IPv4:8}	192.168.1.2	10.1.1.2	ICMP	ICMP:Echo Request Message, From 192.168.1.2 To 10.1.1.2	
5.027229	{IPv4:8}	10.1.1.2	192.168.1.2	ICMP	ICMP:Echo Reply Message, From 10.1.1.2 To 192.168.1.2	
5.598050	{IPv4:7}	172.30.1.2	172.30.1.1	PPP	PPP:Compressed datagram	

Il est visible que sur l'interface paris la commande ping est reconnaissable alors que sur l'interface internet le contenu est encapsulé dans des paquets ppp.

- Pour terminer l'étude du VPN, déconnectez l'interface réseau **VPN\_GENEVE** sur **paris1** puis sur **geneve2**, saisissez de nouveau la commande ping **paris2**. Que se passe-t-il ? Au bout d'une dizaine de secondes, l'interface est reconnectée automatiquement.
- Sur **geneve2** faites un ping de **paris1**. En fonction de l'adresse de **paris1** retournée, vous ne pourrez y accéder (172.30.1.1) ou recevoir une réponse (10.1.1.1). Il n'est donc pas possible d'accéder au segment internet.
- Sur **paris1**, saisissez ipconfig /all et vérifiez que le tunnel est activé comme le montre l'image suivante. Les adresses assignées au tunnel permettent de faire fonctionner le tunnel correctement.

Administrator : Invite de commandes

```
C:\Users\Administrateur>ipconfig
Configuration IP de Windows

Carte PPP UPN_GENEVE :

Suffrage DNS propre à la connexion. . . :
Adresse IPv4. . . . . : 10.100.1.4
Masque de sous-réseau. . . . . : 255.255.255.255
Passerelle par défaut. . . . . :

Carte Ethernet internet :

Suffrage DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . : fe80::d956:3b96:879b:18b3%13
Adresse IPv4. . . . . : 172.30.1.1
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :

Carte Ethernet paris :

Suffrage DNS propre à la connexion. . . :
Adresse IPv6 de liaison locale. . . : fe80::957c:bc73:214e:235%10
Adresse IPv4. . . . . : 10.1.1.1
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :

Carte PPP RAS < Dial In > Interface :

Suffrage DNS propre à la connexion. . . :
Adresse IPv4. . . . . : 10.200.1.1
Masque de sous-réseau. . . . . : 255.255.255.255
Passerelle par défaut. . . . . :
```

Notez que l'adresse 10.100.1.4 est reçue par le point de terminaison geneve1 alors que l'adresse 10.200.1.1 est gérée par paris1.

- Sur paris1, saisissez route print et garantissez que le tunnel est activé. Pour joindre le segment de l'autre site, il faut passer par le tunnel comme le montre la figure suivante :

Administrator : Invite de commandes

IPv4 Table de routage

Itinéraires actifs :	Destination réseau	Masque réseau	Adr. passerelle	Adr. interface	Métrique
	10.1.1.0	255.255.255.0	On-link	10.1.1.1	276
	10.1.1.1	255.255.255.255	On-link	10.1.1.1	276
	10.1.1.255	255.255.255.255	On-link	10.1.1.1	276
	10.100.1.4	255.255.255.255	On-link	10.100.1.4	276
	10.200.1.1	255.255.255.255	On-link	10.200.1.1	306
	127.0.0.0	255.0.0.0	On-link	127.0.0.1	306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1	306
	127.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	172.30.1.0	255.255.255.0	On-link	172.30.1.1	276
	172.30.1.1	255.255.255.255	On-link	172.30.1.1	276
	172.30.1.255	255.255.255.255	On-link	172.30.1.1	276
	192.168.1.0	255.255.255.0	10.200.1.4	10.100.1.4	21
	224.0.0.0	240.0.0.0	On-link	127.0.0.1	306
	224.0.0.0	240.0.0.0	On-link	172.30.1.1	276
	224.0.0.0	240.0.0.0	On-link	10.1.1.1	276
	224.0.0.0	240.0.0.0	On-link	10.200.1.1	306
	255.255.255.255	255.255.255.255	On-link	127.0.0.1	306
	255.255.255.255	255.255.255.255	On-link	172.30.1.1	276
	255.255.255.255	255.255.255.255	On-link	10.1.1.1	276
	255.255.255.255	255.255.255.255	On-link	10.200.1.1	306
	255.255.255.255	255.255.255.255	On-link	10.100.1.4	276

- Sur paris1, saisissez ping 172.30.1.1, l'adresse de Paris sur le segment internet et le résultat est **Défaillance générale**, ce qui est normal car l'interface est inaccessible.

 Vous avez implémenté un tunnel VPN PPTP entre deux sites et approfondi les types de paquets qui peuvent être échangés.



Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 6 - Sécurisation des liaisons intrasites

## 1. Objectifs

Dans cet exercice vous allez configurer l'environnement pour utiliser le protocole **IPsec** au lieu du protocole **IP** pour sécuriser des liaisons de sites en utilisant des règles de pare-feu ainsi que des stratégies **IPsec** comme l'isolation de serveurs.

## 2. Configuration de l'environnement

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (le fichier **WMyDomEni.txt** doit se trouver sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres ordinateurs.
- Sur **paris2**, lancez le script **scriptParis2.bat**.
- Sur **paris5**, lancez le script **scriptParis5.bat**.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**. Ensuite installez le moniteur réseau.
- Sur **geneve2**, placez les scripts **scriptGeneve2.bat** après le redémarrage du serveur geneve1.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt mydom.eni ainsi que serveur **DNS** et routeur. Ses adresses IP sont 10.1.1.1/24 et 10.1.10.5/30.

**paris2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.1.1.2/24). Il dispose de la fonctionnalité client Telnet.

**paris5** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.1.1.5 /24). Il dispose de la fonctionnalité client Telnet.

**geneve1** est membre du domaine **mydom.eni** et routeur. Ses adresses IP fixes sont 10.1.10.6/30 et 10.2.1.17/30. D'autre part, il est serveur SMTP.

**geneve2** est membre du domaine **mydom.eni** et dispose d'une adresse IP fixe (10.2.1.18/30). Il dispose de la fonctionnalité client Telnet.

 Comme par défaut le protocole icmp est bloqué par le pare-feu, les scripts le réactivent pour que vous puissiez effectuer des tests avec la commande ping.

## 3. Référence par rapport à la théorie

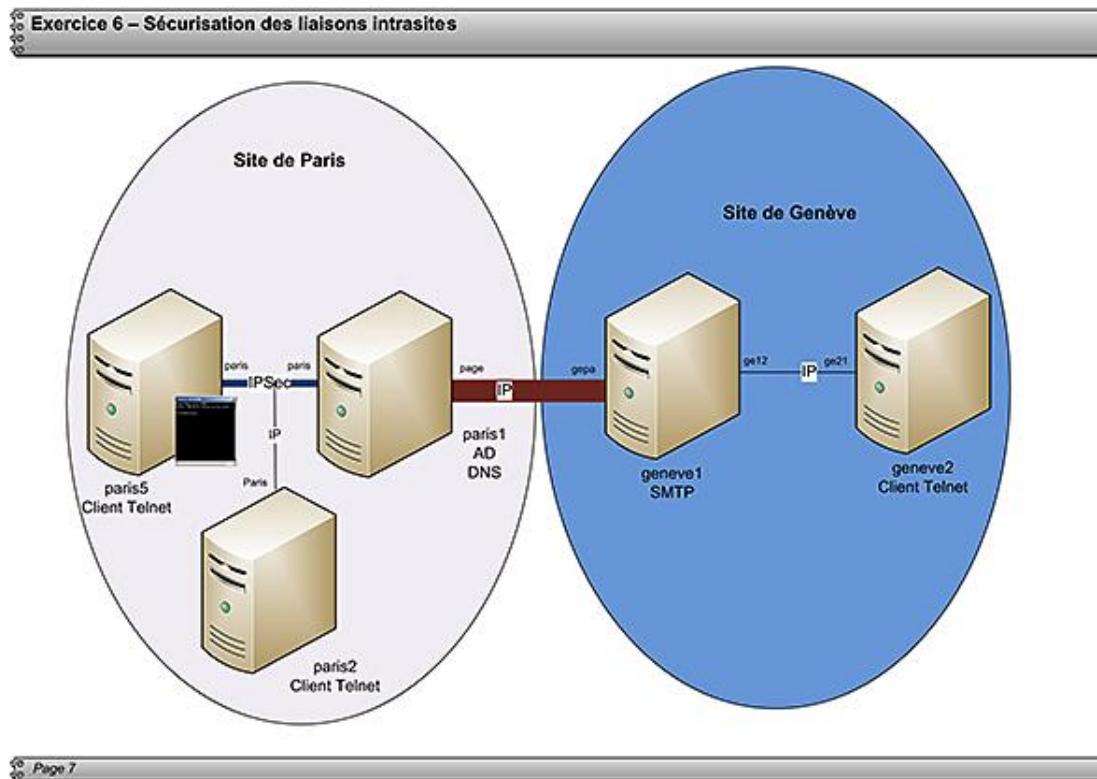
Vous pouvez vous référer au chapitre Configuration des services réseaux avancés et plus particulièrement aux sections consacrées au pare-feu, à IPsec, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion

et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la sécurisation des liaisons intrasites

Les consultants ont déterminé que sur le site de Paris, le serveur **paris5** contient des informations extrêmement sensibles. Afin d'améliorer la sécurité, il est demandé que les ordinateurs se trouvant dans une unité d'organisation spécifique (ici Contrôleurs de domaine) puissent répondre à la demande de **paris5** de communiquer uniquement en IPsec. Les autres ordinateurs de l'entreprise ne doivent pas pouvoir répondre aux sollicitations IPsec.

Enfin, sur le site de Genève, il a été constaté que des personnes *spamment* les utilisateurs de l'entreprise en utilisant des applications qui préparent des messages SMTP puis les envoient sur le serveur **SMTP** de **geneve1**. Depuis l'ordinateur de **paris2**, il vous est demandé de créer une stratégie pare-feu qui empêche d'émettre des messages **SMTP** excepté pour le serveur **geneve1**.



Les tâches à effectuer sont :

- Vérification de la connexion SMTP et des communications entre les serveurs.
- Création d'une stratégie de groupe pour que **paris5** ne communique qu'en **IPsec** avec **paris1**.
- Création d'une stratégie de groupe pour que l'unité d'organisation **Contrôleurs de domaine** réponde aux sollicitations IPsec de **paris5** et accepte également les communications non chiffrées.
- Création, test et déploiement d'une stratégie pour le pare-feu pour limiter les envois SMTP sur le site de Genève.

## 5. Vérification de la connexion SMTP et des communications entre les serveurs

Tous les ordinateurs doivent fonctionner car vous devez travailler sur tous les ordinateurs. Néanmoins, si vous ne disposez pas d'assez de RAM, vous devez garantir que les ordinateurs **paris1** et **geneve1** sont toujours opérationnels. Pour passer facilement d'un ordinateur à l'autre sauvegardez son état.

1. Sur **geneve1**, vérifiez que le service **SMTP** est démarré sinon lancez-le avec la commande

```
net start smtspvc.
```

2. Sur chaque serveur disposant du client **telnet**, lancez la commande suivante dans une invite de commande : telnet genevel 25. Un message commençant par 220 vous informe que vous êtes connecté sur le serveur **SMTP**.

 Dans de rares cas, le message n'apparaît pas, seul le curseur clignote.

1. Saisissez **quit** pour vous déconnecter du serveur **SMTP**. Vous avez la confirmation que tous les ordinateurs de l'entreprise peuvent envoyer des messages de spam.
2. Vérifiez que vous pouvez communiquer entre **paris2** et **paris5** à l'aide de la commande **ping**.
3. Vérifiez que vous pouvez communiquer entre **geneve2** et **paris5** à l'aide de la commande **ping**.
4. Vérifiez que vous pouvez communiquer entre **paris2** et **geneve2** à l'aide de la commande **ping**.

 La communication en utilisant le protocole SMTP est vérifiée entre tous les ordinateurs.

## 6. Mise en œuvre de la stratégie IPsec pour paris5

 paris1, paris2 et paris5 doivent fonctionner, les tâches s'effectuent sur tous les ordinateurs.

Il est important de garantir que seul **paris1** peut dialoguer avec **paris5** mais il faut également que **paris2** puisse dialoguer avec **paris1** tout en conservant la possibilité de communiquer avec **geneve1** et **geneve2**.

Bien qu'il s'agisse d'une mise en œuvre du protocole **IPsec**, il faut l'utiliser de manière à isoler **paris5** pour qu'il ne puisse dialoguer qu'avec **paris1** ; **paris2** doit donc pouvoir dialoguer de manière chiffrée avec **paris5** et non chiffrée avec le reste de l'entreprise. Pour cela, il est nécessaire de créer une règle de sécurité de connexion basée sur l'isolation pour **paris5**. Pour **paris1**, il faudra créer une règle pour permettre de répondre avec **IPsec**. Aucune modification n'est à prévoir pour paris2.

### a. Création d'une règle de pare-feu (IPsec) pour paris5

Pour créer une règle de sécurité de connexion sur **paris5**, il faut soit le faire localement avec les commandes **netsh**, soit créer une stratégie de groupe, soit le faire à distance avec la console **Pare-feu avec fonctions avancées de sécurité**. Cette dernière solution est choisie ici.

1. Sur **paris5**, il faut autoriser la gestion du pare-feu à distance avec la commande suivante : netsh advfirewall set currentprofile settings remotemanagement enable.
2. Sur **paris1**, créez une nouvelle console **MMC** et ajoutez-y le snap-in **Pare-feu avec fonctions avancées de sécurité** et sélectionnez l'ordinateur **paris5**.
3. Une fois la console ouverte, créez une nouvelle règle de sécurité de connexion.
4. Pour l'étape **Type de règle**, sélectionnez **Isolation**.
5. Pour l'étape **Configuration requise**, sélectionnez **Imposer l'authentification des connexions entrantes et sortantes**.
6. Pour l'étape **Méthode d'authentification**, sélectionnez **Avancé** puis cliquez sur **Personnalisé**.
7. Dans la boîte de dialogue qui apparaît, dans la zone **Première authentification**, cliquez sur **Ajouter**.
8. Dans la boîte de dialogue **Première méthode d'authentification**, sélectionnez **Clé pré-partagée (non recommandée)** et saisissez Montest avant de cliquer deux fois sur **OK**. Bien que non recommandée, l'utilisation d'une clé pré-partagée est simple à mettre en

œuvre pour un test.

9. Sur la page **Profil**, contrôlez que tous les profils sont sélectionnés.
10. Sur la page **Nom**, saisissez **Isolation paris5** puis cliquez sur **Terminer**. La règle est modifiée sur **paris5** puis il y a perte de connexion avec **paris5** car **paris1** n'est pas encore configuré pour dialoguer avec **paris5**.

 paris5 exige une communication sécurisée.

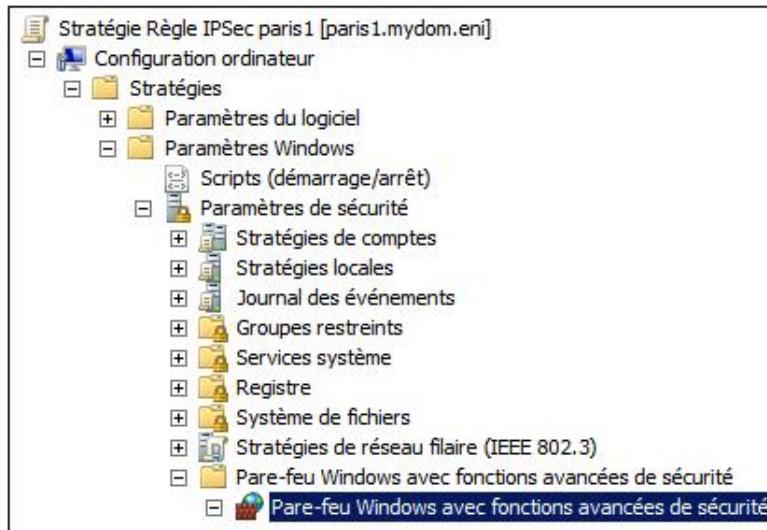
## b. Création d'une règle de pare-feu (IPsec) pour paris1

Pour **paris1**, vous allez utiliser les stratégies de groupe.

1. Sur **paris1**, ouvrez la console **Gestion des stratégies de groupe**.
2. En cliquant avec le bouton droit de la souris sur l'unité d'organisation **Domain Controllers**, créez **un objet GPO dans ce domaine, et le lier ici** appelé **Règle IPSec paris1** comme le montre la figure suivante.



1. Dans la console, sélectionnez avec le bouton droit de la souris la stratégie **Règle IPSec paris1** puis cliquez sur **Modifier**.
2. Dans l'éditeur de gestion de stratégies de groupe, déplacez-vous dans l'arborescence comme le montre l'image suivante.



1. Créez une nouvelle règle de sécurité de connexion.
2. Pour l'étape **Type de règle**, sélectionnez **Isolation**.
3. Pour l'étape **Configuration requise**, sélectionnez **Demander l'authentification des connexions entrantes et sortantes**.
4. Pour l'étape **Méthode d'authentification**, sélectionnez **Avancé** puis cliquez sur **Personnalisé**.

5. Dans la boîte de dialogue qui apparaît, dans la zone **Première authentification**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Première méthode d'authentification**, sélectionnez **Clé pré-partagée (non recommandée)** et saisissez Montest avant de cliquer deux fois sur **OK**. La clé doit être identique à celle de la règle écrite pour **paris5**.
7. Sur la page **Profil**, contrôlez que tous les profils sont sélectionnés.
8. Sur la page **Nom**, saisissez Règle IPSec paris1 puis cliquez sur **Terminer**. La règle n'est pas encore active.
9. Fermez l'**éditeur de gestion des stratégies de groupe** ainsi que **Gestion de stratégie de groupe**.
10. Saisissez `gpupdate /force` dans une invite de commande pour rafraîchir les stratégies de groupe appliquées.
11. Saisissez `gpresult /v > t`.
12. Saisissez `notepad t`. À l'aide du Bloc-notes, recherchez dans la section paramètres de l'ordinateur les stratégies qui sont appliquées, vous devriez y trouver la stratégie créée, ensuite vous pouvez également rechercher les paramètres appliqués.
13. Maintenant saisissez `ping paris5` et vous devriez obtenir une réponse, faites de même avec **paris2** et vous devez avoir le même résultat.
14. Sur **paris2**, saisissez `ping paris5` et vous ne devez pas recevoir de réponse.
15. Enfin saisissez `telnet geneve1 25` sur **paris2** et **paris5**. Vous ne devez pas recevoir de réponse depuis **paris5**.

➤ paris1 communique de manière sécurisée avec paris5 et non sécurisée avec les autres ordinateurs.

➤ Vous venez d'isoler paris5 comme demandé.

## 7. Limitation de l'accès SMTP

➤ paris1, paris2, geneve1 et geneve2 doivent fonctionner, les modifications s'effectuent sur geneve1 et les tests à partir de geneve2 et paris2.

La méthode la plus simple à mettre en œuvre est de restreindre l'étendue des adresses distantes qui peuvent envoyer des messages SMTP en autorisant uniquement l'adresse de geneve1 10.1.1.0/24. Pour cela, il faut modifier la règle SMTP correspondante.

➤ D'autres solutions pourraient être acceptables mais seraient plus lourdes à mettre en œuvre. Conservez à l'esprit que la solution la plus simple, mais qui est robuste, est souvent la meilleure.

Si plusieurs serveurs **SMTP** existaient sur le site de Genève, l'utilisation d'une stratégie de groupes filtrée sur le groupe **Serveur SMTP de Genève**, dont feraient partie les serveurs SMTP du site de Genève, serait une meilleure méthode que la modification directe de la règle du pare-feu présentée ici.

1. Sur **geneve1**, modifiez l'étendue de la règle de trafic entrant **Propriétés de Simple Mail Transfer Protocol (SMTP-In)** de manière à n'autoriser que le trafic provenant de 10.2.1.18 (trafic distant).
2. Testez la connexion **SMTP** à l'aide de la commande `telnet` à partir des serveurs geneve2 et paris2. Seul geneve2 devrait pouvoir se connecter. Par contre paris2 peut recevoir une réponse à la commande `ping` ou visualiser les partages (`\\\geneve1`).

➤ Vous avez vu comment modifier une règle du pare-feu.

---

 Dans cet exercice vous avez vu comment mettre en œuvre les stratégies de sécurité permettant de créer des filtres au niveau du pare-feu ainsi que la création de stratégies IPsec, et l'avantage apporté par l'utilisation des nouveaux assistants.

---

 Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 5 - Mise en œuvre de la résolution de noms

## 1. Objectifs

Dans cet exercice vous allez installer, configurer et examiner des serveurs DNS pour les sites de Paris et Genève. D'autre part pour un bureau distant rattaché à Paris, il vous faudra déterminer s'il est nécessaire d'y ajouter un serveur DNS et comment les utilisateurs de ce bureau distant puisse accéder au réseau Intranet d'un partenaire.

## 2. Configuration de l'environnement

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat** (les fichiers **WMyDomEni.txt** et **EnableRouting.vbs** doivent se trouver sur le Bureau). Après le redémarrage, vous pouvez continuer le lancement des scripts sur les autres serveurs.
- Sur **paris2**, lancez le script **scriptParis2.bat**.
- Sur **paris3**, lancez le script **scriptParis3.bat**. (le script **EnableRouting.vbs** doit se trouver sur le Bureau).
- Sur **paris4**, lancez le script **scriptParis4.bat**.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**.

Après le lancement des scripts, **paris1** est contrôleur de domaine pour la forêt mydom.eni ainsi que serveur DNS. Ses adresses sont 10.1.1.1/24 pour le réseau de Paris et 172.30.1.1/24 pour le réseau Internet. Il sert également de routeur.

**paris2** n'est pas membre du domaine et son adresse IP est de 192.168.1.1/24 sur le réseau partenaire.

**paris3** est membre du domaine mydom.eni et le service de routage est activé. Ses adresses sont 10.1.1.3/24 sur le réseau de Paris et 192.168.1.2/24 sur le réseau partenaire.

**paris4** n'est pas membre du domaine et son adresse IP est de 10.1.1.4/24 sur le réseau Paris.

**geneve1** n'est pas membre du domaine mydom.eni et son adresse IP est 172.30.1.2/24 sur le réseau Internet.

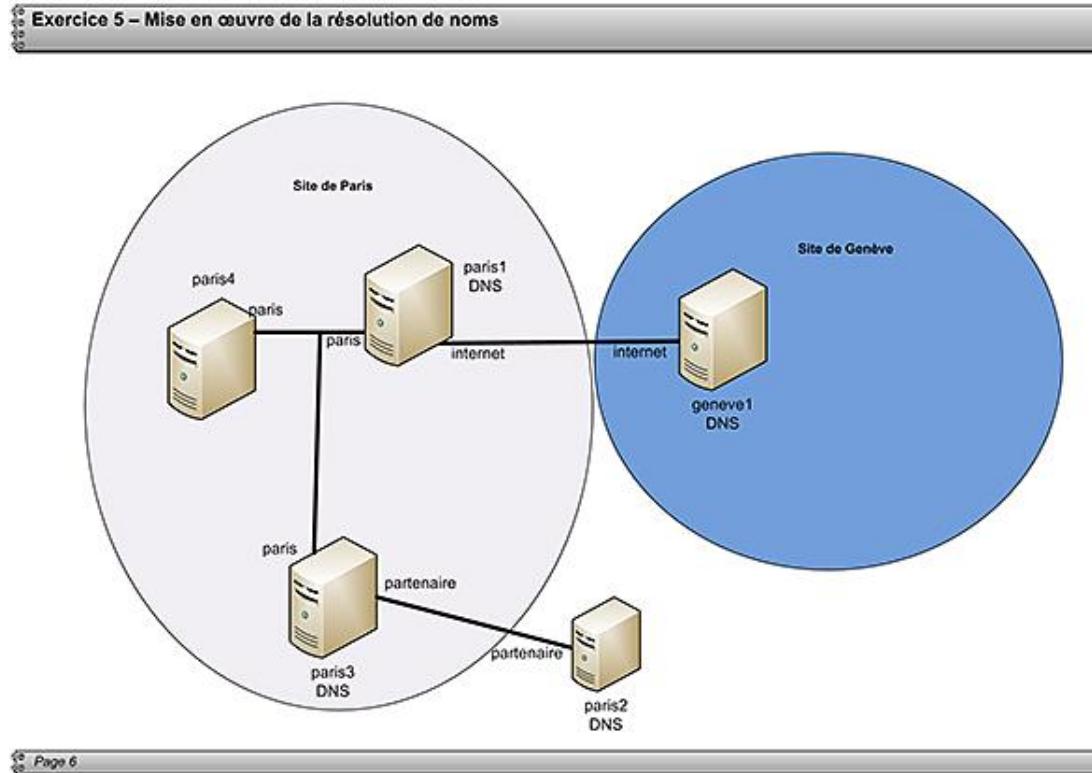
 Comme par défaut le protocole **icmp** est bloqué par le pare-feu, les scripts le réactivent pour que vous puissiez effectuer des tests avec la commande ping.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Mise en œuvre du serveur de fichiers consacré à la mise en œuvre du DNS. Les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre du rôle du serveur de noms DNS

Les consultants pensent qu'il est nécessaire d'installer un second serveur DNS sur le site de Genève dont la zone doit être intégrée. Un bureau distant qui dispose d'un serveur appelé paris3 doit pouvoir se connecter et avoir accès aux données de l'entreprise et avoir accès à l'Intranet d'un partenaire très proche. Enfin vous voulez tester et voir comment les ordinateurs clients réagissent à l'enregistrement selon qu'ils sont dans ou hors du domaine.



Veuillez noter que l'ordinateur paris2 représente le serveur DNS de l'entreprise partenaire.

Les tâches à effectuer sont :

- Installation de l'Active Directory sur **geneve1** puis installation et configuration du serveur DNS pour qu'il gère la zone **mydom.eni**.
- Installation du serveur DNS sur **paris3** en tant que serveur de cache.
- Installation d'un serveur DNS sur **paris2** et configuration de la zone **partenaire.eni**.
- Configuration du serveur DNS paris2 pour qu'il héberge une zone stub de la zone **partenaire.eni**.
- Permission d'accès au serveur paris2 (partenaire.eni) à partir du serveur paris1.
- Mise en œuvre d'une zone déléguée sur paris3 et d'un redirecteur conditionnel sur paris2.
- Mise en œuvre des globalnames.
- Mise en œuvre des paramètres DNS à l'aide d'une stratégie de groupe.

## 5. Installation et configuration du rôle serveur DNS sur geneve1

- Les ordinateurs **paris1** et **geneve1** sont requis.

---

Il vous faut installer sur **geneve1** les services Active Directory afin qu'ils deviennent **Replica** pour le domaine **mydom.eni**. Ensuite, vous allez installer le serveur DNS et attendre quelques minutes que la réPLICATION s'effectue car la zone doit apparaître automatiquement.

1. Sur **geneve1**, installez les services Active Directory pour en faire un serveur Réplica en utilisant les deux fichiers **ScriptGeneve1AddReplica.bat** et **WAddReplicaMyDomEni.txt**. Exécutez le fichier **bat**. Le script n'inclut pas l'installation du serveur DNS en même temps que l'Active Directory.
2. Installez le rôle **Serveur DNS**, par exemple en saisissant la commande `ServerManagerCmd -install DNS`. Le serveur DNS est déjà démarré.
3. Lancez la console DNS et vous verrez que la zone **mydom.eni** est répliquée. Si ce n'est pas le cas, attendez quelques minutes. En effet, le type de zone intégré Active Directory permet de répliquer la zone sans aucune manipulation sur les autres serveurs DNS.

---

 L'installation et la configuration sont déjà terminées. Remarquez que votre travail a été réduit au minimum.

---

## 6. Installation et configuration du rôle serveur DNS sur paris3

 Les ordinateurs **paris1** et **paris3** sont requis.

---

Vous allez installer un serveur DNS sur **paris3** et le transformer en serveur DNS de cache.

1. Installez le rôle **Serveur DNS** par exemple en saisissant la commande `ServerManagerCmd -install DNS`.
2. Lancez la console DNS, et passez en affichage détaillé afin de faire apparaître le conteneur de mises en cache en cliquant dans l'arborescence avec le bouton droit de la souris sur DNS puis sur **Affichage détaillé**.
3. Il vous faut maintenant configurer le serveur de cache de manière à ce que **paris1** soit le serveur DNS de recherche. Pour cela, cliquez dans l'arborescence avec le bouton droit de la souris sur **paris3** puis sur **Propriétés**.
4. Sur l'onglet **Redirecteurs**, ajoutez les adresses IP des serveurs **paris1** et **geneve1**. Votre serveur de cache est opérationnel.
5. Modifiez l'adresse du serveur DNS de **paris3** de manière à ce qu'il utilise le serveur DNS local.
6. Videz le cache local puis saisissez `ping geneve1`, vous devez recevoir une réponse.
7. Modifiez l'adresse IP de **paris3** à 10.1.1.9.
8. Enregistrez l'adresse de **paris3** auprès du serveur DNS avec `ipconfig /registerdns`.
9. Puis sur la console DNS de **paris1** vérifiez l'adresse IP inscrite. Elle doit être 10.1.1.9
10. Modifiez l'adresse IP de **paris3** à 10.1.1.3 pour ne pas compromettre la suite des procédures.

---

 Vous venez d'installer un serveur de cache et avez vu comment les ordinateurs clients peuvent mettre à jour leur information auprès du DNS.

---

## 7. Installation et configuration du rôle serveur DNS sur paris2

 Seul l'ordinateur **paris2** est requis.

---

Après avoir installé le serveur DNS, il vous faut créer deux zones principales qui acceptent les mises à jour dynamiques, une appelée **partenaire.eni** et **mazone.eni** pour la seconde. Ensuite, modifiez le suffixe principal pour qu'il corresponde à **partenaire.eni** et le suffixe de la connexion à mazone.eni. Bien entendu, les noms DNS doivent pouvoir s'enregistrer automatiquement.

1. Sur **paris2**, installez le rôle **Serveur DNS**, par exemple en saisissant la commande suivante : ServerManagerCmd -install DNS.
2. Lancez la console **DNS** puis créez une zone principale qui accepte les mises à jour dynamiques appelée **partenaire.eni**.
3. Créez également une seconde zone principale qui accepte les mises à jour dynamiques appelée **mazone.eni**.
4. Modifiez la configuration de l'adressage IP afin que le serveur paris2 devienne **client DNS** de son propre **serveur DNS**.
5. Dans une invite de commande, enregistrez **paris2** auprès du serveur DNS avec la commande suivante ipconfig /registerdns. Le serveur DNS ne reçoit pas la mise à jour car paris2 n'est pas associé à un suffixe DNS. Modifiez le suffixe principal de l'ordinateur en cliquant sur **Paramètres systèmes avancés** de **Système** du **Panneau de configuration**.
6. Dans la boîte de dialogue **Propriétés système**, cliquez sur **Modifier** de l'onglet **Nom de l'ordinateur**.
7. Dans la boîte de dialogue **Modification du nom ou du domaine de l'ordinateur**, cliquez sur **Autres** puis saisissez **partenaire.eni** dans la zone de texte **Suffixe DNS principal pour cet ordinateur**. Il vous faut redémarrer l'ordinateur.
8. Vous allez maintenant modifier le suffixe DNS pour la connexion. Saisissez ncpa.cpl pour ouvrir les connexions réseau puis cliquez avec le bouton droit de la souris sur la carte réseau **partenaire** et enfin sur **Propriétés**.
9. Dans la boîte de dialogue **Propriétés de partenaire**, double cliquez sur **Protocole Internet version 4 (TCP/IPv4)**, puis sur **Avancé**.
10. Sur l'onglet **DNS**, saisissez **mazone.eni** pour le **Suffixe DNS pour cette connexion** et cochez les cases **Enregistrer les adresses de cette connexion dans le système DNS** et **Utiliser le suffixe DNS de cette connexion pour l'enregistrement DNS**.
11. Fermez les boîtes de dialogue ouvertes.
12. Saisissez ipconfig /all et recherchez les suffixes que vous avez ajouté.
13. Saisissez ipconfig /registerdns puis regardez dans la **console DNS** que l'enregistrement pour **paris2.mazone.eni** a bien été ajouté.

---

 Après avoir installé un serveur DNS, vous avez examiné comment gérer les suffixes DNS pour un ordinateur.

---

## 8. Ajout d'une zone de stub pour paris3

---

 Les ordinateurs **paris2** et **paris3** sont requis.

---

Plusieurs collaborateurs du site distant sur lequel se trouve le serveur **paris3** travaillent de manière étroite avec la société partenaire. D'autre part, des négociations sont en cours pour l'acquérir. De leur poste de travail, les utilisateurs doivent disposer d'un accès direct aux serveurs de la société partenaire grâce à un tunnel VPN point à point entre les deux entreprises. Il vous est demandé d'implémenter sur paris3 une zone de stub car il vous est permis d'effectuer des transferts de zone partielle.

1. Sur **paris3**, lancez la console **DNS**, puis créez une zone de stub pour la zone **partenaire.eni** dont le serveur est 192.168.1.1 (**paris2**). La zone de stub est opérationnelle et maintenant il est possible d'utiliser les noms pour atteindre un ordinateur provenant de **partenaire.eni**.
2. Tentez de joindre successivement **paris2.partenaire.eni** et **paris2.myzone.eni**. Dans ce

dernier cas, comme la zone est inconnue, il n'est pas possible d'effectuer la résolution du nom.

- 
-  Vous venez de voir comment implémenter une zone de stub.
- 

## 9. Extension de l'utilisation de la zone de stub sur le site principal de Paris

- 
-  Les ordinateurs **paris1**, **paris2** et **paris3** sont requis.
- 

La collaboration avec la société partenaire s'étend au niveau du site de Paris. Il vous est demandé de permettre aux personnes se trouvant sur ce site d'avoir accès à la zone **partenaire.eni**. Il n'est pas possible de créer une zone secondaire dont le **maître** serait la zone de stub sur **paris3**. Par contre, il est possible :

- 1) d'utiliser une zone de stub dont le maître est sur **paris3** ou **paris2** ;
- 2) un redirecteur conditionnel pour la zone sur **paris3** ou **paris2** ;
- 3) une zone secondaire basée sur **paris2**.

Vous allez implémenter ici la création d'une zone de stub basée sur **paris3**.

1. Sur **paris1**, lancez la console **DNS**, puis créez une zone de stub pour la zone **partenaire.eni** dont le serveur est 10.1.1.3 (**paris3**). La zone de stub est opérationnelle et maintenant il est possible d'utiliser les noms pour atteindre un ordinateur provenant de **partenaire.eni**.
2. Tentez de joindre successivement **paris2.partenaire.eni** et **paris2.myzone.eni**. Dans ce dernier cas, comme la zone est inconnue, il n'est pas possible d'effectuer la résolution du nom.

- 
-  Vous venez de voir comment implémenter une zone de stub.
- 

## 10. Mise en place d'une zone déléguée et d'un redirecteur conditionnel

- 
-  Les ordinateurs **paris1**, **paris2** et **paris3** sont requis.
- 

Les utilisateurs du Bureau distant de Paris doivent partager de plus en plus d'informations avec la société partenaire. Néanmoins vous ne voulez pas permettre une redirection ni la création d'une zone de stub qui exposerait tous les ordinateurs de votre entreprise. Le choix s'est porté sur la création d'une zone pour le Bureau distant et l'utilisation de la redirection conditionnelle pour les partenaires.

Il vous est demandé de créer un sous-domaine appelé **bureau.mydom.eni** puis de déléguer cette zone à **paris3**. Ensuite, sur **paris2**, de créer un redirecteur conditionnel.

1. Sur **paris3**, modifiez le suffixe DNS principal pour qu'il corresponde à **bureau.mydom.eni** puis redémarrez l'ordinateur.
2. Sur **paris3**, créez une zone principale appelée **bureau.mydom.eni** qui permet les mises à jour dynamiques.
3. Pour enregistrer correctement **paris3** comme faisant partie de la zone, la commande **ipconfig /registerdns** n'est pas suffisante. Il faut soit un redémarrage, soit désactiver puis réactiver la carte réseau **paris**.
4. Sur **paris1**, créez une zone déléguée pour **bureau.mydom.eni**.
5. Sur **paris3** et **paris1**, utilisez **nslookup** en mode **debug** pour rechercher **paris3** sans suffixe, puis avec le suffixe. Par défaut, sur **paris1** il vous retourne un enregistrement qui existe toujours et n'a pas été effacé dans la zone de **mydom.eni**. Si vous le supprimez, aucun enregistrement n'est retourné car la zone de suffixe DNS est uniquement **mydom.eni** sur **paris1**.

- Sur **paris2**, créez un redirecteur conditionnel pour la zone **bureau.mydom.eni** puis essayez successivement avec la commande **ping** d'atteindre **paris3.bureau.mydom.eni** et **paris1.mydom.eni**. Vous devez être capable de joindre uniquement **paris3**.

➤ Vous venez de voir comment implémenter une zone déléguée et un redirecteur conditionnel.

## 11. Création d'une zone GlobalNames

➤ Les ordinateurs **paris1**, **paris2** et **paris3** sont requis.

Pour simplifier la gestion des enregistrements DNS en utilisant une zone **GlobalNames**.

- Sur **paris1**, saisissez `DnsCmd paris1 /config /Enableglobalnamessupport 1` dans une invite de commande pour activer le support des zones globales.
- Lancez la console DNS et créez une zone principale intégrée Active Directory appelée **GlobalNames** qui n'accepte pas les enregistrements dynamiques.
- Créez un enregistrement pour l'hôte **toto** avec l'adresse IP **10.1.1.9** dans la zone **GlobalNames**.
- Successivement, sur **paris1** et **paris3** saisissez la commande `ping toto` qui doit effectuer la résolution du nom.
- Faites de même sur **paris2** mais en utilisant `ping toto.bureau.mydom.eni` et la résolution ne doit pas fonctionner.

➤ Vous avez vu comment implémenter une zone **GlobalNames** dans une forêt mono domaine.

## 12. Gestion des paramètres du DNS via une stratégie de groupe

➤ Les ordinateurs **paris1**, **paris3** et **paris4** sont requis.

Pour simplifier la gestion des informations concernant le serveur DNS, il a été décidé que les ordinateurs clients recevront ces informations via une stratégie de groupe appelée **GPO\_DNS**. Il faut spécifier les valeurs pour les paramètres suivants :

- Suffixe DNS principal : **bureau.mydom.eni**.
- Serveur DNS : **10.1.1.3**
- Mise à jour dynamique : activé

Il faut filtrer cette stratégie pour que seul l'ordinateur **paris4** y soit soumis.

- Sur **paris1**, contrôlez que l'ordinateur **paris4** n'a pas d'enregistrement dans la zone **mydom.eni**, mais qu'il est possible de communiquer avec **geneve1** en utilisant son nom (`ping geneve1`).
- Sur **paris4**, saisissez `ipconfig /all` dans une invite de commande pour voir les informations concernant le suffixe principal et l'adresse du serveur DNS actuel. Il faut préciser qu'il n'est pas encore dans le domaine.
- Modifiez son suffixe principal en **mydom.eni**. puis répétez l'opération précédente.
- Ni la désactivation/réactivation de la carte réseau, ni le réenregistrement via `ipconfig /registerdns` ne permettent d'enregistrer cet ordinateur dans la zone DNS **mydom.eni** car elle n'accepte que des mises à jour sécurisées.

5. Saisissez paris4 au domaine **mydom.eni**.
6. Saisissez ipconfig /all. Les informations doivent être identiques au cas précédent.
7. Sur **paris1**, lancez la console Gestion de stratégie de groupes.
8. Dans l'arborescence sous le nœud **mydom.eni**, créez **un objet GPO dans ce domaine et lier le ici** appelé **GPO\_DNS** en cliquant avec le bouton droit de la souris sur le nœud **mydom.eni**. Ensuite il faut le modifier.
9. Dans l'**éditeur de gestion des stratégies de groupe**, développez **Configuration ordinateur - Stratégies - Modèles d'administration - Réseau - Clients DNS**. Ensuite modifiez les valeurs des paramètres comme demandé.
10. Fermez l'**éditeur de gestion des stratégies de groupe**, puis dans la fenêtre de détail sur l'onglet **Etendue** dans la zone **Filtrage de sécurité**, supprimez **utilisateurs authentifiés** et ne filtrez que sur l'ordinateur **paris4** (modifiez le type d'objets pour permettre d'ajouter un ordinateur).
11. Sur **paris4**, redémarrez l'ordinateur car certains paramètres de la stratégie de groupe exigent un redémarrage de l'ordinateur pour qu'il soit pris en compte.
12. Saisissez gpupdate /force puis examinez si la stratégie de groupe est bien appliquée en utilisant les commandes gpresult > t puis notepad t. Recherchez si la stratégie **GPO\_DNS** s'est bien appliquée, ainsi que les paramètres que vous avez modifiés.
13. Saisissez ipconfig /all. Notez que le suffixe DNS principal a bien été modifié mais pas le serveur DNS car ce paramètre est uniquement valable pour un ordinateur disposant de Windows XP.
14. Contrôlez que l'enregistrement de **paris4** se trouve bien dans la zone **bureauumydom.eni**.

- 
-  Vous avez vu comment implémenter une stratégie de groupe pour gérer des paramètres DNS et éprouvé également certaines limitations.
- 
-  Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.
-

# Exercice 4 - Mise en œuvre d'un système DHCP

## 1. Objectifs

Dans cet exercice vous allez installer et configurer plusieurs serveurs DHCP pour explorer plusieurs scénarios comme la simulation d'une panne d'un serveur DHCP ou l'installation d'un serveur DHCP parasite voire encore l'utilisation d'un serveur relais DHCP.

## 2. Configuration de l'environnement

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

Cet exercice requiert une configuration spécifique pour les machines virtuelles suivantes :

- Sur **paris1**, lancez le script **scriptParis1.bat**.
- Sur **paris2**, lancez le script **scriptParis2.bat**.
- Sur **paris4**, lancez le script **scriptParis4.bat**.
- Sur **paris5**, lancez le script **scriptParis5.bat**.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**.
- Sur **geneve2**, lancez le script **scriptGeneve2.bat**.

Après le lancement des scripts, tous les ordinateurs ont leur carte réseau renommée et sont clients **DHCP**. Sur **paris1**, **paris4** et **geneve1** le routage est activé et le protocole RIP installé et configuré. Les échanges RIP auront lieu lorsque les interfaces disposeront d'adresses IP situées dans des réseaux différents.

 Comme par défaut le protocole **icmp** est bloqué par le pare-feu, les scripts le réactivent pour que vous puissiez effectuer des tests avec la commande ping.

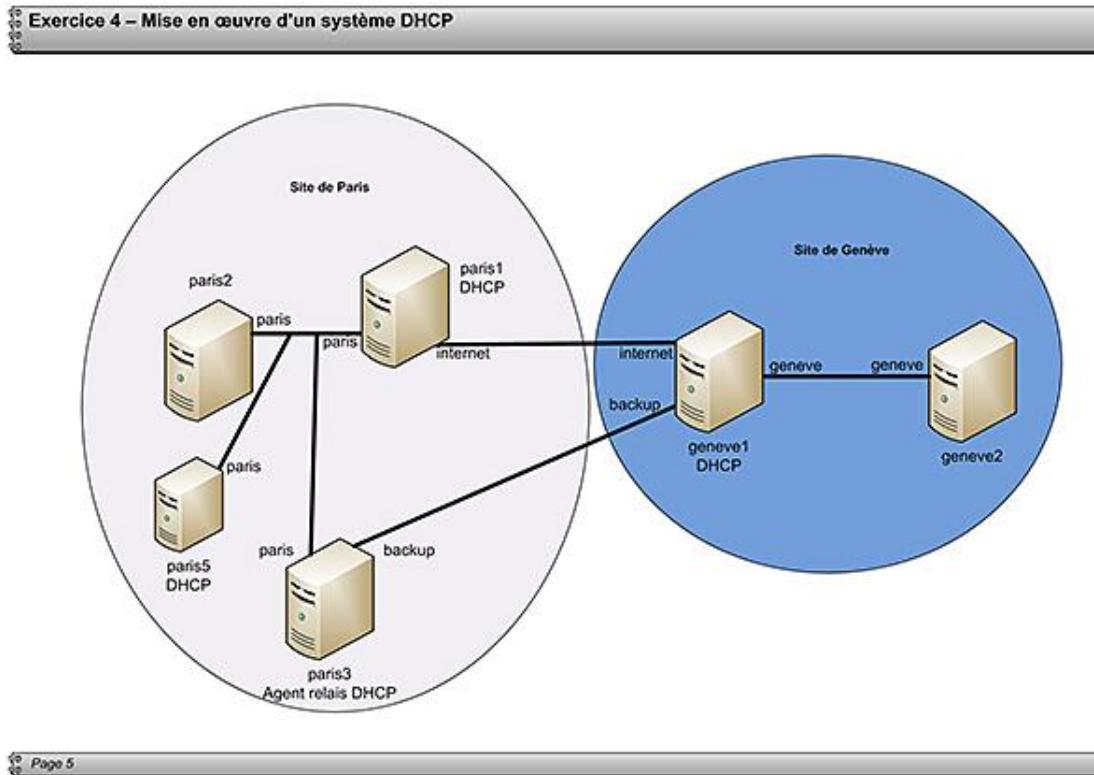
## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Configuration autour du protocole DHCP. Les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre du rôle du serveur d'impression

Les consultants veulent installer un serveur DHCP sur le site de Paris ainsi qu'un autre sur le site de Genève. Afin de garantir une disponibilité maximale sur le site de Paris en cas de coupure de la liaison principale ou de panne du

serveur de Paris, une liaison secondaire existe entre Paris et Genève et un serveur relais DHCP doit y être placé. Enfin un serveur DHCP non autorisé est installé et son comportement sera examiné dans le cas où il est hors Active Directory et lorsqu'il est dans l'Active Directory.



Il n'est pas possible d'effectuer cet exercice en utilisant le même réseau physique c'est-à-dire en utilisant **local seul** pour le mappage des cartes réseaux virtuelles car c'est comme si tous les ordinateurs se trouvaient sur le même réseau et il n'est pas possible de prédire dans ce cas quel serveur DHCP fournira une adresse IP à l'ordinateur client.

Les tâches à effectuer sont les suivantes :

- Installation du rôle **DHCP** sur **paris1** en utilisant les paramètres suivants :
  - interface paris : 10.1.1.1/24
  - interface Internet : 172.31.1.1/24
  - configuration du mappage des cartes réseaux : toutes
- Installation du rôle **DHCP** sur **geneve1** en utilisant les paramètres suivants :
  - interface geneve : 10.2.1.1/24
  - interface Internet : 172.31.1.2/24
  - Interface backup : 192.168.1.1/24
  - configuration du mappage des cartes réseaux : toutes
- Installation de l'agent relais **DHCP** sur **paris3** en utilisant les paramètres suivants :
  - interface paris : 10.1.1.3/24

- Interface backup : 192.168.1.2/24
- configuration du mappage des cartes réseaux : toutes
- Mise en œuvre des étendues pour le site de Paris et de Genève soit en plaçant 80 % des adresses de l'étendue de Paris sur le serveur DHCP de Paris et les 20 % restants sur le serveur DHCP de Genève pour garantir une haute disponibilité en utilisant les paramètres suivants :
  - étendue de Paris : 10.1.1.10 à 10.1.1.254 masque 255.255.255.0
  - passerelles par défaut: 10.1.1.1 et 10.1.1.3
  - Serveur DNS : 10.1.1.1
  - Nom de domaine DNS : mydom.eni
- Création d'une option personnalisée **MaPropreOption** code 100 de type chaîne ayant comme valeur **Ceci est un test.**
  - étendue de Genève : 10.2.1.10 à 10.2.1.254 masque 255.255.255.0
  - passerelle par défaut: 10.2.1.1
  - Serveur DNS : 10.1.1.1
  - Nom de domaine DNS : mydom.eni
  - Tester les étendues créées.
- Créer une classe utilisateur appelée **MaClasseENI**, ajouter le serveur **DNS** pour la classe et activer la classe au niveau de **paris2**.
- Mettre en œuvre l'**agent de relais DHCP**.
- Tester la configuration avec l'**agent de relais DHCP**.
- Ajouter un autre serveur DHCP dans un environnement Groupe de travail.
- Ajouter un autre serveur DHCP dans un environnement Active Directory.
- Tester pour supporter un client PXE en installant le rôle WDS.

## 5. Installation du rôle DHCP sur paris1



Seul l'ordinateur **paris1** est requis.

1. Sur **paris1**, configurez les interfaces avec des adresses IPv4 statiques définies :
  - interface paris : 10.1.1.1/24
  - interface Internet : 172.31.1.1/24
2. Installez le rôle DHCP par exemple en utilisant la commande `ServerManagerCmd -install DHCP`. Dans ce cas, n'oubliez pas de modifier le type de démarrage du **service DHCP** de

**Désactivé à Automatique** et de faire démarrer le service.

3. Modifiez le mappage des cartes réseaux virtuelles de la manière suivante :

- **Carte 1** : local seul
- **Carte 2** : carte physique de l'ordinateur identique à la carte1 de geneve1.

---

 Le serveur DHCP est installé mais pas configuré.

---

## 6. Installation du rôle DHCP sur geneve1

---

 Seul l'ordinateur **geneve1** est requis.

---

1. Sur **geneve1**, configurez les interfaces avec les adresses IPv4 statiques définies :
  - Interface geneve : 10.2.1.1/24
  - Interface internet : 172.31.1.2/24
  - Interface backup : 192.168.1.1/24
2. Installez le rôle DHCP par exemple en utilisant la commande `ServerManagerCmd -install DHCP`. Dans ce cas, n'oubliez pas de modifier le type de démarrage du service DHCP de **Désactivé à Automatique** et de faire démarrer le service.
3. Modifiez le mappage des cartes réseaux virtuelles de la manière suivante :
  - **Carte 1** : carte physique de l'ordinateur identique à **carte2** de **paris1**.
  - **Carte 2** : même carte que la carte 1 de **geneve1**.
  - **Carte 3** : sur une autre carte de l'ordinateur ou sur la même carte que la carte 1 de **geneve1**.

---

 Le serveur DHCP est installé mais pas configuré.

---

## 7. Installation du relais DHCP sur paris3

---

 Seul l'ordinateur **paris3** est requis.

---

1. Sur **paris3**, configurez les interfaces avec des adresses IPv4 statiques définies :
  - Interface paris : 10.1.1.3/24
  - Interface backup : 192.168.1.2/24
2. Ajoutez le protocole de routage Agent de relais DHCP. Il sera configuré plus tard.
3. Modifiez le mappage des cartes réseaux virtuelles de la manière suivante :

- **Carte 1** : local seul
- **Carte 2** : même carte que la **carte 2 de geneve1**.

➤ Avant de passer aux étapes suivantes, il est nécessaire de garantir que les trois ordinateurs puissent communiquer ensemble (utilisez la commande ping).

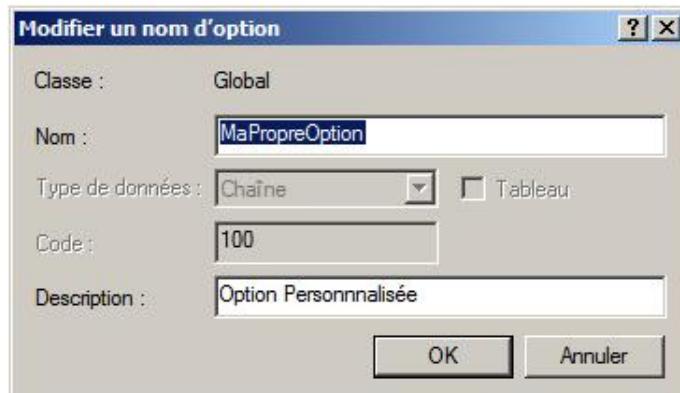
➤ L'agent relais DHCP est installé mais pas configuré.

## 8. Mise en œuvre des étendues

➤ Les ordinateurs **paris1** et **geneve1** sont requis.

### a. Pour le serveur DHCP paris1

1. Démarrez la console **DHCP**.
2. Vous allez commencer par définir l'option personnalisée. Cliquez avec le bouton droit de la souris sur le nœud **IPv4** puis sur **Définir les options prédefinies**.
3. Dans la boîte de dialogue **Options et valeurs prédefinies**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Type d'option**, remplissez les valeurs comme le montre la figure suivante :



1. Cliquez deux fois sur **OK**.
2. Comme l'option du serveur DNS est identique pour les deux étendues, elle pourrait être définie en tant qu'option de serveur.
3. Cliquez avec le bouton droit de la souris sur le nœud **Options de serveur sous IPv4** puis sur **Configurer les options**.
4. Configurez l'option **006 Serveurs DNS** avec l'adresse 10.1.1.1.
5. Configurez l'option **012 Nom d'hôtes** avec **mydom.eni**.
6. Cliquez avec le bouton droit de la souris sur le nœud **IPv4** puis sur **Nouvelle étendue**.
7. Saisissez **Etendue de Paris** pour le nom et **80%** des adresses dans la description.
8. La première adresse est 10.1.1.10 et la dernière est 10.1.1.200 avec un masque de 255.255.255.0, ne modifiez pas les autres valeurs et configurez les options après la création de l'étendue.

## 9. Configurez les options de l'étendue soit :

- 003 Routeur avec 10.1.1.1 et 10.1.1.3
- 100 MaPropreOption

Il est possible que le nœud IPv4 soit arrêté bien que les services aient démarré puisque vous pouvez créer une étendue. Cela provient du fait qu'une des cartes réseau utilisées dans le mappage se trouve sur un réseau disposant déjà d'un serveur DHCP. Pour résoudre ce problème, vous pouvez modifier les liaisons de l'onglet **Avancé des Propriétés IPv4** et ne conserver que la liaison avec la carte mappée sur Local seul. L'autre possibilité est de débrancher le câble de la carte réseau pour effectuer cet exercice.

1. Activez l'étendue. D'ici quelques minutes, **paris2** et **paris5** devraient acquérir une adresse IP.
2. Faites de même pour l'étendue 20% de Genève (10.2.1.201 à 1.2.1.254) et l'option d'étendue 003 **Routeur** 10.2.1.1.

Les étendues nécessaires ont été créées sur paris1.

## b. Pour le serveur DHCP de Genève

1. Créez les étendues complémentaires au serveur DHCP de Paris, soit une étendue de 20 % pour Paris et 80 % pour Genève. Il vous faut également créer l'option personnalisée sur ce serveur.

Les étendues nécessaires ont été créées sur geneve1.

## 9. Test des étendues

Les ordinateurs **paris1**, **geneve1**, **paris2** et **geneve2** sont requis.

Il est nécessaire de vérifier si les étendues sont opérationnelles. Normalement, vous devez voir que sur le site de Paris, paris2 et paris5 ont reçu une adresse IP du serveur DHCP de Paris.

geneve2 devrait en avoir reçu une du serveur DHCP de Genève.

Parmi les tests, effectuez des libérations et des renouvellements d'adresses IP en désactivant l'étendue du serveur DHCP. Dans ce cas, le client ne doit pas recevoir de nouvelles adresses.

Les étendues DHCP sont fonctionnelles.

## 10. Mise en œuvre d'une classe utilisateur

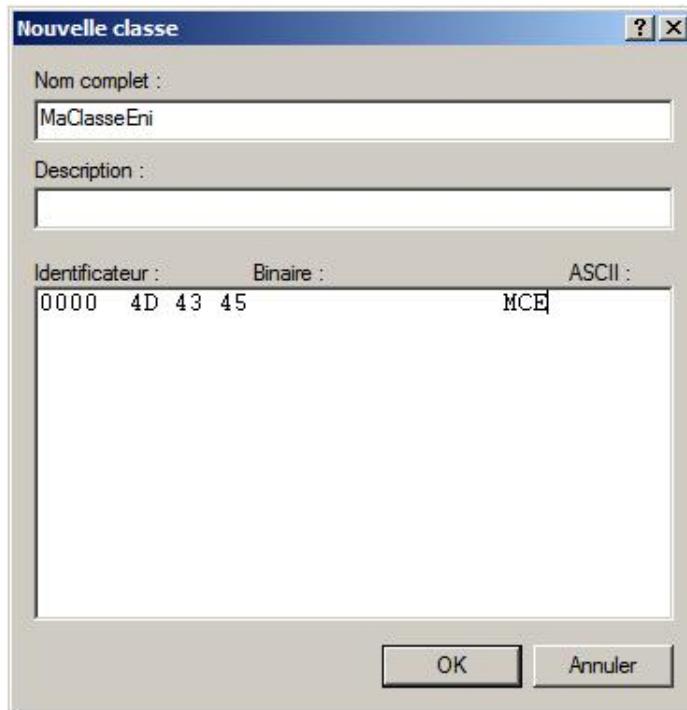
Les ordinateurs **paris1**, **paris2**, et **paris5** sont requis.

Sur le serveur DHCP, il faut créer une classe utilisateur puis configurer l'option DNS pour qu'elle ne soit distribuée qu'aux ordinateurs faisant partie de la classe.

Pour qu'un ordinateur client reçoive l'option il faut lui indiquer qu'il est membre de la classe.

1. Sur **paris1** dans la console DHCP, cliquez avec le bouton droit de la souris sur le nœud IPv4 puis sur **Définir les classes utilisateurs**.

2. Dans la boîte de dialogue **Classe des utilisateurs DHCP**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Nouvelle classe**, saisissez MaClasseEni pour le nom puis **MCE** dans la partie ASCII comme le montre la figure suivante :



1. Cliquez sur **OK** puis **Fermer**.
2. Pour l'étendue de Paris, créez une nouvelle option d'étendue mais pour la classe MaClasseEni l'option est 006 Serveur DNS avec une valeur de 190.190.190.1. Remarquez que dans les options d'étendues, votre nouvelle option est associée à la classe MaClasseEni et non pas à **Aucun**. Vous avez terminé la configuration sur le serveur.
3. Sur **paris2**, saisissez ipconfig /setclassid "paris" "MCE".
4. Libérez et renouvelez l'adresse IP, enfin saisissez ipconfig /all et vérifiez que vous avez bien l'**ID** de la classe et le serveur DNS supplémentaire.
5. Sur **paris5**, libérez et renouvelez l'adresse IP, enfin saisissez ipconfig /all et vérifiez que vous n'avez pas l'ID de la classe ni le serveur DNS supplémentaire.

 Vous avez vu comment implémenter une classe utilisateur pour passer par exemple des informations spécifiques à certains clients.

## 11. Mise en œuvre d'un agent relais DHCP sur le site de Paris

 L'ordinateur **paris3** est requis.

1. Lancez la console **Routage et accès distant**.
2. Cliquez avec le bouton droit de la souris sur le nœud **Agent de relais DHCP** puis sur **Nouvelle interface**.
3. Dans la boîte de dialogue **Nouvelle interface pour Agent de relais DHCP**, sélectionnez l'interface paris puis cliquez sur **OK**.
4. Dans la boîte de dialogue **Propriétés de Propriétés de relais DHCP -paris**, cliquez sur **OK**.

5. Cliquez avec le bouton droit de la souris sur le nœud **Agent de relais DHCP** puis sur **Propriétés**.
6. Dans la boîte de dialogue **Propriétés de relais DHCP**, ajoutez l'adresse du serveur de Genève, soit 10.2.1.1 (selon la configuration de vos liaisons, 192.168.1.1 n'écoute pas les requêtes DHCP), puis cliquez sur **OK**.

➤ L'agent relais DHCP est opérationnel.

## 12. Test de l'agent relais DHCP

➤ Les ordinateurs **paris1**, **geneve1**, **paris2**, et **paris3** sont requis.

Il faut désactiver l'étendue de Paris sur le serveur DHCP de Paris afin de simuler une défaillance puis libérer et renouveler l'adresse IP sur paris2.

1. Sur **paris1**, désactivez l'étendue **Etendue de Paris**.
2. Sur **paris2**, saisissez ipconfig /release, ipconfig /renew puis ipconfig /all et examinez la valeur indiquée pour **serveur DHCP** qui correspond au serveur **DHCP** de Genève.
3. Sur **paris3**, examinez les statistiques propres au relais dans la fenêtre de détail de **l'Agent de relais DHCP**.
4. Sur **paris1**, activez l'étendue **Etendue de Paris**.
5. Sur **paris2**, saisissez ipconfig /release, ipconfig /renew puis ipconfig /all et examinez la valeur indiquée pour **serveur DHCP** qui correspond au serveur DHCP de Genève.

➤ Le bon fonctionnement de l'agent relais DHCP a été testé.

## 13. Ajout d'un serveur DHCP dans un environnement Groupe de travail

➤ Les ordinateurs **paris1** et **paris5** sont requis.

Vous allez installer et configurer paris5 pour qu'il devienne serveur DHCP.

1. Sur **paris5**, modifiez l'adresse IP afin qu'elle soit statique en utilisant la commande suivante : netsh interface ipv4 set address name="paris" source=static address=10.1.1.5 mask=255.255.255.0
2. Dans l'invite de commande, saisissez start /w pkgmgr /iu:DHCPServerCore.
3. Ensuite, il faut activer le service avec la commande sc config DHCPServer start=auto.
4. Puis démarrer le service : net start dhcpserver.
5. Enfin pour permettre une gestion à distance, saisissez netsh advfirewall firewall set rule group="administration distante" new enable=yes.
6. Sur **paris1**, ajoutez dans la console DHCP le serveur **paris5** en utilisant son adresse IP.

➤ Le serveur paris5 peut automatiquement distribuer des adresses IP, un conflit potentiel entre les serveurs est donc possible.

## 14. Mise en œuvre de l'Active Directory pour paris1

- Les ordinateurs **paris1**, **paris2** et **paris5** sont requis.

Vous allez installer une Active Directory sur paris1 et voir l'effet sur paris5.

1. Sur **paris1**, lancez le script **ScriptAddAD.bat**, le fichier **WMydomEni.txt** doit également être placé sur le Bureau.
2. Sur **paris5**, saisissez pendant l'installation de l'Active Directory la commande `netsh dhcp server \\localhost show all`, puis cherchez dans la section **Etat du serveur** s'il est autorisé ou non.
3. Sur **paris1**, dans la console DHCP, cliquez avec le bouton droit de la souris sur le serveur **paris1.mydom.eni** puis sur **Autoriser**. Ensuite actualisez l'affichage, le serveur doit maintenant être autorisé.
4. Sur **paris5**, saisissez pendant l'installation de l'Active Directory la commande `netsh dhcp server \\localhost show all`, puis cherchez dans la section **Etat du serveur** s'il est autorisé ou non. Son état doit être à **False**.

- Le serveur paris5 détecte automatiquement qu'il existe un autre serveur DHCP faisant partie d'une Active Directory, donc il se met dans un état Non autorisé.

## 15. Clients PXE

- Les ordinateurs **paris1** et **paris2** sont requis.

Vous allez installer le rôle Services de déploiement Windows sur paris1 afin qu'il permette également à des clients PXE de se connecter puis vous effectuerez un démarrage PXE à partir de paris2.

1. Sur **paris1**, installez avec les paramètres par défaut le rôle de **Services de déploiement Windows**.
2. Lancez la console **Services de déploiement Windows**, puis avec le bouton droit de la souris, cliquez sur **paris.mydom.eni** puis sur **Configurer le serveur**.
3. Sur la page d'**Accueil**, cliquez sur **Suivant**.
4. Sur la page **Emplacement du dossier d'installation à distance**, cliquez sur **Suivant**. Sur le message, qui apparaît, cliquez sur **Oui**.
5. Sur la page **Option DHCP 60**, cochez les deux options pour les sélectionner puis cliquez sur **Suivant**.
6. Sur la page **Paramètres initiaux du serveur PXE**, sélectionnez **Répondre à tous les ordinateurs clients (connus et inconnus)** puis cliquez sur **Terminer**. N'ajoutez pas d'image. Votre serveur WDS est opérationnel.
7. Dans la **console DHCP**, vous trouverez que l'option **60 PXEClient** a été ajoutée comme option serveur.
8. Pour tester, redémarrez le serveur **paris2** puis soyez suffisamment rapide pour appuyer sur la touche [Suppr] afin de rentrer dans le **Bios**, déplacez-vous sur **Boot** puis sur **Boot Device Priority**. Modifiez **1st Boot Device** pour que **[PXE UNDI(Bus0 Slot)]** soit sélectionné. Enfin sauvegardez le tout en appuyant la touche [F10]. Appuyez sur **[OK]**.
9. Au redémarrage, l'ordinateur acquiert une adresse IP et vous demande d'appuyer sur la touche [F12] le résultat doit être le suivant :

Windows failed to start. A recent hardware or software change might be the cause. To fix the problem:

1. Insert your Windows installation disc and restart your computer.
2. Choose your language settings, and then click "Next."
3. Click "Repair your computer."

If you do not have this disc, contact your system administrator or computer manufacturer for assistance.

File: \Boot\BCD

Status: 0xc0000098

Info: The Windows Boot Configuration Data file does not contain a valid OS entry.

1. Sur **paris2**, modifiez l'ordre de démarrage pour démarrer sur PXE. Vous verrez qu'il n'acquiert pas d'adresse IP provenant du serveur DHCP.

➤ Dans cet exercice, vous avez installé et configuré le rôle du serveur DHCP dans différentes configurations y compris une mise en haute disponibilité avec l'utilisation d'un relais DHCP.

➤ N'oubliez pas de modifier le mappage afin de remettre toutes les cartes sur local seul.

➤ Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

# Exercice 3 - Mise en œuvre de l'adressage IPv6

## 1. Objectifs

Dans cet exercice vous allez vous familiariser avec la configuration des ordinateurs et des serveurs transformés en routeur pour l'utilisation de l'adressage IPv6.

Plusieurs scénarios sont joués vous permettant d'approfondir un élément unique à chaque fois.

## 2. Configuration de l'environnement

Cet exercice requiert le lancement de scripts et les machines virtuelles suivantes.

➤ Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels en cliquant sur **Eteindre et supprimer les modifications**.

➤ Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de Fermer du menu Action de Virtual PC.

➤ Placez les scripts sur le Bureau des ordinateurs virtuels.

- Sur **paris1**, lancez le script **scriptParis1.bat**.
- Sur **paris2**, lancez le script **scriptParis2.bat**.
- Sur **geneve1**, lancez le script **scriptGeneve1.bat**.
- Sur **geneve2**, lancez le script **scriptGeneve2.bat**.

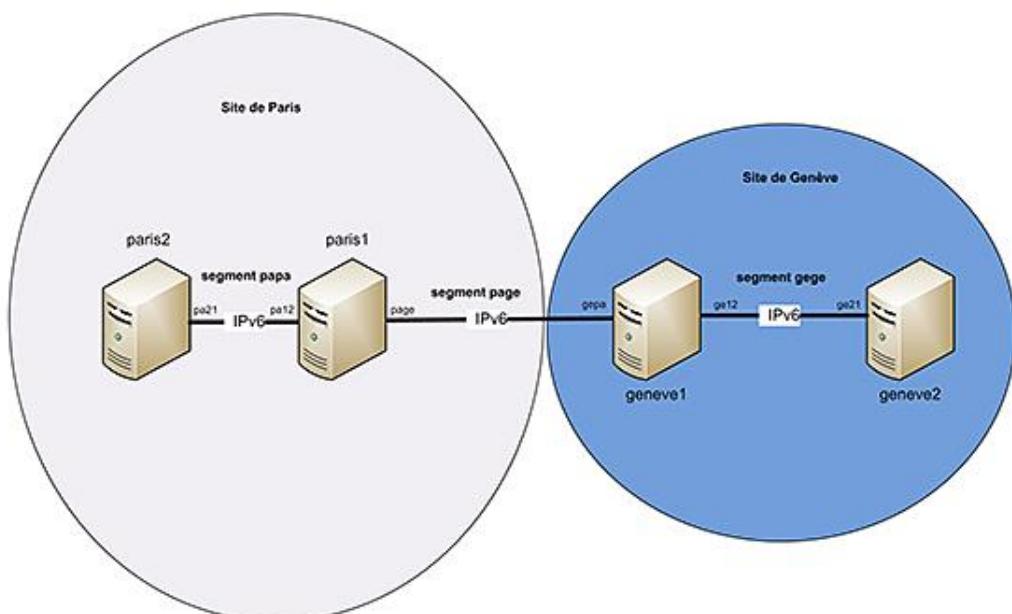
Après le lancement des scripts, tous les ordinateurs sont dans un groupe de travail. **paris1** et **geneve1** sont configurés en tant que routeur. **paris2** et **geneve2** ne disposent que du protocole IPv6.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Configuration des services réseaux de base, principalement aux sections consacrées à l'adressage IPv6 ainsi qu'au routage. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et le chapitre Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre de l'adressage IPv6

Votre direction a entendu parler d'IPv6 et il faudrait l'implémenter très rapidement mais au préalable il vous est demandé d'effectuer une étude de faisabilité dans le but de minimiser au maximum les risques le jour de la migration vers IPv6. Pour cela, vous créez un banc de test composé de quatre ordinateurs selon la topologie suivante :



Il vous est demandé d'évaluer plusieurs scénarios :

- 1) Dans ce scénario, vous devez garantir que chaque hôte puisse dialoguer avec son homologue sur le même segment de réseau utilisant une adresse **IPv6** de lien local en modifiant le mappage des cartes virtuelles sur la machine physique.
- 2) Dans ce scénario, vous devez implémenter des adresses globales ainsi qu'activer le routage sur les ordinateurs **paris1** et **geneve1**.

Les tâches à effectuer sont :

- Tester le fonctionnement de la pile IPv6 sur chaque ordinateur local.
- Modifier le mappage des cartes virtuelles afin de simuler réellement trois segments de réseaux.
- Transformer **paris1** et **geneve1** en routeur IPv6 et permettre une auto configuration d'ordinateurs clients pour les adresses IPv6 basées sur la publication du réseau, et enfin tester la communication.

Normalement, il est nécessaire de réserver auprès du IANA (*Internet Assigned Numbers Authority*) les adresses IPv6. Néanmoins, il est possible d'utiliser des adresses de documentation telle que celles prévues dans la **RFC 3849**, l'espace d'adressage commence par **2001:db8::/32**.

Pour le segment **papa**, utilisez **2001:DB8:1:1::/64**.

Pour le segment **page**, utilisez **2001:DB8:1:2::/64**.

Pour le segment **gege**, utilisez **2001:DB8:1:3::/64**.

## 5. Garantir la communication IPv6 sur chaque segment de réseau

 paris1, paris2, geneve1 et geneve2 doivent fonctionner, les opérations s'effectuent sur tous les ordinateurs.

Pour tester le fonctionnement de la pile **IPv6**, il suffit d'effectuer un **ping** sur l'adresse **localhost** de chaque ordinateur.

1. Dans une invite de commande, saisissez ping localhost ou ping ::1.

Il faut maintenant modifier le mappage des cartes réseaux virtuelles sur les cartes réseaux physiques. Pour effectuer cette opération, il est nécessaire de disposer d'au moins 2 cartes réseaux sur son ordinateur. Si ce n'est pas le cas, vous pourrez le faire en plaçant deux segments sur le même réseau physique comme indiqué dans la procédure.

### a. Modification à effectuer pour créer le segment réseau gege

Cette procédure est à effectuer dans tous les cas (ordinateur physique disposant d'une ou plusieurs cartes réseau).

1. Sur **geneve2**, ouvrez la boîte de dialogue **Paramètres de la machine virtuelle de la console Virtual PC**, puis sélectionnez le paramètre réseau.
2. Dans **réseau**, pour la **carte 1**, modifiez la sélection de la carte de local seul vers une de vos carte réseau physique comme par exemple Contrôleur Ethernet Gigabit Marvell Yukon 88E8053 PCI-E #2. Ne sélectionnez pas Réseau Partagé (NAT).
3. Sur **geneve1**, faites de même mais uniquement pour la **carte 1** qui doit normalement porter le nom de **page**. Vous pouvez vérifier en lisant le script.

### b. Test du segment de réseau gege

Cette procédure est à effectuer dans tous les cas (ordinateur physique disposant d'une ou de plusieurs cartes réseau).

1. Sur **geneve1**, saisissez la commande ipconfig.
2. Dans le résultat, recherchez les informations pour la carte réseau **ge12**.
3. Récupérez l'adresse IPv6 de liaison locale en l'écrivant sur un papier ou en la copiant dans le presse-papiers. Elle ressemble à : fe80::f1c3:5c64:7ec1:4c02%10.
4. Sur **geneve2**, saisissez la commande ping suivi de l'adresse IPv6 provenant de l'ordinateur **geneve1**. Normalement, vous devriez recevoir une réponse. Si ce n'est pas le cas, veuillez contrôler que l'adresse IPv6 est exacte, puis que le mappage est bien correct. Vous pouvez vous aider en utilisant l'indice de zone : **%10** correspond à la première carte physique et **%17** à la seconde.
5. Testez également à partir de **geneve2** un ping mais sans ajouter l'indice de zone comme le montre l'exemple suivant : ping fe80::f1c3:5c64:7ec1:4c02.
6. Ensuite sur **geneve1**, faites de même pour contacter **geneve2**.

 Veuillez noter que lorsque votre ordinateur dispose de plusieurs cartes réseaux, il est nécessaire d'ajouter sur quelle interface vous désirez communiquer. La bonne pratique est d'ajouter systématiquement l'indication de l'interface à utiliser.

### c. Modification à effectuer pour créer le segment réseau papa

Cette procédure est à effectuer uniquement si votre ordinateur physique dispose de plusieurs cartes réseau.

1. Sur paris2, ouvrez la boîte de dialogue **Paramètres de la machine virtuelle de la console Virtual PC**, puis sélectionnez le paramètre réseau.
2. Dans réseau, pour la carte 1, modifiez la sélection de la carte de local seul vers une de vos carte réseau physique qui n'est pas déjà utilisée par le segment réseau gege comme par exemple Contrôleur Ethernet Gigabit Marvell Yukon 88E8053 PCI-E. Ne sélectionnez pas Réseau Partagé (NAT).
3. Sur paris1, faites de même mais uniquement pour la carte 1 qui doit normalement porter le nom de pa12.

### d. Test des segments de réseau papa et page

Ces procédures sont à effectuer dans tous les cas (ordinateur physique disposant d'une ou de plusieurs cartes

réseau).

Pour chaque segment soit :

- **papa** avec **paris1** et **paris2**
- **page** avec **paris1** et **geneve1**

Suivez la même procédure que pour le segment **gege**.

Aucune modification n'est à effectuer sur le segment **page** car il utilise le mappage sur réseau local.

➤ Si vous n'avez qu'une seule carte réseau, les segments **papa** et **page** se trouvent mappés sur local seul. Dès lors, il est possible de communiquer directement entre **paris2** et **geneve1** !

➤ Il est important d'établir la communication précitée avant de passer au prochain scénario.

## 6. Utilisation d'adresses globales unicast IPv6

➤ **paris1**, **paris2**, **geneve1** et **geneve2** doivent fonctionner, les opérations s'effectuent sur tous les ordinateurs.

Pour chaque routeur, il faut permettre aux paquets qui arrivent sur l'interface d'être routés et pour que les ordinateurs clients représentés par **paris2** et **geneve2** reçoivent une adresse globale unicast **IPv6**, il faut configurer les routeurs pour qu'ils puissent indiquer aux ordinateurs clients quelles adresses IPv6 globales ils peuvent utiliser.

### a. Pour geneve1

1. Avant de modifier **geneve1**, saisissez ipconfig dans une invite de commande sur **geneve1** et **geneve2**.

2. Ouvrez une autre invite de commande puis entrez dans le contexte ipv6 de netsh interface.

3. Saisissez la commande suivante pour activer le routage et permettre d'avertir les clients :

```
set interface interface="ge12" forwarding=enabled advertise=enabled
```

4. Saisissez maintenant la commande pour indiquer et publier le sous-réseau IPv6 :

```
add route 2001:db8:1:3::/64 interface="ge12" publish=yes
```

5. Saisissez la commande suivante pour activer le routage et permettre d'avertir les clients :

```
set interface interface="gepa" forwarding=enabled advertise=enabled
```

6. Saisissez maintenant la commande pour indiquer et publier le sous-réseau IPv6 :

```
add route 2001:db8:1:2::/64 interface="gepa" publish=yes
```

7. Maintenant il faut encore ajouter la route du segment **papa** avec la commande suivante :

```
netsh interface ipv6 add route 2001:db8:1:1::/64 interface="gepa" publish=yes  
nexthop=fe80::4f9:1a01:b86d:2d54
```

où l'adresse indiquée pour nexthop correspond à l'adresse IPv6 de lien local de **paris1** sur l'interface **page**.

8. Saisissez ipconfig sur **geneve1** et **geneve2** et visualisez les modifications par rapport aux valeurs obtenues précédemment.

### b. Pour paris1

1. Créez un script pour modifier **paris1**. Il doit ressembler à la figure suivante :

```
REM 1) Modifie paris2 pour devenir routeur via un script  
netsh interface ipv6 set interface interrface="pa21" forwarding=enabled  
advertise=enabled  
netsh interface ipv6 set interface interrface="page" forwarding=enabled  
advertise=enabled  
netsh interface ipv6 add route 2001:db8:1:1::/64 interface="pai2" publish=yes  
netsh interface ipv6 add route 2001:db8:1:2::/64 interface="page" publish=yes  
netsh interface ipv6 add route 2001:db8:1:3::/64 interface="page" publish=yes  
nexthop=fe80::4f9:1a01:b86d:2d54  
pause
```

1. Lancez le script sur **paris1**.

### c. Tester la connectivité entre paris2 et geneve2

Vous pouvez maintenant tester la connectivité en utilisant la commande ping depuis **paris2** pour joindre **geneve2**. Il est nécessaire d'utiliser l'adresse globale et pas l'adresse de lien local.

1. Saisissez la commande suivante :

```
ping 2001:db8:1:3:b03d:72ba:61c7:2a97
```

---

► Il est important d'établir la communication précitée avant de passer au prochain scénario. En cas d'erreur, vous pouvez effectuer un **ping** sur une autre adresse globale plus proche, vous pouvez également utiliser la commande **route print** pour voir si les routes sont correctes.

---

► Dans cet exercice vous avez vu comment configurer le protocole IPv6 et activer le routage sur des ordinateurs Windows Server 2008.

---

► N'oubliez pas de modifier le mappage afin de remettre toutes les cartes sur local seul.

---

► Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel exercice.

---

# Exercice 2 - Mise en œuvre de l'adressage IPv4 au niveau des sites de Paris et de Genève

## 1. Objectifs

Dans cet exercice, vous allez configurer l'adressage IP pour plusieurs ordinateurs en utilisant les plages d'adresses définies dans l'exercice précédent. Ensuite, vous allez transformer plusieurs serveurs en routeurs et y implémenter d'abord le routage statique, puis passer au routage dynamique. À l'aide du moniteur réseau, il vous faudra solutionner une panne.

## 2. Configuration de l'environnement

Cet exercice ne requiert pas de configuration spécifique mais uniquement les machines virtuelles suivantes.

 Pour que les scripts s'exécutent correctement, il est nécessaire d'annuler toutes les modifications effectuées lors d'un autre exercice en fermant au préalable les ordinateurs virtuels sur **Eteindre et supprimer les modifications**.

 Si vous désirez interrompre l'exercice, il est conseillé de fermer les ordinateurs virtuels en sélectionnant **Enregistrer l'état et Enregistrer les modifications** et en décochant la case à cocher **Ecrire les modifications sur le disque virtuel** de **Fermer** du menu **Action** de Virtual PC.

- paris1
- paris2
- paris3
- geneve1
- geneve2

Dans les questions il peut vous être demandé d'exécuter un des scripts suivants.

 Placez les scripts sur le Bureau des ordinateurs virtuels.

- ActiveIcmp.bat
- ScriptInstallAndConfigureRoutage.bat
- ScriptetRoutes.bat
- ScriptResetRoutes.bat
- ScripttestRoutesStatiques.bat

## 3. Référence par rapport à la théorie

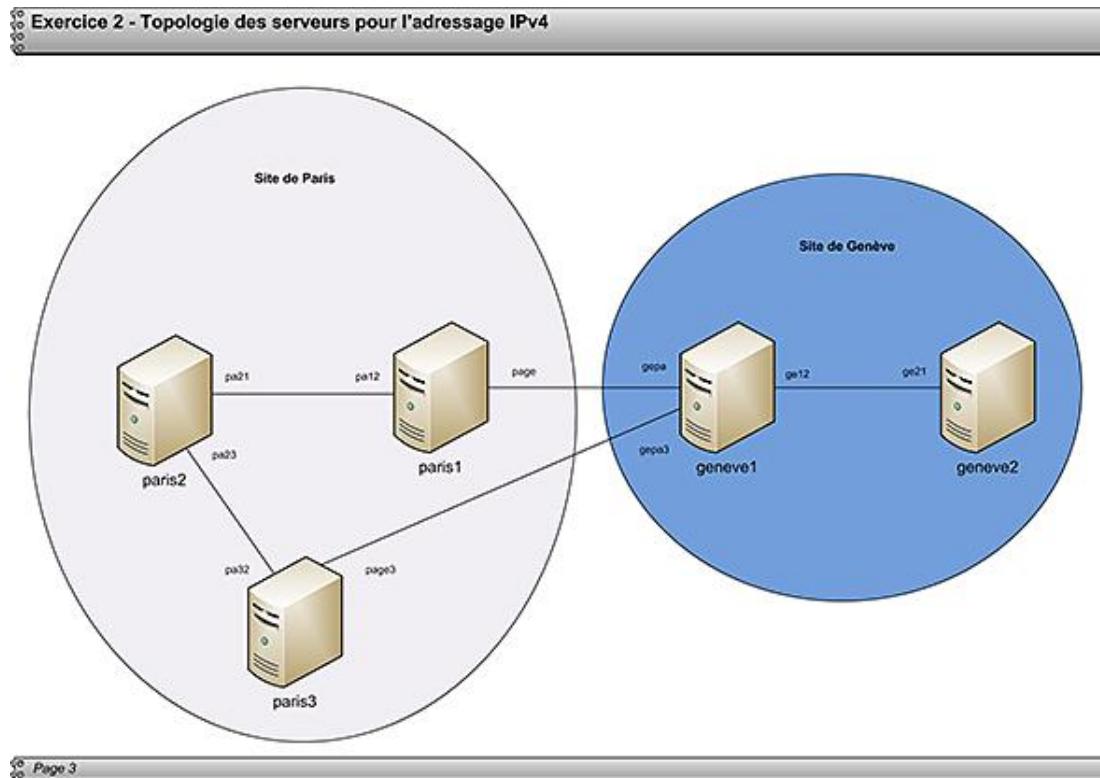
Vous pouvez vous référer au chapitre Configuration de base des services réseau. Néanmoins, les chapitres Rôles et fonctionnalités, Outils de configuration et de gestion et Gestion et surveillance d'une infrastructure réseau vous seront également utiles.

## 4. Scénario et questions pour la mise en œuvre de l'adressage IPv4

Dans ce scénario, vous devez configurer l'adressage IPv4 de plusieurs serveurs des sites de Genève et de Paris comme le montre le schéma suivant en utilisant les éléments d'adresses du tableau. La méthode de configuration vous permet d'utiliser plusieurs voies pour arriver à l'objectif.

Il est également nécessaire de renommer l'interface réseau comme indiqué sur le schéma et de contrôler la connectivité entre les deux interfaces se trouvant sur le même sous-réseau.

Ensuite, vous allez mettre en œuvre le routage. Vous allez d'abord étudier le routage statique car cela vous semble une bonne solution, puis le routage dynamique. Enfin vous devez créer une documentation pour vos stagiaires sur les messages d'erreur retournés par la commande ping.



Les tâches à effectuer sont :

- Configurer les ordinateurs suivants en utilisant les méthodes de configuration indiquées :

Nom du serveur	Nom de l'interface	Adresse IP	Méthode de configuration
paris1	pa12	10.1.1.1/24	ncpa.cpl
	page	10.1.10.5/30	netsh
paris2	pa21	10.1.1.2/24	script
	pa23	10.1.2.129/26	script
paris3	pa32	10.1.2.130/26	script
	page3	10.2.1.1/29	script
geneve1	ge12	10.2.1.17/30	script
	gepa	10.1.10.6/30	script

	gepa3	10.2.1.2/29	script
geneve2	ge21	10.2.1.18/30	script

- Tester la connectivité de chaque segment.
- Mettre en œuvre le routage statique entre les différents segments.
- Mettre en œuvre le routage dynamique entre les différents segments.
- Décrire les types de messages d'erreur de la commande ping.

## 5. Mise en œuvre de l'adressage IPv4

 paris1, paris2, paris3, geneve1 et geneve2 sont requis.

### a. Pour paris1 interface pa12

 Seul paris1 est requis.

1. Démarrez la machine virtuelle **paris1** et connectez-vous en tant qu'administrateur.
2. Dans la zone de texte **Rechercher** du menu **Démarrer**, saisissez `ncpa.cpl` puis appuyez sur [Entrée].
3. Dans la boîte de dialogue **Connexions réseau**, cliquez avec le bouton droit de la souris sur l'icône **Connexion au réseau local** pour faire apparaître le menu contextuel puis cliquez sur **Propriétés**.
4. Dans la boîte de dialogue **Propriétés de Connexion au réseau local**, double cliquez sur **Protocole Internet version 4 (TCP/IPv4)**.
5. Dans la boîte de dialogue **Propriétés de Protocole Internet version 4 (TCP/IPv4)**, sélectionnez l'option **Utiliser l'adresse IP suivante:** puis remplissez les zones de texte **Adresse IP** et **Masque de sous-réseau** avec respectivement les valeurs `10.1.1.1` et `255.255.255.0`.
6. Cliquez deux fois sur **OK**.
7. Dans la boîte de dialogue **Connexions réseau**, cliquez avec le bouton droit de la souris sur l'icône **Connexion au réseau local** pour faire apparaître le menu contextuel puis cliquez sur **Renommer**.
8. Renommez **Connexion au réseau local** en **pa12**.

 L'interface pa12 de paris1 a été configurée en utilisant la méthode manuelle classique.

### b. Pour paris1 interface page

 Seul paris1 est requis.

1. Démarrez la machine virtuelle **paris1** et connectez-vous en tant qu'administrateur.
2. Dans la zone de texte **Rechercher** du menu **Démarrer**, saisissez `cmd` puis appuyez sur

[Entrée].

3. Dans l'invite de commande saisissez netsh interface set interface name="Connexion au réseau local 2" newname="page" puis appuyez sur [Entrée].
4. Dans l'invite de commande saisissez netsh interface ipv4 set address name="page" source=static address=10.1.10.5 mask=255.255.255.252 puis appuyez sur [Entrée].

---

 L'interface page de paris1 a été configurée en utilisant la méthode netsh.

---

### c. Pour paris2

 Seul paris2 est requis.

Il faut créer un script qui modifie les noms et l'adressage IP des interfaces **pa21**, **pa23** ainsi qu'un contrôle de la connexion vers paris1 ; pour cela procédez de la manière suivante :

1. Démarrez la machine virtuelle **paris2** et connectez-vous en tant qu'administrateur.
2. Dans la zone de texte **Rechercher** du menu **Démarrer**, saisissez worpad puis appuyez sur [Entrée].
3. Dans Wordpad, saisissez les commandes suivantes :

```
netsh interface set interface name="Connexion au réseau local" newname="pa21"

netsh interface set interface name="Connexion au réseau local 2" newname="pa23"

netsh interface ipv4 set address name="pa21" source=static address=10.1.1.2
mask=255.255.255.0

netsh interface ipv4 set address name="pa23" source=static address=10.1.2.129
mask=255.255.255.192
```

Echo

rem 10 requêtes sont envoyées afin que l'ordinateur ait le temps de finir la configuration des interfaces.

echo

ping 10.1.1.1 -n 10

pause

4. Cliquez sur l'icône **Enregistrer**. Dans la boîte de dialogue **Enregistrer sous**, saisissez ScriptParis2.bat pour le nom, modifiez éventuellement l'emplacement puis sélectionnez Document texte **MS-DOS** pour le type. Enfin cliquez sur **Enregistrer**.
5. Lancez le script **ScriptParis2.bat** puis contrôlez dans l'invite de commande que tout s'est bien exécuté.

### d. Pour paris3

 Seul paris3 est requis.

Afin d'optimiser la procédure, vous allez récupérer le fichier **ScriptParis2.bat** créé précédemment, le modifier et lui donner un nouveau nom. Pour cela procédez de la manière suivante :

1. Démarrez la machine virtuelle **paris3** et connectez-vous en tant qu'administrateur.

2. Récupérez le script **ScriptParis2.bat** puis renommez-le en **ScriptParis3.bat**.
3. Éditez le script **ScriptParis3bat**, modifiez-le pour qu'il ressemble au script suivant puis sauvegardez-le.

```
netsh interface set interface name="Connexion au rseau local" newname="pa32"
netsh interface set interface name="Connexion au rseau local 2" newname="page3"
netsh interface ipv4 set address name="page3" source=static address=10.2.1.1
mask=255.255.255.248
netsh interface ipv4 set address name="pa32" source=static address=10.1.2.130
mask=255.255.255.192
echo
rem 10 requêtes sont envoyées afin que l'ordinateur ait le temps de finir
la configuration des interfaces.
echo
ping 10.1.2.129 -n 10
pause
```

1. Lancez le script **ScriptParis3.bat** puis contrôlez dans l'invite de commande que tout s'est bien exécuté.

 L'ordinateur paris3 a été configuré en utilisant un script.

#### e. Pour geneve1

 Seul geneve1 est requis.

Afin d'optimiser la procédure, vous allez récupérer le fichier **ScriptParis3.bat** créé précédemment, le modifier et lui donner un nouveau nom. Pour cela procédez de la manière suivante :

1. Démarrez la machine virtuelle **geneve1** et connectez-vous en tant qu'administrateur.
2. Récupérez le script **ScriptParis3.bat** puis renommez-le en **Scriptgeneve1.bat**.
3. Éditez le script **Scriptgeneve1.bat**, modifiez-le pour qu'il ressemble au script suivant puis sauvegardez-le.

```
netsh interface set interface name="Connexion au rseau local" newname="ge12"
netsh interface set interface name="Connexion au rseau local 2" newname="gepa"
netsh interface set interface name="Connexion au rseau local 3" newname="gepa3"

netsh interface ipv4 set address name="ge12" source=static address=10.2.1.17
mask=255.255.255.252
netsh interface ipv4 set address name="gepa" source=static address=10.1.10.6
mask=255.255.255.252
netsh interface ipv4 set address name="gepa3" source=static address=10.2.1.2
mask=255.255.255.248
echo
rem 10 requêtes sont envoyées afin que l'ordinateur ait le temps de finir
la configuration des interfaces.
echo
ping 10.1.10.5 -n 10
ping 10.2.1.1
pause
```

1. Lancez le script **Scriptgeneve1.bat** puis contrôlez dans l'invite de commande que tout s'est bien exécuté.

 L'ordinateur geneve1 a été configuré en utilisant un script.

#### f. Pour geneve2



Seul geneve2 est requis.

La procédure est similaire à celle utilisée pour geneve1 :

1. Démarrez la machine virtuelle **geneve2** et connectez-vous en tant qu'administrateur.
2. Récupérez le script **Scriptgeneve1.bat** puis renommez-le en **Scriptgeneve2.bat**.
3. Éditez le script **Scriptgeneve2.bat**, modifiez-le pour qu'il ressemble au script suivant puis sauvegardez-le.

```
netsh interface set interface name="Connexion au réseau local" newname="ge21"
netsh interface ipv4 set address name="ge21" source=static address=10.2.1.18
mask=255.255.255.252
echo
rem 10 requêtes sont envoyées afin que l'ordinateur ait le temps de finir
la configuration des interfaces.
echo
ping 10.2.1.17 -n 10
pause
```

1. Lancez le script **Scriptgeneve2.bat** dans l'invite de commande puis contrôlez que tout s'est bien exécuté.



L'ordinateur geneve2 a été configuré en utilisant un script.

## 6. Test de connexion des segments de réseau



paris1, paris2, paris3, geneve1 et geneve2 sont requis.

Vous allez tester la connectivité de chaque segment en utilisant la commande ping et l'adresse IP de l'ordinateur distant du segment. En cas d'erreur, contrôlez la configuration de chaque ordinateur ainsi que la connectivité de l'ordinateur virtuel en contrôlant le mappage des cartes virtuelle et physique, sinon vous pouvez considérer que la connectivité est parfaite.

### a. Pour le segment paris1-paris2



paris1 et paris2 sont requis.

1. Sur paris1, saisissez la commande ping 10.1.1.2.
2. Éventuellement sur paris2 saisissez la commande ping 10.1.1.1.



La connectivité devrait être parfaite sinon relisez la section Test de connexion des segments de réseau.

### b. Pour le segment paris2-paris3



paris2 et paris3 sont requis.

1. Sur paris2, saisissez la commande ping 10.1.2.130.
2. Éventuellement sur paris3 saisissez la commande ping 10.1.2.129.



La connectivité devrait être parfaite sinon relisez la section Test de connexion des segments de réseau.

---

#### c. Pour le segment paris3-geneve1



paris3 et geneve1 sont requis.

---

1. Sur paris3, saisissez la commande `ping 10.2.1.2`.
  2. Éventuellement sur geneve1 saisissez la commande `ping 10.2.1.1`.
- 



La connectivité devrait être parfaite sinon relisez la section Test de connexion des segments de réseau.

---

#### d. Pour le segment geneve1-geneve2



geneve1 et geneve2 sont requis.

---

1. Sur geneve1, saisissez la commande `ping 10.2.1.18`.
  2. Éventuellement sur geneve2 saisissez la commande `ping 10.2.1.17`.
- 



La connectivité devrait être parfaite sinon relisez la section Test de connexion des segments de réseau.

---

#### e. Pour le segment paris1-geneve1



paris1 et geneve1 sont requis.

---

1. Sur paris1, saisissez la commande `ping 10.1.10.6`.
  2. Éventuellement sur geneve1 saisissez la commande `ping 10.21.10.5`.
- 



La connectivité devrait être parfaite sinon relisez la section Test de connexion des segments de réseau.

---



Dans cette section, vous avez appris à configurer de manière statique les cartes réseaux d'un serveur en employant différentes méthodes y compris en créant un script et en le modifiant pour automatiser la tâche. Chaque connexion a été testée à l'aide de la commande `ping` et doit fonctionner correctement, ce qui garantit la connectivité au niveau de la couche 3 du modèle OSI.

---

## 7. Mise en œuvre du routage statique

Dans les sections précédentes, vous avez configuré l'adressage IP de manière statique et garantit un bon fonctionnement des connexions entre deux ordinateurs voisins. Dans cette section, il vous faut décider quels ordinateurs doivent être transformés en routeurs et y ajouter des routes statiques, et pour les autres ajouter simplement la passerelle par défaut.

**geneve2** ne dispose que d'une seule carte réseau, donc d'un seul chemin possible pour communiquer, lui ajouter une passerelle est la solution. Pour les autres serveurs, la topologie montre une boucle et chacun dispose d'au moins deux cartes. Les transformer en routeur et leur assigner des routes semble la meilleure solution. Cela implique que chaque routeur connaisse au moins deux routes soit celles de ses interfaces ; il faut donc lui ajouter les routes inconnues.

La procédure suivante montre une solution pour ajouter la passerelle par défaut à **geneve2**.

1. Démarrez la machine virtuelle **geneve2** et connectez-vous en tant qu'administrateur.
2. Lancez une invite de commande.
3. Saisissez netsh interface ipv4 set address name=ge21 source=static address=10.2.1.18 mask= 255.255.255.252 gateway=10.2.1.17.
4. Contrôlez avec ipconfig que la passerelle a été ajoutée.

La procédure suivante montre une solution pour installer et activer le routage :

1. Démarrez la machine virtuelle considérée et connectez-vous en tant qu'administrateur.
2. Le plus simple est de créer un script appelé **ScriptInstallAndConfigureRoutage.bat** que vous pourrez réutiliser sur les autres routeurs. Il doit contenir les commandes suivantes :

```
REM 1) Install le service de rôle de routage  
servermanagercmd -install NPAS-Routing  
  
REM 2) Démarrer le service RAS  
sc config remoteaccess start= auto  
sc start remoteaccess  
  
REM 3) Configure RAS en tant que routeur  
netsh ras set type ipv4rtrtype=lanonly ipv6rtrtype=none rastype=none
```

3. Exécutez le script **ScriptInstallAndConfigureRoutage.bat**. Contrôlez le résultat en utilisant les commandes, le gestionnaire de services, le gestionnaire de serveur et la console du routage et d'accès distant.

La procédure suivante montre une solution pour ajouter des routes statiques :

1. Démarrez la machine virtuelle considérée et connectez-vous en tant qu'administrateur.
2. Saisissez la commande suivante dans une invite de commande ou créez un script :

```
route add 10.1.1.0 MASK 255.255.255.0 10.1.10.5
```

où 10.1.1.0 est le nom du réseau distant et 10.1.10.5 est l'adresse de la passerelle pour atteindre ce réseau. Cette commande n'est valable que pour le routeur **geneve1** afin de connaître la route pour le réseau paris1-paris2.

Vous devez ajouter les routes suivantes sur chaque routeur. Notez qu'il existe plusieurs routes. Le routeur utilisera toujours la route dont le métrique est le plus faible.

### **geneve1**

Soit les routes pour les réseaux **paris1-paris2** et **paris2-paris3** :

- route add 10.1.1.0 MASK 255.255.255.0 10.1.10.5 METRIC 2
- route add 10.1.1.0 MASK 255.255.255.0 10.2.1.1 METRIC 5
- route add 10.1.2.128 MASK 255.255.255.192 10.1.10.5 METRIC 5
- route add 10.1.2.128 MASK 255.255.255.192 10.2.1.1 METRIC 2

### **paris1**

Soit les routes pour les réseaux **geneve1-geneve2**, **geneve1-paris3** et **paris2-paris3** :

- route add 10.1.2.128 MASK 255.255.255.192 10.1.1.2 METRIC 2
- route add 10.1.2.128 MASK 255.255.255.192 10.1.10.6 METRIC 3

- route add 10.2.1.0 MASK 255.255.255.248 10.1.10.6 METRIC 2
- route add 10.2.1.0 MASK 255.255.255.248 10.1.1.2 METRIC 3
- route add 10.2.1.16 MASK 255.255.255.252 10.1.10.6 METRIC 5
- route add 10.2.1.16 MASK 255.255.255.252 10.1.1.2 METRIC 5

## **paris2**

Soit les routes pour les réseaux **geneve1-geneve2**, **geneve1-paris3** et **geneve1-paris1** :

- route add 10.1.10.4 MASK 255.255.255.252 10.1.1.1 METRIC 2
- route add 10.1.10.4 MASK 255.255.255.252 10.1.2.130 METRIC 4
- route add 10.2.1.0 MASK 255.255.255.248 10.1.1.1 METRIC 4
- route add 10.2.1.0 MASK 255.255.255.248 10.1.2.130 METRIC 2
- route add 10.2.1.16 MASK 255.255.255.252 10.1.1.1 METRIC 5
- route add 10.2.1.16 MASK 255.255.255.252 10.1.2.130 METRIC 5

## **paris3**

Soit les routes pour les réseaux **geneve1-geneve2**, **paris1-paris2** et **geneve1-paris1** :

- route add 10.2.1.16 MASK 255.255.255.248 10.2.1.2 METRIC 2
- route add 10.2.1.16 MASK 255.255.255.248 10.1.2.129 METRIC 4
- route add 10.1.10.4 MASK 255.255.255.252 10.2.1.2 METRIC 6
- route add 10.1.10.4 MASK 255.255.255.252 10.1.2.129 METRIC 2
- route add 10.1.1.0 MASK 255.255.255.0 10.2.1.2 METRIC 4
- route add 10.1.1.0 MASK 255.255.255.0 10.1.2.129 METRIC 2

Pour contrôler que tout fonctionne, vous pouvez effectuer la procédure suivante à partir de **geneve2**.

1. Démarrez la machine virtuelle **geneve2** et connectez-vous en tant qu'administrateur.
2. Lancez une invite de commande.
3. Saisissez ping 10.1.1.2.
4. Saisissez ping 10.1.2.129.

---

 Vous pouvez remplacer la commande **ping** par **tracert** ou **pathping** afin d'obtenir également des informations sur les routeurs utilisés.

---

1. Nous allons simuler une panne en arrêtant le serveur **paris2** (enregistrer l'état et les modifications), veillez à décocher **Ecrire les modifications sur le disque dur virtuel**. Ensuite vous allez lancer le script appelé **Scripttestroutes.bat** qui exécute la commande **ping** sur tous les serveurs restants. Comme résultat, vous devez recevoir des réponses aux ping qui indique que la communication fonctionne toujours.

- Redémarrez le serveur **paris2** et arrêtez **paris1** puis relancez le script **Scripttestroutes.bat**. Le résultat doit être identique car rappelez-vous, toutes les routes possibles ont été ajoutées manuellement.

 Vous venez de transformer le serveur en routeur puis vous avez ajouté des routes statiques. Si vous avez effectué cet exercice sans vous aider de la réponse, vous avez sûrement dû rencontrer des difficultés car il est très difficile de configurer manuellement le routage statique et la moindre erreur conduit à des résultats non souhaités. La maintenance d'un tel réseau n'est pas efficace. Néanmoins son avantage réside dans le fait qu'aucun trafic n'est dû à l'échange des routes.

## 8. Mise en œuvre du routage dynamique

Dans la section précédente, vous avez vu la difficulté pour gérer un réseau à l'aide de routes statiques. Ici, vous allez utiliser le routage dynamique en activant le protocole RIP.

Si vous avez effectué les opérations de la section précédente, lancez le script **ScriptResetRoutes.bat** sur chaque serveur, sinon effectuez uniquement les procédures décrites pour **geneve2** et pour installer et activer le routage.

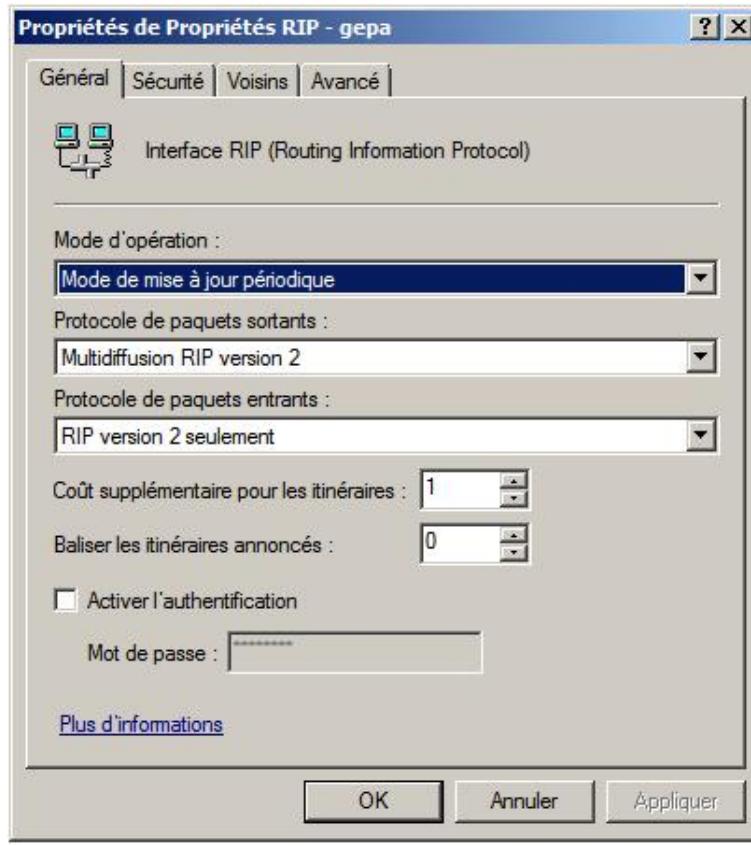
RIP s'installe et s'active à partir de la console routage et accès distant. D'autre part il est nécessaire de connaître les interfaces qui vont envoyer ou recevoir des messages RIP. Selon la topologie, les serveurs paris1, paris2 et paris3 vont activer RIP sur toutes leurs interfaces. Sur geneve1, l'interface pour la connexion vers geneve2 n'a pas besoin d'envoyer ou recevoir des messages RIP.

Concernant le serveur geneve2, il n'y a rien à modifier.

La procédure suivante est à répéter sur les serveurs dont le routage est activé.

- Démarrez la machine virtuelle considérée et connectez-vous en tant qu'administrateur.
- Cliquez sur **Démarrer - Outils d'administration** puis sur **Routage et accès distant**.
- Dans la console développez l'arborescence à partir du nom du serveur, puis l'arborescence sur le nœud **IPv4**.
- Cliquez avec le bouton droit de la souris sur le nœud **Général** d'IPv4, puis sur **Nouveau protocole de routage**.
- Dans la boîte de dialogue **Nouveau protocole de routage**, sélectionnez **Protocole RIP version 2 pour Internet**, puis cliquez sur **OK**.
- Avec le bouton droit de la souris, cliquez sur le nouveau nœud RIP puis sur **Nouvelle interface**.
- Dans la boîte de dialogue **Nouvelle interface pour Protocole RIP version 2 pour Internet** sélectionnez une interface puis cliquez sur **OK**. Dans la boîte de dialogue qui apparaît, sélectionnez pour chaque onglet les éléments comme affichés dans les figures suivantes.

Comme toutes les interfaces utilisent un hub virtuel appelé local, il est nécessaire de séparer les annonces RIP en fonction des interfaces sous peine de ne pouvoir communiquer correctement et de voir des annonces RIP pour des itinéraires rattachés à l'interface locale. Pour cela, dans l'onglet **Voisins**, sélectionnez **Utiliser les voisins à la place de la mono ou de la multidiffusion** puis ajoutez l'adresse du serveur se trouvant sur la même connexion virtuelle. Par exemple pour le serveur **paris1** sur l'interface **pa12**, ajoutez l'adresse de **pa21** du serveur **paris2**. Ensuite cliquez sur **OK**.



**Le mode d'opération** permet de mettre à jour périodiquement les annonces RIP, soit toutes les 30 secondes qui correspond à la sélection par défaut, soit en utilisant le mode auto statique, c'est-à-dire un mode où l'ordinateur attend qu'un routeur lui demande les routes. Ce dernier mode est utilisé dans le scénario des connexions à la demande. Par contre les routes sont marquées comme étant persistantes y compris si le service RIP est désactivé.

La zone **Protocole de paquets sortants** permet d'indiquer comment les annonces RIP sont envoyées vers les autres routeurs :

- diffusion RIP V1.
- diffusion RIP V2 pour environnement mixte RIP V1 et RIP V2.
- multidiffusion RIP V2 pour environnement RIP V2.
- RIP silencieux, n'envoie pas d'annonces mais peut écouter.

La zone **Protocole de paquets entrants** permet d'indiquer comment les annonces RIP sont reçues :

- Ignorer les paquets entrants n'écoute pas les annonces.
- RIP V1 et V2 pour les environnements mixtes.
- RIP V1 accepte uniquement des annonces RIP V1.
- RIP V2 accepte uniquement des annonces RIP V2.

Le **Coût supplémentaire pour les itinéraires** est par défaut de 1. Attention le coût maximum entre un émetteur et un destinataire ne peut dépasser 15.

**Baliser les itinéraires annoncés** permet d'ajouter une balise dans les annonces RIP V2.

**Activer l'authentification** est une fonctionnalité de RIP V2 qui permet d'ajouter un mot de passe qui circule en clair sur le réseau afin de créer une mini authentification entre plusieurs routeurs. Le mot de passe est défini par interface.

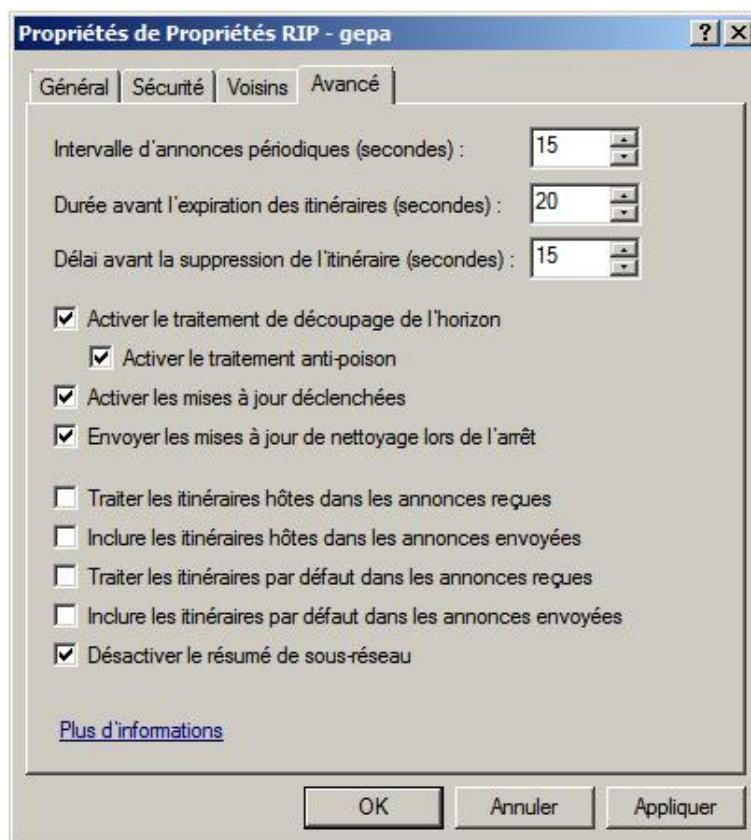
Dans l'onglet **Sécurité**, aucune modification n'est effectuée. Il existe une action pour les itinéraires entrants ou sortants afin de définir un comportement face aux annonces d'itinéraire entrantes, les choix sont :

- Accepter tous les itinéraires
- Accepter tous les itinéraires dans les plages listées.
- Ignorer tous les itinéraires dans les plages listées.

Dans l'onglet **Voisins**, aucune modification n'est effectuée. Vous pourriez ici définir des exceptions sur la méthode d'interaction pour les annonces entrantes ou sortantes. Les choix sont :

- Utiliser uniquement la monodiffusion ou la multidiffusion selon ce qui a été défini dans l'onglet **Général** (dEFAULT).
- Utiliser les voisins en plus de la mono ou de la multidiffusion permet d'envoyer aux voisins définis dans la liste des annonces en mono diffusion en plus de la méthode définie dans l'onglet **Général**.
- Utiliser les voisins à la place de la mono ou de la multidiffusion indique que les annonces sont envoyées uniquement aux voisins de la liste en monodiffusion. Les annonces n'utilisent plus ce qui a été défini dans l'onglet **Général**.

Enfin pour l'onglet **Avancé**, modifiez les paramètres comme le montre l'image suivante :



Si le mode de mise à jour est périodique, vous pouvez définir les valeurs suivantes :

- **Intervalle d'annonces périodiques** définit la période entre l'envoi de deux annonces (15 à 86 400 secondes).
- **Durée avant l'expiration des itinéraires** définit la durée de vie apprise par une annonce RIP. Si le routeur ne reçoit pas une nouvelle annonce dans le délai défini, la route expire (15 à 259 200 secondes).
- **Délai avant la suppression de l'itinéraire** correspond au délai avant la suppression de la route de la table de routage dès que la route a expiré (15 à 259 200 secondes).

**Activer le traitement de découpage de l'horizon** permet d'éviter d'annoncer un itinéraire sur une interface dont on a

également appris cet itinéraire.

**Activer le traitement antipoison** permet d'envoyer des itinéraires avec des métriques de 16 (route inaccessible) ; ne peut être activée que si le découpage d'horizon est activé.

**Activer les mises à jour déclenchées** permet de définir l'envoi immédiat des modifications uniquement lorsqu'une modification intervient.

**Envoyer les mises à jour propres lors de l'arrêt** permet d'envoyer des annonces avec un métrique de 15 afin d'avertir les autres routeurs que le routeur n'est plus disponible et qu'il faut trouver une nouvelle route.

**Traiter les itinéraires hôtes dans les annonces reçues**, par défaut elles sont ignorées.

**Inclure les itinéraires hôtes dans les annonces envoyées**, par défaut elles sont ignorées.

**Désactiver le résumé de sous-réseau**, c'est-à-dire la manière dont le sous-réseau est envoyé. Uniquement disponible si les paquets sortants sont **Diffusion RIP version 2** ou **Multidiffusion RIP version 2**.

1. Répétez les deux dernières opérations pour chaque interface qui doit envoyer ou recevoir des annonces RIP.
2. Testez si vous le désirez la communication à l'aide du script **Scripttestroutes.bat** et examinez les tables de routage pour confirmer que certaines routes sont locales alors que d'autres sont marquées RIP.
3. Sur **geneve2**, saisissez la commande `ping 10.1.1.2 -t` car nous allons tester une panne du serveur **paris1**.
4. Arrêtez le serveur **paris1** (Enregistrer l'état et enregistrer les modifications), veillez à décocher **Ecrire les modifications sur le disque dur virtuel** ; vous devez voir sur **genève2** que certains ping sont perdus puis au bout de quelques temps la communication revient car une nouvelle route a été déterminée. A priori, cela semble moins efficace qu'avec le routage statique, mais rappelez-vous du travail à fournir pour un réseau dont la topologie est simple comme ici, alors imaginez ce qu'il peut en être lorsque la topologie est vraiment complexe.

 Vous venez de transformer le serveur en routeur puis vous avez ajouté des routes statiques. Il est plus aisément de configurer le routage dynamique RIP que le routage statique. Néanmoins, il faut veiller à ne pas utiliser de hubs comme indiqué dans la procédure.

## 9. Dépannage à l'aide de la commande ping

Vous allez examiner ici qu'en fonction de certaines situations les réponses à la commande **ping** peuvent être différentes.

Pour effectuer les procédures suivantes, il est nécessaire d'avoir réalisé les procédures de la section précédente.

### a. Délai de la demande dépassé

Ce message survient lorsqu'un destinataire ne répond pas lorsque vous êtes sur une station de travail ou un serveur. Par exemple, si vous saisissez `ping 192.168.1.1` sur **geneve2**, vous recevez ce message, de même pour l'adresse **10.1.1.3**. Il n'est pas précisé s'il n'est pas possible de joindre le réseau ou si le destinataire n'est pas disponible.

### b. Échec de la transmission ; code d'erreur 1231

Ce message survient lorsqu'il n'est pas possible de joindre le réseau du destinataire par exemple lorsque vous êtes sur un routeur. Pour vous en convaincre, saisissez la commande `ping 192.168.1.1` sur **paris1**.

La commande **tracert** vous permet de supposer qu'il n'existe pas d'itinéraire car dès le premier saut il n'y a pas de réponse, ce qui indique que le routeur ne connaît pas la route alors qu'il répond si la route est connue.

 Ce sont les deux principaux types de message que vous rencontrez lorsqu'il y a une erreur quelque part.

 Cet exercice est maintenant terminé, veuillez éteindre chaque ordinateur virtuel utilisé en prenant soin de ne pas sauvegarder les modifications sinon les scripts ne fonctionneront pas pour débuter un nouvel

exercice.

---

# Exercice 1 - Planification de l'adressage IPv4 pour les sites principaux

## 1. Objectifs

Dans cet exercice vous allez définir les plages d'adresses utilisables en IPv4 pour l'ensemble des sites de l'entreprise.

## 2. Configuration de l'environnement

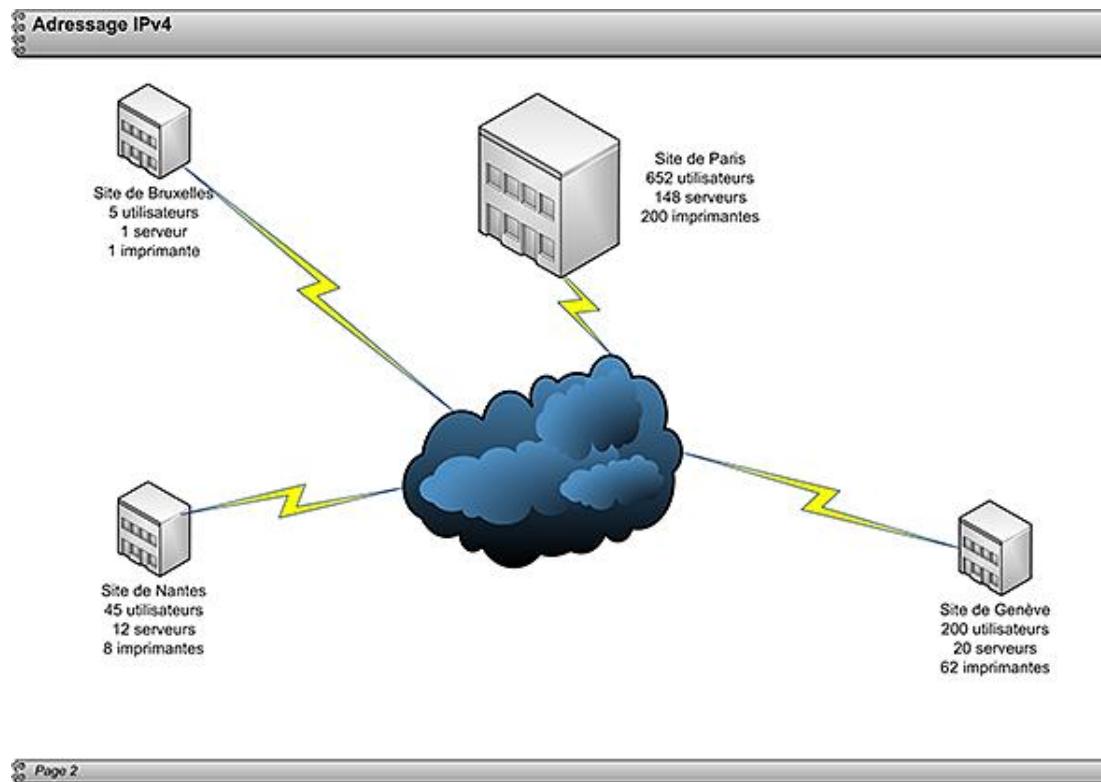
Cet exercice ne requiert pas de machines virtuelles.

## 3. Référence par rapport à la théorie

Vous pouvez vous référer au chapitre Configuration de base des services réseau.

## 4. Scénario et questions pour la planification de l'adressage IPv4

Les consultants proposent d'utiliser l'adressage IPv4 selon le schéma ci-dessous :



Votre travail consiste ici à calculer les réseaux, les masques de sous-réseaux afin de respecter les contraintes suivantes :

- Ne pas avoir plus de 200 adresses utilisées par sous-réseau.
- Limiter le nombre d'hôtes par sous-réseau uniquement à ce qui est requis.
- Utiliser le second octet pour définir un site.
- Utiliser le troisième octet pour définir, s'il est précisé, un étage ou un bâtiment pour un site.

- Créer des sous-réseaux logiquement organisés par type.

La plage d'adresses que vous pouvez utiliser est 10.0.0.0/8.

Les tâches à effectuer sont :

- Déterminer les plages d'adresses globales.
- Déterminer les adresses IP pour le site de Paris.
- Déterminer les adresses IP pour le site de Genève.
- Déterminer les adresses IP pour le site de Nantes.
- Déterminer les adresses IP pour le site de Bruxelles.

## 5. Détermination des plages d'adresses à utiliser

Il faut commencer par déterminer l'adressage global pour chaque site, soit utiliser le second octet pour définir un site comme par exemple :

- 10.1.0.0/16 pour le site de Paris.
- 10.2.0.0/16 pour le site de Genève.
- 10.3.0.0/16 pour le site de Nantes.
- 10.3.0.0/16 pour le site de Bruxelles.

Ensuite pour chaque site, il faut encore déterminer le masque de sous-réseau réel à utiliser en tenant compte des restrictions suivantes :

- Ne pas avoir plus de 200 adresses utilisées par sous-réseau.
- Limiter le nombre d'hôtes par sous-réseau uniquement à ce qui est requis.
- Utiliser le troisième octet pour définir, s'il est précisé, un étage ou un bâtiment pour un site.
- Créer de sous-réseaux logiquement organisés par type.

## 6. Adresses IP pour le site de Paris

**Pour le site de Paris**, il y a 1000 hôtes (652+148+200), donc a priori cinq sous-réseaux mais en fait il nous en faut 6 car :

- Il n'est pas possible de disposer de plus de 200 adresses par sous-réseau.
- Chaque routeur est placé sur 2 sous-réseaux donc il utilise 2 adresses IP. Il faut donc au minimum 6 routeurs ce qui fait au total 1006 adresses IP.
- Le nombre 1006 correspond aux adresses utilisables et non aux adresses théoriques. Avec 6 sous-réseaux, il nous faut un total de 12 adresses ( $2 \times 6$ ) supplémentaires pour définir le nom du réseau et l'adresse de diffusion locale pour chaque sous-réseau.

Dans cette proposition de solution, il n'est pas tenu compte d'une organisation logique par type, donc cette solution n'est pas encore bonne.

Il existe 148 serveurs, 200 imprimantes et 652 utilisateurs, selon ces informations, il faut :

- 1 sous-réseau pour les serveurs.
- 2 sous-réseaux pour les imprimantes, car il faut 200 adresses pour les imprimantes plus 2 adresses (soit une pour le nom du réseau et une pour l'adresse de diffusion locale) pour un total de 202, donc plus de 200 adresses.
- 4 sous-réseaux pour les utilisateurs.

Pour un total de 7 sous-réseaux. Avec ces informations, on répond positivement aux exigences concernant la limite à 200 du nombre d'adresses utilisées par sous-réseau et la création de sous-réseaux par type.

Pour le calcul du masque de sous-réseau :

- Pour les serveurs, il n'est pas possible de diminuer le nombre d'hôtes possibles par sous-réseau ( $148 > 2^7$  soit 128), il faut donc utiliser une plage de 256 adresses soit un masque de 255.255.255.0.
- Pour les imprimantes, le résultat est différent car si l'on tient compte des 200 imprimantes réseaux plus des deux adresses des routeurs cela nous donne 202 adresses utilisables. Auxquelles il faut ajouter deux adresses par sous-réseau (adresse du sous-réseau et adresse de diffusion locale) ce qui nous donne 206 adresses en tout, soit 103 adresses par sous-réseau. La prochaine puissance de 2 est égale à 128, donc il est possible de limiter le nombre d'hôtes à 128 au lieu de 256 et le masque de sous-réseau peut être 255.255.255.128.
- Pour les ordinateurs, le nombre d'hôtes dépassant 128, il n'est pas possible de limiter le nombre d'hôtes par sous-réseau, le masque de sous-réseau est donc 255.255.255.0.

Le tableau suivant montre une possibilité d'utilisation des plages d'adresses :

Quoi	Nombre	Nombre de sous-réseaux	Sous-réseau	Nombre d'hôtes par sous-réseau	Masque de sous-réseau
Serveurs	148	1	10.1.1.0/24	256	255.255.255.0
Imprimantes	200	2	10.1.2.0/25	128	255.255.255.128
			10.1.2.128/25	128	255.255.255.128
Ordinateurs	652	4	10.1.3.0/24	256	255.255.255.0
			10.1.4.0/24	256	255.255.255.0
			10.1.5.0/24	256	255.255.255.0
			10.1.6.0/24	256	255.255.255.0

## 7. Adresses IP pour le site de Genève

Pour le site de Genève, il existe 20 serveurs, 62 imprimantes et 200 utilisateurs ; selon ces informations, il faut :

- 1 sous-réseau pour les serveurs.
- 1 sous-réseau pour les imprimantes.
- 2 sous-réseaux pour les utilisateurs, car il faut 200 adresses pour les imprimantes plus 2 adresses (soit une pour le nom du réseau et une pour l'adresse de diffusion locale) en tout 202, donc plus de 200 adresses.

Pour un total de 4 sous-réseaux. Avec ces informations, on répond positivement aux exigences concernant la limite à 200 du nombre d'adresses utilisées par sous-réseau et la création de sous-réseaux par type.

Pour le calcul du masque de sous-réseau :

- Pour les serveurs, le nombre d'adresses théorique est 22, la puissance de 2 immédiatement supérieure ou égale à 22 est 32 ( $2^5$ ), le masque est donc égal à 255.255.255.224 (256-32).
- Pour les imprimantes, le nombre d'adresses théorique est 64, la puissance de 2 immédiatement supérieure ou égale à 64 est 64 ( $2^6$ ), le masque est donc égal à 255.255.255.192 (256-64).
- Pour les ordinateurs, le résultat est différent car si l'on tient compte des 200 utilisateurs réseaux plus des deux adresses des routeurs cela nous donne 202 adresses utilisables. Auxquelles il faut ajouter deux adresses par sous-réseau (adresse du sous-réseau et adresse de diffusion locale) ce qui nous donne 206 adresses en tout, soit 103 adresses par sous-réseau. La prochaine puissance de 2 est égale à 128 donc il est possible de limiter le nombre d'hôtes à 128 au lieu des 256 et le masque de sous-réseau peut être 255.255.255.128.

Le tableau suivant montre une possibilité d'utilisation des plages d'adresses :

Quoi	Nombre	Nombre de sous-réseaux	Sous-réseau	Nombre d'hôtes par sous-réseau	Masque de sous-réseau
Serveurs	20	1	10.2.1.0/27	32	255.255.255.224
Imprimantes	62	1	10.2.1.64/26	64	255.255.255.192
Ordinateurs	200	2	10.2.2.0/25 10.2.2.128/25	128 128	255.255.255.128 255.255.255.128

## 8. Adresses IP pour le site de Nantes

Pour le site de Nantes, il existe 12 serveurs, 8 imprimantes et 45 utilisateurs ; selon ces informations, il faut :

- 1 sous-réseau pour les serveurs.
- 1 sous-réseau pour les imprimantes.
- 1 sous-réseau pour les utilisateurs.

Pour un total de 3 sous-réseaux. Ainsi, on répond positivement aux exigences concernant la limite à 200 du nombre d'adresses utilisées par sous-réseau et la création de sous-réseaux par type.

Pour le calcul du masque de sous-réseau :

- Pour les serveurs, le nombre d'adresses théorique est 14 donc la puissance de 2 immédiatement supérieure ou égale à 14 est 16 ( $2^4$ ), le masque est donc égal à 255.255.255.240 (256-16).
- Pour les imprimantes, le nombre d'adresses théorique est 10 donc la puissance de 2 immédiatement supérieure ou égale à 10 est 16 ( $2^4$ ), le masque est donc égal à 255.255.255.240 (256-16).
- Pour les ordinateurs, le nombre d'adresses théorique est 47 donc la puissance de 2 immédiatement supérieure ou égale à 47 est 64 ( $2^6$ ), le masque est donc égal à 255.255.255.192 (256-64).

Le tableau suivant montre une possibilité d'utilisation des plages d'adresses :

Quoi	Nombre	Nombre de sous-réseaux	Sous-réseau	Nombre d'hôtes par sous-réseau	Masque de sous-réseau
Serveurs	12	1	10.3.1.0/28	16	255.255.255.240

Imprimantes	8	1	10.3.1.16/28	16	255.255.255.240
Ordinateurs	45	1	10.3.1.64/26	64	255.255.255.192

## 9. Adresses IP pour le site de Bruxelles

Pour le site de Bruxelles, il existe 1 serveur, 1 imprimante et 5 utilisateurs ; selon ces informations, il faut :

- 1 sous-réseau pour les serveurs.
- 1 sous-réseau pour les imprimantes.
- 1 sous-réseau pour les utilisateurs.

 C'est loin d'être efficace, mais il faut répondre aux exigences de la question !

Pour un total de 3 sites. Ainsi, on répond positivement aux exigences concernant la limite à 200 du nombre d'adresses utilisées par sous-réseau et la création de sous-réseaux par type.

Pour le calcul du masque de sous-réseau :

- Pour les serveurs, le nombre théorique d'adresses est 3 donc la puissance de 2 immédiatement supérieure ou égale à 3 est 4 ( $2^2$ ), le masque est donc égal à 255.255.255.252 (256-4).
- Pour les imprimantes, le nombre théorique d'adresses est 3 donc la puissance de 2 immédiatement supérieure ou égale à 3 est 4 ( $2^2$ ), le masque est donc égal à 255.255.255.252 (256-4).
- Pour les ordinateurs, le nombre théorique d'adresses est 7 donc la puissance de 2 immédiatement supérieure ou égale à 7 est 8 ( $2^3$ ), le masque est donc égal à 255.255.255.248 (256-8).

Le tableau suivant montre une possibilité d'utilisation des plages d'adresses :

Quoi	Nombre	Nombre de sous-réseaux	Sous-réseau	Nombre d'hôtes par sous-réseau	Masque de sous-réseau
Serveurs	1	1	10.4.1.0/30	4	255.255.255.252
Imprimantes	1	1	10.4.1.4/30	4	255.255.255.252
Ordinateurs	5	1	10.4.1.8/29	8	255.255.255.248

# Ordinateurs virtuels

Si vous ne l'avez pas déjà fait, il faut créer les ordinateurs virtuels nécessaires à chaque exercice selon les procédures indiquées dans le chapitre Crédit du bac à sable pour effectuer les ateliers. Seulement ensuite vous pourrez effectuer les exercices. Pour éviter toutes erreurs lors du lancement de scripts, il est requis d'utiliser les noms et les paramètres indiqués dans la prochaine section.

D'autre part, cette méthode de travail permet de coller au plus près à la réalité donc d'utiliser autant d'ordinateurs que nécessaire. Pour chaque section, le nombre maximal d'ordinateurs pouvant être utilisé simultanément est de cinq. Néanmoins, la majorité en utilise au maximum quatre. En cas de problème dû à un manque de mémoire, il est toujours possible :

- de diminuer la mémoire RAM allouée à chaque ordinateur virtuel.
- d'arrêter tous services ou applications non nécessaire de l'ordinateur hôte.
- d'augmenter la RAM (4 Go et un système d'exploitation 64 bits pour l'hôte est recommandé), attention à la limite de 3 Go si l'hôte utilise un système d'exploitation 32 Bits.

Il faut compter un espace disque de 50 Go, plus une dizaine de gigaoctets pour les disques d'annulation et la sauvegarde de l'état.

Vous ne pouvez réaliser qu'un exercice à la fois.



L'expérience montre qu'il n'est pas superflu de créer une sauvegarde de vos machines virtuelles, une fois créées.

## 1. Machine virtuelle paris1

### a. Paramètres à utiliser pour la machine virtuelle paris1

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\labs\paris1</b>
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>500 Mo</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
	Carte 2	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur

Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	paris1
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Rôle	aucun
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 2. Machine virtuelle paris2

### a. Paramètres à utiliser pour la machine virtuelle paris2

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\labs\paris2
Système d'exploitation		Windows Server 2008
Mémoire vive		500 Mo
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
	Carte 2	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	paris2

Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Rôle	aucun
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 3. Machine virtuelle paris3

### a. Paramètres à utiliser pour la machine virtuelle paris3

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\labs\paris3
Système d'exploitation		Windows Server 2008
Mémoire vive		500 Mo
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
	Carte 2	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	paris3
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)

Rôle	aucun
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 4. Machine virtuelle paris4

### a. Paramètres à utiliser pour la machine virtuelle paris4

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\labs\paris4</b>
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>500 Mo</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	paris4
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Rôle	aucun
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 5. Machine virtuelle paris5

### a. Paramètres à utiliser pour la machine virtuelle paris5

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\labs\paris5</b>
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>500 Mo</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise ( <b>minimale</b> )
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	paris5
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Rôle	aucun
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 6. Machine virtuelle paclient1

#### a. Paramètres à utiliser pour la machine virtuelle paclient1

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		D:\eni\labs\ paclient1
Système d'exploitation		Windows Vista
Mémoire vive		500 Mo
Disque dur 1		Nom et emplacement par défaut
Taille du disque dur		Valeur proposée par défaut
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

#### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Vista SP1
Nom d'utilisateur	p
Mot de passe administrateur	Pas de mot de passe
Nom de l'ordinateur	paclient1
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Compléments virtuels	installés

#### c. Configuration post-installation requise

- Ajouter l'utilisateur **p** sans mot de passe.
- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 7. Machine virtuelle geneve1

#### a. Paramètres à utiliser pour la machine virtuelle geneve1

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\labs\geneve1</b>
Système d'exploitation		<b>Windows Server 2008</b>
Mémoire vive		<b>500 Mo</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>
Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
	Carte 2	local seul
	Carte 3	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

#### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	geneve1
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Rôle	aucun
Compléments virtuels	installés

#### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 8. Machine virtuelle geneve2

#### a. Paramètres à utiliser pour la machine virtuelle geneve2

Paramètre	Nom du paramètre	Valeur

Nom et emplacement	<b>D:\eni\labs\geneve2</b>	
Système d'exploitation	<b>Windows Server 2008</b>	
Mémoire vive	<b>500 Mo</b>	
Disque dur 1	<b>Nom et emplacement par défaut</b>	
Taille du disque dur	<b>Valeur proposée par défaut</b>	
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Server 2008 Entreprise (Complète)
Mot de passe administrateur	Pa\$\$word
Nom de l'ordinateur	geneve2
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Rôle	aucun
Compléments virtuels	installés

### c. Configuration post-installation requise

- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 9. Machine virtuelle geclient1

### a. Paramètres à utiliser pour la machine virtuelle geclient1

Paramètre	Nom du paramètre	Valeur
Nom et emplacement		<b>D:\eni\labs\ geclient1</b>
Système d'exploitation		<b>Windows Vista</b>
Mémoire vive		<b>500 Mo</b>
Disque dur 1		<b>Nom et emplacement par défaut</b>

Taille du disque dur		<b>Valeur proposée par défaut</b>
Disques d'annulation	Activer les disques d'annulation	<b>Case à cocher</b> sélectionnée
Réseau	Carte 1	local seul
Virtualisation par matériel	Activer la Virtualisation assistée par matériel	<b>Case à cocher</b> sélectionnée

### b. Paramètres à utiliser pour installer le système d'exploitation

Paramètre	Valeur
Système d'exploitation	Windows Vista SP1
Nom d'utilisateur	p
Mot de passe administrateur	Pas de mot de passe
Nom de l'ordinateur	paclient1
Adressage IP	Par défaut (dynamique)
Domaine	Par défaut (groupe de travail)
Compléments virtuels	installés

### c. Configuration post-installation requise

- Ajouter l'utilisateur **p** sans mot de passe.
- Changer le nom de l'ordinateur.
- Installer les compléments pour ordinateur virtuel.

## 10. Scripts

Vous trouverez tous les scripts nécessaires sur le site des Éditions ENI à l'adresse suivante : <http://www.editions-eni.fr>. Saisissez la référence ENI de l'ouvrage **CE08WINIR** dans la zone de recherche et validez. Cliquez sur le titre du livre puis sur le lien de téléchargement.

Téléchargez puis décompressez les fichiers. Dans l'arborescence appelée **Exercice récapitulatif** vous trouverez des sous-dossiers pour chaque exercice et à l'intérieur les scripts nécessaires à chaque exercice. Attention à ne lancer les scripts que pour l'exercice considéré car même si leurs noms sont identiques pour plusieurs exercices, leur contenu peut changer. Vous y trouvez également les figures des topologies propres à chaque exercice.

# Présentation de l'entreprise fictive

## 1. Introduction

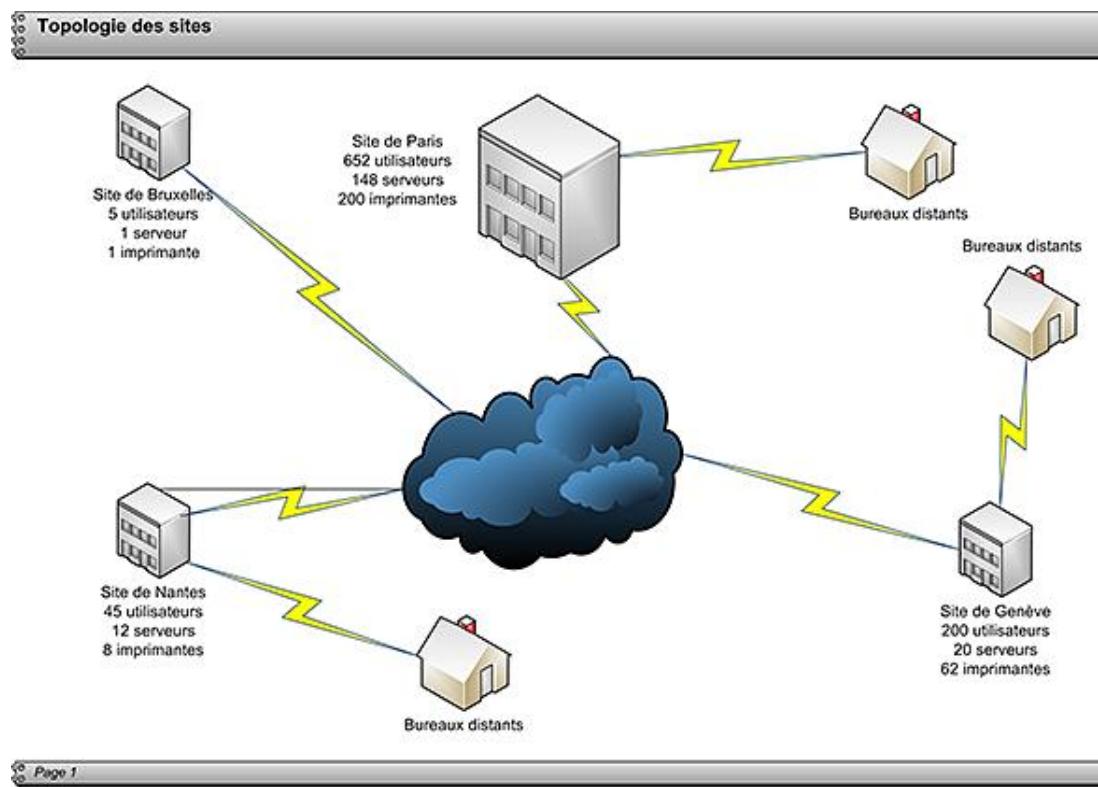
Vous venez d'être engagé en tant qu'administrateur pour la société XXX leader dans son domaine. En tant que spécialiste Windows Server 2008, il vous est demandé de migrer et d'implémenter la totalité du réseau de l'entreprise vers Windows 2008. La conception a été réalisée par une société de consulting externe avant votre venue et il ne vous reste plus qu'à suivre les directives proposées pour l'implémentation.

Actuellement votre entreprise dispose d'un réseau hétérogène composé d'ordinateurs fonctionnant sous Unix, Linux et Windows NT4 pour les serveurs, alors que pour les clients vous trouvez aussi bien des ordinateurs tournant sous Windows 2000, Windows XP que Windows Vista. Il n'existe pas d'Active Directory. Après l'installation de Windows Server 2008, seuls les ordinateurs clients fonctionnant sous Windows Vista, voire sous Windows 7 dès qu'il sera disponible, seront conservés. Concernant les ordinateurs Linux/Unix, certains vont rester alors que d'autres vont disparaître car certaines applications n'existent que sous ces systèmes d'exploitations et il n'est pas prévu de les migrer sous les technologies Windows.

Il a été prévu de recréer un réseau parallèle au réseau existant et de migrer sur ce nouveau réseau tout ce qui peut l'être, vous pouvez considérer que votre travail consiste à la mise en œuvre d'un nouveau réseau.

## 2. Topologie des sites

Votre société se compose d'un site principal à Paris relié à Internet par une ligne à haut débit permettant aussi bien de naviguer sur Internet que de relier les autres sites en utilisant des VPNs et d'une multitude de sites plus petits comme le montre la figure suivante.



Cette figure que vous pouvez télécharger et imprimer à partir du site des Éditions ENI porte le nom **TopologieDesSites.jpg**.

Deux sites moyens, soit les sites de Nantes et de Genève, servent également de point central pour des bureaux distants régionaux permettant à des collaborateurs de se connecter soit en utilisant leur ordinateur portable depuis Internet, soit à partir de bureaux distants. Certains de ces bureaux disposent d'un serveur et de quelques ordinateurs. Enfin à Bruxelles une nouvelle implantation a été réalisée afin de pénétrer le marché belge.

## 3. Votre travail

Comme indiqué précédemment, votre travail consiste à installer, configurer, gérer et dépanner l'ensemble du réseau de votre entreprise.

Comme il s'agit d'un exercice, vous n'allez implémenter que quelques-uns des serveurs et ce pour quelques sites uniquement. Si vous le désirez, vous pouvez ajouter d'autres ordinateurs, voire d'autres sites, afin de pratiquer plus intensivement Windows Server 2008 en créant vos propres scénarios.

Chaque exercice se compose de plusieurs sections où pour chacune une question précise vous est posée et une solution possible est indiquée. Elle comprend une procédure plus ou moins détaillée ainsi que des explications voire des commentaires. Certaines étapes sont détaillées, d'autres le sont moins. Dans tous les cas, n'hésitez pas à recourir à la théorie et aux procédures montrées pour répondre aux questions.

Généralement la réponse proposée contient plus d'éléments que la réponse attendue ceci dans le but de vous montrer certains aspects intéressants.

Après la création des machines virtuelles, veillez à activer les disques d'annulation afin de démarrer chaque nouvel exercice avec des machines virtuelles vierges. Pour chaque exercice, votre premier travail consiste à préparer l'environnement de l'exercice en lançant des scripts qui vont configurer les machines virtuelles pour vous. Veillez à respecter l'ordre de lancement des scripts et attendez le redémarrage des ordinateurs lorsque cela est précisé. Dès que l'environnement est prêt, vous pouvez commencer à répondre aux questions posées dans les sections. Pour chacune d'elle, il est indiqué quelle machine virtuelle est requise et doit donc fonctionner en mémoire. Il est également indiqué sur quelle machine effectuer l'opération. Les sections sont souvent interdépendantes entre elles.

Enfin, pour chaque section, des procédures de contrôle sont proposées afin de vérifier si le résultat obtenu est celui attendu.

Maintenant c'est à vous de jouer, soit vous tentez l'exercice en utilisant vos propres connaissances soit vous pouvez vous aider de la solution présentée à l'aide des procédures pas à pas. Bon courage !

## **Documents à télécharger**

Ces documents sont téléchargeables à partir du site de Microsoft.

Valeurs TCP/IP de la base de registre pour Windows Server 2008 et Windows Vista :

**TCPIP\_Reg.doc**

Paramètres de stratégies de groupe :

**WindowsServer2008andWindowsVistaSP1GroupPolicySettings.xls**

Référence des commandes Windows :

**WinCmdRef.exe**

Référence technique de Netsh pour Windows Server 2008 :

**Netsh.exe**

