1. Windows Vista et le Welcome Center

Le **Welcome Center** permet d'accéder immédiatement à différentes configurations de paramètres. Il permet d'avoir un résumé des caractéristiques de la machine, mais aussi d'installer de nouveaux matériels, de transférer des fichiers et des paramètres sur Windows Vista mais aussi l'ajout et la suppression d'utilisateurs.

1.1. Add or remove user accounts

Dans cette section, il est possible de gérer les comptes utilisateurs. Ainsi, on pourra ajouter, supprimer ou modifier le compte. Cependant, il faudra bien faire attention car avec Windows Vista, les comptes des utilisateurs ne devront posséder des droits d'administrateur uniquement s'il doit modifier des données sensibles sur le système: comme gérer les disques ou installer des applications. Par rapport à

Windows XP, la plupart des actions pourront se faire en mode *Utilisateur*. Windows Vista gère en fait **3 types de comptes utilisateurs**:

- Tout d'abord, le compte **Administrateur**: qui est en fait un super-administrateur, comme le compte "Root" sur Linux, qui possède tous les droits sur le système.
- Puis, les comptes **administrateurs** qui permettent de lancer les applications avec des droits limités. Si un programme demande plus de privilèges, alors 3 méthodes ont été prévues::
  - une ***élévation silencieuse***: aucune confirmation n'est demandée à l'utilisateur.
  - une ***élévation par consentement***: une demande de confirmation est faite à l'utilisateur. C'est la fonctionnalité faite active **par défaut**.
  - une ***élévation par mot de passe***: un couple login-mot de passe d'un compte administrateur est demandé.
- Et enfin, les comptes **utilisateurs**: sont des comptes avec des droits limités avec **élévation par mot de passe** par défaut.

Cette gestion des comptes est nommée **User Account Control(UAC)**, comme cela est expliqué dans cet article sur **le principe du moindre privilège**. UAC a été ajouté afin d'éviter aux administrateurs de donner à tout le monde les droits du compte administrateur. En fait, si un utilisateur lance une application qui doit écrire dans le dossier "%windir%", UAC va rediriger l'écriture dans le dossier **Virtual Store** de l'utilisateur en cours! Ensuite, lorsque le fichier est demandé, le système le fournit à l'application. Cette technique est également utilisée pour l'écriture dans la **base de registre**.
Afin de sécuriser au mieux le système, les applications .NET s'exécute dans une machine virtuelle et sont alors isolées du système, ce qui permet ainsi d'intégrer la technologie **CAS**. Le **CAS** permet d'assigner des permissions de code aux programmes .NET. On peut ainsi donner des permissions tel que l'accès aux zones DNS, à la base de registre...

1.2. Transfert files and settings

Transfert files and settings permet de transférer des comptes utilisateurs, des fichiers et dossiers, des paramètres Internet, des favoris, des mails et des contacts. Cette fonction est disponible pour les systèmes Windows 2000, XP et Vista, souhaitant faire une migration vers Windows Vista. Cet utilitaire, remplaçant de **USMT** (User System Migration Tool), permet de migrer rapidement et de façon intuitive, les différents paramètres cités sur la capture d'écran. Deux actions distinctes sont possibles:

- Sauvegarder les documents de son ordinateur actuel
- Restaurer les documents de son ancien ordinateur

Dans les deux cas, il y a trois méthodes de sauvegarde/restauration:

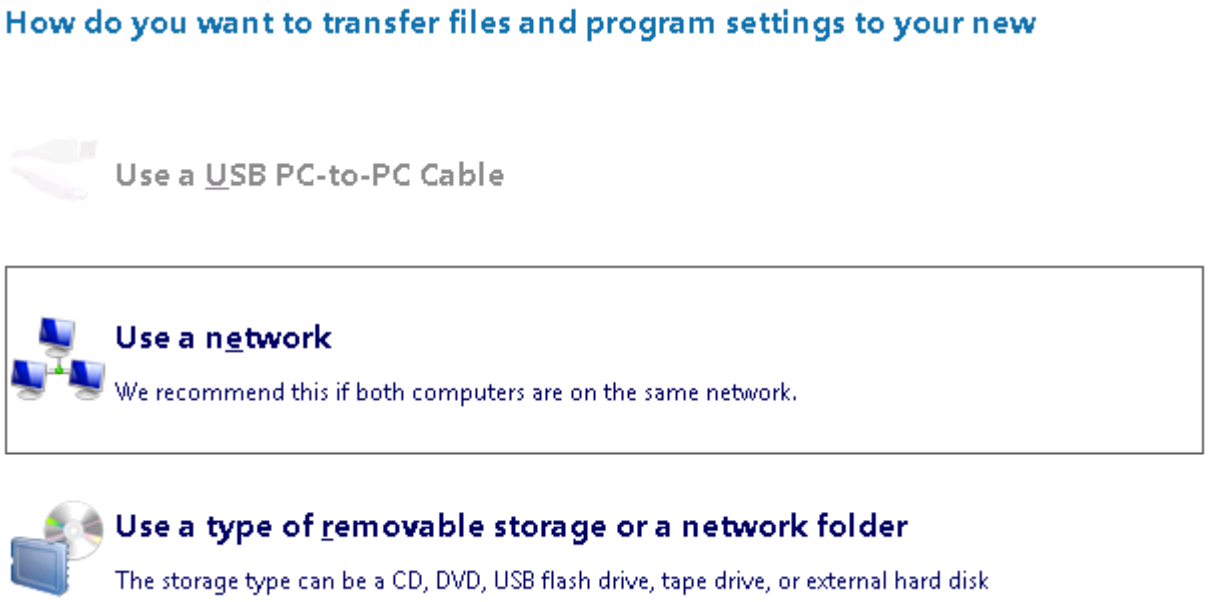
- Par le réseau
- Par une méthode de stockage externe: CD, DVD, Clé USB etc...
- Utilisation d'un câble USB PC-à-PC

Il est aussi possible de reprendre un transfert déjà en cours en cas de problème, afin de ne pas avoir à tout recommencer!

1.2.1 Sauvegarde

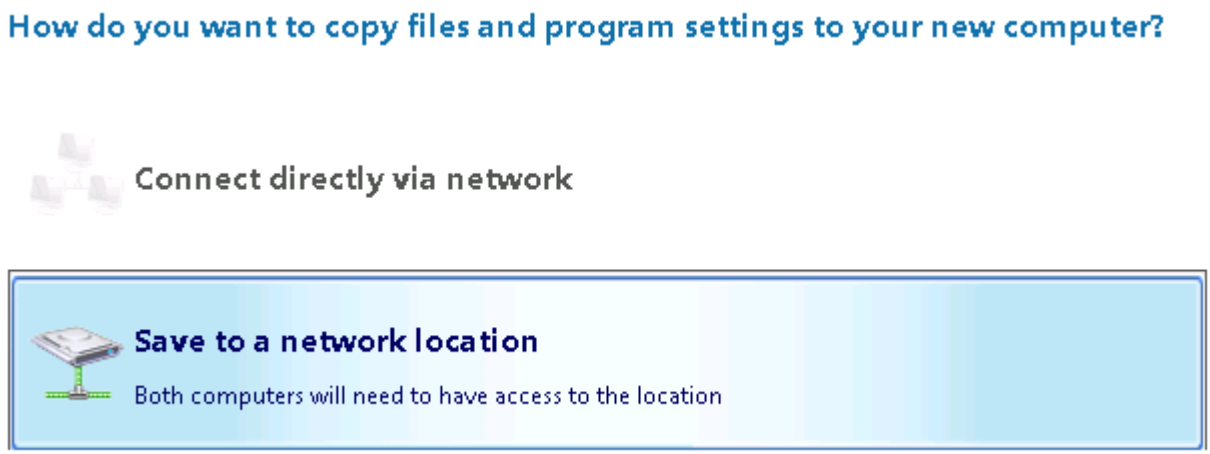
Si vous souhaitez faire une sauvegarde de vos paramètres, il faudra choisir *"this is my old computer"*, lorsque vous lancer l'utilitaire **Transfert files and settings**.

Ensuite, il faut choisir quelle méthode vous souhaitez utiliser pour réaliser la sauvegarde, trois choix sont offerts:

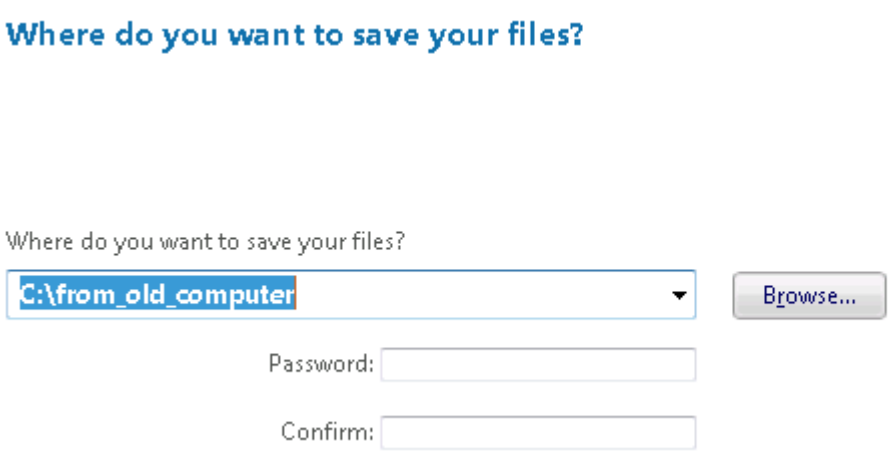


1. **Utiliser un câble USB** afin de faire un raccordement PC à PC. Ceci peut être intéressant lorsque l'on ne dispose d'aucun autre moyen de sauvegarde externe.
2. **Utiliser le réseau** afin de stocker celui-ci sur un ordinateur distant. Cette méthode peut être utile, si vous souhaitez placer la sauvegarde sur le nouvel ordinateur qui devra récupérer tous les nouveaux paramètres.
3. **Utiliser un support de stockage externe**: les CD-RW, DVD-RW, lecteur de bandes magnétiques peuvent servir si vous souhaitez conserver les informations à long terme afin de faire une restauration plus éloignée dans le temps.

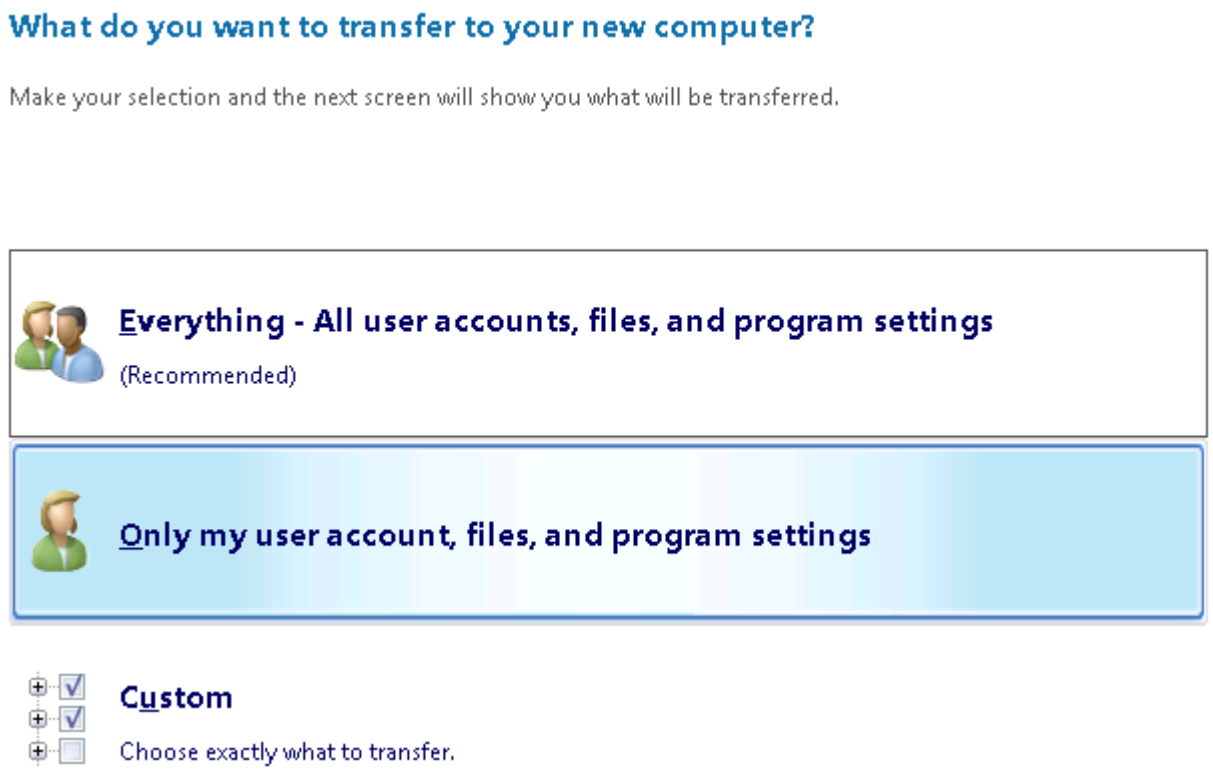
Nous ne détaillerons ici que la méthode faite par le réseau. Dans ce cas, il faudra choisir entre se connecter directement à la machine cible sur le réseau, ou alors utiliser un partage disponible sur un serveur de fichier. Nous choisiront le deuxième possibilité, pour les besoins de la démonstration :



Une fois le choix de la méthode de sauvegarde effectuée, il faut définir l'emplacement de sauvegarde. Il est alors possible de mettre un mot de passe afin que ces informations restent confidentielles et donc que personne ne puisse y accéder.



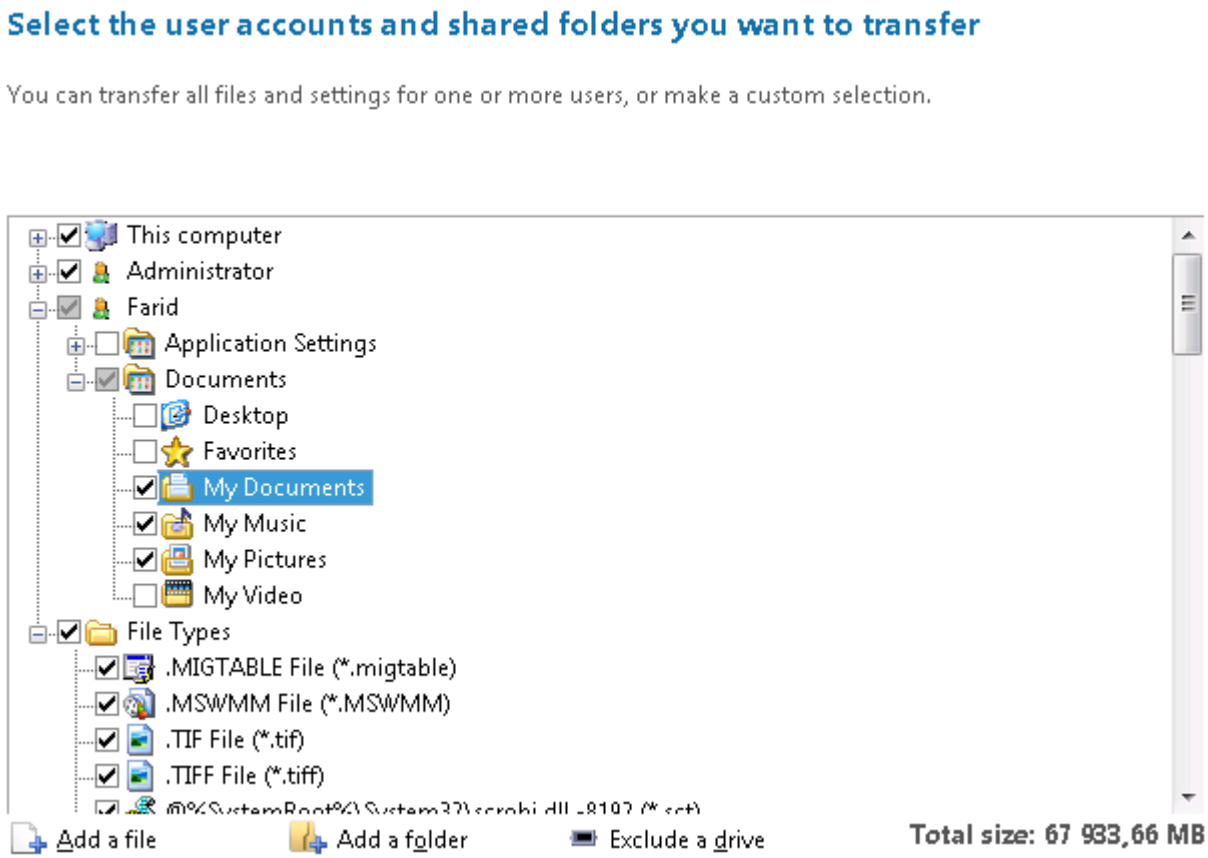
Ceci fait, l'étape suivante concerne la sauvegarde en elle-même, c'est-à-dire que l'on va choisir les données à sauvegarder, en commençant par le choix des comptes.



En fait, l'utilitaire **Transfert Files and Settings** demande quels sont les comptes que vous souhaitez sauvegarder. Vous pouvez sauvegarder tous les comptes utilisateurs disponibles sur le PC ou ne sauvegarder que le compte en cours:

- Vous pouvez choir la première possibilité si le poste en cours va être échangé
- Mais il sera utile de choisir la deuxième proposition, si un des utilisateurs va disposer d'une nouvelle station de travail .

Enfin, il faut choisir les répertoires que l'on souhaiter rétablir sur le nouveau PC. Il est bon de noter qu'une option intéressante permet de sauvegarder un certain type de fichier. Vous pouvez ainsi choisir de ne sauver que des *.txt*, *.doc*, *.avi* etc... et alors de gagner de la place mais aussi de ne sauver que les données critiques et spécifiques.

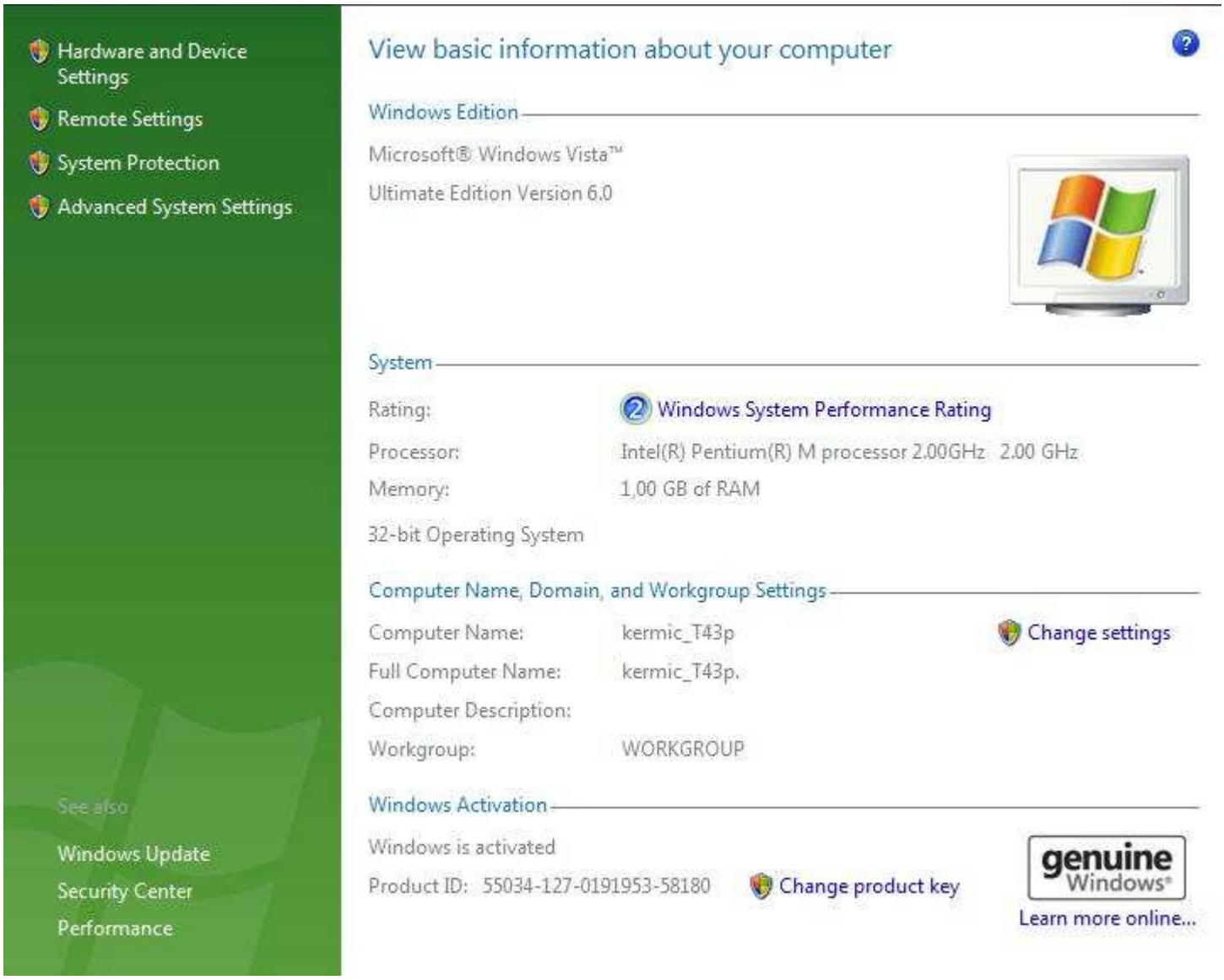


Une fois ces étapes remplies, la sauvegarde se lance.

1.2.2 Restauration

La restauration correspond à *"This is my new Computer"*. Si c'est la première fois, Windows installera **Windows Easy Transfert**. Malheureusement lors de nos essais, un message d'erreur apparaissait ce qui ne nous permet pas de tester toutes les fonctionnalités.

1.3. View your computer details



Les propriétés systèmes sont directement accessibles depuis le Welcome Center. Celles-ci ont bénéficié d'une nouvelle interface. Dans la fenêtre principale, on peut voir les caractéristiques matérielles de la machine, ainsi que le nom de l'ordinateur, le nom de domaine, le groupe de travail. De plus, il est possible de retrouver des informations sur l'activation de windows, voir l'identifiant de produit et modifier sa clé. Par contre, les différents onglets tel que Computer Name, Hardware, Advanced, System Protecion, Remote n'ont pas changés.

On peut également trouver , dans *Control Panel->Performance Rating and Tools* un petit utilitaire qui permet de "noter" en quelque sorte son ordinateur et ainsi de voir quelles sont les performances du systèmes comme expliqué dans ce White Paper de Microsoft. Un outil en ligne de commande existe également, il se nomme *WINSAT* mais nous aborderons ce sujet en détail par la suite...

1.4. Set up devices

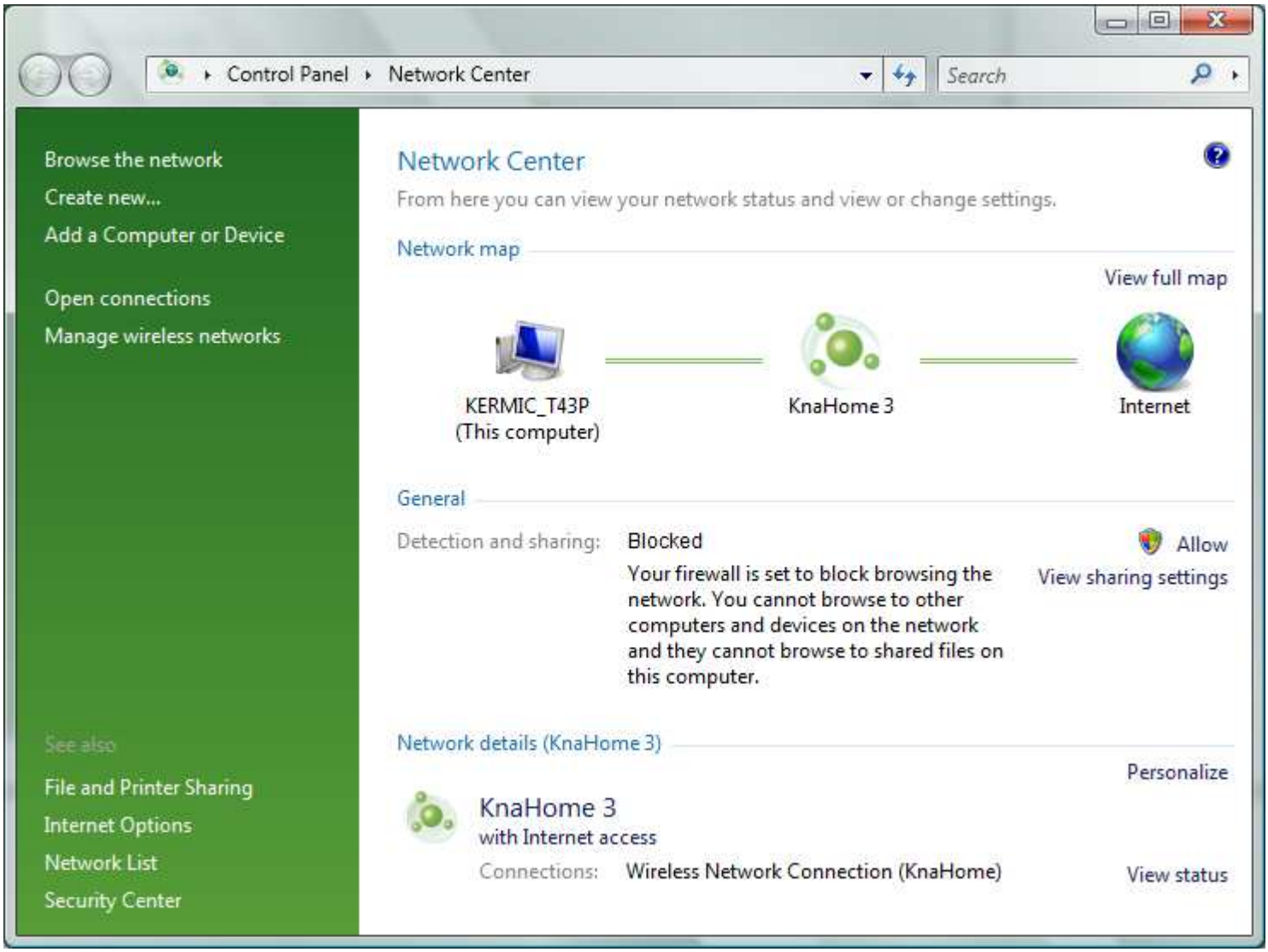
Avec **Windows Vista**, l'installation des drivers a été repensée. Maintenant, seuls les pilotes signés seront utilisables et une nouvelle stratégie est appliquée lorsque l'on connecte un nouveau périphérique. Il est possible de configurer le système pour qu'il utilise Windows Update de trois façons concernant l'installation de ces drivers:

- **Chercher un pilote automatiquement**: le système ira tout d'abord vérifier la présence du driver sur Windows Update et demandera un CD à l'utilisateur uniquement s'il n'a pas trouvé d'information sur ce centre de mises à jour.
- **Me demander à chaque fois que je connecte un nouveau périphérique avant de chercher des drivers**: Le système d'exploitation demandera à chaque fois à l'utilisateur s'il souhaite vérifier la présence des drivers sur Windows Update
- **Ne jamais vérifier les pilotes quand je connecte un périphérique**: Windows Update ne sera jamais utilisé.

Alors, depuis le **Welcome Center** une fonctionnalité nommée *Set up Devices* permet de chercher automatiquement les pilotes sur **Windows Update** de tous les périphériques non reconnu.

2. Windows Vista et le réseau

C'est à partir de cette nouvelle interface de gestion du réseau, **Network Center**, que vous allez dorénavant pouvoir interagir avec vos différentes connexions réseaux! Mais voyons de plus près les avancées technologiques apportée par Windows Vista en terme de gestion du réseau et de la sécurité...



2.1. Une nouvelle sous couche système réseau

2.1.1. Présentation du modèle

Avec son nouveau système d'exploitation, Microsoft a totalement repensé la gestion des réseaux. En effet, les besoins en terme de **sécurité**, de **stabilité** et d'**évolutivité** ont amené la firme à recoder intégralement la sous couche réseau de son système d'exploitation Windows. Microsoft a alors mis en place la technologie **Receive-Side Scaling** qui permet de partager la charge réseau entre plusieurs processeurs! En outre, plusieurs mécanismes destinés à déléguer des tâches, exécutées jusque là par le processeur, ont été implémentés. Par contre, toutes les cartes réseaux ne sont pas compatibles mais les cartes réseaux récentes permettent leurs utilisations!

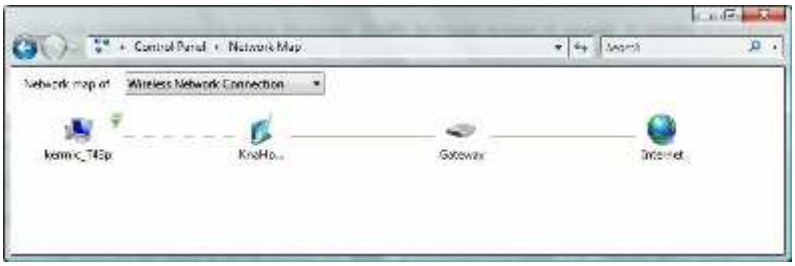
- Les traitements TCP et IP sont délégués aux processeurs des cartes réseaux grâce à **TCP Chimney**
- Les échanges de données entre deux ordinateurs se font sans utilisation CPU avec **RDMA Chimney**

- Le cryptage IPSec n'est plus consommateur de temps processeur et est exécuté directement par la carte réseau avec **IPSec Chimney**

Mais l 'un des avantages principaux de cette nouvelle sous couche réseau est son évolutivité: elle pourra implémenter, sans trop de difficultés, les futurs protocoles.

2.1.2. Nouveau drivers réseau et périphériques réseaux

Ces nouveaux modules ont été étudiés pour rendre beaucoup plus simple le développement des drivers, en implémentant en plus la **version 6** de Network Driver Interface Specification (**NDIS**). De ce fait, un nouveau modèle de driver réseau fait son apparition: **LWF** (Leigth Weight Filter) qui permet d'améliorer la stabilité des connexions. En effet, si un utilisateur met à jour ses drivers réseaux (par le biais de Windows Update ou autre...), les connexions ne seront pas perdues pour autant!
En outre, les connexions WIFI, qui étaient **jusqu'à Windows XP,** gérées comme des connexions réseaux filaires, ont été totalement revues et corrigées. En effet, l'ancienne méthode avait pour effet de limiter les possibilités d'évolution de cette technologie. Maintenant, les réseaux filaires et les réseaux sans fils sont totalement séparés ce qui a permis d'implémenter de façon plus complète la **norme 802.11**, qui définit les réseaux sans fil. Ainsi, de toutes nouvelles possibilités de gestion sont offertes aux connexions WIFI.
Afin de faciliter les connexions de périphériques sans fils, de nouveaux protocoles voient leurs apparitions : **PnP-X, UPNP** et **DPWS**. Ils ont pour but de détecter les périphériques réseaux et de les connecter plus facilement. PnP-X utilise les deux autres protocoles pour installer les périphériques réseaux, à l'instar du service Plug & Play pour les périphériques physiquement connectés. Ces protocoles sont utilisés par un ensemble de composants nommés **Windows Connect Now** dont l'implémentation joue un rôle important dans la convivialité de Windows Vista, qui se veut être un système d'exploitation "over connected ".



Comme vous pouvez le voir, les différents périphériques réseaux peuvent être représentés afin de pouvoir déterminer leur état. Il est aussi possible de récupérer des informations sur les divers composants, comme l'**adresse MAC et IP**, le modèle, le fabricant et leurs sites respectifs... Mais il est

aussi possible de se **connecter en HTTP,** pour une maintenance ou autre, aux différents périphériques en un simple clic!

2.1.3. IP v6 par défaut:

Windows Vista intègre dorénavant la gestion d'**IP version 6** dans la même pile TCP que celle de la version 4. L'avantage réside dans le fait qu'il sera possible de gérer de la même façon tous les paquets IP, indifféremment de leurs versions! En effet, il est aussi possible d'utiliser IP v6 sur windows XP et Server 2003 mais deux piles sont utilisée: l'implémentation en est que plus compliquée.
Afin de mieux comprendre l'enjeu, il peut être bon de rappeler les avantages d'IP v6:

- Les adresses IP sont codées sur **128 bits** au lieux de 32, ce qui permet de se passer des routeurs NAT, en augmentant considérablement le nombre d'adresse disponibles (2^128 adresses!)
- Le routage est amélioré car les échanges entres les routeurs sont plus rapides et les tables de routage sont plus courtes.
- Le cryptage IPSec est implémenté par défaut, permettant ainsi **d'authentifier et de crypter** les connexions IP
- IP v6 permet aussi une **évolution future** et est compatible avec IP v4!

Les connexions à internet seront alors plus faciles et plus sécurisées. Ainsi le nombre de périphériques connectés pourra augmenter en toute tranquillité et IP v6 supportera alors l'arrivée massive des périphériques WIFI tel que les PDA, smartphone, appareils photos et autres... Il faut quand même signaler que le protocole est défini dans son intégralité depuis plus de 10 ans et que son implémentation se faisait attendre.
En plus du support natif d'IP v6, la notion de **QoS** a été revue à la hausse sur Windows Vista et les possibilités de configurations ont été nettement améliorées. Si vous souhaitez en savoir plus, je vous renvoie vers ce White Paper de Microsoft sur le sujet.

2.1.4. Network Diagnostics Framework (NDF)

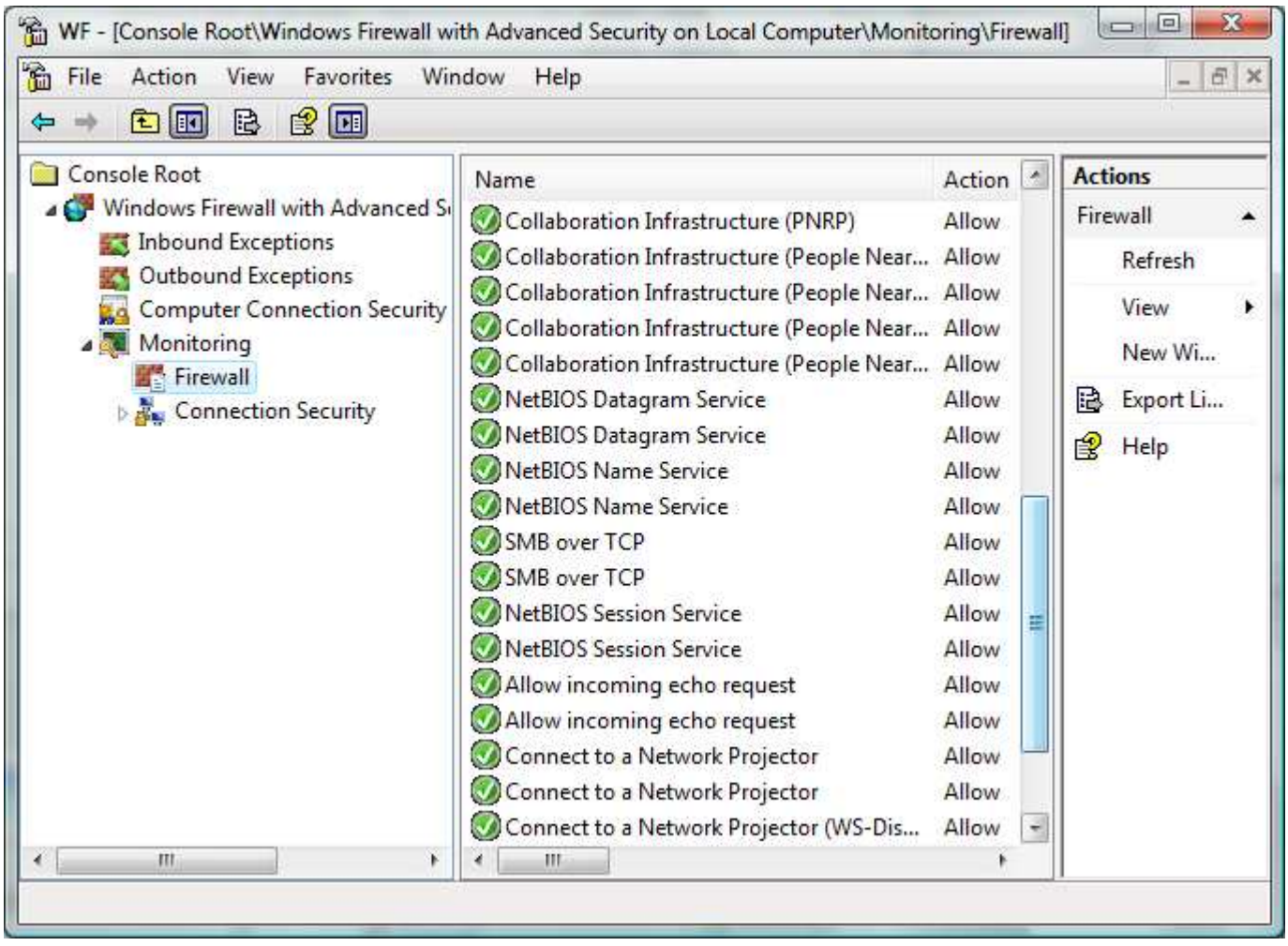
Afin de faciliter la maintenance des connexions réseaux, Windows Vista introduit un nouveau **framework de diagnostique réseau**. En effet, bon nombre d'utilisateurs sont incapables de réparer eux-même leurs connexions réseaux. Ainsi, afin de limiter les demandes d'aide à un administrateur ou un autre utilisateur plus qualifié (ce qui peut prendre du temps), le système d'exploitation propose interactivement de comprendre quel est le problème et quelle solution y apporter.
De cette façon, si vous essayez d'accéder à un partage par son chemin UNC (\\NomServeur\partage\ ) et que celui-ci est inaccessible, Windows Vista propose de trouver la solution pour vous. Alors le

système va faire une série de tests qui va aboutir à une ou plusieurs propositions de solution ou alors à une explication! L'utilisateur se sent donc valorisé, il peux lui même corriger ses problèmes ou alors il possède l'explication de l'impossibilité de connexion. Il est ainsi possible de gagner beaucoup de temps administrateur, temps qui pourra être investi dans d'autres tâches plus productives.

2.2. Windows Filtering Platform (WFP)

2.2.1. Filtrage entièrement repensé

Avec Windows XP est apparu la notion de Firewall Windows. Celui-ci a été mis à jour avec le SP2, il comprend une interface d'administration plus complète et des fonctionnalités plus étendues. Mais Windows Vista, grâce à l'API **Windows Filtering Platform**, met en oeuvre un vrai firewall: il est maintenant capable de faire du **filtrage entrant et sortant**. Par défaut, les connexions sortantes sont acceptées sauf exception et les connexions entrantes sont bloquées sauf exception. Deux profils peuvent être gérés: **Domain Profile** et **Standard Profile**. Mais, seul un profil peut être actif à la fois, en fonction de l'environnement de la machine.



Pour chaque profil:

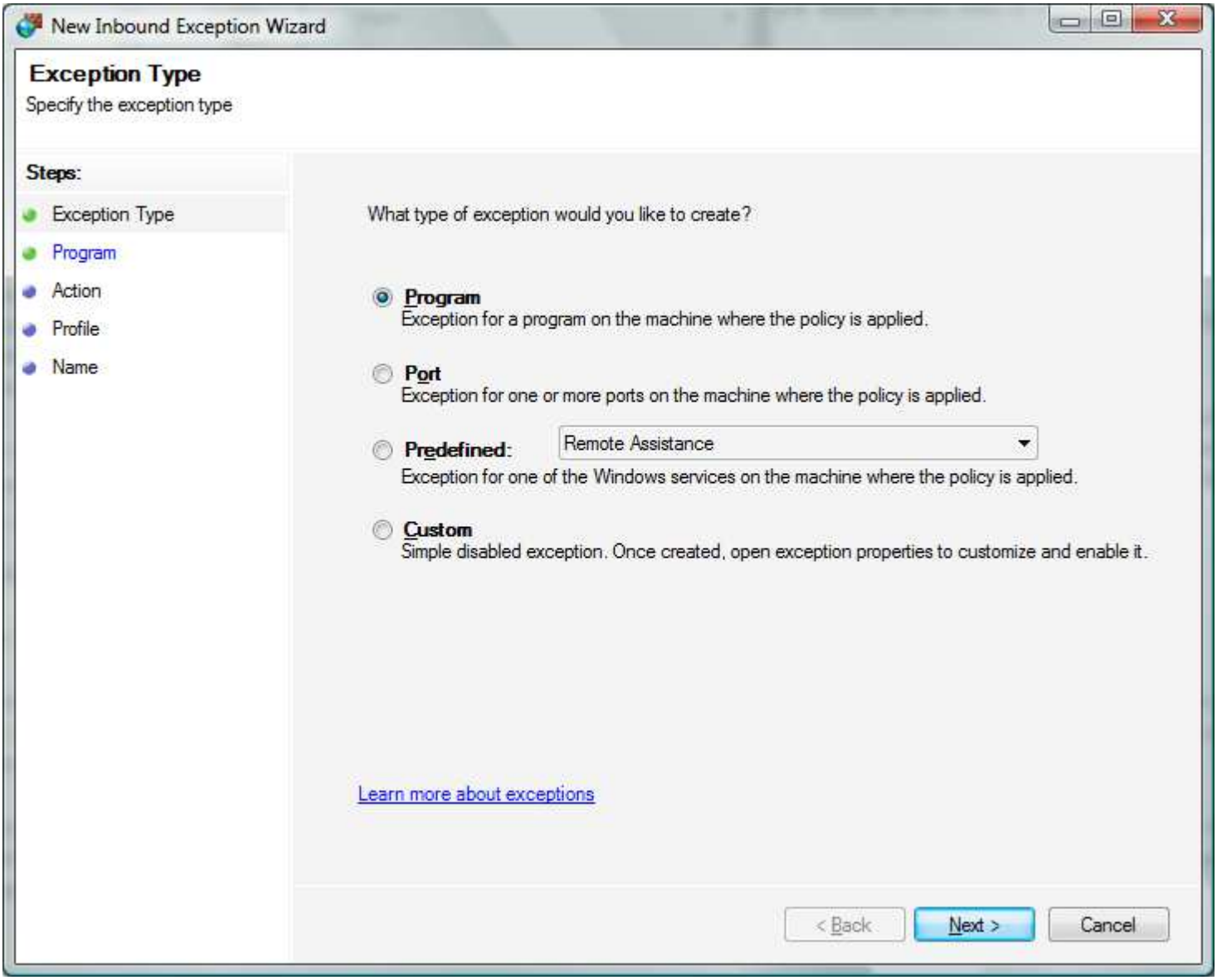
- Il est possible de créer un **fichier de log** pour enregistrer les connexions établies et/ou les paquets supprimés: celui-ci est par défaut stocké dans le répertoire *%windir%\pfirewall.log*.
- **Quatres paramètres** peuvent être configurés:
    1. Autoriser les administrateurs locaux à faire des exceptions
    2. Autoriser les administrateurs locaux à faire des règles de sécurité de connexion de l'ordinateur
    3. Avertir l'utilisateur lorsqu'une connexion entrante est refusée (par défaut)
    4. Autoriser les réponse unicast à des requêtes en diffusion ou en multi-diffusion (par défaut)
- Enfin, l'administrateur peut configurer la **gestion d'IPSec** pour la sécurisation des connexions:
    - **Échange des clés:** Plusieurs méthodes peuvent être gérées mais une durée de vie commune par défaut (en minute et en session) est appliquée pour la fréquence d'actualisation des clés. Pour chaque méthode, vous pouvez choisir entre plusieurs possibilités pour ces trois paramètres:
        - l'**algorythme de cryptage**: *AES-256, AES-192, AES-128 (par défaut), 3DES, DES (du plus sécurisé au moins sécurisé)*
        - l'**algoryhtme d'échange** de clés: *Elliptic Curve Diffie-Hellman P-384, Elliptic Curve Diffie-Hellman P-256, Diffie-Hellman groupe 14, Diffie-Hellman groupe 2 (par défaut), Diffie-Hellman groupe 1 (du plus sécurisé au moins sécurisé)*
        - l'**algorythme d'intégrité**: *SHA-1 (par défaut) ou MD5*
    - **Protection des données:** Il est en effet aussi possible de choisir les protocoles de cryptage et d'intégrité qui peuvent être différent de ceux choisis précédemment. De cette façon, vous pouvez avoir des méthodes différentes et personnalisables entre les établissements de connexion et les échanges proprement dits de données. Vous pouvez choisir un méthode plus sécurisée pour les établissements de connexion (qui n'ont lieu qu'une fois et qui peuvent contenir des informations critiques: login/mots de passe!) et choisir une méthode moins sécurisée mais surtout moins consommatrice de ressources pour les échanges de donnée.
    - **Méthode d'authentification:** En ce qui concerne l'authentification vous avez plusieurs choix
        - Par défaut
        - Utilisateur : utilise Kerberos
        - Ordinateur : utilise Kerberos
        - Utilisateur et Ordinateur : utilise Kerberos
        - Certificat d'origine connue
        - Custom: Deux authentification sont possibles: l'ordinateur et l'utilisateur! L'authenfication de l'ordinateur peut être défini comme optionnel mais sinon vous pouvez choisir si l'authentification se fait par clé pré-partagée (déconseillé) ou par certificats. Si vous choisissez l'authentification par clé pré-partagée pour l'ordinateur vous ne pouvez plus choisir cette possibilité pour l'utilisateur (et vice et versa). Pour authentifier l'utilisateur, vous avez le choix entre Kerberos, NTLM (boite de dialogue) ou avec des certificats.

Avec cette nouvelle mouture de son firewall, Microsoft fait un pas de géant et les autres logiciels firewalls ont du souci à se faire. À l'utilisation, celui-ci est très souple à gérer tous en fournissant un niveau de sécurité évolutif et paramètrable. Les protocoles implémentés sont de très haute qualité et reconnu par toutes les professionnels de la sécurité! De plus IPSec fait l'office d'une implémentation complète dans le système, ce qui ne pourra que faire du bien à la sécurité des échanges dans les réseaux d'entreprise.

2.2.2. Ajout/suppression de nouvelles règles

Afin de rendre ce firewall digne d'intérêt, les administrateurs peuvent voir les règles actives, activer ou désactiver certaines règles défini par défaut et s'ils en ont les droits, créer des règles personnelles. De plus, il est possible d'importer et d'exporter les règles afin de simplifier le déploiement de celles-ci! Mais attardons nous un instant sur la création de règles.

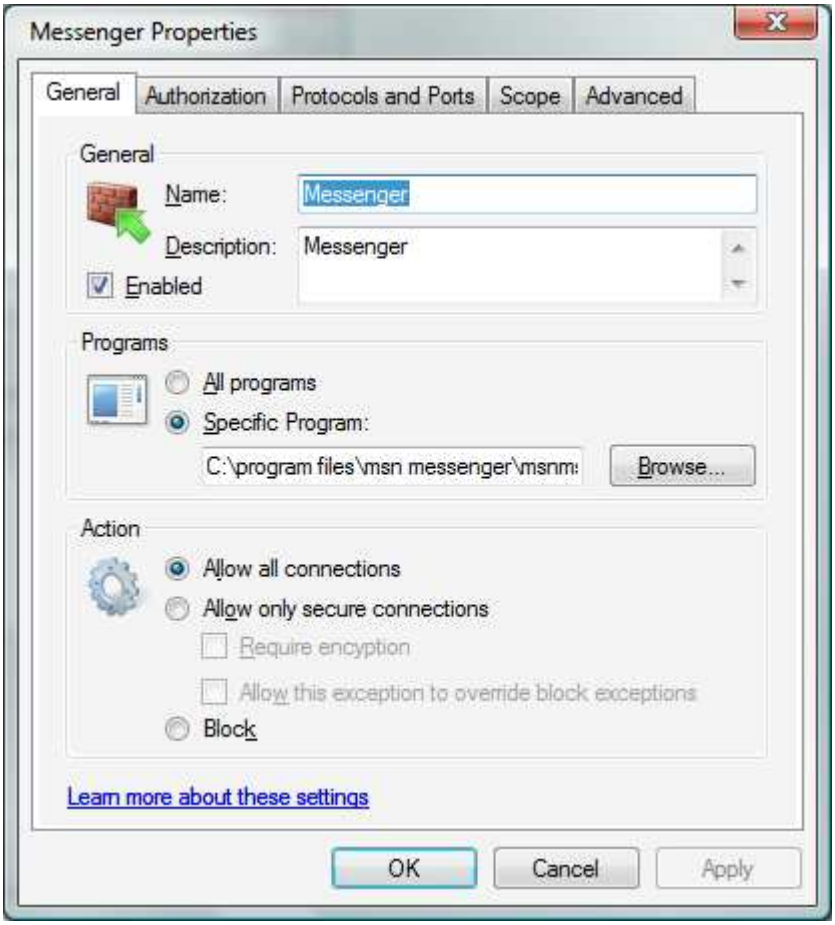
En développant **Windows Firewall with Advanced Security** et en cliquant sur les exceptions entrantes ou sortantes, vous avez la possibilité dans le menu Action à droite de créer des exceptions ! Ce menu de droite est un bénéfice non négligeable de l'implémentation de **MMC version 3.0**. En cliquant sur *New Exception...*, un assistant se lance pour vous guider dans la création de votre nouvelle règle.



Quatres types d'exceptions sont au choix:

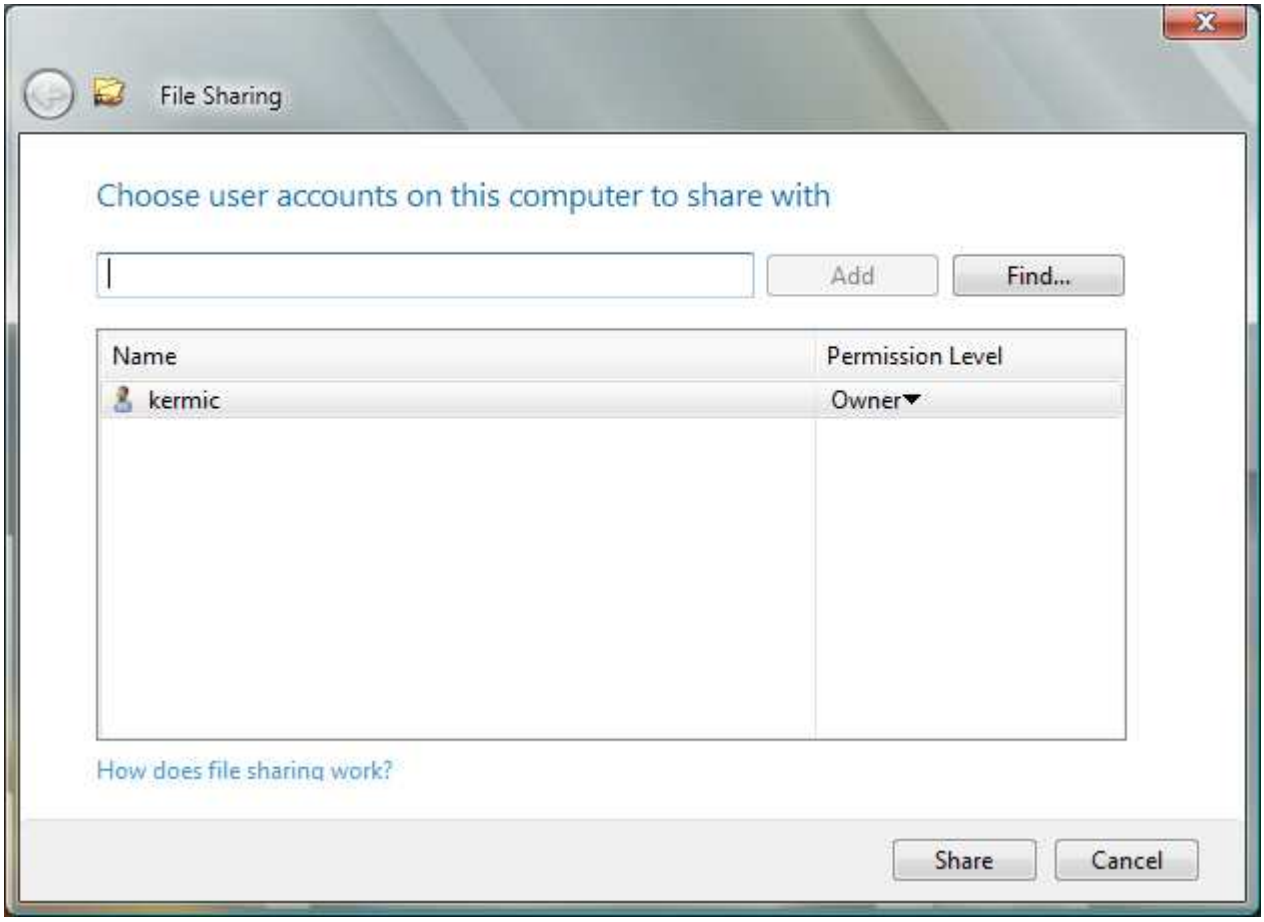
1. **Programme:** appliquer des paramètres de gestion de connexion associés à un programme au choix. Il faudra alors choisir un programme ou tous les programmes; puis choisir d'accepter toutes les connexions, seul les connexions sécurisés ou aucunes connexions; choisir le profile pour lequel la règle sera appliquée et enfin nommer et décrire la règle.
2. **Port:** appliquer des paramètres sur un port, quelque soit le processus qui souhaite l'utiliser. Dans ce cas, il faudra choisir entre le protocole TCP ou UDP puis le ou les ports voire tous les ports; ensuite les étapes sont identiques aux exceptions de programmes
3. **Prédéfinie:** Règles types définie par les développeurs de Microsoft. Cinq propositions sont faites, il ne reste plus qu'à les nommer et les décrire:
    - Assistance à distance
    - Partage de fichiers et d'imprimantes
    - Bureau à distance
    - Framework UPnP
    - Echo Request ICMP (v4)
4. **Custom** : il ne reste plus qu'à donner un nom et une description, ensuite toutes les configurations se font dans les propriétés de la règle!

Dans tous les cas, vous avez la possibilité de vérifier les propriétés des règles, que vous avez créées ou qui existent par défaut:



2.3. Partage de Fichiers et d'Imprimante

Le partage de fichier est devenu pour de nombreuses personnes une action oubliée car bien trop compliquée! En effet, il est facile de se perdre dans la commutation des droits de partage et les droits NTFS, de plus il est impératif de bien comprendre la différence entre les deux... Pour cela Windows Vista propose une nouvelle interface beaucoup plus conviviale et plus simple pour les utilisateurs:

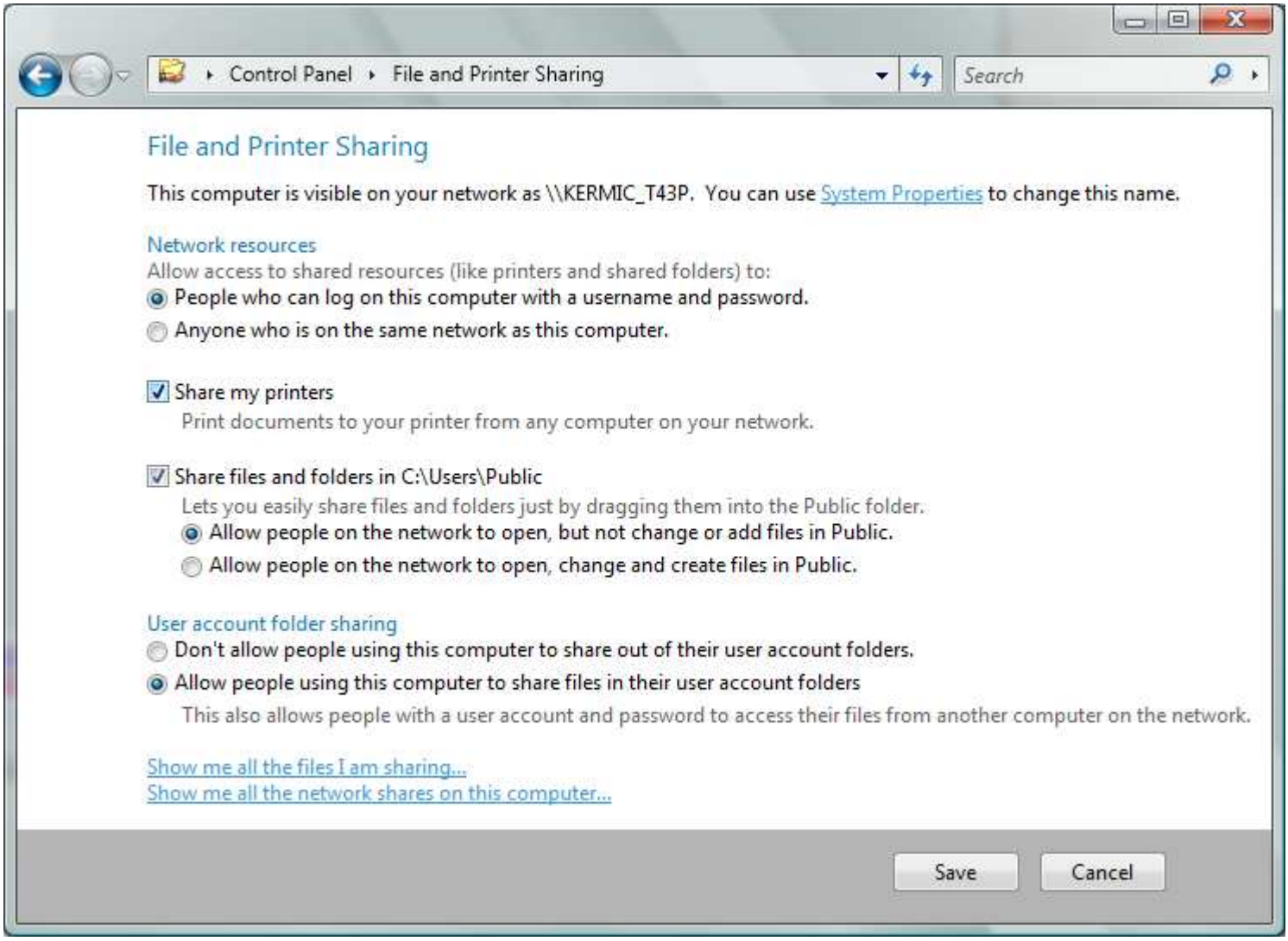


En partageant un dossier avec le menu contextuel (clic droit), cet assistant se lance. La présentation a été épurée au maximum pour ne contenir que le minimum nécessaire, c'est à dire la liste des personnes autorisées, une fonction d'ajout et de l'aide! De cette façon, le partage se fait en quelques clics et le quotidien des utilisateurs est révolutionné. Pour ce qui est de la gestion des droits, 4 niveaux de permissions existent :

- **Owner** (propriétaire): C'est l'utilisateur à qui appartient le dossier et qui configure le partage.
- **Reader**: les lecteurs sont tous les utilisateurs auxquels vous souhaitez donner des droits en lecture seule.
- **Contributor**: Le contributeur aura quant à lui des droits de modification des fichiers
- **Co-owner**: Le copropriétaire lui, aura aussi les droits de modifications mais ceux de gestion des permissions en plus

Pour les autres, il est toujours possible, en regardant les propriétés d'un dossier, de le partager comme avant! La console gestion de l'ordinateur et son extension partage permet elle encore de gérer les

partages de façon centralisée. Mais une possibilité apparaît depuis le **Network Center** et le **Panneau de Configuration** :



En effet dans la barre d'action du Network center, il y a un lien vers **Files and Printers Sharing**, un nouveau composant du panneau de configuration. Depuis ce dernier, il faut se diriger dans la partie **Network and Internet** ou alors entrer dans l'affichage classique. Avec ce nouveau composant, il est possible de gérer le comportement par défaut du système pour la gestion des partages de dossiers et d'imprimantes. De cette façon, vous pouvez configurer:

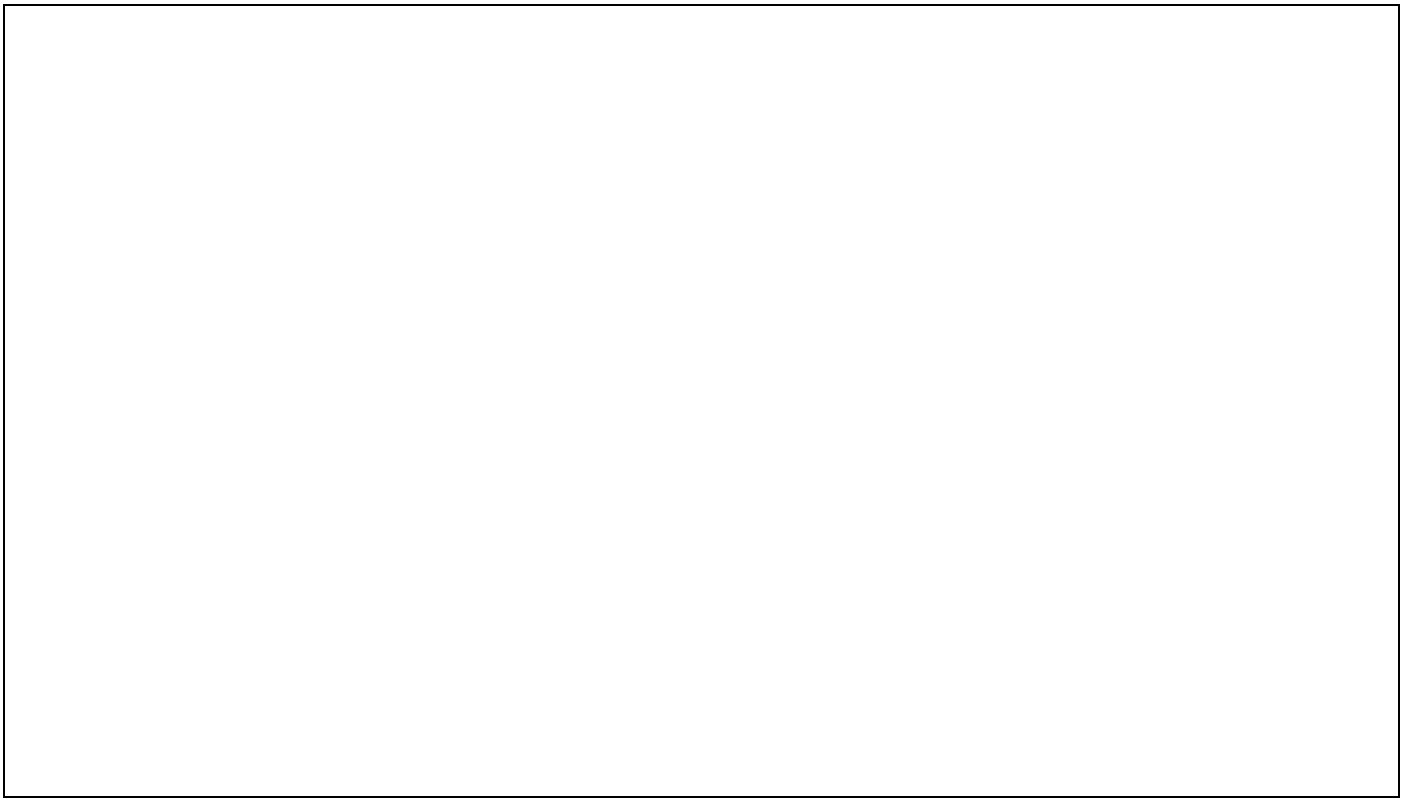
- la **méthode d'authentification**: par un couple de login/mots de passes comparé aux autorisations sur les partages ou alors sans, c'est a dire ouvert à toutes les personnes sur le même réseau. Cette dernière méthode est moins contraignante que la première, mais elle est à utiliser avec parcimonie car très peu sécurisée!
- Le **partage des imprimantes**: il est enfin possible de ne pas partager uniquement ses imprimantes. En effet, cette action n'était pas possible avec Windows XP: le partage des imprimantes était confondu avec le partage des dossiers. Vous pouvez maintenant choisir de ne partager que vos imprimantes ou au contraire partager uniquement vos dossiers!

- Le **partage des dossiers partagées**: ainsi, vous pouvez choisir de mettre à disposition, ou pas, les dossiers partagées de votre ordinateur. Du même coup, vous avec la possibilité en un clic de donner des droits de lecture ou d'écriture dans ces dossiers.
- L'**autorisation de partager**: en effet, vous avez aussi la possibilité ici de donner l'opportunité aux utilisateurs de partager des dossiers ou des imprimantes (autres que ceux définis par les administrateurs), ou a contrario, leur empêcher ces actions, pour des raisons de sécurité ou de confidentialité par exemple.

Ainsi, Windows Vista a été repensé pour mieux regrouper les informations aux bons endroits, tous en améliorant la disponibilité de ces dites informations. À l'instar des partages, toute la navigation a été revue et corrigée pour rendre cette nouvelle version du système d'exploitation Windows beaucoup plus conviviale et accessible.

2.4. Gestion des imprimantes

Maintenant que nous avons vu comment s'opèrent les partages de dossier, nous allons voir un peu plus en détails la gestion des imprimantes partagées. Depuis **Windows server 2003 R2**, une nouvelle console d'administration a fait son apparition, **Print Management**. C'est alors tous naturellement que cette console se retrouve sur Windows Vista, les postes de travail vont alors de transformer en véritables petits serveurs: en effet, Print Management permet d'optimiser la gestions des imprimantes en mettant en place un vrai service de partage d'imprimante, fini les imprimantes isolées derrière un poste de travail!

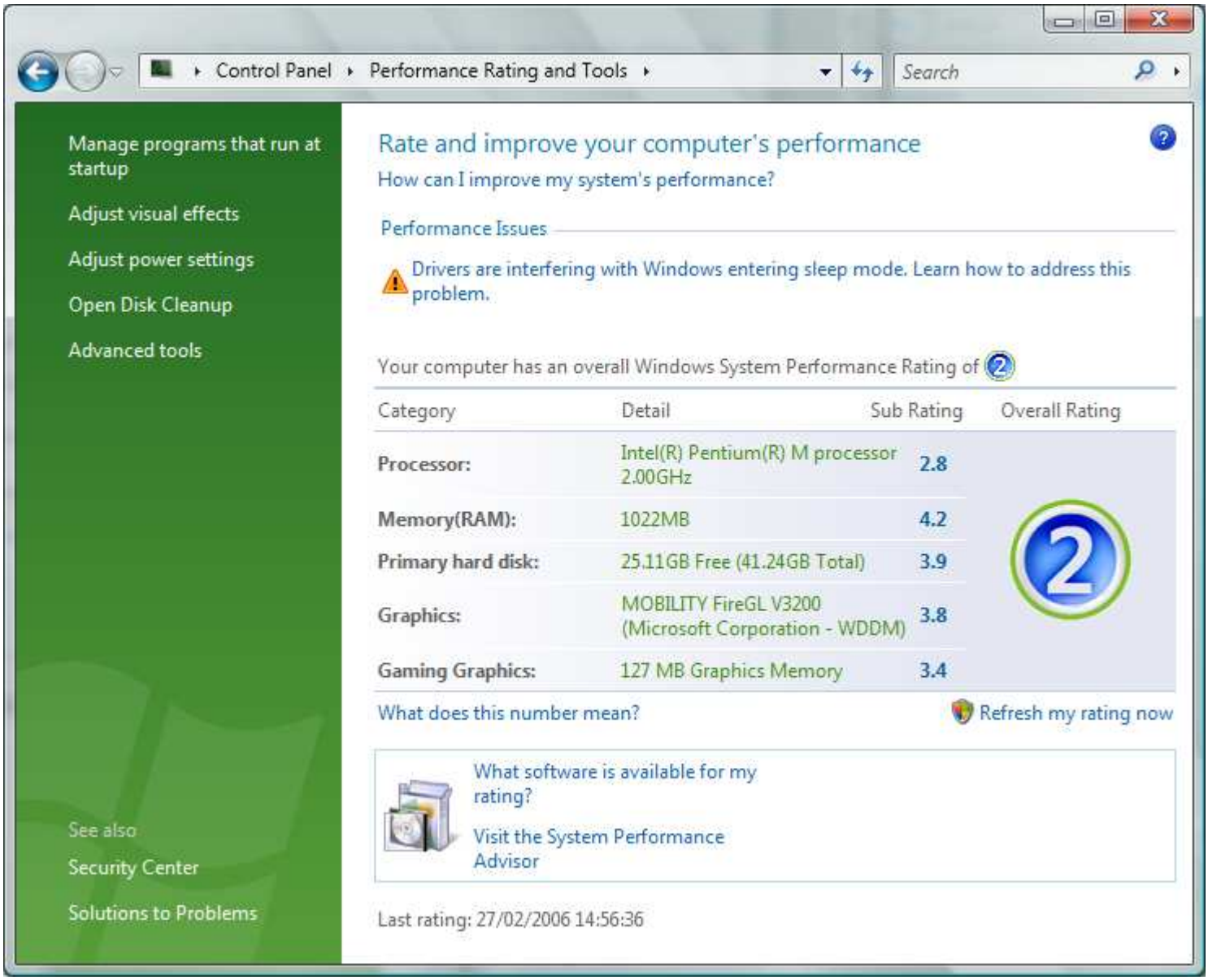


En effet, cette console permet enfin de pouvoir gérer les imprimantes de façon centralisée et efficace! Combien d'administrateurs se sont déjà cassés les dents à l'idée de vouloir gérer l'intégralité des imprimantes partagées de leur entreprise! Nous n'allons pas trop nous étendre sur cette console étant donné qu'un article complet sur le sujet a déjà été rédigé par *Joachim Gomard*. Bien sûr, l'article parle de la gestion des imprimantes avec Windows Server 2003 R2 mais le principe est exactement le même sur Windows Vista et les deux se complètent.

3. La gestion du système Windows Vista

3.1. Performance Rating and tool

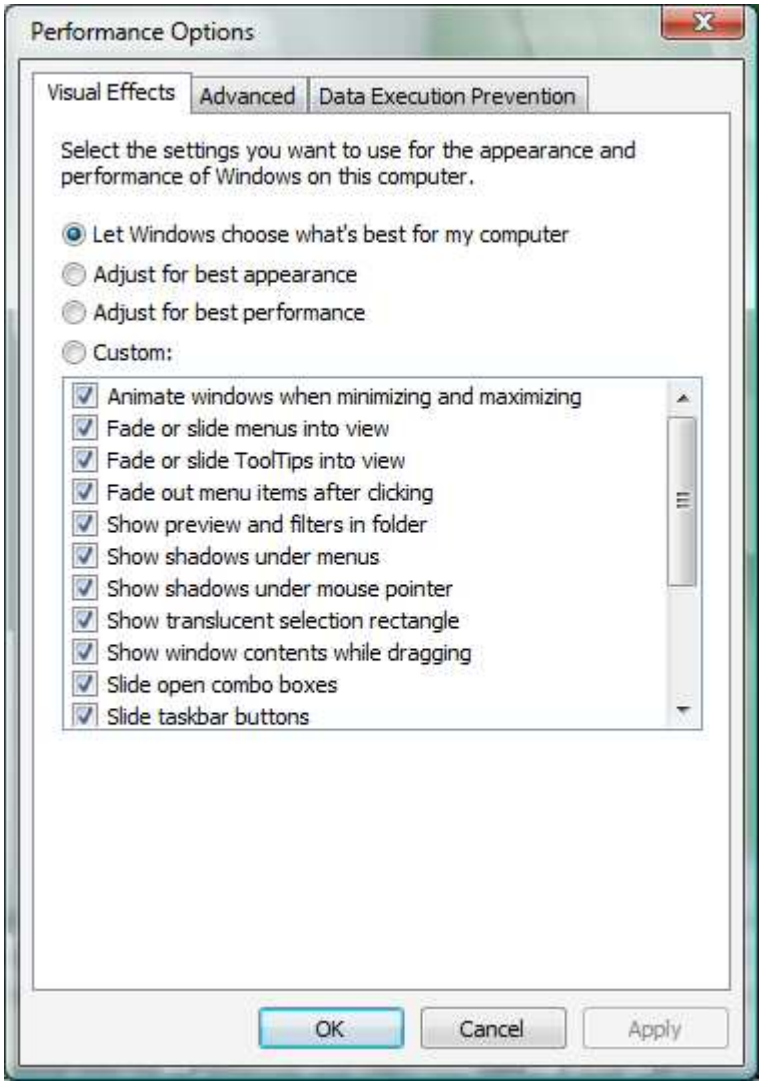
Comme nous en avons parler dans la partie sur le **Welcome Center**, Microsoft a ajouté un outil notation matériel sur lequel Windows Vista est installé. De plus des informations sur les performances actuelles sont affichées avec des avertissement, comme ci-dessous. En effet, quelques problèmes surviennent sur mon ordinateur lorsque je le sort de la veille prolongée:



Cet outils est indispensable pour comprendre pourquoi le système ne s'exécute pas dans une fluidité optimum, c'est à dire qu'il "rame". En effet, Windows Vista requière une **configuration matérielle** récente et plutôt puissante! De très nombreux PC sur le marché actuellement ne seront pas pleinement compatible avec ce nouveau système d'exploitation, gourmand en performance mais si convivial et pratique. Avec cet outils, l'utilisateur pourra comprendre quel composant lui fait défaut (processeur, mémoire vive, disque dur, carte graphique, mémoire graphique) et alors faire une mise à jour matérielle si cela est encore possible.

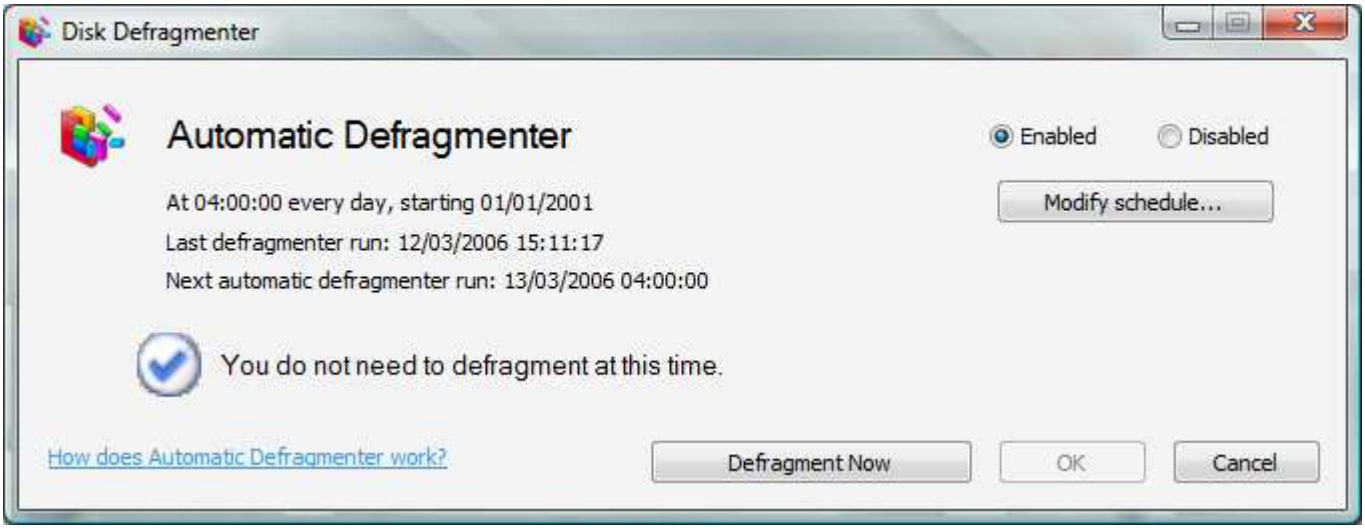
Pour ceux qui choisiront de changer leur matériel, il est alors possible de renoter l'ordinateur en cliquant sur **Refresh my rating now** ou alors en exécutant la commande **Winsat.exe**. Les notes sont comprises entre 0 et 5; et comme cette news l'a annoncé, des notes inférieurs à 3 sont significatives de performance à la baisse. Si la note générale est inférieure à 3, les performances ne pas vraiment irréprochable, pourtant les tests se font sur de portable de dernières générations (IBM thinkpad T43p)!

Par contre, il faut souligné que lors de nos essais, nous avons constaté que la fonction permettant de renoter le système d'exploitation relevait une erreur et désactiverait **Aero**!
Mais pour ceux qui ne veulent pas ou ne peuvent pas faire ces mises à jour, qui peuvent se révéler coûteuses, il reste toujours possible d'ajuster les paramètres du système pour tenir compte de ce manque de performance. Il est ainsi possible d'ajuster les performances visuelles comme on peux le faire avec des ordinateurs ayant moins de 128Mo de RAM pour supporter l'utilisation de Windows XP, en cliquant sur **Advanced tools** puis sur **Adjust the appearance and performance of Windows**, comme suit:



En cliquant sur **Advanced tools** de la console **Performance Rating and Tools** , plusieurs raccourcit sont disponibles. Certains nécessites des droit d'administrations comme la **défragmentation**, la **lecture des journaux d'événement** et l'accès à **la console de diagnostique des performances**. D'autres, par contre peuvent être exécuter en tant qu'utilisateur! Une de ces fonctionnalité à été revue pour prendre en compte les lancements programmés, c'est l'outils de défragmentation: **defrag.exe**. Il est maintenant

possible de programmer un défragmentation quotidienne, hebdomadaire ou mensuel. De plus vous savez au premiers coup d'œil si votre ordinateur à besoin d'une défragmentation ou pas!



Toutes ses actions dont nous venons de parler sont encore disponible dans **la console de gestion de l'ordinateur** avec bien d'autre fonctionnalité... Cette console n'a pas subit énormément de changement, mis à part certains composants comme **les journaux d'événement** et **la console de diagnostique des performances** (que nous allons développer juste après).

3.2. Windows Defender

En outre, ce composant du panneau de configuration, **Performance Rating and Tools**, permet d'accéder à différents outils. Ainsi, il est possible de faire un nettoyage du disque, gérer l'alimentation mais aussi les programmes qui se lancent au démarrage. Cette dernière fonction est gérer par **Windows Defender**, l'outils antimalware disponible aussi pour Windows XP SP2 en version 32 bits et en version 64 bits :

Cette partie est accessible en cliquant sur l'icone **Tools** dans **Windows Defender**, puis en cliquant sur **Software explorer**. Depuis cette console, il est possible de voir

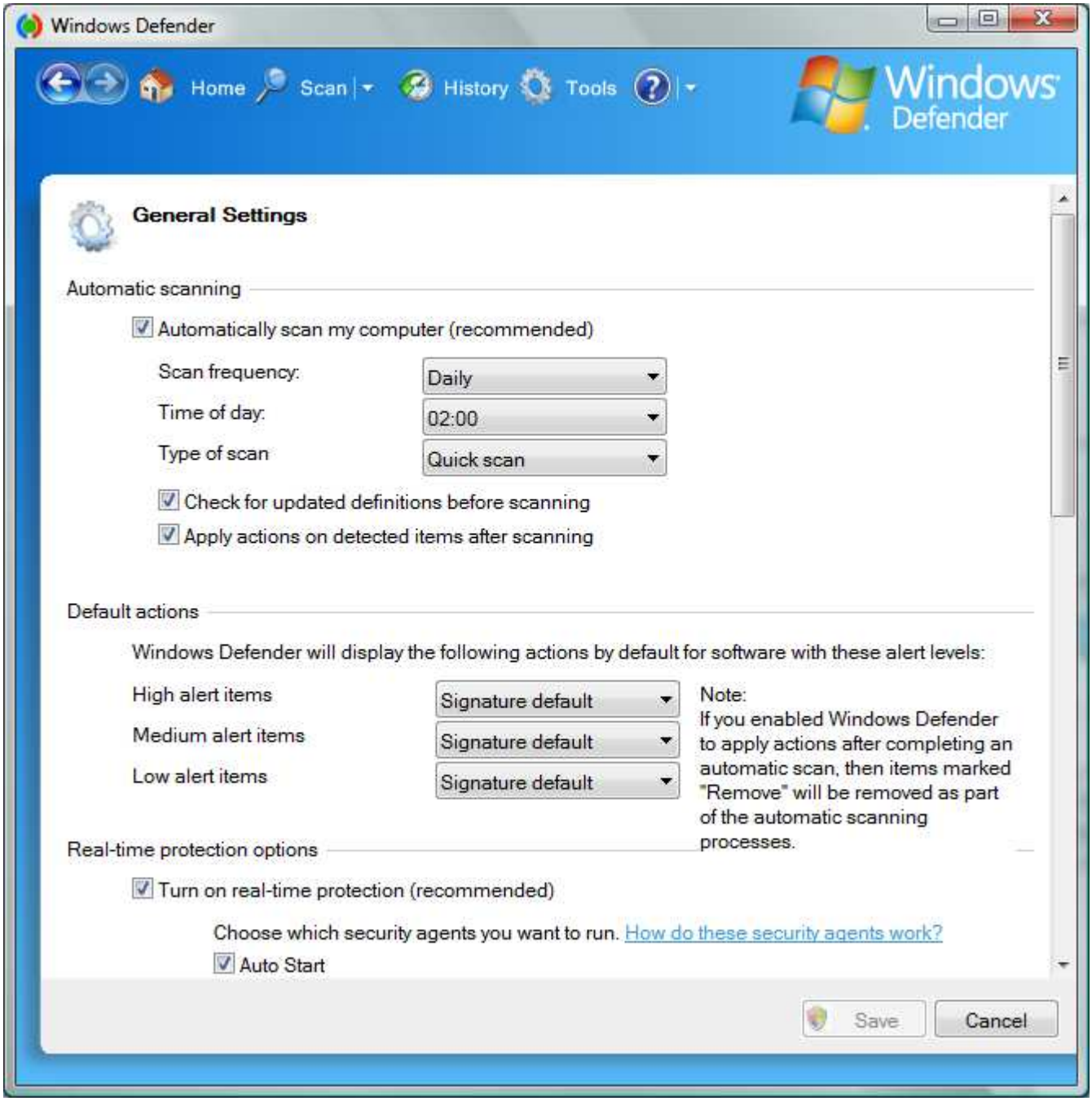
- **Les programmes qui se lancent au démarrage**: vous avez alors la possibilité d'enlever le programme dans la liste des programmes qui se lancent au démarrage ou alors de lui interdire de se lancer
- **Les programmes actuellement lancés**: vous pouvez lancer **Task Manager** depuis cette catégorie, ou alors quitter le programme que vous voulez
- **Les programmes connectés au réseau**: à partir de cette catégorie, vous avez la possibilité de terminer des programmes ou alors de bloquer leur utilisation du réseau.
- **Les fournisseurs de services Winsock**: avec cette catégorie, vous pouvez simplement voir les fournisseurs de services Winsock autorisés comme **NTDS**, **tcpip**...

Mais **Software Explorer** n'est pas le seul outils disponible avec **Windows Defender**. On peux citer ainsi 3 autres outils:

- **Quarantined items**: Avec cet outils, vous pouvez voir la listes de objets en quarantaine, en restaurer, en supprimer ou tous les supprimer

- **Allowed items**: Ici, vous trouverez tous les objets qui ne seront pas surveillés car considérés sûrs (gestion autonome ou autre). Si vous supprimer un objet, alors celui-ci retournera sous le contrôle de Windows Defender!
- **Windows Defender Website**: Si vous cliquer sur cet outils, vous allez être redirigés vers le site Web de Windows Defender.

En outre, des options de configuration sont possibles, en cliquant sur **General Settings**.



À partir des paramètres généraux, il est possible de gérer le comportement de **Windows Defender**. Ainsi il est possible de configurer le lancement automatique en choisirent la fréquence (quotidien, un jour par semaine), l'heure et le type de scan (rapide ou complet). De plus, il est possible de forcer la **mise à jour des définitions** avant de lancer une recherche sur la machine et de permettre de faire automatiquement

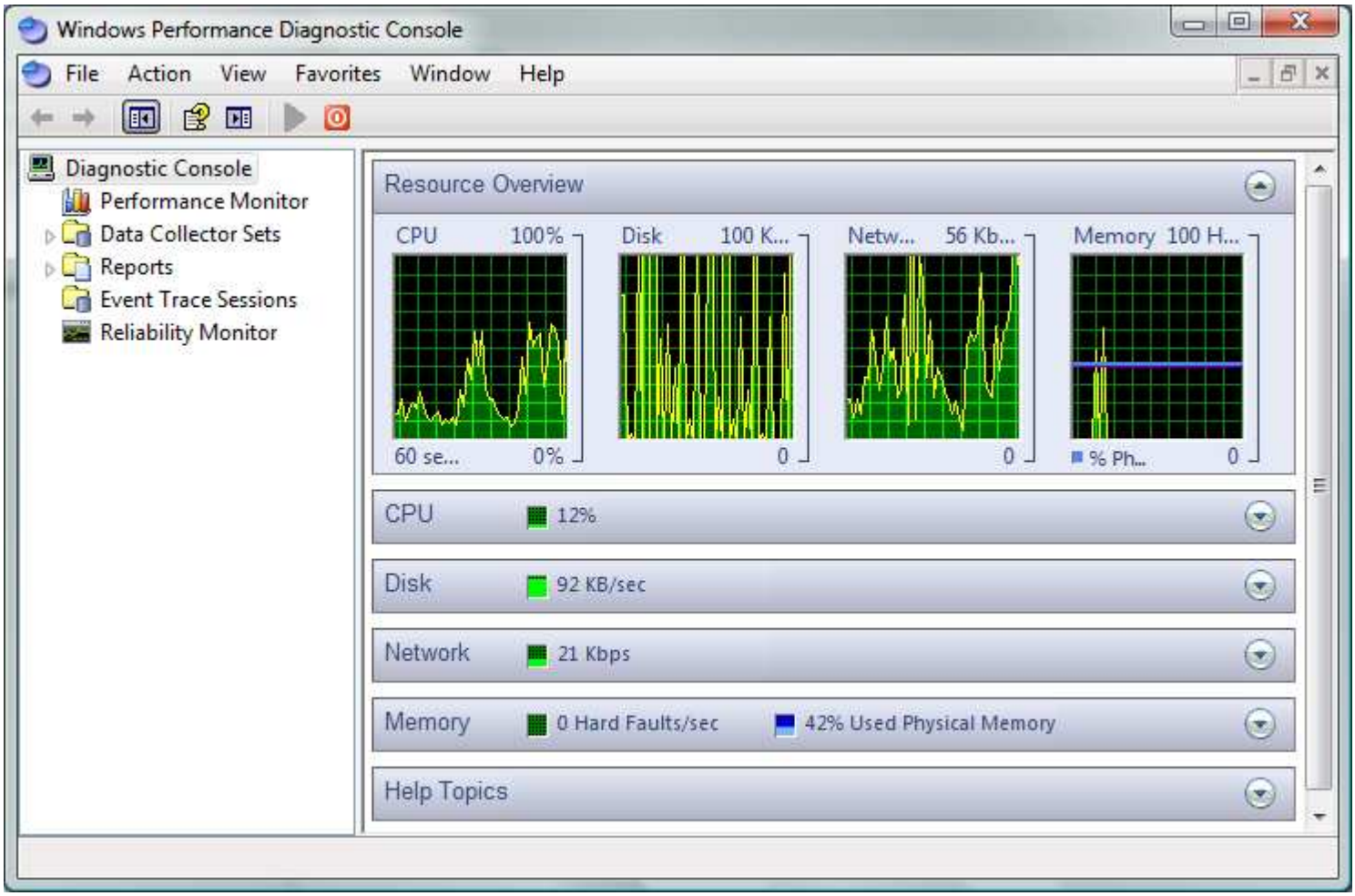
des **actions de maintenance** une fois terminé. Si vous choisissez cette dernière possibilité et que vous modifier les actions par défaut avec la valeur **Remove**, la suppression sera considérée comme partie intégrante de la recherche! Trois actions par défaut sont configurables en fonction du **niveau de menace** (high, medium and low), pour lesquels vous pouvez choisir les options suivantes: *signature default*, *ignore* et *remove*.
En outre vous pouvez configurer la protection en temps réel pour prendre en compte:

- Le lancement automatique
- La configuration système
- Les add-ons Internet Explorer
- La configuration d'Internet Explorer
- Les téléchargements d'Internet Explorer
- Les services et les dirvers
- L'exécutions des applications
- L'enregistrement des applications
- Les add-ons Windows

Il est possible de configurer Windows Defender pour faire des **notifications** quand des changement ont été opérer sur des programmes non autorisés et/ou lorsque des changement sont exécutés sur des programmes autorisés. Ensuite, dans les options avancées, il est possible de configurer la recherche **à l'intérieur des archives** et utiliser des **méthodes heuristiques** pour détecter les dossiers douteux. De plus, il est possible d'enlever des répertoires de la recherche en créant une liste exhaustive de chemins proscrits. Enfin, vous avez la possibilité de **donner des droits** (de lancer des recherches sur le système et de supprimer les divers programmes malicieux) aux **utilisateurs ayant les droits administrateurs**.
La dernière option permet d'arrêter **Windows Defender** mais il faut être conscient que la protection temps réelle ne sera possible et aucune notification ne sera faite! Il ne vaut mieux pas utiliser cette option à moins d'un problème interne à Windows Defender.

3.3. Surveillance de l'ordinateur

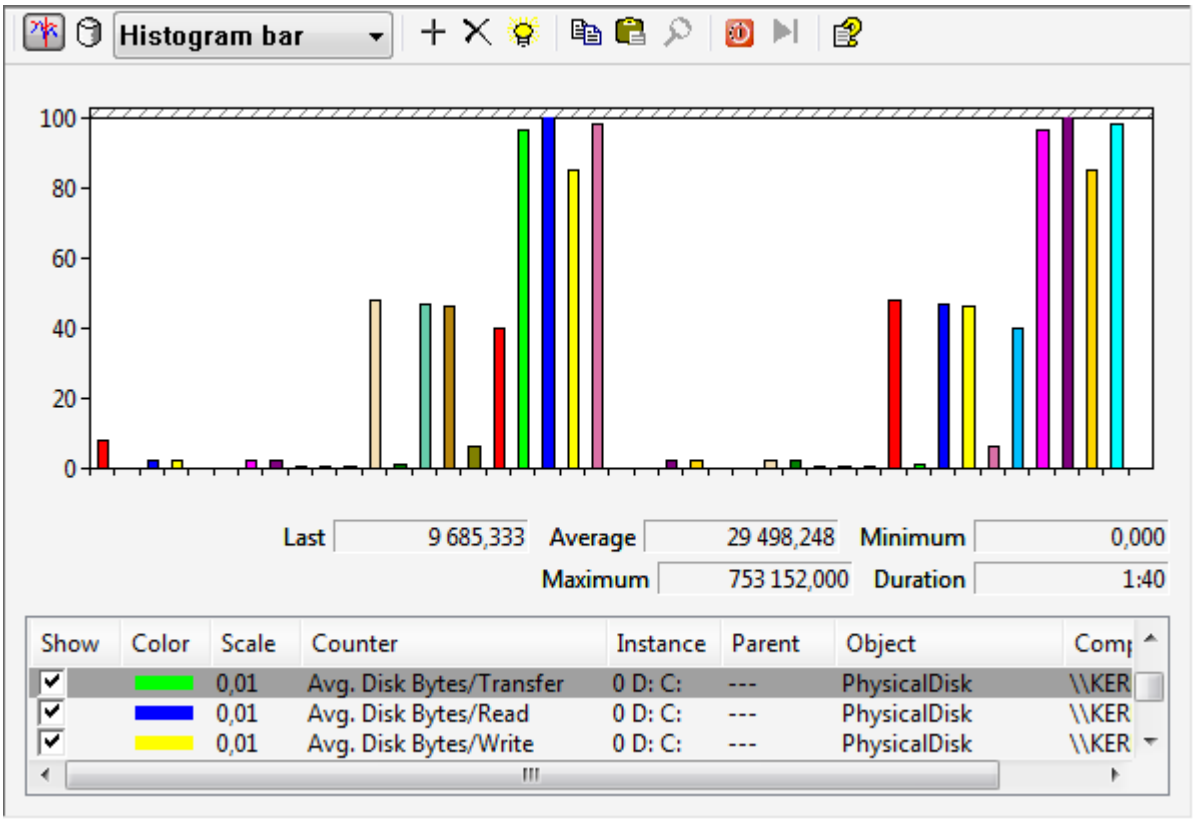
Comme nous en avons parlé dans la partie sur le Firewall, Windows Vista implémente **MMC v3.0**. Cette nouvelle version de MMC offre des perspectives très intéressantes dans les fonctionnalités d'administration de l'ordinateur. Nous allons prendre exemple sur **la console performance**:



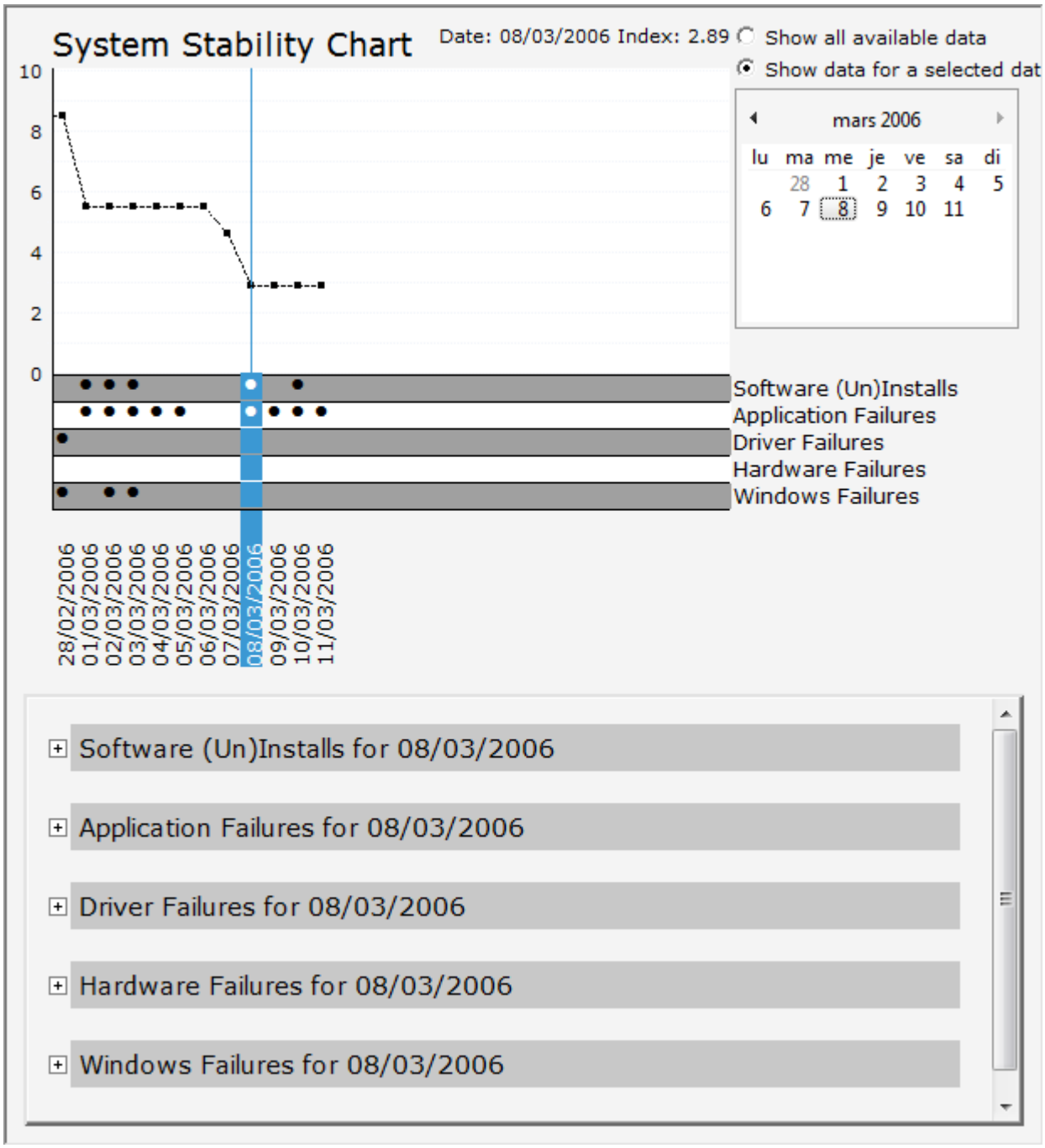
La console a aussi été revue et corrigée! La présentation n'a plus rien à voir avec celle de Windows XP... Comme montré ci dessus, une vue instantanée de l'utilisation du processeur, du disque, du réseau et de la mémoire est illustré sur la page d'accueil de la console. En développant chaque partie, vous retrouvez les informations suivantes pas catégorie:

- **CPU**: nom de tous les processus, son PID (identifiant unique de processus), le nombre de thread, l'utilisation en unité de CPU et l'utilisation à 0,01% près du CPU
- **Disk**: le nom du processus, son PID, le fichier utilisé, l'utilisation du disque (en Byte/minute) en lecture et en écriture ainsi que l'utilisation totale
- **Network**: le nom du processus, son PID, l'adresse de destination, l'utilisation (en Byte/minute) en émission et en réception.
- **Memory**: le nom du processus, son PID, le nombre de fautes matériels/minute et l'utilisation concrète de la mémoire.

Ces informations combinée avec les vue graphique peuvent se révélée intéressantes à analyser en cas de problème de performance. mais cette console n'est pas limité qu'à ces vues prédéfinies et statiques: en cliquant sur **Performance Monitor**, il est possible de construire soi-même en peu d'actions ses propres relevés d'informations:



La présentation à été améliorée pour permettre un affichage plus lisible, trois modes d'affichage sont toujours possibles: courbes, Histogramme à barres et rapport. De cette façon, il est possible de jongler entre les trois modes pour choisir la vue la plus représentative de ce que l'on souhaite afficher! Ces actions sont aussi possible sons Windows XP mais l'accessibilité à grandement était améliorée mais maintenant, il est possible de choisir d'affiché un compteur ou pas: ainsi, il est possible de choisir une multitude de compteur mais n'afficher, sur la représentation graphique, que les compteurs pertinents. La seconde nouveauté est le **System Stability Chart** qui permet de donner une note de 1 à 10 sur la stabilité du système. La version que nous utilisons pour cette article, à savoir la build 5308, n'est encore qu'une bêta et le matériel sur lequel nous la testons n'est pas encore complètement supporter ce qui explique peut-être les résultats suivants:



Comme vous pouvez le voir, un suivi de l'état général du système est relaté par un note par jour. De plus, un résumé des problèmes d'applications, de drivers, du matériel et de Windows ainsi que les installation et désinstallation des applications est accessible ici! Il est alors possible de comprendre la baisse de performance notée par l'utilisateur et représente donc une mine d'informations utiles pour la maintenance du système et la sensibilisation des utilisateurs. Deux possibilités d'affichage de ces résumé est possible: soit tous ensemble soit regroupée par jour! En développant chaque catégorie, les informations sont affichées avec une explication du problème:

- **Software (Un)Installs**: Vous pouvez retrouver ici, le nom du logiciel, la version, l'action (installation/désinstallation) et la date

- **Application Failures**: Dans cette partie, vous pouvez voir le nom du logiciel, la version, le type d'erreur et la date
- **Drivers Failures**: le nom du driver, la version, le type d'erreur et la date
- **Hardware Failures**:
- **Windows Failures**: le type d'erreur, la version, la description de l'erreur et la date

4. La sécurité et Windows Vista

4.1. NAP: Network Access Protection

4.1.1. Principe

NAP est un système permettant de vérifier la conformité des postes de travail d'un réseau local. Cette solution rejoint la solution de Cisco: **NAC(Network Admission Control)** dans ce domaine. Par exemple, si un ordinateur ne possède pas certains correctifs essentiels installés, lorsqu'il se connecte au réseau local, il ne peut pas ou avoir accès qu'à une partie limitée de celui-ci; de la même façon que le réseau de quarantaine VPN avec ISA Server 2004. La solution intègre deux niveaux:

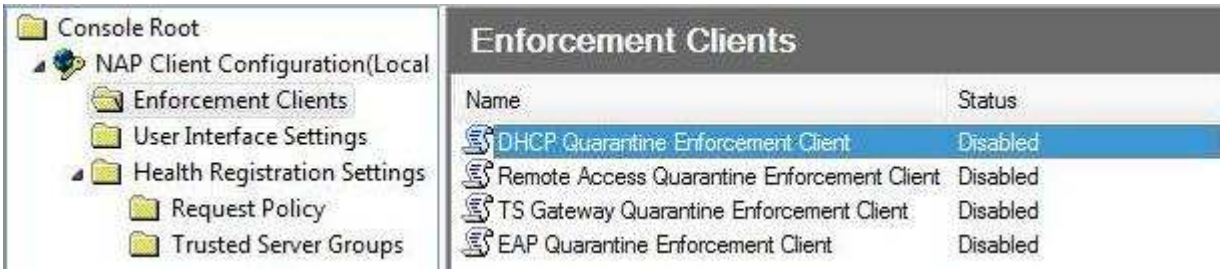
1. Au niveau client, des agents vont vérifier la santé de l'ordinateur, par exemple les correctifs.
2. Au niveau du serveur, un agent vérifie si la réponse de santé envoyée par les agents clients correspond aux politiques du serveur.

Pour plus de renseignements, vous pouvez consulter cet article: Découvrez Network Acces Protection : NAP

4.1.2. Implémentation

Cette partie concerne l'implémentation de la **NAP Console Configuration**. Celle-ci est accessible via la console MMC ou les outils d'administration. Dans cette console il existe différentes sous parties:

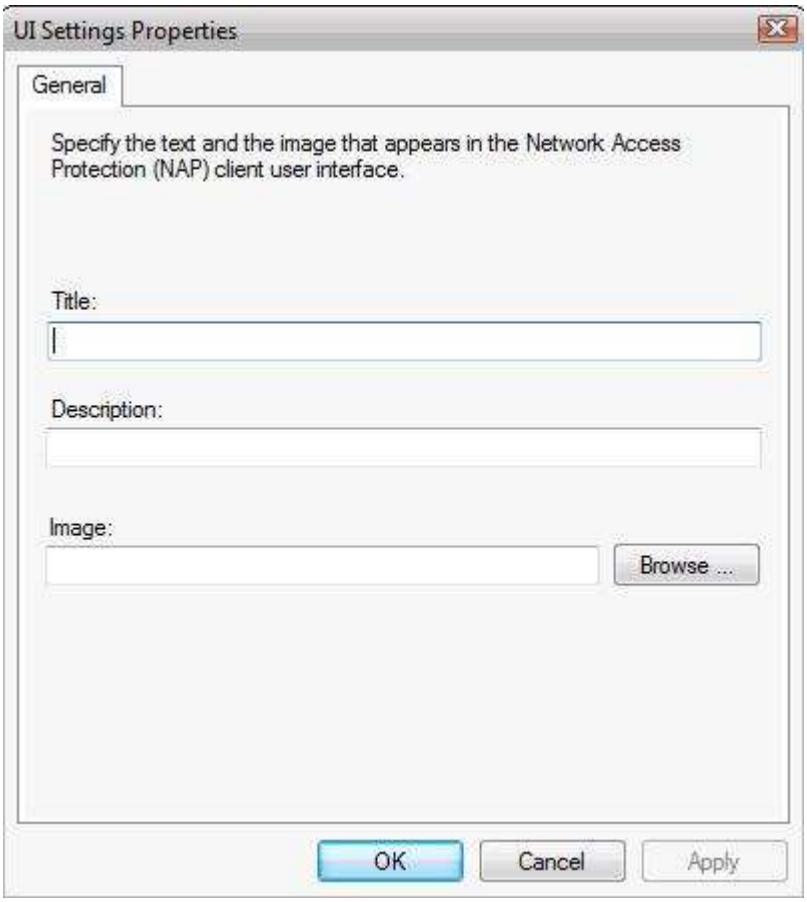
- **Enforcement Clients**



1. **DHCP Quarantine Enforcement Client**: Si vous choisissez d'activer cette option, cela va activer l'agent de quarantaine DHCP. C'est-à-dire que si le client ne répond pas aux exigences de santé du serveur, il sera placé dans une zone ou seule les routes statiques vers les serveurs remèdes seront accessibles.

2. **Remote Access Quarantine Enforcement Client**: Permet d'activer l'agent de quarantaine pour les accès distants.
3. **TS Gateway Quarantine Enforcement Client**: Permet d'activer l'agent de quarantaine pour les clients Terminal Server.
4. **EAP Quarantine Enforcement Client**: Permet d'activer l'agent de quarantaine pour les clients VPN.

- **User Interface Settings**: permet tout simplement de choisir le texte et l'image qui apparaîtra dans la fenêtre **NAP** du client lorsqu'il sera en état d'inconformité.



- **Health Registration Settings**
  A. **Request Policy**: cette partie permet de choisir tout simplement quelle est la solution de cryptage que l'on souhaite utiliser.

En effet, celle-ci est divisé en trois parties:

1. *Asymetric Key Algorithm*: vous permet de choisir l'algorithme à clé asymétrique et sa version que vous souhaitez utiliser. Par exemple: 3DES,AES...
2. *Hash Algorithm*: permet d'utiliser un algorithme de hachage parmi une liste tel que: MD5, SHA...
3. *Cryptographic Service Provider*

B. **Trusted Server Groups**: qui permet de regrouper les serveurs de confiance.

4.2. InfoCard

Infocard est un système qui permet de gérer les identités sur Vista, c'est le nouveau système d'identification unifié comme Passport. En fait, cette solution se comporte comme une carte de visite, vous enregistrez ainsi des informations sur votre statut, votre identité. En fait, chaque carte crée est un certificat numérique signé automatiquement qui présente en fait deux parties une publique et l'autre privée qui contient vos données personnelles comme le numéro de carte bancaire, par exemple. Infocard pourra être utiliser selon deux modes distincts:

- La première méthode consiste en l'**accès sur un site web** tel qu'un forum. Celui-ci, demande diverses informations comme par exemple une adresse email. Alors, **Infocard** va chercher automatiquement une carte qui possèdera les informations demandées, après il enverra uniquement les informations qui sont demandées par le site afin accepter l'inscription de l'utilisateur.
- La deuxième méthode concerne surtout l'**achat en ligne**. Admettons que vous voulez acheter un matériel informatique sur un site: **Infocard** va comme dans le premier cas chercher les cartes appropriées et l'utilisateur choisit la carte qu'il souhaite utiliser. Ensuite, les informations du site seront testées par un site bancaire afin de vérifier l'authenticité du magasin. Ainsi, celui-ci ne pourra récupérer que les informations essentielles.

Infocard pourra également recevoir des identités d'autres fournisseurs ou envoyer son identité pour une validation: ceci permettra une interopérabilité avec des systèmes comme **SecurID** ou **VeriSign**. Ainsi, ce système permettra entre autre à contrer les arnaques en ligne tel que le **Phishing**, le vol de mot de passes et de simplifier la vie des utilisateurs qui auront moins de mot de passes à retenir.

4.3. Bitlocker Drive Encryption

Bitlocker Drive Encryption est une technologie qui permet l'encryption complet d'une partition système.

4.3.1. Principe

Lors de l'encryption, une clé est créée et doit être mis sur une clé USB, sur le réseau, ou autre support de stockage. Il peut aussi être utiliser avec les nouvelles puces TPM intégrées aux cartes mères. Ainsi

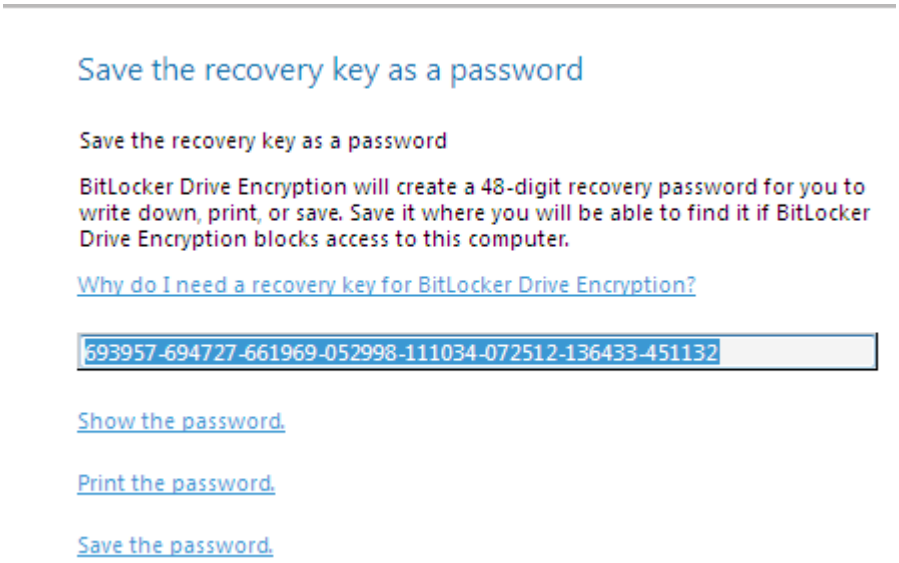
les clés sont stockées sur la puce et seule la puce à accès à l'information. Ainsi, toutes les informations de votre disque dur pourront être crypter comme les fichiers systèmes, les fichiers du secteur d'amorçage. Microsoft espère ainsi, protéger les utilisateurs de l'installation et l'utilisation de logiciels malicieux sur votre PC.

4.3.2 Implémentation sous Windows Vista

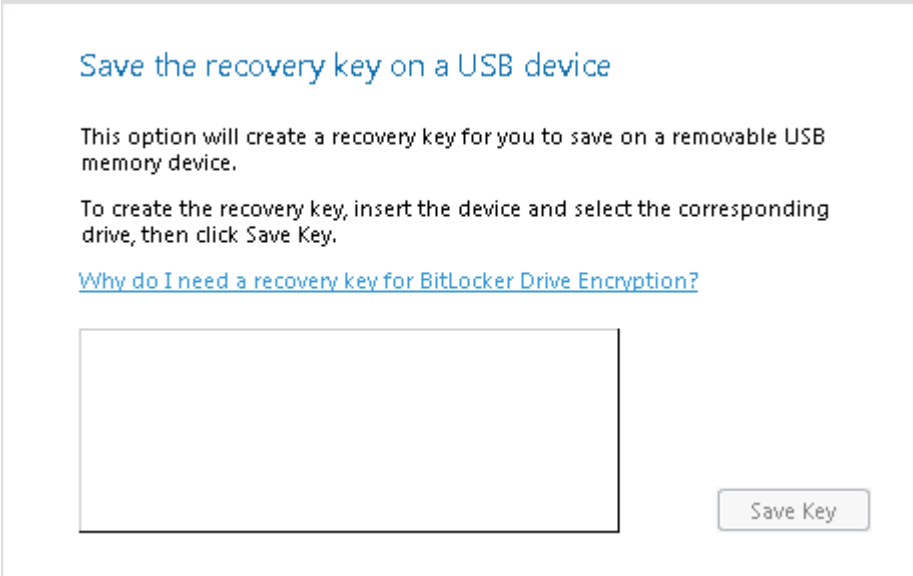
Afin d'acceder à la console de **BitLocker**, il faut aller dans *Control Panel->Security->BitLocker Drive Encryption*. La fenêtre ci-dessous s'ouvre. Elle vous affiche toutes vos partitions sur lesquelles vous pouvez mettre en place une sécurité **BitLocker**. Cliquez sur *Turn On BitLocker*.

Une fois ceci fait, on vous propose de voir la clé de restauration comme un mot de passe. Vous avez trois possibilités:

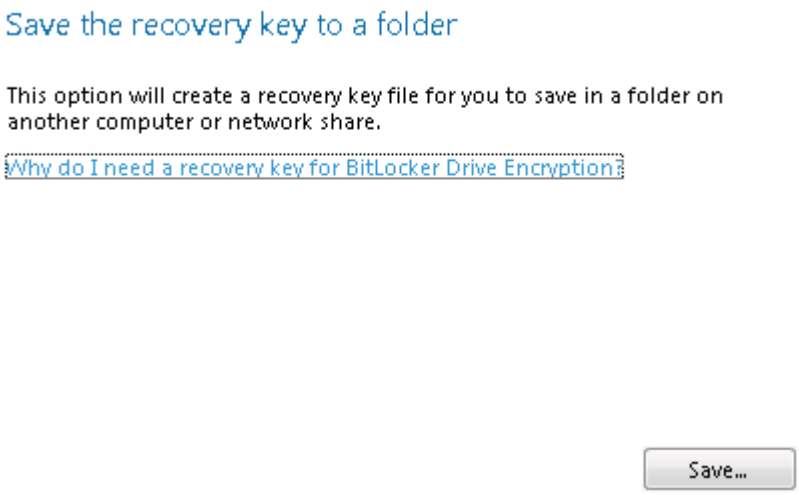
- Voir le mot de passe. Nous vous conseillons de ne pas juste regarder le mot de passe ou de l'apprendre par coeur car il est très long et difficile à retenir. Cette option se dessine plus à voir comment est faite la structure de ce mot de passe.
- Imprimer le mot de passe. Si vous souhaitez le conserver sur un document écrit ceci peut être utile, mais veillez à bien sécuriser et surveiller l'accès au document afin que des personnes mal attentionnées ne puissent pas le dérober.
- Sauvegarder dans un fichier le mot de passe. Ceci est peut être la façon la plus sécuriser de garder cette clé. Mais cependant, veuillez à donner les droits de lecture à ce fichier qu'aux administrateurs.



Ensuite, le système vous propose d'enregistrer la clé sur une clé USB. Il suffit d'en connecter une et de cliquer sur *Save Key*. Cette solution est à privilégier si l'on souhaite posséder cette ressource sur un stockage externe, en effet il serait dommage d'avoir laissé la clé sur sa partition crypté et ne plus avoir accès à celle-ci.



Même chose que précédemment, sauf qu'ici on a le choix d'enregister la clé sur un partage réseau. Ceci peut être utile si vous stocker cette clé sur un serveur sécurisé. Attention tout de même aux autorisations de partage.



Enfin, vous avez le choix de créer une clé de démarrage afin d'ajouter plus de sécurité. **Cette option est très dangereuse.** Effectivement, si vous n'entrez pas la clé USB au démarrage Windows refusera de booter sur la partition cryptée donc réfléchissez bien à deux fois avant d'implémenter cette solution et surtout ne perdez pas la clé.

Voilà, vous disposez maintenant de la sécurité BitLocker. Vos données sont parfaitement protégées grâce à ce système qui a crypté complètement votre partition.