SANSTABOO

Windows 7 avancé

Préface de
Lucas Riedberger

EYROLLES

SANSTABOO

Windows 7 avancé

Windows 7 au doigt et à l'œil

Pour exploiter tout le potentiel de Microsoft Windows 7, chaque utilisateur doit s'approprier un ensemble complexe d'outils. Cet ouvrage vous explique comment paramétrer, administrer et dépanner votre PC pour qu'il réponde parfaitement à vos besoins. Tant pour une utilisation familiale que professionnelle, ce livre présente les bonnes pratiques qui feront de vous un expert de Windows 7.

Thomas Garcia est un passionné d'informatique et de programmation. Administrateur système, il aime découvrir de nouveaux systèmes et en explorer les moindres recoins. Il anime et modère sur son temps libre la rubrique Windows sur Developpez.com.

Expert certifié en administration système et nommé MVP par Microsoft sur Windows Vista, **Louis-Guillaume Morand** est consultant en technologies Microsoft et responsable de publication .NET sur Developpez.com.

Adaptez toutes les facettes de Windows 7 à vos habitudes

- Configurez finement votre système et optimisez-le
- Paramétrez vos périphériques et installez vos programmes
- Gardez la main sur les actions utilisateurs : autorisations, AppLocker…
- Optimisez les partitions et les disques durs
- Chiffrez et sauvegardez vos données
- Sécurisez votre système grâce aux modèles de sécurité
- Luttez contre les spywares et malwares et apprenez à dépanner votre système
- Intégrez votre PC dans tout type de réseau : Wi-Fi, VPN, groupe résidentiel…
- Transformez votre ordinateur en serveur web et mettez en place un espace FTP

À qui s'adresse cet ouvrage ?

- *Aux particuliers qui veulent migrer leur PC vers Windows 7*
- *Aux utilisateurs aguerris de Windows qui souhaitent exploiter les dernières avancées de l'OS*
- *Aux administrateurs système des PME qui doivent maîtriser rapidement Windows 7*

Code éditeur : G12594
ISBN : 978-2-212-12594-8
Conception : Nord Compo
© Photo de couverture : istockphoto

www.editions-eyrolles.com
Groupe Eyrolles | Diffusion Geodif

29,90 €

Windows 7 avancé

Dans la même collection

Mac OS X efficace.
G. Gete.
N°12263, 2008, 476 pages.

Réussir sa compta avec Ciel.
N. Crouzet.
N°12262, 2008, 402 pages.

D'Excel à Access. *Croiser, extraire et analyser ses données.*
T. Capron.
N°12066, 2008, 350 pages.

Sécuriser enfin son PC *Réflexes et techniques contre les virus, spams, phishing, vols et pertes de données.*
P. Legand.
N°12005, 2006, 400 pages.

Mac OS X Snow Leopard efficace.
G. Gete.
À paraître.

RPG Maker. *Créez votre gameplay et déployez votre jeu de rôle.*
S. Ronce.
À paraître.

Composition et mixage avec GarageBand'09. *Manuel de survie pour compositeur en herbe.*
D. Mary.
À paraître.

Dans la même collection

Concevoir et déployer ses sites web avec Drupal
Y. Brault.
N°12465, 2009, 404 pages.

Linux aux petits oignons. *Les meilleures recettes pour bien débuter !*
K. Novak.
N°12424, 2009, 524 pages avec DVD-Rom.

OpenOffice.org 3 efficace.
S. Gautier, G. Bignebat, C. Hardy, M. Pinquier.
N°12408, 2009, 408 pages avec CD-Rom.

MediaWiki efficace. *Installer, utiliser et administrer un wiki.*
D. Barrett, adapté par S. Blondeel.
N°12466, 2009, 374 pages.

Réussir un site web d'association… avec des outils libres !
A.-L. Quatravaux et D. Quatravaux.
N°12000, 2e édition, 2007, 372 pages.

Bien rédiger pour le Web… *et améliorer son référencement naturel.*
I. Canivet.
N°12433, 2009, 412 pages.

Ergonomie web. *Pour des sites web efficaces.*
A. Boucher.
N°12479, 2e édition, 2009, 458 pages.

Améliorer son taux de conversion web.
S. Roukine.
N°12499, 2009, 250 pages.

Joomla et Virtuemart. *Réussir sa boutique en ligne.*
V. Isaksen, T. Tardif.
N°12381, 2008, 306 pages.

Réussir son site web avec XHTML et CSS.
M. Nebra.
N°12307, 2e édition, 2008, 306 pages.

Réussir son site e-commerce avec osCommerce.
D. Mercer.
N°11932, 2007, 446 pages.

Réussir un projet de site web.
N. Chu.
N°12400, 5e édition, 2008, 246 pages.

Ubuntu efficace.
L. Dricot, K. Novak.
N°12362, 3e édition, à paraître 2009, 360 pages avec CD-Rom.

Boostez votre efficacité avec FreeMind.
X. Delengaigne, P. Mongin.
N°12448, 2009, 260 pages.

Gimp 2.4 efficace. *Dessin et retouche photo.*
C. Gémy.
N°12152, 2e édition, 2008, 402 pages avec CD-Rom.

Inkscape efficace. *Réussir ses dessins vectoriels.*
C. Gémy.
N°12425, 2009, 280 pages

La 3D libre avec Blender.
O. Saraja.
N°12385, 3e édition, 2008, 456 pages avec DVD-Rom.

Dessiner ses plans avec QCad. *Le DAO pour tous.*
A. Pascual.
N°12397, 2009, 278 pages.

Mise en page avec OpenOffice.org Writer.
I. Barzilai.
N°12149, 2007, 338 pages.

Scenari – La chaîne éditoriale libre.
S. Crozat.
N°12150, 2007, 200 pages.

PGP/GPG. *Assurer la confidentialité de ses mails et fichiers***.**
M. Lucas, ad. par D. Garance , contrib. J.-M. Thomas.
N°12001, 2006, 248 pages.

Monter son serveur de mails sous Linux
M. Bäck *et al*., adapté par P. Tonnerre.
N°11931, 2006, 360 pages.

Tiny ERP/Open ERP. *Pour une gestion d'entreprise efficace et intégrée.*
F. Pinckaers, G. Gardiner.
N°12261, 2008, 276 pages.

Chez le même éditeur

M. Lavant. **À la découvert de Windows 7**. *Cahier Windows n°1*. N°12595, 2009, 164 pages.
M. Lavant. **À la découvert de son Mac**. *Cahier Mac n°1*. N°12595, 2009, 256 pages.
R. Ostertag. **Gimp spécial débutants**. *Cahier Gimp n 1*. N°12451, 2009, 160 pages.
T. Sarlandie. **Programmation iPhone**. N°12477, 2009, 250 pages.
G. Leblanc. **C# et .NET**. N°12604, 2009, 910 pages.
P. Roques. **UML 2 par la pratique**. N°12565, 7e édition, 2009, 396 pages.

Louis-Guillaume **Morand**
& Thomas **Garcia**

SANSTABOO

Windows avancé 7

Préface de
Lucas Riedberger

EYROLLES

ÉDITIONS EYROLLES
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Remerciements à Romain Pouclet pour sa relecture constructive.

© Groupe Eyrolles, 2010, ISBN : 978-2-212-12594-8

Préface

Le syndrome du « Good enough »

Comme beaucoup d'entre vous, j'ai connu l'arrivée de Windows 95 qui vit l'avènement du 32 bits et une interface graphique nettement améliorée. Puis vint Windows 98, toujours sur un noyau 9x, qui nous a apporté les premières innovations multimédias dignes de ce nom et le début de la connexion à Internet. Nous passerons vite sur la dernière mouture 9x que fut Windows Millenium, test malheureux ou obligation du marché ? Personne ne le saura.

En parallèle, le noyau « entreprise » de Windows, NT 3.5 puis 4, continuait à évoluer positivement, proposant aux entreprises des fonctionnalités innovantes pour les systèmes d'information des entreprises. C'est d'ailleurs à peu près au même moment que les « directeurs informatiques » devinrent « directeur des systèmes d'information ». Couplé aux fonctionnalités de l'Active Directory, Exchange 2000 et Terminal Service, Windows 2000 apporta une valeur et une fiabilité exceptionnelles au système d'entreprise.

Puis vint Windows XP, mélange réussi de la fiabilité de Windows 2000 et des fonctionnalités multimédias de Windows 98, tout cela pour l'utilisation domestique. Basé sur le noyau 5.1 de Windows, Windows XP a profité du développement des drivers et des logiciels effectué sur Windows 2000, basé sur le noyau 5.

Le pauvre Windows Vista, lui, n'a pas pu bénéficier de ce laps de temps pour que l'écosystème des éditeurs de logiciel et des constructeurs se prépare. Pourtant, les atouts n'ont pas manqué à cette mouture de Windows. D'ailleurs, ils sont présents dans Windows 7 et vous allez les découvrir dans ce livre.

Windows XP fut à Vista, ce que Visual Basic 6 fut à .NET. *Fut*, car .NET 2.0 puis les versions suivantes ont fini de décider les développeurs VB6 de se tourner vers .NET, SharePoint, ou d'autres solutions Microsoft.

Le syndrome du « Good enough » – « ça me suffit » – permet à Windows XP, au moment où j'écris ces lignes, de survivre sur le PC. Il est pourtant obsolète par rapport à ce que propose Windows Vista. Ce syndrome du « Good enough » n'est de toute façon pas compatible avec le domaine informatique, ni à aucun autre écosystème. Les raisons en sont simples : une concurrence forte, des usages en constante mutation (notamment avec l'arrivée du triple ou quadruple play dans nos foyers) et une mondialisation de l'économie et de la société.

Divergence des usages, multiplication des périphériques électroniques et convergence technologique

Nous demandons toujours plus à notre bon vieux Windows : faire un montage vidéo ; téléphoner par Internet ; accéder au contenu d'une console... En outre, nous voulons davantage de sécurité, sans que cela ne soit trop contraignant... Le PC doit satisfaire tous ces besoins, les technologies doivent converger vers Windows et vers les logiciels qui peuvent l'habiller.

Il faut également accepter qu'il n'y ait plus un ou deux comportements face à l'écran, mais plusieurs. Les outils s'étant multipliés, le niveau des utilisateurs étant tellement disparate, les utilisateurs de Windows ont des comportements de plus en plus différents pour parvenir à leurs fins.

La multiplication des périphériques de toutes sortes est également un vrai challenge : de la connexion à une borne Wi-Fi d'un hôtel, au branchement d'une oreillette Bluetooth, en passant par l'accès aux films de la console de salon, Windows doit faire des prouesses pour rendre tout cela possible, tout en gardant un minimum de sécurité sur le portable.

Windows doit répondre à tous ces enjeux : terrible et excitant à la fois.

Roman, polar, biographie… bien mieux que tout cela un livre – une bible – informatique !

J'ai connu Louis-Guillaume Morand alors que j'étais en charge du marketing pour les développeurs, période durant laquelle, je me suis toujours

attaché à connaître et à reconnaître les développeurs talentueux. À l'époque, Louis-Guillaume, en charge de la section Windows – aujourd'hui tenue d'une main experte par Thomas Garcia – du fameux site communautaire Developpez.com, partageait déjà son enthousiasme pour le logiciel le plus utilisé au monde.

C'est tout naturellement et surtout légitimement, en se basant sur l'aide qu'il a su prodiguer aux développeurs et autres utilisateurs experts, qu'il a écrit ce qui va probablement devenir une référence.

« LG » fait partie de ces personnes qui donnent envie d'utiliser les outils informatiques, et surtout d'en partager la connaissance. C'est une caractéristique assez peu répandue dans ce monde – même mondialisé – pour que cela mérite d'être souligné.

Alors, pour ne pas déroger à la règle, et puisque, malgré mon rôle marketing, je suis un geek déclaré, et un très mauvais développeur, voici une petite astuce pour enregistrer vos actions Windows. Pour cela, il suffit d'exécuter, via la barre de recherche du menu *Démarrer*, l'applicatif PSR.

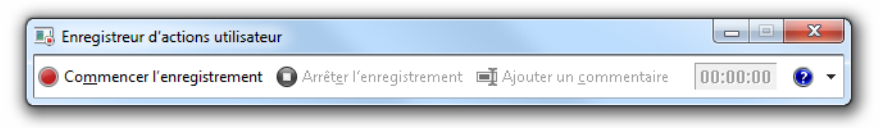


Figure 1
Interface de l'enregistreur d'actions utilisateur : l'outil idéal pour réaliser de petites démonstrations d'utilisation.

Il produit un fichier `mht` avec les captures d'écran de vos actions et les légendes explicatives. Utilisé principalement dans le cadre du support à l'utilisateur, ce petit outil s'avère très pratique pour expliquer « comment faire » à votre entourage, lequel n'aura pas eu la bonne idée de lire ce live. C'est d'ailleurs ainsi que j'ai donné de précieux conseils et astuces à Louis-Guillaume sur Windows 7 :-).

À la fois monstre et entité fragile sous notre clavier, Windows est notre souffre-douleur. Pourtant, nous l'aimons bien. Cela lui vaut bien un livre, pour sa septième version... ne parle-t-on pas alors d'âge de raison ?

Bonne lecture !

Lucas Riedberger

Responsable du site Microsoft.com

Ancien responsable marketing des relations avec les développeurs chez Microsoft France

Table des matières

Avant-propos 1

1. Windows 7, un nouveau système d'exploitation 7

Principe d'un système d'exploitation • 8
Les nouveautés de Windows 7 • 11
Interface graphique • 11
Connexion aux réseaux et mobilité • 12
Sécurité • 13
Administration du système • 14
Les différentes éditions de Windows 7 • 15
Édition Starter, version minimaliste • 16
Édition Familiale (Home Edition Basic), pour les pays émergents • 16
Édition Familiale Premium (Home Premium) • 16
Édition Professionnelle (Professional) • 17
Édition Entreprise (Business) • 17
Édition Intégrale (Ultimate) • 18
Quelle version choisir ? • 18
S'orienter parmi les différentes versions • 18
Choisir la version 32 bits ou 64 bits ? • 19
En résumé • 20

2. Installation du système 23

Préparatifs • 24
Votre ordinateur est-il compatible ? • 24
Quel type d'installation choisir ? • 24
Mise à jour depuis Windows XP • 25
Mise à niveau depuis Windows Vista • 26
Installation complète standard • 26
Installation sur un disque virtuel • 30
Paramétrage du multi-boot • 33
Désinstallation de Windows • 35
En résumé • 36

3. Paramétrer et personnaliser Windows 7 39

Le panneau de configuration : centre névralgique du paramétrage • 40
Le planificateur de tâches • 41
Créer une tâche planifiée • 41
Modifier les paramètres d'une tâche planifiée • 43
Régler l'heure et la date de l'ordinateur • 46
La console de gestion de l'ordinateur • 47
Paramétrage avancé des options de démarrage du système • 48
Propriétés du système • 50
Propriétés avancées du système • 51
Paramètres système avancés • 51
Utilisation à distance • 53
Nom de l'ordinateur • 53
Paramétrer les programmes par défaut • 53
Associer un programme à un type de fichier • 54
Associer manuellement un type de fichier ou un protocole à un programme • 54
Configurer l'exécution automatique • 55
Mettre à jour le système avec Windows Update • 57
Installer les mises à jour « à la demande » • 58
Désinstaller une mise à jour • 59
Paramétrer Windows Update • 59
En résumé • 61

4. Configurer le matériel 63

Signature des pilotes • 64
Gestionnaire de périphériques et pilotes • 65
Afficher l'état d'un périphérique • 66
Installer un périphérique plug and play • 67
Installer un périphérique non plug and play • 68
Afficher les périphériques déconnectés • 68
Afficher la puissance électrique requise par les périphériques USB • 69
Débrancher un périphérique amovible • 70
Gestionnaire de périphériques simplifié : le panneau Périphériques et imprimantes • 71
Installer rapidement des périphériques • 71
Installer des imprimantes • 73
Modifier les propriétés de l'imprimante • 73
Personnaliser l'imprimante • 74
Paramétrer le spool • 75
Définir plusieurs imprimantes par défaut • 75
Configurer le clavier • 76
Configurer la souris • 77
Régler le comportement des boutons • 77
Modifier l'apparence et le comportement du pointeur • 78
Configurer la roulette • 79
Configuration audio • 80
Régler le volume • 80
Configurer les périphériques audio • 81
Les périphériques de lecture • 82
Les périphériques d'enregistrement • 83
Configurer les sons système • 83
Connecter un vidéoprojecteur • 84
Configuration rapide • 84
Configuration avancée • 85
Affichage multiple • 85
Résolution et orientation • 86
Centre de mobilité pour les ordinateurs portables • 87
En résumé • 89

5. Installer et gérer les programmes..... 91

Ajouter un nouveau programme • 92
Désinstaller des programmes • 92
Nettoyer le système et le registre • 93
Ajouter des composants Windows • 95
Ajouter une fonctionnalité Windows • 95
Supprimer une fonctionnalité Windows • 96
Contrôle d'application avec AppLocker • 96
Les enjeux du blocage de logiciel • 97
Configurer AppLocker • 98
Créer des règles d'application • 99
En résumé • 101

6. Stocker les données 103

Optimiser les partitions et les disques durs • 104
Gérer les disques de base • 105
Réduire ou augmenter la taille d'une partition • 106
Changer le système de fichiers • 107
La gestion des disques dynamiques • 107
Les volumes simples • 108
Les volumes fractionnés • 108
Les volumes agrégés par bande • 108
Les volumes en miroir • 109
Les volumes RAID-5 • 109
Chiffrer les données • 110
Encryption File System • 110
BitLocker • 112
Activer BitLocker • 113
BitLocker To Go • 115
Paramétrer BitLocker • 116
En cas de perte de mot de passe • 117
Personnaliser l'indexation des fichiers • 118
Définir les dossiers à indexer • 121
Paramétrage avancé • 122
Déplacer les fichiers d'indexation • 123
Compresser les fichiers • 123
Virtualiser les fichiers avec le virtual store • 125
En résumé • 126

7. Les comptes utilisateur 129

Créer et gérer les comptes utilisateur • 130
La console d'administration des comptes • 130
Créer et modifier les profils • 131
Définir les répertoires utilisateur • 132
Changer le mot de passe utilisateur • 133
Les groupes utilisateur • 134
Créer un groupe • 134
Modifier les propriétés d'un groupe • 134
Le contrôle parental • 135
Configurer le contrôle parental • 136
Activer le contrôle parental • 136

Définir des horaires de connexion • 137
Définir les jeux autorisés • 138
Bloquer ou autoriser certaines applications • 138
Ajouter le filtrage web • 140
Le contrôle utilisateur • 141
Le principe de moindre privilège • 141
Configurer le contrôle utilisateur • 142
Configuration avancée • 143
En résumé • 145

8. Gérer les fichiers : sauvegardes, quotas et mode hors connexion 147
Sauvegarde de fichiers • 148
Les différentes solutions de sauvegarde • 148
Configurer des sauvegardes automatiques • 149
Exploiter les images disque • 152
Fichiers hors connexion • 153
Configurer un répertoire en mode hors ligne • 154
Configurer les documents hors connexion • 155
Forcer les synchronisations de fichiers hors connexion • 156
Versionning de fichiers • 157
Mettre en place des quotas utilisateur • 158
En résumé • 159

9. Les stratégies de sécurité 161
Qu'est-ce qu'une stratégie de sécurité ? • 162
Les différents types de stratégies • 162
Les stratégies de comptes • 162
Les stratégies de droits utilisateur • 163
Les stratégies d'audit • 164
Les stratégies complémentaires • 164
Mettre en place une stratégie de sécurité • 165
Les modèles de stratégies • 166
Créer son modèle de sécurité • 167
Tester son modèle de sécurité • 168
Appliquer un modèle de sécurité • 169
En résumé • 169

10. Configurer le réseau 171
Le centre réseau et partage, centre névralgique de la configuration réseau • 172
Les connexions sans fil • 173
Se connecter à un réseau Wi-Fi • 174
Créer une connexion Wi-Fi ad hoc • 175
Modifier les paramètres des réseaux Wi-Fi configurés • 175
Connexion à un réseau VPN • 176
Afficher l'état de la connexion • 180
Statut de la connexion • 180
En ligne de commande • 181
Modifier les paramètres des cartes réseau • 182
Fenêtre Connexions réseau • 182
Propriétés de la carte réseau • 183
Modifier les options d'adresse IP • 184
Modifier les paramètres de partage • 185
Découverte du réseau • 186
Partage de fichiers et d'imprimantes • 186
Partage de dossiers publics • 186
Diffusion de contenu multimédia • 186
Sécurité des connexions de partage de fichiers • 187
Partage protégé par mot de passe • 187
Voir les ordinateurs du réseau • 187
Le groupe résidentiel d'ordinateurs • 188
Créer un groupe résidentiel • 188
Rejoindre un groupe résidentiel existant • 189
Modifier les paramètres du groupe résidentiel • 189
En résumé • 191

11. Sécurité des fichiers et partage de ressources ... 193
Les autorisations NTFS • 194
Modifier les autorisations standards • 195
Modifier les paramètres d'autorisation avancés • 196
Modifier le propriétaire d'un fichier ou d'un dossier • 198
Auditer l'accès aux fichiers et répertoires • 199
Partage de dossiers sur le réseau • 202
Utiliser l'assistant partage • 203
Utiliser le partage avancé • 204
Voir les dossiers partagés • 205
Définir les permissions pour les dossiers partagés • 206
Arrêter de partager un dossier • 207
Partager des fichiers via l'invite de commandes • 207
Afficher la liste des dossiers partagés • 207
Partager un dossier • 208
Supprimer un partage • 208
Visualiser la liste des fichiers partagés ouverts • 208
Partage d'imprimantes • 209
Configurer le serveur d'impression • 209
Se connecter à une imprimante partagée • 210
Ajouter une imprimante par la recherche automatique • 211
Ajouter une imprimante manuellement • 211

Ajouter une imprimante Ethernet ou Wi-Fi • 212
En résumé • 212

12. Optimiser le système 215
Optimiser le matériel • 216
Analyser les performances de l'ordinateur • 216
Informations et outils de performances • 216
Indice de performance • 217
Lancer l'évaluation • 217
Interpréter l'indice de base • 218
Interpréter les sous-indices • 219
Analyseur de performances : perfmon.exe • 219
Générer un rapport • 219
Performances en temps réel • 221
Moniteur de ressources • 222
Journal d'événements de performances • 223
Éliminer le superflu • 224
Désinstaller les logiciels inutilisés • 224
Faire le ménage dans les programmes de démarrage automatique • 224
L'utilitaire de configuration système MSConfig • 225
Autoruns, utilitaire de gestion des programmes de démarrage • 225
Nettoyer le disque dur • 226
Défragmenter le disque • 228
Comprendre la fragmentation • 228
Défragmenter le disque • 230
En ligne de commande • 231
Optimiser le paramétrage • 232
Modifier les paramètres visuels de Windows • 232
Modifier les options d'alimentation • 234
Améliorer les performances du système de fichiers • 235
Augmenter la mémoire cache avec ReadyBoost • 235
Optimiser la mémoire virtuelle • 237
En résumé • 239

13. Sécuriser son système..... 241
Surveiller et contrôler son système d'exploitation • 242
La checklist de sécurité • 243
La checklist de maintenance • 244
Les enjeux de la sécurité • 244
Se protéger des adwares et spywares • 245
Identifier les fichiers infectés avec l'analyse de Windows Defender • 246
Paramétrer finement Windows Defender • 247
Se protéger des virus • 248
Mettre en place et configurer le pare-feu Windows • 250
Activer ou désactiver le pare-feu Windows • 251
Configurer le pare-feu • 252
Configuration simple • 252
Configuration avancée • 253
Mettre en place une journalisation du pare-feu • 260
En résumé • 262

14. Des données accessibles de partout : mettre en place un serveur web et un FTP.....265
Mettre en place un serveur web • 266
Installer IIS • 266
Créer une page web • 268
Partager des fichiers • 271
Cas d'utilisation avancée d'un site web • 273
Authentification • 274
Compression • 275
En-têtes de réponse HTTP • 275
Exploration de répertoire • 275
Filtrage des demandes • 275
Journalisation • 276
Mappage de gestionnaires • 276
Mise en cache de sortie • 277
Modules • 277
Pages d'erreur • 278
Paramètres SSL • 278
Types MIME • 278
Mettre en place un serveur FTP • 279
Installer le service FTP • 280
Créer le serveur FTP • 280
Définir les accès des utilisateurs • 281
Paramétrage avancé du serveur FTP • 282
Authentification FTP • 282
Exploration des répertoires FTP • 283
Filtrages des demandes FTP • 283
Isolation d'utilisateur FTP • 284
Journalisation FTP • 284
Messages FTP • 285
Paramètres SSL FTP • 286
Prise en charge du pare-feu FTP • 287
Règles d'autorisation FTP • 288
Restrictions liées au domaine et à l'adresse Ipv4 • 288
En résumé • 289

15. Résoudre les problèmes de Windows 7 291

Restaurer le système • 292
Configurer la protection du système • 292
Restaurer un point de sauvegarde • 294
Que faire si la restauration n'a pas résolu le problème ? • 295
L'outil de résolution de problèmes • 296
Journal d'événements • 297
Comprendre le journal d'événements • 297
Exploiter le journal d'événements comme outilde diagnostic • 298
Analyser les journaux d'événements • 298
Trouver l'information pertinente • 300
Personnaliser les vues • 301
Exploiter le journal d'événements comme outil d'alerte • 303
Exploiter le journal d'événements comme outil d'agrégation • 306
Configurer les ordinateurs source • 306
Configurer l'ordinateur hôte • 307
Résoudre les problèmes du journal d'événements • 308
Pourquoi la tâche planifiée ne s'est-elle pas lancée lorsque l'événement s'est déclenché ? • 308
Pourquoi le journal d'événements est-il vide ? • 308
Pourquoi les événements arrivés il y a quelques jours sont-ils absents ? • 309
Pourquoi est-il impossible de se connecter à un ordinateur distant pour y récupérer les journaux d'événements ? • 309
Réparer un ordinateur qui ne démarre plus • 310
Afficher le menu de démarrage alternatif • 310
Dernière bonne configuration connue • 311
Le mode sans échec • 312
Outils de récupération système • 313
Vérifier l'état des fichiers système • 313
De l'aide à distance • 314
Se faire aider • 314
Activer l'assistance à distance • 315
La boîte à outils indispensable • 316
UltraVNC • 317
Les outils SysInternals • 317
Ultimate Boot CD • 318
Spybot Search & Destroy • 318
CCleaner • 318
ClamWin • 318
En résumé • 319

16. Personnaliser le panneau de configuration et les menus contextuels 321

Ajouter des éléments au panneau de configuration • 322
Créer un applet • 322
Créer un GUID • 322
Enregistrer le GUID dans le registre • 323
Enregistrer l'applet • 324
Afficher l'applet dans le panneau de configuration • 325
Ajouter des tâches • 325
Personnaliser l'icône de l'applet • 326
Afficher le bouclier de l'UAC à côté des tâches critiques • 327
Lancer une application à partir du titre de l'applet • 327
Personnaliser les menus contextuels du système • 328
Ajouter des options au menu contextuel de l'explorateur • 328
Ajouter des fonctionnalités Windows au menu contextuel • 329
En résumé • 331

17. PowerShell 333

PowerShell, langage de script de Windows • 334
Premier script • 334
PowerShell et le framework .NET • 336
Le langage PowerShell • 337
Les commandes • 337
Les alias • 338
Les pipelines • 339
Les expressions • 341
Interagir avec WMI • 341
PowerShell et le registre • 344
En résumé • 345

A. Raccourcis clavier 347

Raccourcis clavier généraux • 347
Raccourcis d'accessibilité • 349
Claviers possédant une touche Windows • 349
Raccourcis des boîtes de dialogue • 350
Raccourcis de l'explorateur Windows • 351
Raccourcis de la barre des tâches • 352
Raccourcis de la loupe Windows • 352
Raccourcis du Bureau à distance • 353
Raccourcis de Microsoft Paint • 353
Raccourcis de Microsoft WordPad • 354
Raccourcis de la calculatrice Windows • 355
Raccourcis généraux • 355
Mode Scientifique • 356

Mode Programmeur • 357
Mode Statistiques • 358
Raccourcis de l'aide Windows • 358
Raccourcis clavier Windows Media Center • 359
Raccourcis audio du Windows Media Center • 359
Raccourcis clavier pour contrôler la TV du Windows Media Center • 360
Raccourcis clavier pour la lecture de radios du Windows Media Center • 360
Raccourcis clavier pour la visualisation d'images du Windows Media Center • 360
Raccourcis clavier pour la lecture de vidéos du Windows Media Center • 361
Raccourcis clavier pour la lecture de DVD du Windows Media Center • 361

B. COMMANDES ET ALIAS DE POWERSHELL 363
Liste des commandes • 363
Liste des alias • 371

C. LA PLATE-FORME .NET 377
Une architecture particulière • 377
Un langage de développement pas comme les autres • 378
Des technologies innovantes • 379
Un avantage pour l'administrateur système • 380

INDEX 381

Avant-propos

Depuis une dizaine d'années, le système d'exploitation Windows a fait sa place au sein des entreprises, mais également dans nos foyers. Outil de notre vie de tous les jours, il nous permet de communiquer, de rechercher un emploi, de faire des achats à distance ou, plus généralement, de travailler.

Cependant, bien que Windows réponde à de très nombreuses problématiques, il est difficile pour l'utilisateur, novice ou averti, de connaître et de tirer parti de toutes les fonctionnalités que le système cache en son sein.

Pourquoi ce livre ?

Ce livre est né de notre volonté de présenter à tous les utilisateurs de Windows les fonctionnalités, finalités et avantages de Windows 7, le tout dernier système d'exploitation de Microsoft.

Que ce soit pour une utilisation personnelle ou professionnelle, ce livre vous guidera au fur et à mesure des problématiques que vous rencontrerez, et vous éclairera sur le fonctionnement interne du système. Nous espérons qu'il vous aidera ainsi à mieux appréhender le comportement de Windows 7 et ainsi à mieux l'utiliser au quotidien.

Notre objectif principal est de vous permettre d'acquérir rapidement les connaissances nécessaires pour exploiter au maximum les différentes fonctionnalités que vous propose votre OS. Nous tentons également de vous faire découvrir bon nombre des petites fonctionnalités cachées du système. Nous émaillons également notre propos de bonnes pratiques et de retours d'expérience : ainsi Windows 7 deviendra un outil parfaitement fiable et répondra à tous vos besoins.

À qui s'adresse cet ouvrage ?

Ce livre est destiné à tous ceux qui souhaitent s'initier ou compléter leurs connaissances sur ce vaste sujet qu'est l'administration d'un système d'exploitation Windows :

- les utilisateurs avertis qui désirent parfaire leur maîtrise de leur système ;
- les utilisateurs plus débutants, qui souhaitent acquérir les notions avancées ;
- les administrateurs système qui s'intéressent à la configuration avancée de Windows 7 (bien que certains points comme le déploiement ne soient pas abordés).

Structure de l'ouvrage

Chaque chapitre de ce livre traite une problématique particulière et regroupe thématiquement les fonctionnalités du système. Notre progression est calquée sur la pratique : nous commençons par la mise en place complète d'un système, avant de prendre nos marques lors de la première utilisation. Nous nous intéressons ensuite à la configuration et terminons par l'ajout de fonctionnalités complémentaires.

Néanmoins, il est tout à fait possible de vous rendre directement à un chapitre particulier sans avoir lu les précédents. De même, vous lirez probablement le chapitre PowerShell ou encore celui sur la résolution des problèmes lorsque la situation et le besoin se présenteront.

Le **chapitre 1** présente le nouveau système d'exploitation de Microsoft. Nous décrivons ses nouveautés, ses différentes versions et ses technologies principales afin de percevoir l'intérêt de migrer vers Windows 7.

Le **chapitre 2** présente les différentes étapes de l'installation de Windows 7, selon vos contraintes, qu'il s'agisse d'une installation standard, d'une mise à jour depuis une version antérieure de Windows ou bien d'une installation sur un disque virtuel.

Le **chapitre 3** montre les différents outils et interfaces du système qui vous serviront à paramétrer Windows pour répondre au moindre de vos besoins. Vous y découvrirez notamment comment utiliser le planificateur de tâches ou encore comment configurer les programmes par défaut et les types de fichiers.

Le **chapitre 4** décrit l'installation et la configuration du matériel et des périphériques. Nous nous intéressons au paramétrage du clavier, de la souris, mais également aux affichages multiples avec les vidéoprojecteurs, sans oublier le délicat paramétrage des imprimantes.

Le **chapitre 5** aborde la gestion des programmes et des fonctionnalités Windows. Vous découvrirez comment installer et supprimer des logiciels, mais également comment ajouter des fonctionnalités à votre système. Vous verrez dans un second temps comment bloquer l'utilisation de certains programmes ou bien comment contrôler l'installation des programmes selon les utilisateurs.

Le **chapitre 6** s'intéresse aux fichiers. Qu'il s'agisse de les chiffrer, d'optimiser leur accès grâce à l'indexation, de gagner de la place sur le disque grâce à la compression ou bien de garantir la disponibilité des données grâce aux partitions, vous gérerez vos fichiers avec virtuosité.

Le **chapitre 7** présente la gestion des comptes et groupes utilisateurs, leur intérêt et les stratégies de mise en place.

Le **chapitre 8** traite de la problématique des quotas de disque et de la gestion des fichiers hors ligne, afin de maîtriser la disponibilité à tout moment des données au sein du système.

Le **chapitre 9** présente la manipulation des stratégies de sécurité au sein du système. De leur mise en place à leur paramétrage, en passant par les techniques de déploiement, vous y découvrirez toutes les bonnes pratiques à avoir pour garder la main sur votre système.

Le **chapitre 10** explique comment mettre en place un réseau et comment s'y connecter. Qu'il soit filaire ou Wi-Fi, nous apprendrons ici à partager fichiers et périphériques distants.

Le **chapitre 11** s'intéresse à la sécurité des fichiers. Nous commençons par les restrictions de sécurité limitant l'accès de certaines ressources, puis nous détaillons la manière d'ouvrir l'accès aux ressources pour les partager avec d'autres utilisateurs du réseau.

Le **chapitre 12** décrit différentes solutions afin d'améliorer la rapidité et la réactivité du système. Nous n'y abordons que les principales améliorations dont l'efficacité n'est plus à prouver.

Le **chapitre 13** traite de ce sujet sensible qu'est la sécurité. Qu'il s'agisse de *malwares*, de virus ou d'attaques, nous envisageons les différents moyens de protection disponibles et décrivons leur configuration.

Le **chapitre 14** est un exemple d'utilisation avancée d'un système Windows : il explique comment transformer son ordinateur de bureau en serveur web ou en serveur FTP.

Le **chapitre 15** présente les différentes manières de résoudre les problèmes de Windows. Nous nous appuyons sur de bonnes pratiques, mais surtout sur des méthodologies de prévention éprouvées.

Le **chapitre 16** montre comment adapter le système à ses besoins. Les utilisateurs en quête d'efficacité apprendront à modifier le système et à

l'améliorer en intégrant des outils ou de nouvelles fonctionnalités au sein des différentes interfaces.

Le **chapitre 17** présente les bases de PowerShell, la nouvelle technologie de *scripting* de Microsoft. Nous détaillons également des cas d'utilisation avancée, afin de vous donner envie d'approfondir ce vaste sujet.

Remerciements

Nous tenons en premier lieu à remercier les éditions Eyrolles pour nous avoir soutenus et accompagnés tout au long de la rédaction de ce livre, et plus particulièrement Muriel Shan Sei Fan et Sandrine Paniel. Nous remercions également Romain Pouclet pour sa relecture et ses conseils avisés.

Je remercie tous ces *Microsoftees*, Lucas Riedberger (*aka* Malabar), Antoine Emond (*aka* le BG), Mitsuru Furuta (mon idôle ;-)), Vincent Bellet (*aka* ma poule) et tant d'autres qui, au fil des années, m'ont transmis leur passion et leurs connaissances des produits Microsoft. Un grand merci à Marie Molinié, Sophie Galais et Virginie Freire, trois personnes qui me sont chères et qui m'ont soutenu durant ces quelques mois malgré le peu de temps que je pouvais leur consacrer. Un merci spécial à mes parents qui ont toujours cru en moi et m'ont toujours donné les moyens de réaliser mes envies. Enfin, merci à Thomas Garcia pour m'avoir accompagné dans cette aventure, et pour avoir résisté à mon (sale) caractère !

Louis-Guillaume Morand

lgm@lgmorand.com
http://www.lgmorand.com

Je remercie Louis-Guillaume pour m'avoir fait confiance et pour m'avoir permis de participer à ses cotés à la rédaction de cet ouvrage. Je remercie également mes parents, et je pense tout particulièrement à ma maman qui traverse actuellement une épreuve difficile.

Thomas Garcia

thomas.garcia.12@gmail.com


7
TM

chapitre 1

Windows 7, un nouveau système d'exploitation

Bien des raisons peuvent expliquer votre choix de Windows 7 : vous êtes déçu de Windows Vista, vous venez d'acquérir un ordinateur prééquipé de Windows 7, ou bien vous avez simplement le goût de la nouveauté. Il est temps d'apprendre à découvrir (ou redécouvrir) ce système et de profiter au maximum des fonctionnalités qu'il propose.

SOMMAIRE

- Comprendre ce qu'est un système d'exploitation
- S'orienter parmi les différentes éditions de Windows 7
- Les nouveautés

MOTS-CLÉS

- Interface graphique
- Histoire
- Connexion au réseau
- Task-list
- Aero
- Home Group
- Agil VPN
- BitLocker
- SafeGard
- Éditions
- 64 bits

Ce chapitre présente le nouveau système d'exploitation Windows 7, depuis son histoire jusqu'à ses nouvelles fonctions, en passant par ses différentes versions.

Windows 7 (prononcez *sept*) est le petit dernier d'une série de systèmes d'exploitation commencée il y a presque 25 ans. Comme toute nouvelle version, celle-ci apporte son lot de nouveautés que nous allons vous présenter dans les grandes lignes.

Principe d'un système d'exploitation

Le système d'exploitation (*Operating System* ou OS en anglais) est le logiciel qui permet à l'ordinateur d'exécuter des programmes sur un ordinateur. Il assure pour cela la liaison entre trois parties :

- les composants physiques (processeur, carte mère, mémoire vive, etc.) ;
- les programmes (jeux, suite bureautique…) ;
- l'utilisateur.

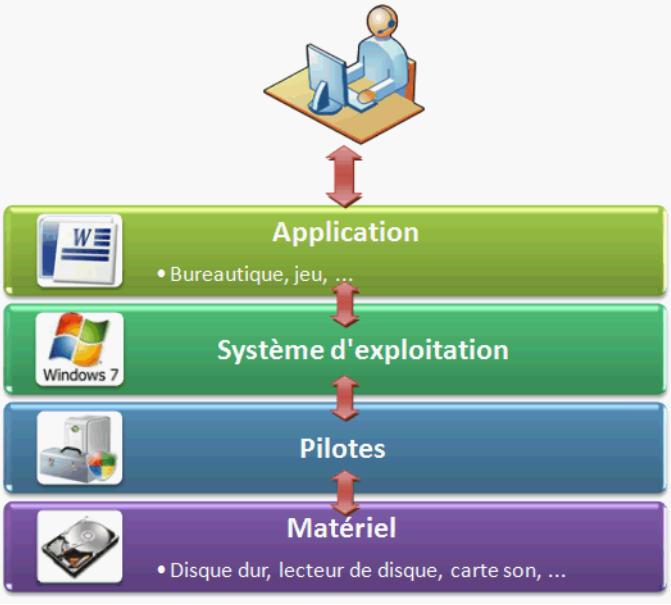


Figure 1–1
Rôle du système d'exploitation

Aux développeurs et aux utilisateurs, il permet de s'affranchir de la complexité de la machine physique (contrôler la mémoire, les informations envoyées au processeur, écrire sur les disques durs, qu'importe leur système de fichiers, etc.). Le système d'exploitation remplit donc plusieurs rôles.

Tout d'abord, il assure l'allocation des ressources du processeur aux différentes applications qui le demandent. À l'aide d'un algorithme d'ordon-

nancement, il valorise un processus plutôt qu'un autre et donne ainsi l'impression que plusieurs tâches sont exécutées en parallèle. Avant l'apparition des processeurs à plusieurs cœurs, c'était impossible.

Le système d'exploitation gère ensuite la mémoire physique (également appelée mémoire vive). Cette mémoire fonctionne sur un principe d'accès aléatoire (d'où son appellation anglaise *Random Access Memory* ou RAM), et permet de stocker temporairement des informations utiles aux processus en cours d'exécution. Sur les ordinateurs actuels, on trouve en général entre 2 et 4 Go de mémoire vive. Lorsque cette mémoire est saturée, le système d'exploitation peut en décharger une partie sur le disque dur grâce à un système dit de mémoire virtuelle ou *swap*.

Comme nous l'avons vu précédemment, le système d'exploitation établit la communication avec les composants physiques de la machine. Cette communication s'établit via les pilotes (en anglais *drivers*), programmes écrits par les constructeurs des composants. Ces programmes permettent d'envoyer des instructions au composant et de traiter les informations reçues en retour. Le système d'exploitation est ainsi capable de communiquer avec les disques durs ou la carte graphique, mais également avec les périphériques externes comme la souris, le clavier ou l'imprimante.

Enfin, la gestion du système de fichiers est assurée par le système d'exploitation. Le système de fichiers définit la façon dont les données sont stockées sur le disque dur, assurant ainsi la lecture et l'écriture des données et fichiers. Ce processus s'accompagne bien entendu de plusieurs vérifications : le fichier est-il modifiable (donc pas en mode lecture seule) ? l'utilisateur a-t-il les droits pour consulter et/ou modifier ce fichier ?, etc.

Le système d'exploitation est également capable de communiquer avec d'autres machines sur le même réseau ou sur des réseaux distants.

Dotés d'une IHM (Interface Homme-Machine), les systèmes d'exploitation permettent à l'utilisateur de communiquer avec l'ordinateur via une interface graphique. Cette interface est très évoluée dans la dernière version de Windows. L'amélioration de son ergonomie permet une meilleure expérience utilisateur. Dans les systèmes d'exploitation modernes, il est désormais possible d'utiliser de nouveaux modes de saisie de données comme la reconnaissance de la voix ou de l'écriture.

Un système d'exploitation est donc un organe logiciel essentiel de l'ordinateur. Sans lui, rien ne pourrait fonctionner et c'est grâce à lui que vous pouvez utiliser vote ordinateur au quotidien pour effectuer du traitement de texte, retoucher vos photos numériques, surfer sur Internet ou encore jouer à vos jeux favoris.

Voyons maintenant ce qui fait de Windows 7 un OS pas tout à fait comme les autres.

TECHNIQUE Système de fichiers NTFS

Le système de fichiers de Windows 7 est NTFS (*New Technology File System*). Il est présent dans les systèmes Windows depuis Windows NT. Il permet notamment la configuration d'autorisations (ACL), le chiffrement des fichiers via EFS (*Encrypting File System*) et la compression des fichiers.

HISTOIRE ENIAC : le premier ordinateur

L'ENIAC est le tout premier ordinateur électrique. Il pesait 30 tonnes et avait une surface au sol de 167 m². Au niveau puissance de calcul, il était moins puissant qu'une simple calculatrice de poche que vous achèteriez aujourd'hui.

Culture Histoire de Microsoft Windows

Microsoft Windows 7 est le tout dernier système d'exploitation produit par Microsoft. Il est le fruit d'années de recherches et d'évolutions tirant expérience des précédentes versions de Windows éditées depuis plusieurs années. L'évolution de ce système d'exploitation, de ses tout premiers pas à la version actuelle, est intéressante à tous points de vue, notamment lorsque l'on retrace ses évolutions majeures au fil des versions. Si pour vous, le fait d'avoir un menu *Démarrer*, de pouvoir visionner une vidéo ou encore simplement d'afficher des fenêtres à l'écran vous semble acquis, vous verrez au fur et à mesure de ce chapitre, que ce fut loin d'être toujours le cas.

L'aventure de Microsoft a commencé un matin d'avril 1975 lorsque William Henri Gates III (dit Bill Gates) et Paul Allen, deux jeunes (20 et 22 ans) férus d'informatique forment la société Micro-Soft (avec le tiret !). Le nom ne deviendra définitivement Microsoft que plusieurs mois plus tard. Parallèlement, la société Apple créée par Steve Jobs et Steve Wozniak est lancée au cours du mois d'avril de l'année 1976 avec pour objectif de vendre un micro-ordinateur.

En ce temps-là, l'informatique n'en est qu'à ces balbutiements et Microsoft n'a alors pour objectif que de commercialiser un logiciel : Microsoft Basic. Il s'agit-là du tout premier logiciel destiné à être commercialisé. C'est ce premier logiciel, mis en avant sur le marché grâce à un gros contrat avec IBM, qui permettra à Microsoft d'engranger ses premiers fonds et de commencer plusieurs projets informatiques.

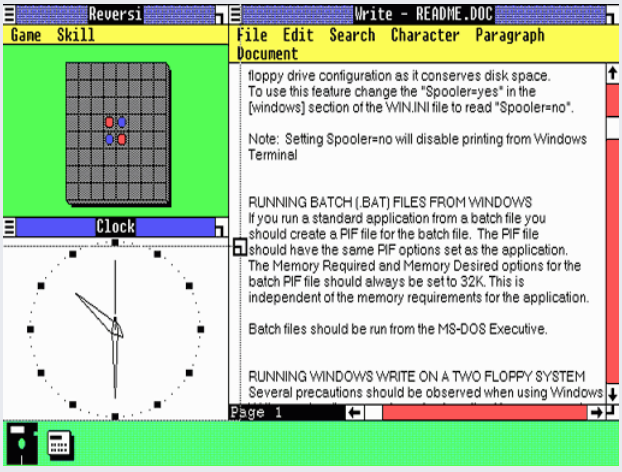


Figure 1–2 Interface de Microsoft Windows 1.0

Le déclic de l'idée d'éditer un système d'exploitation a lieu en 1981, Microsoft rachète pour seulement 50 000 $ tous les droits concernant QDOS, alors développé par un certain Tim Patterson de Seattle Computer Products (SCP), qui deviendra MS-DOS. C'est en étant installé sous une version modifiée nommée PC-DOS sur le nouvel IBM 5150, que MS-DOS fait son apparition dans l'univers du grand public. Depuis ce jour, MS-DOS ne cessera d'envahir le marché et s'imposera rapidement face à une concurrence réduite et dépassée.

Le 10 novembre 1983, Microsoft dévoile Windows 1.0, sa première mouture de système d'exploitation. Doté d'une interface graphique, et basé sur MS-DOS, voici le socle des premières applications de traitement de texte et d'images et d'affichages de graphes.

Un an plus tard, le 24 janvier 1984, c'est au tour d'Apple de lancer son nouveau système : Macintosh.

S'en suivent les versions Windows 2.0 (1987) et Windows 3.0 (1990) qui constituent enfin un vrai système d'applications fenêtrées. Ils apportent également les notions d'icônes, la gestion des couleurs et surtout un gestionnaire de fichiers, ancêtre de l'explorateur Windows.

Le premier ordinateur (ENIAC) avait fait son apparition en 1946, il aura fallu attendre 44 ans pour entrevoir un système d'exploitation ressemblant aux systèmes actuels.

Ce n'est qu'en 1993 que Microsoft annonce la sortie de Windows NT 3.1 (NT pour *New Technology*). Contrairement à ce que l'on pourrait croire, il ne s'agit pas d'une version succédant à Windows 3.0, mais bel et bien d'un système repris de zéro afin de fournir une base stable pour le développement de futurs systèmes d'exploitation professionnels répondant aux besoins des entreprises.

En 1995, Windows 1995, premier système possédant une barre des tâches, se destine au grand public. À cette époque, Windows est présent sur une majorité des ordinateurs du monde. La version 1995 sera vite remplacée par Windows 98, qui tire meilleur parti des ordinateurs 32 bits et prend en charge les périphériques USB. Au même moment, la version professionnelle de Windows, Windows NT, sort en version 4.0. Un peu plus tard, Windows 2000 sort, version de Windows que beaucoup d'informaticiens ont apprécié pour sa stabilité au point de la préférer aux versions futures telles que Windows XP (sorti en 2001) et Windows Vista, sorti fin 2006.

Si Windows XP a conquis les foyers en tant que système très facile à utiliser par les néophytes, Windows Vista a essayé une façon plus contrôlée et plus sécurisée d'utiliser son ordinateur, – et en même temps plus intuitive. Une trop grande sécurité (confirmation demandée à l'utilisateur à chaque action), des problèmes de pilotes, et une certaine lenteur lui sont reprochées par de nombreux utilisateurs et Microsoft a dû prendre en compte ces aspects dans le développement de son nouveau système, Windows 7. C'est d'ailleurs après de nombreuses plaintes des utilisateurs peu enclins à passer à Windows Vista, que Microsoft a décidé d'assurer le support de Windows XP plus longtemps que prévu.

Le chemin parcouru pour en arriver à Windows 7 ne fut donc pas simple. Plusieurs objectifs ont été fixés pour le développement de cette dernière version :

- mettre en œuvre une sécurité fiable mais non intrusive ;
- améliorer les performances ;
- améliorer la gestion des pilotes ;
- améliorer l'ergonomie et la facilité d'utilisation.

Pour un article complet sur l'histoire de Microsoft, lisez l'introduction d'Aurélien Regat-Barrel :

- http://arb.developpez.com/histoire-microsoft-windows/

Les nouveautés de Windows 7

Windows 7 arrive avec son lot d'améliorations et de nouveautés. Celles-ci touchent plusieurs éléments clés du système : l'interface graphique bien sûr, mais également la sécurité, la mobilité, le réseau et l'administration du système.

Interface graphique

Les plus gros changements sont perceptibles au niveau de l'interface. On peut tout d'abord remarquer que la barre des tâches a été remaniée, tant au niveau esthétique qu'au niveau fonctionnel. Les vignettes qui apparaissent au survol de la souris sont légèrement plus grandes, ce qui en améliore la visibilité mais c'est surtout l'aspect graphique des icônes qui a été revu. Dans Windows 7, les applications sont représentées par des icônes carrées, pouvant être fixées à la barre des tâches, comme c'est le cas avec le Dock du système d'exploitation d'Apple.

Figure 1–3
Barre des tâches de Windows 7

Figure 1–4
Dock du système d'exploitation Mac OS

Il est possible de réorganiser les icônes représentant les programmes par simple glisser-déposer afin de les placer dans l'ordre de son choix. Notons également que le clic droit a maintenant une plus grande importance dans la barre des tâches : pour chaque élément présent dans celle-ci, le clic droit permet d'accéder à un certain nombre de raccourcis propres à chaque programme. Nommée *task-list*, cette fonctionnalité permet ainsi de lancer un document récent de son choix simplement en cliquant avec le bouton droit sur l'icône Microsoft Word sans à avoir à ouvrir l'application. Il s'agit là d'un gain de temps certain.

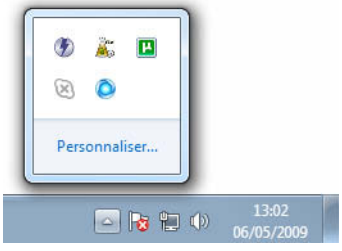


Figure 1–5
La zone de notification

En bas à droite de l'écran, la zone de notification système est désormais mieux gérée et n'affiche plus que les icônes les plus importantes. Les autres icônes sont accessibles en cliquant sur la petite flèche présente dans la zone de notification.

Enfin, le dernier point à remarquer sur cette nouvelle barre des tâches est le bouton semi-transparent présent à l'extrémité droite. Si vous avez activé l'interface Aero, un simple survol de ce bouton avec la souris affiche toutes les fenêtres ouvertes en transparence sur l'écran. En cliquant sur le bouton,

toutes les fenêtres sont réduites et le Bureau apparaît. Ceci remplace l'icône *Afficher le bureau* qui était présente dans la barre de lancement rapide depuis les toutes premières versions de Windows.

Connexion aux réseaux et mobilité

L'accès à tous les réseaux sans fil (qu'il s'agisse de Wi-Fi ou de 3G) et le paramétrage des réseaux filaires se gèrent et se configurent désormais grâce à une seule et même interface : *Centre Réseau et partage*.

La configuration d'un réseau domestique (petit réseau familial contenant plusieurs ordinateurs) a été facilitée dans Windows 7 grâce à l'arrivée de Home Group (Groupe résidentiel). Home Group propose un réseau logiciel au sein d'un réseau physique et facilite à l'extrême le partage de ressources en transformant chaque ordinateur du réseau en serveur multimédia, de façon sécurisée et contrôlée.

Pour configurer un Home Group, il suffit de noter le code fourni par l'assistant de création et de l'enregistrer dans tous les ordinateurs devant faire partie du groupe. Les groupes sont conçus de manière à partager rapidement et facilement des documents ou des fichiers multimédias au sein du réseau.

VOUS VENEZ DE WINDOWS VISTA

Configuration de l'accès aux réseaux

Sous Windows Vista, le centre de réseau proposait plusieurs assistants tant pour la définition des réseaux sans fil, que pour la configuration générale des réseaux (partage d'imprimante, découverte des ordinateurs, etc.). Dans Windows 7, le nombre d'assistants est réduit tout en permettant plus de liberté (comme définir des configurations différentes pour chaque réseau).

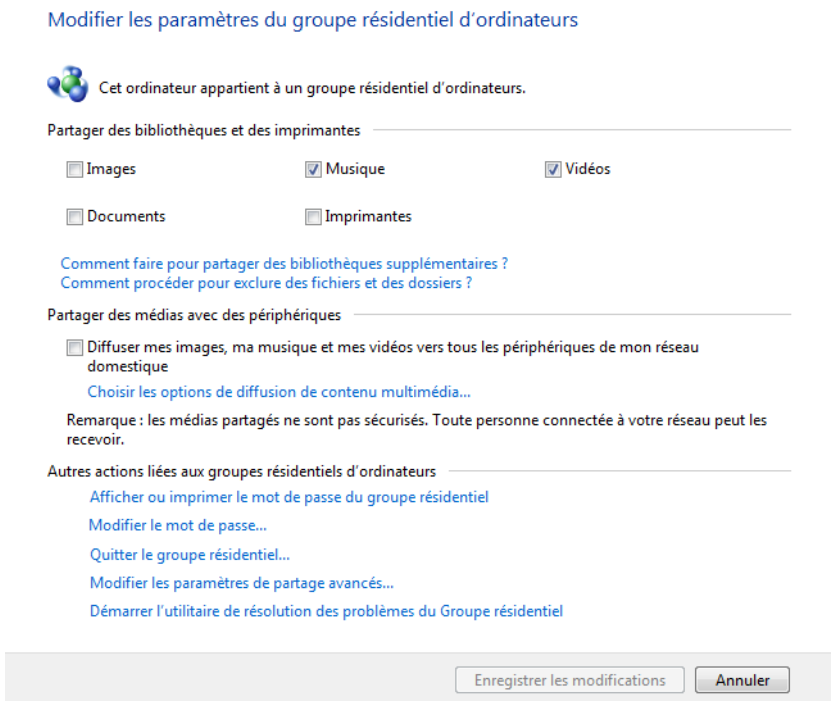


Figure 1–6
Interface simplifiée de partage de ressources

Autre nouveauté de Windows 7, Agile VPN permet aux utilisateurs de connexions VPN (*Virtual Private Network*) de ne plus rencontrer de problème de reconnexion à leur VPN après une coupure réseau. En effet, après déconnexion intempestive du réseau VPN, la connexion au VPN se rétablit automatiquement dès qu'il est de nouveau disponible, et ce, de façon transparente pour l'utilisateur.

Au niveau entreprise, l'une des nouveautés à souligner est Direct Access. Il s'agit d'un mécanisme permettant la connexion au système d'information de l'entreprise en englobant un ensemble de technologies sous-jacentes. Cette technologie a pour vocation de remplacer les réseaux VPN, souvent trop complexes à mettre en place, afin de permettre aux utilisateurs finaux de ne plus se soucier de la configuration de la connexion au réseau d'entreprise. Cette connexion s'effectue de manière transparente par Direct Access.

Une nouvelle version du client du bureau à distance (client Terminal Server) est présente dans Windows 7. Cette nouvelle version s'appuie sur le nouveau protocole RDP 7.0 (*Remote Desktop Protocol*) qui introduit notamment la communication audio bidirectionnelle et l'utilisation à distance d'Aero et de DirectX.

La connexion de vidéoprojecteurs est facilitée par l'apparition d'une nouvelle interface qui permet de choisir rapidement les réglages souhaités.

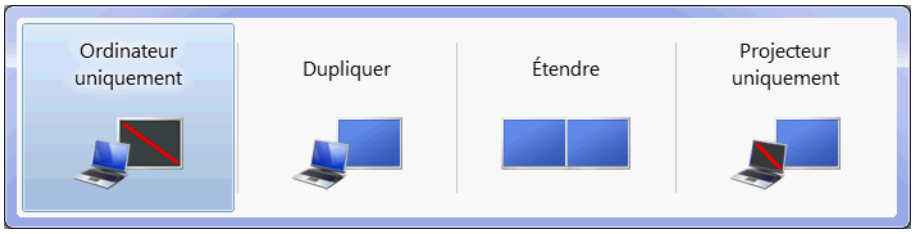


Figure 1–7
Fenêtre de configuration rapide du vidéoprojecteur

Windows 7 propose également une solution qui optimise les réseaux d'agences. En effet, la nouvelle solution Branch Cache met en cache les données présentes sur l'intranet de l'entreprise ou sur des serveurs de fichiers. Ainsi, les employés des filiales, lorsqu'ils se trouvent à distance, ne subiront plus de latence dans le téléchargement de données depuis leur maison mère.

Sécurité

Lors d'une installation par défaut de Windows 7, les disques durs sont automatiquement préparés pour utiliser BitLocker. Cette fonctionnalité de chiffrement des disques internes sécurise les données du disque dur qui ne seront lisibles que sur cet ordinateur et uniquement par l'utilisateur qui les a chiffrées.

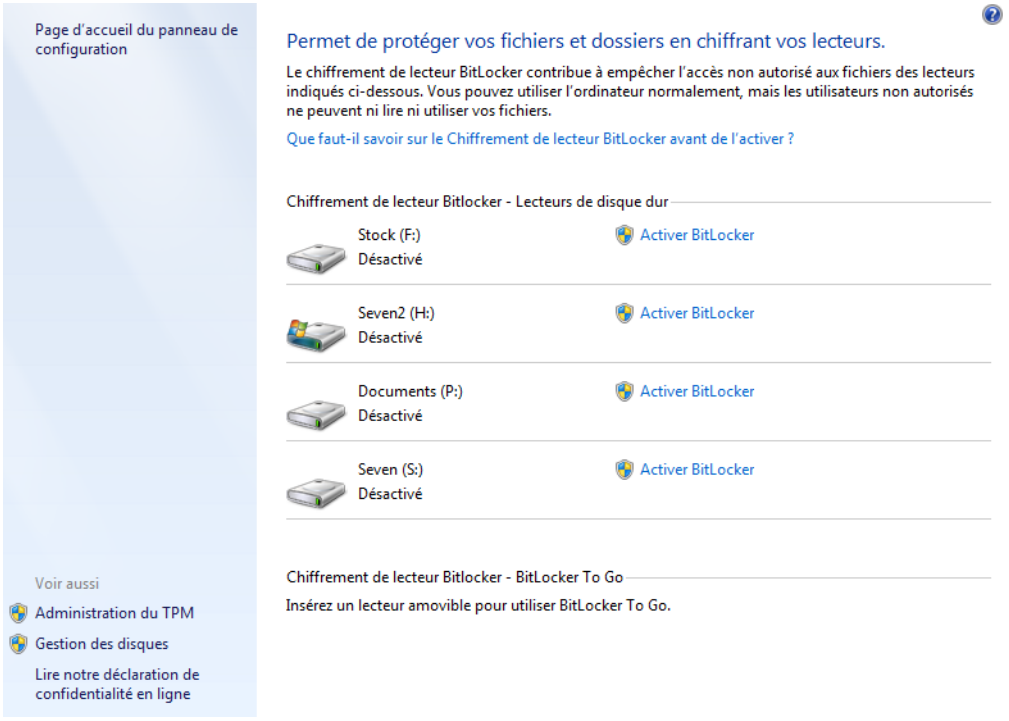


Figure 1–8
Console de gestion BitLocker

Les périphériques de stockage externes tels que les clés USB ou les disques durs externes ne sont bien évidement pas oubliés puisque Windows 7 comprend également BitLocker To Go. Cette fonctionnalité est l'équivalent de celle que nous venons de citer, mais pour les disques amovibles.

Enfin, toujours à propos de sécurité, notons que Windows 7 supporte nativement le protocole DNSSEC (*Domaine Name System Security Extension*) qui pallie les problèmes de sécurité liés aux DNS, tels que le déni de service (*DoS Attack*) ou encore l'interception de paquet.

Administration du système

Windows 7 a également été conçu de manière à faciliter le déploiement, le suivi et l'administration des postes de travail en entreprise. Il est possible pour les administrateurs de gérer les postes de travail, qu'ils soient connectés ou non au réseau local.

Souvent désactivé par les utilisateurs, rarement apprécié à cause de son caractère intrusif, mais cependant fort utile, le contrôle des comptes utilisateur (ou UAC, *User Account Control*), apparu avec Windows Vista, a été amélioré dans Windows 7 afin d'apporter plus de souplesse et de confort. Auparavant, le seul choix de configuration possible était de l'activer ou de

le désactiver. Avec Windows 7, il est maintenant possible de choisir le niveau de protection souhaité, du plus permissif au plus strict.

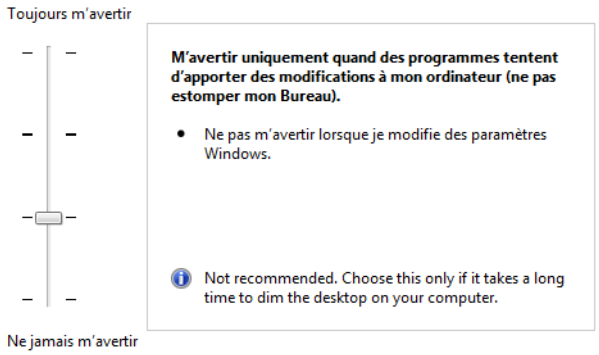


Figure 1–9
Panneau de configuration du contrôle utilisateur

Grâce à une nouvelle fonctionnalité baptisée SafeGuard, il est possible de créer un compte utilisateur qui ne sauvegardera aucun changement opéré par l'utilisateur. Qu'il s'agisse des fichiers téléchargés, des fichiers temporaires, des historiques de navigation ou encore de la personnalisation du Bureau, tout sera automatiquement rétabli à l'état initial dès que l'utilisateur fermera sa session.

Les administrateurs système pourront également contrôler l'exécution des applications sur le système grâce à AppLocker qui définit les droits d'exécution de chaque application.

Autre nouveauté, PowerShell V2 est intégré par défaut à Windows 7. Il s'agit d'un langage de script comptant près de 130 commandes exécutables pour administrer le système d'exploitation. Avantage de taille, les administrateurs ont ainsi la possibilité de lancer des scripts PowerShell à distance.

Les différentes éditions de Windows 7

À l'instar de Windows Vista, Windows 7 est décliné en plusieurs versions proposant des fonctionnalités bien différentes. Chaque version est destinée à un public particulier et possède un prix propre, relatif au nombre de fonctionnalités qu'elle possède. L'intérêt de dériver un même produit en plusieurs versions est de permettre à tout un chacun de n'acheter que le produit correspondant à ses besoins sans être contraint d'acquérir une version complète et onéreuse destinée uniquement au marché professionnel. Windows 7 est distribué en six versions distinctes.

Édition Starter, version minimaliste

Cette version minimaliste ne comprend pas l'interface Aero Glass. Elle est destinée à être installée sur des ordinateurs dont les performances sont limitées. Cette version n'est disponible qu'en édition 32 bits et ne permet l'exécution que de trois applications simultanément. Ce nombre ne prend pas en compte les applications système telles que l'explorateur Windows ou encore les outils comme l'antivirus. En revanche, toute autre application comme Internet Explorer ou Word est prise en compte dans cette limitation. Dans cette version, la gestion du réseau s'avère fortement simplifiée.

TECHNIQUE Processeurs 32 et 64 bits

Les nombres 32 et 64 bits font référence à la taille des données manipulées par le processeur. Un processeur 64 bits peut donc traiter bien plus de données qu'un processeur 32 bits au même instant, et peut utiliser plus de 4 Go de mémoire, limite de l'espace adressable par un processeur 32 bits, c'est-à-dire la taille maximale des instructions (opérations) qu'il peut charger en mémoire pour les utiliser. Plus les instructions sont grandes, plus les tâches peuvent être importantes.

Édition Familiale (Home Edition Basic), pour les pays émergents

L'édition Familiale (dite *basic*) est, quant à elle, réservée aux pays émergents comme le Brésil, la République de Chine, l'Inde, l'Indonésie, le Mexique, le Pakistan, les Philippines et bien d'autres encore. Comme la version Starter Edition, elle n'est disponible qu'en version 32 bits et possède une interface allégée (sans Aero Glass). Le nombre d'applications lancées simultanément n'est pas limité.

Cette version, comme la Starter Edition, n'est pas capable de lire les DVD.

CULTURE Aero Glass

Aero Glass est le nom de code donné à la nouvelle interface graphique de Windows (apparue avec Vista) qui apporte des effets de transparence, de 3D et des animations sur les fenêtres. Aero signifie Authentique, Énergétique, Réfléchi et Ouvert (*Authentic, Energetic, Reflective and Open*).

Édition Familiale Premium (Home Premium)

Il s'agit de la version grand public et qui, de par ses fonctionnalités, répond aux besoins de 75 % des utilisateurs. Cette version, capable de tourner sur tout type d'ordinateur récent, y compris les netbooks, possède un grand nombre de fonctionnalités supplémentaires. Nous pouvons y compter :

- l'interface Aero Glass ;
- une navigation Windows avancée (le thème d'affichage Aero Glass, Aero Background, des fonctionnalités telles ques le Switch3D (*Windows+Tab*) ou encore les miniatures de prévisualisation dans la barre des tâches) ;
- une fonctionnalité de partage réseau simplifiée ;
- une version améliorée de Windows Media Center, permettant le visionnage de photos, vidéos, DVD et l'écoute de musique ;
- un support amélioré des codecs vidéo (WMV, WMA, MEPG-4, H.264) ;
- une reconnaissance tactile améliorée (pour les ordinateurs ou écrans tactiles) ;
- une série de petits jeux Premium.

CULTURE Netbook versus ultra-portable

Le terme *netbook* est utilisé pour parler des ordinateurs portables de très petite taille (diagonale inférieure à 12 pouces). Pour les tailles supérieures, nous utilisons le terme ultra-portable, puis portable.

Édition Professionnelle (Professional)

Il s'agit cette fois de la version destinée aux utilisateurs des petites et moyennes entreprises. Cette édition permet notamment de joindre un domaine réseau d'entreprise. Elle contient également et surtout des utilitaires de chiffrement pour protéger les données sensibles. On y trouve également un utilitaire de sauvegarde réseau, servant à copier les fichiers importants sur un autre ordinateur ou périphérique réseau.

Version fétiche des professionnels utilisant leur ordinateur portable aussi bien à domicile qu'en entreprise, elle possède une fonction de reconnaissance du réseau et de détection de l'imprimante par défaut. Il n'est donc plus nécessaire de reconfigurer l'imprimante à chaque fois que l'on change d'environnement. D'une certaine manière, cette version correspond à la Familiale Premium enrichie de fonctionnalités propres au monde de l'entreprise.

Il est également possible de mieux contrôler un ensemble d'ordinateurs utilisant la version Professionnelle à l'aide de Stratégies de Groupe, thème que nous aborderons au chapitre 10.

Édition Entreprise (Business)

L'édition Entreprise est, quant à elle, destinée aux grandes entreprises et n'est achetable qu'en grande quantité (500 licences ou plus). Destinée à des parcs informatiques complexes, elle possède également quatre nouvelles fonctionnalités (que nous décrirons en détail dans le chapitre suivant). Il s'agit de :

- BitLocker et BitLocker To Go, fonctionnalités de chiffrement de données.
- DirectAccess qui permet la mise en place d'une connexion à un réseau d'entreprise sans recourir à un VPN.
- BranchCache qui fonctionne avec Windows Serveur 2008 R2. Cette fonctionnalité sert à mettre en cache les fichiers les plus utilisés, afin de limiter les transferts réseau et de préserver la bande passante.
- AppLocker permet à un administrateur d'interdire l'exécution de certaines applications.

Cette version propose également des fonctionnalités de virtualisation qui permettent notamment de faire tourner des applications spécifiques à Windows XP, qui ne tourneraient pas sur Windows 7.

Virtualisation

La virtualisation consiste à faire fonctionner plusieurs systèmes d'exploitation simultanément sur un même ordinateur. Cela peut se réaliser via des techniques matérielles ou logicielles.

Édition Intégrale (Ultimate)

Comme c'était déjà le cas avec Vista, la version Intégrale de Windows 7 regroupe à elle seule toutes les fonctionnalités disponibles sur les autres versions. C'est donc une version principalement destinée aux grandes entreprises ou aux professionnels de l'informatique qui souhaitent profiter pleinement des fonctionnalités de ce nouveau système d'exploitation.

Sur ces six versions, seules trois peuvent être achetées dans le commerce. Il s'agit des versions Familiale Premium, Professionnelle et Intégrale. Les trois autres sont distribuées par les fabricants d'ordinateurs de bureau ou d'ordinateurs portables et préinstallées sur les ordinateurs vendus.

Quelle version choisir ?

Cette simple question peut en réalité se révéler un peu plus complexe qu'il n'y paraît, et nécessiter de prendre le temps de faire la liste des besoins auxquels on veut répondre avec son ordinateur.

S'orienter parmi les différentes versions

Pour ceux qui penseraient qu'il est plus simple de payer la version la plus complète (et la plus chère par la même occasion), sachez que Mike Ybarra, directeur général de la division Windows de Microsoft explique que « pour la majorité des clients, le choix est vraiment simple : soit Windows 7 Édition Familiale Premium soit Windows 7 Édition Professionnelle. La version Intégrale ne se destinant donc qu'à un public averti ayant des besoins particuliers et bien souvent relatifs au monde de l'entreprise et aux très grands réseaux ».

Néanmoins, si vous hésitez encore, ce tableau comparatif devrait vous aider à prendre une décision.

Tableau 1–1 Comparatif des versions de Windows 7

	Édition Familiale (Basic)	Édition Familiale Premium	Édition Professionnelle	Édition Entreprise et Édition Intégrale
Groupe Résidentiel (Home Group), ou le partage simplifié	Oui	Oui	Oui	Oui
Barre des tâches améliorée	Oui	Oui	Oui	Oui
Prévisualisation miniature	Oui	Oui	Oui	Oui
Support avancé du réseau	Oui	Oui	Oui	Oui
Centre de configuration de la mobilité	Oui	Oui	Oui	Oui
Aero Glass		Oui	Oui	Oui

Tableau 1–1 Comparatif des versions de Windows 7 (suite)

	Édition Familiale (Basic)	Édition Familiale Premium	Édition Professionnelle	Édition Entreprise et Édition Intégrale
Windows Media Center		Oui	Oui	Oui
Support Média Amélioré		Oui	Oui	Oui
Réseau facile, configuration simplifiée		Oui	Oui	Oui
Multi-Touch		Oui	Oui	Oui
Intégration aux domaines d'entreprise			Oui	Oui
Chiffrement de fichier			Oui	Oui
Détection des imprimantes			Oui	Oui
Bureau à distance			Oui	Oui
BitLocker				Oui
AppLocker				Oui
BranchCache				Oui
DirectAccess				Oui
Support du multilangage				Oui
Démarrage depuis un disque dur virtuel (VHD)				Oui

Choisir la version 32 bits ou 64 bits ?

Dernier détail qu'il faut prendre en compte lors de l'achat d'une version boîte de Windows 7 et surtout lors de l'installation : le choix entre la version 32 bits et la version 64 bits. Dans l'absolu, tout nouvel ordinateur neuf acheté en 2009 (à l'exception des ordinateurs premiers prix possédant des processeurs vieillissants Celeron, Sempron, ou Pentium 4) sera doté d'un processeur utilisant une architecture 64 bits. L'architecture 64 bits permettant de réaliser plus de calculs à un moment donné que l'architecture 32 bits, un ordinateur 64 bits est par conséquent logiquement plus rapide qu'un ordinateur 32 bits pour réaliser une même tâche, à condition que le système d'exploitation, ici Windows 7, soit optimisé pour utiliser cette architecture processeur. Une première réaction pourrait donc être d'acheter et d'installer une version 64 bits de Windows 7.

Malheureusement, les choses sont plus complexes que cela, et choisir une version 64 bits pourrait s'avérer plus gênant qu'autre chose. Elle possède en effet certains inconvénients à prendre en considération :

- Une installation de Windows 7 64 bits prend plus d'espace disque que la version 32 bits. Il en sera de même pour les pilotes de périphériques ou les applications spécifiques au 64 bits.

- Il est plus difficile de réaliser un programme ou un pilote 64 bits, ce qui peut causer des problèmes pour trouver des pilotes de périphériques. Prenons un exemple simple : il est courant qu'un fabricant de webcams ne fournisse le pilote que pour les versions 32 bits de Windows. Votre périphérique est alors inutilisable sur une version 64 bits. Windows 7 est livré avec un certain nombre de pilotes préinstallés et intégrés au système, donc, ce cas de figure ne devrait pas se produire, mais dans le cas où cela arriverait, vous n'auriez d'autre choix que d'attendre la sortie d'une version 64 bits du pilote ou de réinstaller un système en 32 bits.

En résumé

Maintenant que vous avez aperçu ce que propose ce système d'exploitation, munissez-vous de votre DVD-Rom d'installation et passez au chapitre suivant, l'installation du système.


7
TM

chapitre 2

Installation du système

La première étape de mise en place de Windows 7 sur votre ordinateur est bien évidemment son installation. La méthode que vous allez choisir pour cette opération va sceller une partie des fondations de votre système d'exploitation.

SOMMAIRE

- Prérequis matériels
- Types d'installation
- Installation complète standard
- Mise à jour depuis Vista
- Installation sur un disque virtuel
- Désinstallation

MOTS-CLÉS

- Installation
- Mise à jour
- Windows XP
- Windows Vista
- SATA
- Multi-boot
- Disque virtuel
- Migration des données

Dans ce chapitre, nous allons décrire les différents modes d'installation du système. En effet, vous pouvez installer Windows 7 sur un disque dur vierge, sur une installation de Vista déjà présente ou ecnore sur un disque dur virtuel.

Préparatifs

Avant de vous lancer dans l'installation de Windows 7, commencez par vous assurer que votre matériel correspond bien aux caractéristiques attendues par le système d'exploitation. Vous devrez ensuite choisir parmi les différents modes d'installation proposés par Windows.

Votre ordinateur est-il compatible ?

Pour installer Windows 7, votre ordinateur doit posséder au minimum la configuration suivante :

- un processeur 32 ou 64 bits d'une fréquence d'au moins 1 GHz ;
- au minimum 1 Go de mémoire vive ou RAM (*Random Access Memory*) ;
- un disque dur possédant au moins 16 Go d'espace libre.

Si vous avez acheté votre ordinateur au moment de la sortie de Windows 7 ou plus tard, il y a fort à parier qu'il soit largement conforme à ces exigences. En revanche, si votre ordinateur est plus ancien, prenez le temps de bien vérifier ces différents critères. Pour cela, vous pouvez utiliser les outils mis à votre disposition par Microsoft tels que le Conseiller de mise à niveau ou la liste de compatibilité matérielle (HCL).

Astuce Utilitaire de conseil pour la mise à niveau

Microsoft propose un utilitaire de mise à niveau appelé Conseiller de mise à niveau (ou en anglais *Windows Upgrade Advisor*) qui teste automatiquement un ordinateur pour s'assurer qu'il supportera correctement Windows 7. Cet outil gratuit analyse les composants de votre ordinateur : disque dur, mémoire, carte graphique, etc. Les périphériques externes seront également testés. Pensez à les brancher à votre ordinateur avant de démarrer le test. À la fin de l'analyse, l'outil génère un rapport, qui indique les points à corriger pour profiter pleinement de Windows 7.

Astuce Hardware Compatibility List

Il est également possible de tester si votre matériel est compatible grâce à la liste des compatibilités matérielles ou HCL (*Hardware Compatiblity List*). Vous y trouverez une liste évoluant chaque jour, contenant tous les matériels certifiés fonctionnels par Microsoft. Elle contient le pilote ou la méthode pour rendre le matériel pleinement fonctionnel avec votre système.

▸ http://www.microsoft.com/windows/compatibility/.

Quel type d'installation choisir ?

Si vous possédez Windows XP, oubliez la possibilité de procéder à une mise à niveau tout en conservant vos programmes et vos paramètres. En effet, en raison d'un grand nombre de changements profonds dans la structure du système d'exploitation (7 années séparent Windows XP de Windows 7), la mise à niveau de Windows XP à Windows 7 est impossible. La seule solution valable est l'installation complète standard du nouveau système.

Si vous venez d'acheter un ordinateur qui ne possède pas de système d'exploitation installé ou si les systèmes installés ne permettent pas de mise à jour directe (par exemple, votre ordinateur est équipé de Windows XP), la seule solution qui s'offre à vous est d'effectuer une installation complète de Windows 7.

Si votre ordinateur fonctionne sous Windows Vista SP1, vous disposez de trois choix d'installation.

- L'installation complète standard – Elle installe le système à partir de zéro. De ce fait, les paramètres utilisateur sont supprimés ainsi que tous les programmes que vous utilisiez. L'avantage de ce mode d'installation est qu'il permet d'avoir un système propre et stable et donc de démarrer l'utilisation du système d'exploitation sur de bonnes bases. Lors d'une installation complète, vous pouvez choisir de l'effectuer sur une partition dédiée de votre disque dur ou bien dans un disque dur virtuel.
- La mise à niveau du système – Cette conversion de Vista en Windows 7 présente l'avantage de conserver tous vos paramètres personnels, vos documents, les comptes utilisateur, ainsi que les programmes installés. L'inconvénient est qu'elle prend comme base un système qui n'est sans doute plus tout à fait propre et stable.

Si votre ordinateur possède un disque dur qui n'est pas formaté, vous ne pourrez effectuer qu'une installation complète standard.

Avant de commencer l'installation de Windows, munissez-vous du DVD-Rom d'installation de Windows 7 ainsi que de la clé produit. Si Windows est fourni avec l'ordinateur, cette clé est inscrite sur un autocollant sur votre ordinateur (ou dessous, pour un ordinateur portable). Si vous avez acheté une version boîte de Windows, votre clé est fournie dans le boîtier contenant le DVD-Rom.

Détaillons à présent ces différents modes d'installation.

EN PRATIQUE Windows.old

Si vous choisissez ce type d'installation sur un disque contenant déjà une version de Windows, les fichiers et les dossiers déjà présents seront déplacés dans un répertoire nommé `Windows.old`. Vous pourrez bien entendu consulter le contenu de ce dossier, mais vous ne pourrez plus utiliser votre ancien système.

EN PRATIQUE Programmes déjà installés

Dans le cas d'une mise à niveau, les programmes déjà présents sur votre ordinateur continueront de fonctionner s'ils sont compatibles avec Windows 7.

TESTER Installer Windows 7 dans un disque dur virtuel

Si vous ne souhaitez pas partitionner votre disque et que vous désirez uniquement tester Windows 7 sans toucher à la structure physique de votre disque dur, installez Windows 7 dans un disque dur virtuel. Cette solution présente l'avantage d'installer le système dans un fichier sur une partition existante de votre disque dur. Cependant, ce type d'utilisation réduira légèrement les performances d'accès au disque dur.

Mise à jour depuis Windows XP

Bien que Windows XP soit très présent sur les ordinateurs actuels et que beaucoup d'utilisateurs souhaitent migrer vers Windows 7 sans passer par la case Vista, il est pourtant impossible de procéder à une mise à jour depuis Windows XP. Il vous faudra donc soit mettre votre ordinateur à jour vers Vista pour pouvoir ensuite passer à Windows 7 (c'est-à-dire deux mises à jour), soit installer de zéro Windows 7. Plus rapide et moins onéreuse, cette seconde solution est bien entendu celle que nous vous recommandons.

Nous expliquons en détail l'installation complète de Windows 7 un peu plus loin dans ce chapitre. Mais avant de vous lancer, vous devez savoir que cette installation entraine la perte des données. Il est donc nécessaire de les sauvegarder avant d'installer le nouveau système. Si Windows XP possède un utilitaire dédié à cette tâche, intitulé Utilitaire de sauvegarde

ou NTBackup.exe, le format de la sauvegarde n'est malheureusement pas géré par Windows 7 : nous vous déconseillons donc de l'utiliser dans ce cadre. Sauvegardez vos fichiers manuellement sur un média externe (clé USB, DVD -Rom ou disque dur externe).

Mise à niveau depuis Windows Vista

À l'inverse de Windows XP, il est tout à fait possible de mettre à jour Windows Vista vers Windows 7 sans réinstaller tous les programmes et recopier vos données. Seul pré-requis, il faut que vous ayez comme système Windows Vista SP1 (si vous n'avez pas encore installé le SP1 de Windows Vista, c'est le moment de sauter le pas... ou de choisir un autre mode d'installation).

1. Insérez le DVD-Rom d'installation de Windows 7 dans le lecteur. Si l'exécution automatique est activée, le lancement de l'installateur vous est proposé. Si ce n'est pas le cas, ouvrez l'explorateur Windows dans *Ordinateur*, cliquez avec le bouton droit sur votre lecteur DVD et cliquez sur *Ouvrir*. Double-cliquez ensuite sur le fichier `setup.exe`.
2. L'assistant d'installation vous demande tout d'abord de choisir la langue et les options géographiques.
3. Il vérifie ensuite la compatibilité de votre système avec Windows 7. Si le test est concluant, l'installation démarre.
4. L'installateur copie les fichiers nécessaires à l'installation sur le disque dur, puis redémarre la machine.

TÉLÉCHARGER Service Pack 1 de Vista

Indispensable pour la mise à niveau, le SP1 (ou supérieur) est disponible directement depuis Windows Update (ouvrez le menu *Démarrer* de Windows Vista, saisissez `windows update` dans la barre de recherche, puis appuyez sur *Entrée*), mais il est également disponible dans le centre de téléchargement Microsoft :

- http://www.microsoft.com/france/

BON À SAVOIR
Durée de la mise à jour depuis Vista

L'avantage principal d'une mise à jour par rapport à une installation complète est de vous faire gagner du temps pour obtenir un système entièrement opérationnel. Lors de la mise à jour, Windows 7 récupère les programmes et les données se trouvant sur la partition de l'ancien système et les replace dans la nouvelle installation. Cependant, si votre ancienne partition contient énormément de données, la mise à jour peut nécessiter plusieurs heures. Pour être exact, la mise à jour depuis un Vista vierge de données dure environ 30 minutes, tandis qu'une mise à jour depuis un Vista pesant 650 Go peut prendre jusqu'à 21 heures ! Ainsi, si votre ancien système possède plus d'une partition, déplacez vos données sur une autre partition : vous réduirez ainsi le temps de la mise à jour.

Installation complète standard

L'installation complète standard correspond à l'installation d'un Windows 7 vierge de tous paramètres et de documents. Vous installez le système avec des paramètres par défaut.

1. Démarrez depuis le DVD-Rom d'installation de Windows 7.
2. Après le chargement des fichiers, l'interface graphique de l'installateur s'affiche. Le premier écran vous propose de choisir la langue et les options du clavier. Cliquez sur *Suivant*, puis sur le bouton *Installer maintenant*.
3. Vous devez alors, comme dans les versions antérieures de Windows, accepter le contrat de licence utilisateur final (CLUF) : cochez la case appropriée, puis cliquez sur le bouton *Suivant*.

COMPRENDRE Accepter le CLUF

En acceptant le contrat, vous vous engagez à respecter les conditions d'utilisation imposées par l'éditeur, Microsoft. Si vous n'acceptez pas ce contrat, l'installation de Windows sera impossible.

4 L'assistant vous demande ensuite quel type d'installation vous souhaitez réaliser. Pour une installation complète standard, il vous faudra cliquer sur *Personnalisée* (les anciens paramètres ne seront pas repris).

5 Vous devez maintenant choisir la partition qui accueillera Windows. L'écran affiche la liste des partitions déjà existantes sur vos différents disques durs.

PROBLÈME **Disque dur non reconnu**

Si votre disque dur n'est pas reconnu, utilisez le bouton *Charger un pilote*. Vous avez la possibilité de fournir un pilote sur CD-Rom, DVD-Rom ou encore sur une clé USB. Insérez le disque ou la clé USB, puis cliquez sur *OK*. Utilisez le bouton *Parcourir* pour sélectionner un emplacement dans le système de fichiers.

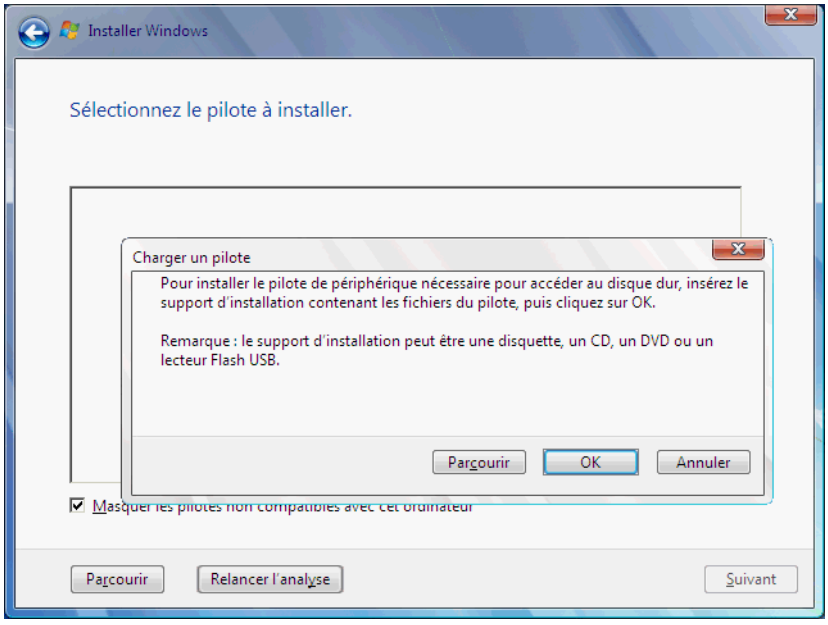


Figure 2–1 Installation de pilote de disque dur

Si besoin, l'assistant d'installation vous permet de formater, supprimer et créer de nouvelles partitions sur vos disques en cliquant sur le bouton *Options de lecteur (avancées)*.

Utilisez le bouton *Supprimer* pour effacer l'une des partitions de votre disque dur. Attention, toutes les données contenues dans la partition seront irrémédiablement perdues. Pour effacer uniquement le contenu de la partition, utilisez le bouton *Formater*.

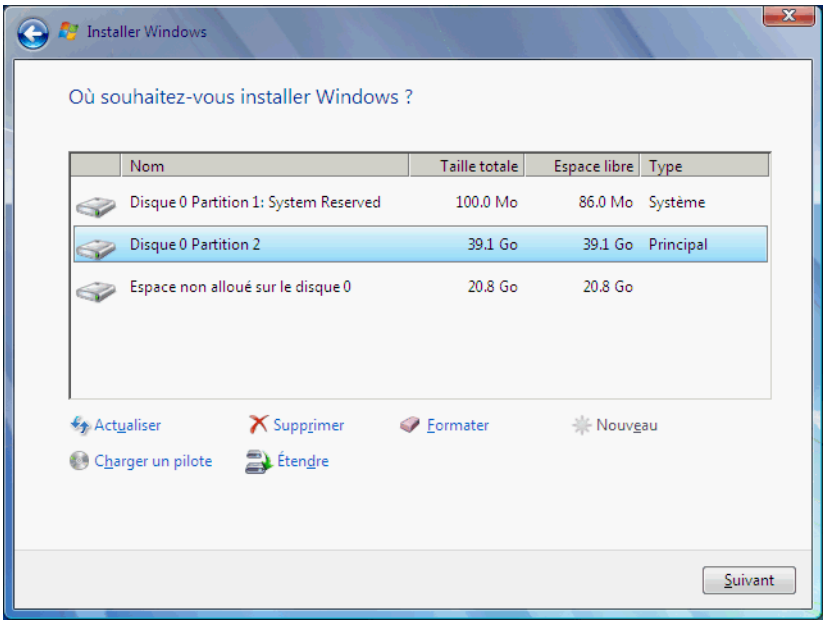


Figure 2–2
Outil de gestion des partitions

Le bouton *Nouveau* permet de créer de nouvelles partitions pour installer Windows 7. Il n'est accessible que s'il reste de l'espace disque non alloué. Dans le cas contraire, pensez éventuellement à supprimer des partitions existantes. Sélectionnez une ligne *Espace non alloué sur le disque X*, puis cliquez sur le bouton *Nouveau*. Après une demande de confirmation, l'assistant crée deux partitions : une petite partition de 100 Mo dédiée au système et une autre partition de la taille que vous avez indiquée.

S'il reste de l'espace non alloué sur votre disque dur, vous avez la possibilité d'étendre une partition attenante. Pour cela, cliquez sur la partition à agrandir, puis utilisez le bouton *Étendre*.

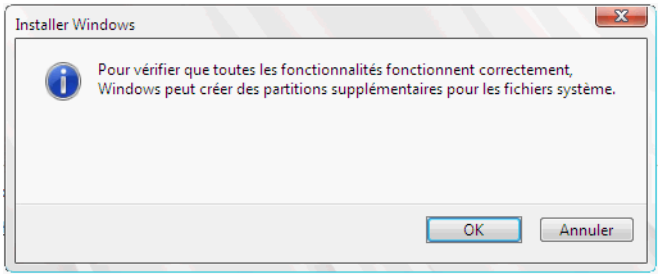


Figure 2–3
Message de confirmation lors de la création de partition

Si vous tentez d'installer Windows sur une partition ne disposant pas de suffisamment d'espace libre, vous obtiendrez le message *Impossible d'installer Windows sur le disque X Partition Y*.

6 Après avoir mis en place la configuration disque de votre choix et sélectionné la partition d'installation, cliquez sur *Suivant* pour continuer le processus d'installation.

7 L'installation se déroule ensuite de manière totalement automatique. Vous pouvez sans crainte aller vous servir un café, car l'assistant ne vous demandera pas d'autres informations avant la fin de l'installation.

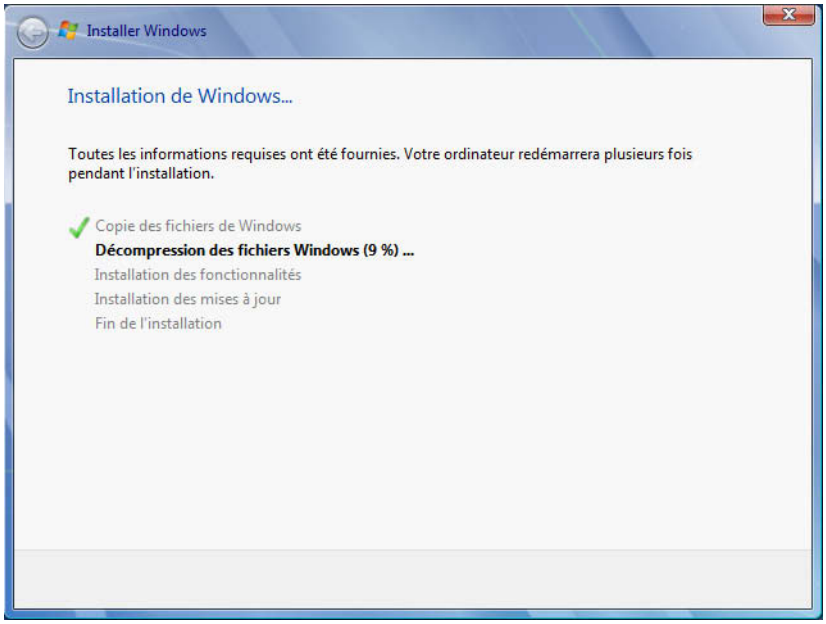


Figure 2–4
Étapes d'installation de Windows 7

EN COULISSE **Format WIM**

Depuis Vista, il n'existe plus qu'un seul DVD-Rom pour installer les différentes versions du système. Celle qui va s'installer dépendra de la clé produit que vous indiquez. Il est ainsi possible d'installer n'importe quelle version de Windows 7 avec un seul DVD-Rom. Derrière cette simplicité se cache WIM (*Windows Image Format*).
WIM est un format d'image disque orienté fichier développé par Microsoft. On dit que ce format est « orienté fichier » car contrairement aux formats « orientés secteur » (tels que `.iso` ou `.cue`) WIM stocke les informations sur les fichiers contenus dans la partition. Ceci présente l'avantage de ne stocker, par exemple, qu'un seul exemplaire d'un fichier se trouvant en plusieurs exemplaires dans la partition. Une image WIM peut être montée comme un répertoire pour faciliter l'ajout de fichiers. Un fichier de type WIM peut contenir plusieurs images indicées par un numéro d'index. Ainsi, le fichier `INSTALL.WIM`, présent dans le dossier `sources` du DVD-Rom d'installation de Windows 7, contient les images disque de toutes les versions.

Installation sur un disque virtuel

Windows 7 propose un nouveau procédé d'installation qui n'existait pas dans les versions antérieures. Il installe le système dans un simple fichier sur le disque dur. Appelé disque dur virtuel, ce fichier porte l'extension `.vhd` (pour *Virtual Hard Disk*).

L'installation de Windows sur un disque virtuel est relativement similaire à une installation standard, mais présente l'avantage d'installer plusieurs versions de Windows 7 sur un disque sans avoir à créer de partitions supplémentaires. Ainsi, si vous désirez par la suite supprimer cette installation de Windows, il vous suffit de démarrer depuis une autre installation de Windows et de supprimer le fichier `.vhd` correspondant au disque dur virtuel.

Windows 7 permet nativement de créer et de monter ce type de fichier, et même de démarrer (*booter*) directement à partir d'un disque dur virtuel.

Voici comment se passe pas à pas l'installation de Windows 7 sur un disque dur virtuel.

1. Insérez le DVD-Rom d'installation dans la machine, puis démarrez-la sur ce disque. Vous arrivez alors dans le programme d'installation du système. La première boîte de dialogue vous demande de choisir la langue et la disposition de clavier à utiliser. Faites votre choix, puis cliquez sur *Suivant*.

Disque dur virtuel

Un disque dur virtuel est un format de fichier particulier qui représente la structure et le contenu d'un disque dur. Il est généralement utilisé avec les machines virtuelles, par exemple avec Microsoft Virtual PC. Dans le cas de l'installation de Windows 7 sur un disque dur virtuel, ce n'est pas une machine virtuelle qui l'utilise mais bel et bien l'ordinateur sur lequel vous effectuez l'installation.

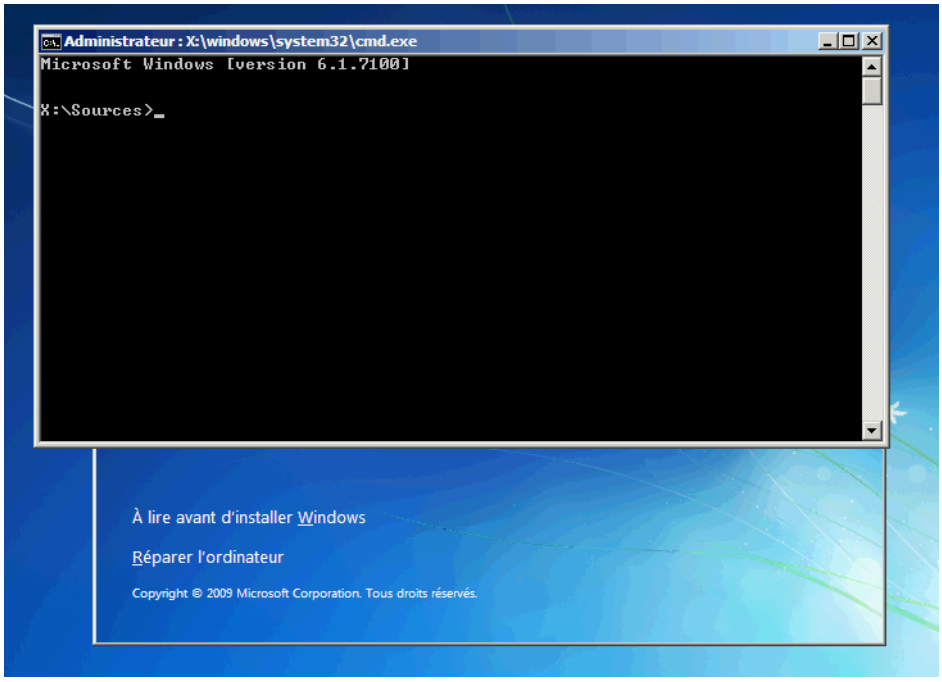


Figure 2–5
Invite de commandes d'installation de Windows

2 L'assistant vous propose alors d'installer le système. Avant de commencer cette installation, il faut créer un disque dur virtuel et le monter pour qu'il soit visible par l'assistant d'installation. Pour cela, rendez vous dans la console en utilisant la combinaison de touches *Maj+F10*.

3 Dans l'invite de commandes qui s'ouvre alors, appelez l'utilitaire Diskpart en entrant la commande `diskpart`. L'utilitaire Diskpart se présente sous la forme d'une console dans laquelle vous saisissez vos commandes.

4 Tout d'abord, créez un fichier VHD (disque dur virtuel). Pour cela, entrez la commande suivante :

```
CREATE VDISK FILE="D:\Windows7.vhd" MAXIMUM=15000 TYPE=EXPANDABLE
```

Cette ligne demande à Diskpart de créer un disque dur virtuel dans le répertoire `D:\Windows7.vhd` de taille maximale 15 000 Mo (15 Go) et de type extensible.

L'emplacement du fichier spécifié par `FILE=` pointe sur une partition déjà existante de votre disque dur (ici `D:`). Si vous précisez un sous-répertoire, celui-ci doit exister.

EN DÉTAIL Type d'allocation

Il est possible de préciser comment le disque virtuel doit être alloué sur le disque à l'origine :

- Si l'on choisit le type extensible (`TYPE=EXPANDABLE`), le fichier VHD est créé avec une taille minimale et s'agrandira au fur et à mesure que vous ajouterez des données dans le disque virtuel. Ce type de fonctionnement présente l'avantage d'économiser l'espace disque puisque le fichier du disque dur virtuel n'utilise que l'espace dont il a besoin. Cependant, la procédure d'agrandissement du fichier est gourmande en ressources.
- Le second type d'allocation est dit fixe (`TYPE=FIXE`). Ce mode d'allocation indique que le disque dur virtuel doit être créé avec sa taille maximale. Dans notre exemple, le fichier VHD créé occuperait alors dès le départ 15 Go, même s'il ne contient pas de données. La création d'un disque dur virtuel avec le type fixe est plus longue qu'avec le type extensible, car il faut allouer la totalité de l'espace spécifié en taille maximale. Cependant, il n'y aura plus de perte de performance lors de l'utilisation, car il ne sera pas nécessaire de réallouer de l'espace disque.

5 Après avoir créé le fichier VHD, sélectionnez-le. Pour cela, utilisez la ligne de commande suivante :

```
SELECT VDISK FILE="D:\Windows7.vhd"
```

6 Il ne reste plus qu'à monter le disque pour qu'il soit visible par l'assistant d'installation. Saisissez alors dans la console l'instruction suivante :

```
ATTACH VDISK
```

PRÉCISION Diskpart

Déjà présent dans les versions antérieures, Diskpart a été mis à jour pour prendre en charge le support des disques durs virtuels.

```
X:\Sources>diskpart

Microsoft DiskPart version 6.1.7100
Copyright (C) 1999-2008 Microsoft Corporation.
Sur l'ordinateur : MINWINPC

DISKPART> CREATE VDISK FILE="d:\Windows7.vhd" MAXIMUM=15000 TYPE=EXPANDABLE

  100 pour cent effectués

DiskPart a correctement créé le fichier de disque virtuel.

DISKPART> SELECT VDISK FILE="d:\Windows7.vhd"

DiskPart successfully selected the virtual disk file.

DISKPART> ATTACH VDISK

  100 pour cent effectués

DiskPart a correctement attache le fichier de disque virtuel.

DISKPART> exit

Quitte DiskPart...

X:\Sources>exit_
```

Figure 2–6
Commandes de création et de montage du disque dur virtuel

7 Le disque dur virtuel est à présent créé et monté. L'installation de Windows va pouvoir commencer. Pour cela, il faut quitter la commande `diskpart` en entrant `exit` dans la console. Fermez ensuite la console soit en cliquant sur la croix, soit en saisissant à nouveau la commande `exit`.

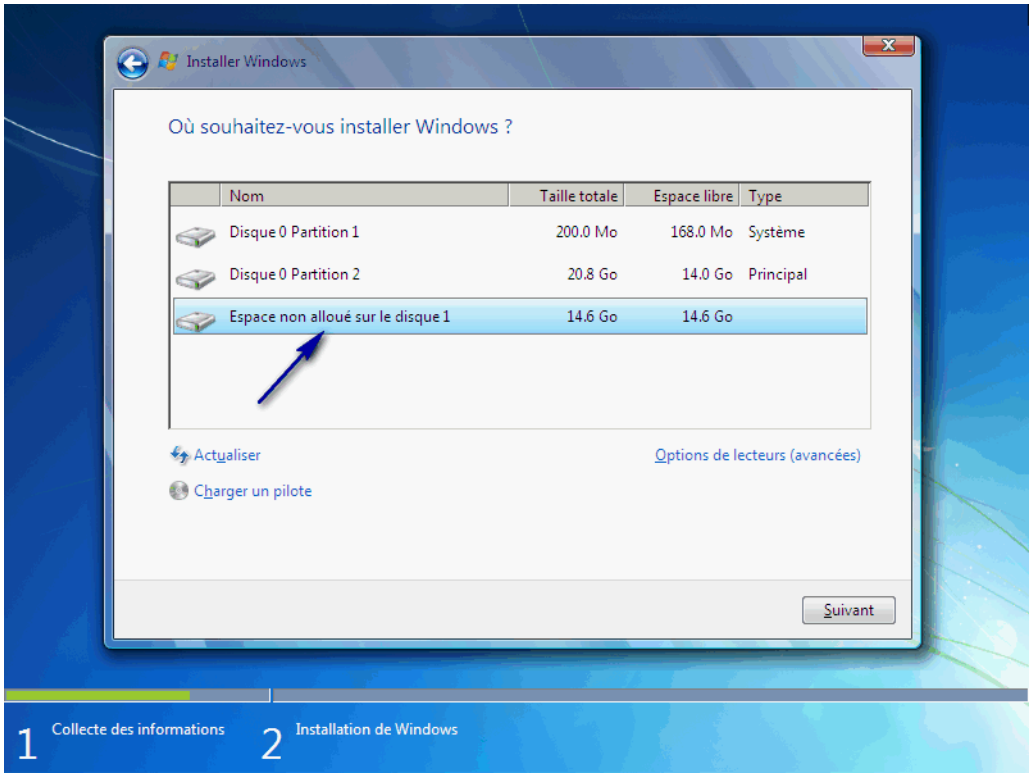


Figure 2–7
Choix de la partition d'installation

8 Lancez l'installation via le bouton présent dans l'interface d'installation. Lorsque l'assistant vous demande de choisir une partition, votre disque dur virtuel apparaît sous l'appellation *Espace non alloué sur le disque X*. Cette partition est de la taille que vous avez spécifiée lors de la création du disque dur virtuel. Sélectionnez cette partition et poursuivez en cliquant sur *Suivant*. L'installation se déroule alors comme une installation standard du système.

Une fois l'installation terminée, vous remarquez que le menu de démarrage est celui de Windows 7 et qu'il vous permet de démarrer directement ce système nouvellement installé sans avoir à monter de nouveau le disque virtuel.

Paramétrage du multi-boot

Le terme multi-boot (ou démarrage multiple, en français) désigne le fait d'installer plusieurs systèmes d'exploitation sur la même machine et de pouvoir démarrer sur celui de son choix. Sur un ordinateur, le multi-boot est géré par un logiciel appelé Boot Loader (c'est-à-dire chargeur d'amorçage dans la langue de Molière). Ce logiciel est automatiquement installé par les systèmes d'exploitation au moment de leur installation.

Le chargeur de démarrage de Windows 7 n'est autre que `winload.exe`. Il est situé dans le répertoire `Windows\System32\`. Il a pour rôle de charger le noyau du système et les drivers nécessaires au démarrage. Similaire à celle de Vista, la configuration de démarrage de Windows 7 s'intitule BCD (*Boot Configuration Data*). Elle remplace le fichier texte `boot.ini` utilisé par XP. Elle est stockée dans le répertoire `\Boot\` du disque de démarrage dans un fichier binaire nommé BCD et est formatée de la même manière que le registre Windows.

Ce fichier de configuration contient la description des entrées de menu apparaissant dans le menu de démarrage (qui apparaît au démarrage de l'ordinateur si plusieurs versions de Windows sont installées ou en appuyant sur la touche *F8*). Chaque entrée contient les informations suivantes :

- des options pour démarrer les systèmes (Windows 7 ou Vista) ;
- des options pour restaurer Windows depuis la veille prolongée ;
- des options pour démarrer des versions antérieures de Windows (XP, par exemple) en appelant le gestionnaire de démarrage NTLDR ;
- des options pour prendre en charge le démarrage sur un disque dur virtuel.

ASTUCE Réparer le menu de démarrage

Les systèmes d'exploitation ont la fâcheuse habitude d'écraser les chargeurs de démarrage précédents. Par exemple, si vous installez Windows après Linux, le chargeur de démarrage de Linux (GRUB, LILO, etc.) sera remplacé par celui de Windows.
Si vous écrasez par erreur le chargeur de démarrage de Windows, il est possible de le réparer en démarrant sur le DVD-Rom d'installation de Windows 7 et en choisissant l'option *Réparer l'ordinateur*, puis *Réparation du démarrage*.

NTLDR

NTLDR signifie NT Loader. Il s'agit du chargeur d'amorçage de la branche NT des systèmes d'exploitation Microsoft utilisé depuis Windows NT jusqu'à Windows XP. Il a été abandonné dans Windows Vista car remplacé par `winload.exe`.

Cette configuration peut être modifiée de plusieurs façons :

- via les paramètres système avancés ;
- via la commande `bcdedit.exe` ;
- ou bien en utilisant des outils tiers comme EasyBCD.

Vous pouvez modifier quelques paramètres de base du multi-boot tels que le système d'exploitation par défaut ou la durée d'affichage du menu de démarrage depuis les propriétés avancées du système.

1. Ouvrez le menu *Windows* (symbolisé par une bulle bleue appelée Orbe). Cliquez avec le bouton droit sur *Ordinateur*, puis choisissez *Propriétés* dans le menu contextuel.
2. Dans la colonne de gauche de la fenêtre *Système*, choisissez *Paramètres système avancés*.
3. Cliquez sur le bouton *Paramètres* dans le cadre *Démarrage et récupération*. La fenêtre de configuration du démarrage s'affiche :

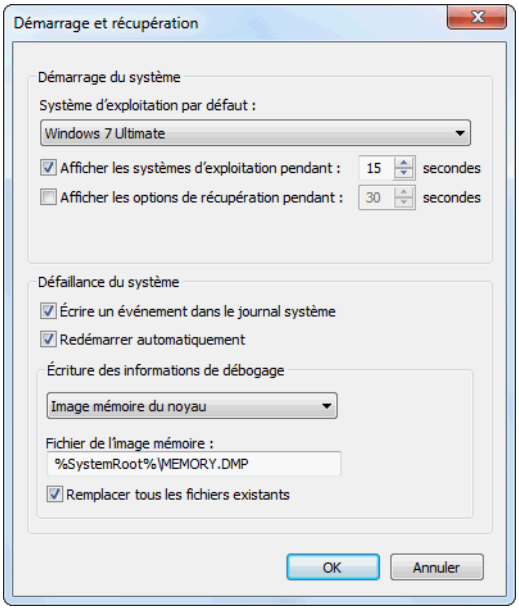


Figure 2–8
Fenêtre de paramétrage des options de démarrage

Situé dans la partie supérieure de la fenêtre, le cadre *Démarrage du système* vous permet de définir le système d'exploitation par défaut, c'est-à-dire le système qui se lance automatiquement si vous n'effectuez aucune action particulière au démarrage de l'ordinateur. Lorsque la case *Afficher la liste des systèmes d'exploitation pendant* est cochée, la liste des systèmes d'exploitation installés sur votre machine s'affiche au démarrage de l'ordinateur pour que vous puissiez choisir celui que vous voulez lancer. La liste est affichée pendant le nombre de secondes spécifiées. Passé ce délai, le système d'exploitation par défaut démarre automatiquement.

ASTUCE Accéder à la fenêtre d'informations système

Vous pouvez également afficher les informations système via le panneau de configuration en choisissant la catégorie *Système et sécurité*, puis en cliquant sur *Système*. Pour y accéder encore plus rapidement, passez par la combinaison de touches *Windows+Pause*.

Voici comment effectuer une configuration plus précise du multi-boot :

1. Saisissez `bcdedit.exe` dans l'invite de commandes.
2. Vous pouvez tout d'abord visualiser la liste des entrées du menu de démarrage. Pour cela, il faut commencer par ouvrir une invite de commandes en mode administrateur : ouvrez le menu *Démarrer*, saisissez `cmd` ou `invite de commandes` dans la barre de recherche. Le programme `cmd.exe` apparaît en haut du menu. Faites un clic droit sur cet élément, puis choisissez *Exécuter en tant qu'administrateur*.
3. Dans la console qui s'ouvre alors, entrez la commande `bcdedit`. La liste des entrées s'affiche alors. Chaque entrée possède un identificateur.
4. Ces identificateurs sont utilisés dans toutes les commandes. Ainsi, pour renommer l'entrée de menu de démarrage correspondant au système en cours d'exécution, ouvrez une invite de commandes en mode administrateur, puis saisissez la commande suivante :

```
bcdedit.exe /set {current} description "Windows 7 Home Premium"
```

Pour changer la durée d'affichage du menu de démarrage, utilisez l'option `timeout`. La ligne de commande ci-dessous configure le temps d'affichage du menu à 15 secondes :

```
bcdedit.exe /timeout 15
```

Pour définir l'entrée du menu de démarrage qui doit être sélectionnée par défaut, il faut utiliser l'option `default` en précisant l'ID de la ligne. La syntaxe ci-dessous définit le système actuel comme choix par défaut au démarrage.

```
bcdedit.exe /default {current}
```

Identificateur

Comme son nom l'indique, un identificateur sert à désigner de manière unique chaque entrée du fichier de configuration. Il se présente en général sous la forme d'un GUID (*Globally Unique Identifier*, identifiant unique) au format suivant : `{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}`
Certains éléments du fichier de configuration du démarrage portent également un identificateur « en clair » appelé « bien connu ». Vous pouvez en obtenir la liste en utilisant la commande `bcdedit /? ID`

ATTENTION **Installer une version antérieure**

L'opération ne conserve pas vos programmes et fichiers. Veillez à procéder à une sauvegarde préalable.

Désinstallation de Windows

Si vous ne disposez que d'une seule installation de Windows 7 sur votre ordinateur, vous ne pouvez pas désinstaller le système d'exploitation. Cependant, vous pouvez réinstaller une version antérieure de Windows.

Si votre ordinateur est configuré en multi-boot, il est possible de supprimer ou de formater la partition contenant Windows 7. Pour cela, vous devez démarrer dans une autre installation de Windows que celle que vous voulez désinstaller.

Une fois le formatage ou la suppression de la partition de Windows 7 terminée, la désinstallation est effectuée. Il ne manque qu'une étape pour ne conserver aucune trace de Windows 7 : supprimer l'option *Windows 7*

ATTENTION
Avant de se lancer dans le formatage

Sur un ordinateur configuré en multi-boot, ne supprimez pas la partition contenant une version antérieure de Windows. En effet, cette partition contient les informations nécessaires au démarrage de l'ordinateur. Si vous les supprimez, l'ordinateur ne démarrera plus.
Si vous avez installé une version antérieure après avoir installé Windows 7, la suppression de la partition contenant Windows 7 peut empêcher l'ordinateur de démarrer.

dans le menu de démarrage. Dans Windows 7 ou Vista, cette opération est simple :

1. Ouvrez le menu *Démarrer*.
2. Saisissez `msconfig` dans la barre de recherche, puis cliquez sur *msconfig.exe*.
3. Sélectionnez l'onglet *Démarrer*.
4. Dans la liste des systèmes d'exploitation installés, sélectionnez celui à supprimer du menu de démarrage, puis cliquez sur le bouton *Supprimer* en bas de la liste.

LOGIQUE Suppression impossible

Vous ne pouvez pas supprimer du menu de démarrage le système actuellement en cours d'exécution.

De manière générale, pour éviter des problèmes dans la configuration du multi-boot, il est fortement recommandé d'installer les différentes versions de Windows dans l'ordre de leur sortie. Installez par exemple XP, puis Vista et enfin Windows 7. Le menu de démarrage sera alors directement fonctionnel pour exécuter l'édition de Windows de votre choix : aucune configuration future et manuelle du multi-boot ne sera alors nécessaire. Dans le cas où vous installeriez Windows XP en dernier, celui-ci enlèvera le bootloader de Windows 7 et ce dernier ce sera plus accessible. Il vous faudra utiliser la commande `fixboot` à l'aide du DVD d'installation de Windows 7.

En résumé

L'installation du système est la première étape à réaliser pour mettre en place Windows 7 sur un ordinateur. Cette étape est inutile si Windows 7 est pré-installé sur le disque dur de votre ordinateur.

Maintenant que le système est en place, voyons comment l'utiliser et l'administrer au quotidien.


7
TM

chapitre 3

Paramétrer et personnaliser Windows 7

Administrer et utiliser un système est une affaire de tous les jours. Puisque l'incidence de chaque action est plus ou moins importante, l'administration d'un système d'exploitation exige d'acquérir des bonnes pratiques.

SOMMAIRE

- Configuration du système
- Console d'administration avancée
- Planificateur de tâches
- Paramétrage du démarrage
- Paramétrage des programmes par défaut
- Mise à jour du système avec Windows Update

MOTS-CLÉS

- Panneau de configuration
- Planificateur de tâches
- Date, heure, horloge
- Utilitaires de gestion
- Propriétés système
- Extensions
- Windows Update
- Services

Le système d'exploitation regorge de centaines d'outils et de panneaux de paramétrages afin de vous permettre d'obtenir un système répondant très précisément à vos besoins. La difficulté est alors d'être capable de trouver rapidement l'outil de configuration dont vous avez besoin et de pouvoir en tirer partie. Ce chapitre présente les principaux centres de contrôle du système et détaille les plus importants tels que le démarrage du système ou la gestion de certains points dits sensibles.

Le panneau de configuration : centre névralgique du paramétrage

Inutile de présenter le panneau de configuration, il a peu changé au fil des différentes versions de Microsoft Windows. Cependant, Windows 7 apporte quelques modifications que nous allons aborder.

Figure 3–1
Aperçu du panneau de configuration

Le panneau de configuration permet d'accéder à l'ensemble du paramétrage du système. Pour certains paramétrages avancés, il vous faudra cependant utiliser les consoles de management ou certains écrans qui ne sont pas accessibles depuis ce panneau.

Le tableau 3-1 dresse la liste des huit catégories de panneau de configuration. Elles regroupent plusieurs éléments ou fonctionnalités du système.

ATTENTION Choix des auteurs

Nous aborderons, au fil des différents chapitres de ce livre, certaines fonctionnalités du système et comment les configurer. Nous avons délibérément omis certaines parties pour nous focaliser sur celles que nous estimons les plus critiques ou les plus intéressantes à décrire pour un utilisateur averti.

À SAVOIR Personnaliser le panneau de configuration

Il est tout à fait possible de paramétrer les éléments présents dans le panneau de configuration, que ce soit pour enlever des éléments ou en ajouter. Vous pouvez y faire apparaître vos propres éléments. Au chapitre 16, vous découvrirez comment réaliser cela.

ASTUCE Retrouver l'affichage « à l'ancienne » du panneau de configuration

Jusqu'à Windows XP, tous les éléments du panneau de configuration étaient affichés dans la même fenêtre et triés par ordre alphabétique. Leur nombre croissant, Microsoft a ajouté, sous Windows Vista, un affichage par catégorie. Même s'il est clair et logique, il n'est pas forcément au goût de tous, surtout pour les habitués de l'ancien affichage. Pour retrouver l'affichage détaillé, cliquez dans le panneau de configuration sur la liste déroulante située en haut de la fenêtre et choisissez un affichage par petites ou grandes icônes. Tous les éléments du panneau de configuration sont alors affichés devant vous.

Tableau 3–1 Catégories du panneau de configuration

Options	Action
Système et sécurité	Configure les mises à jour, le pare-feu, le chiffrement (BitLocker, EFS, etc.), la sauvegarde et restauration.
Réseau et Internet	Administre tout ce qui est relatif au réseau comme les connexions, les partages, mais également les options des navigateurs web.
Matériel et audio	Contrôle les périphériques fixes et amovibles, mais également les sons système ou encore l'affichage du système.
Programmes	Point de départ pour gérer les programmes installés, tout comme les gadgets ou encore les fonctionnalités système particulières telles que les serveurs web ou FTP.
Comptes et protection utilisateurs	Gère tout ce qui a trait aux comptes utilisateur.
Apparence et personnalisation	Thèmes, fond d'écran, affichage des dossiers et des fichiers.
Horloge, langue et région	Moins utilisé que les autres, cette catégorie permet de paramétrer l'heure du système ainsi que les paramètres régionaux.
Options d'ergonomie	Paramètres facilitant l'utilisation du système, soit par l'affichage, soit par la voix (reconnaissance vocale).

Le planificateur de tâches

Le planificateur de tâches existait déjà dans les versions antérieures de Windows. Dans Windows 7, de nombreuses améliorations ont été apportées. Voici comment accéder au planificateur de tâches :

1. Ouvrez le menu *Démarrer*.
2. Saisissez `planificateur de tâches`.
3. Appuyez sur *Entrée*.

Toutes les tâches contenues dans le planificateur sont stockées dans la bibliothèque du planificateur de tâches.

Créer une tâche planifiée

Pour créer une tâche, utilisez les liens présents dans la colonne *Actions* (à droite de la fenêtre). Vous pouvez alors créer votre tâche :

- soit via l'assistant, en cliquant sur *Créer une tâche de base...*
- soit en passant par les options avancées, en cliquant sur *Créer une tâche...*

Étant donné que le mode avancé reprend les options de la fenêtre de modification que nous décrirons dans la section « Modifier les paramètres d'une tâche planifiée », concentrons-nous ici sur l'assistant.

1. Dans la première étape de l'assistant, définissez le nom de la tâche et donnez-en une brève description. Après avoir saisi ces informations, cliquez sur le bouton *Suivant*.
2. La deuxième étape consiste à choisir le déclencheur de la tâche. Ce déclencheur peut être temporel (déclenchement à des dates données) ou bien événementiel (déclenchement à l'ouverture de session, au démarrage de l'ordinateur, etc.). Choisissez l'option qui convient le mieux à votre tâche, puis cliquez sur *Suivant*.
3. Dans l'étape suivante, indiquez l'action que doit réaliser la tâche. Elle peut être de plusieurs types différents : vous pouvez choisir de *Démarrer un programme*, d'*Envoyer un message électronique* ou d'*Afficher un message*. Faites votre choix puis, en fonction de l'action à réaliser, indiquez le programme à lancer, le contenu et les destinataires de l'e-mail à envoyer ou le texte du message à afficher. Cliquez ensuite sur *Suivant* pour poursuivre.

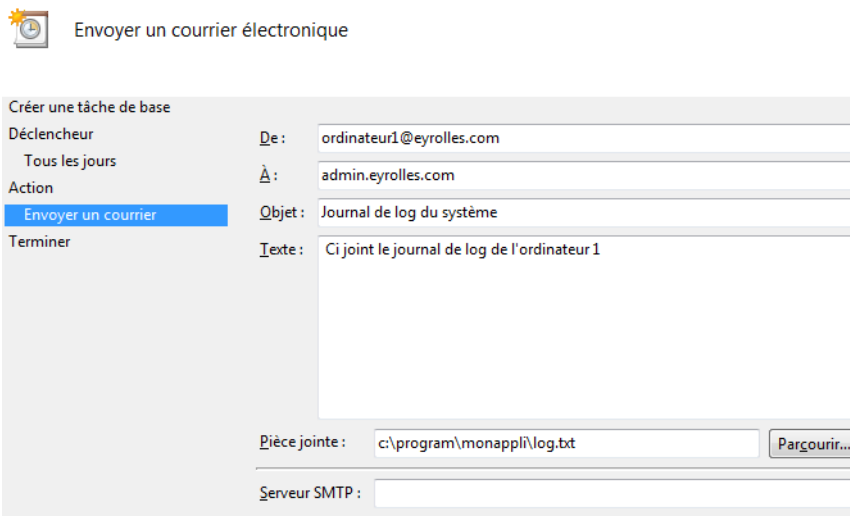


Figure 3–2
Exemple de paramétrage de l'envoi automatique d'un e-mail

4. L'assistant affiche alors un résumé de la tâche qu'il va créer. Si les informations indiquées ne vous conviennent pas, utilisez le bouton *Précédent* pour les modifier. Si les informations correspondent à vos attentes, confirmez la création de la tâche en cliquant sur le bouton *Terminer*. Vous accédez directement à des options supplémentaires après la création de la tâche en cochant la case adéquate.

PRÉCISION

Déclencheur temporel ou événementiel

Selon le déclencheur que vous avez choisi, vous pourrez être amené à donner plus d'informations. Par exemple, si vous avez choisi de déclencher la tâche chaque semaine, l'assistant vous demande quels jours et à quelle heure.

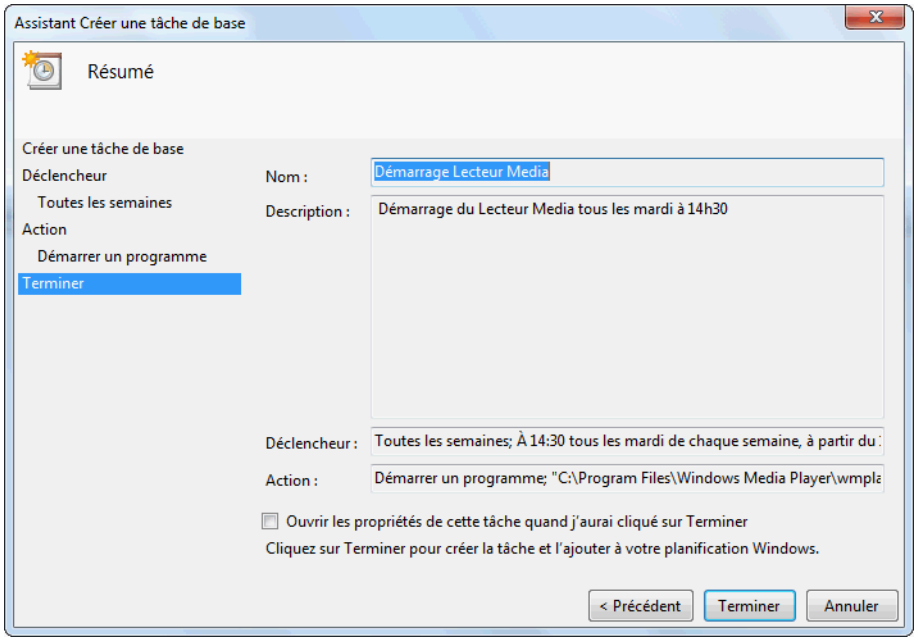


Figure 3–3
Résumé de la création de la tâche planifiée

Votre tâche est maintenant enregistrée dans le système et sera exécutée suivant les options que vous avez définies. Elle apparaît dans la bibliothèque du planificateur. Si ce n'est pas le cas, cliquez sur le bouton *Actualiser* de la colonne *Actions*.

Modifier les paramètres d'une tâche planifiée

Pour modifier les détails d'une tâche planifiée, ouvrez la bibliothèque du planificateur et cliquez sur la tâche planifiée à modifier. La partie inférieure de la fenêtre affiche alors les informations détaillées concernant la tâche sélectionnée.

Vous pouvez supprimer une tâche en cliquant dessus avec le bouton droit, puis en cliquant sur *Supprimer*. Vous la désactivez en choisissant *Désactiver* dans son menu contextuel. La colonne *État* affiche *Désactivée*. La tâche ne s'exécutera plus jusqu'à ce que vous la réactiviez.

Double-cliquez sur la tâche dans la liste en haut de la fenêtre pour modifier ses propriétés avancées. À partir de cette fenêtre, reconfigurez les paramètres de la tâche à votre guise, qu'il s'agisse des déclencheurs, des actions réalisées ou encore des conditions de lancement. Penchons-nous sur les différents onglets qu'elle propose.

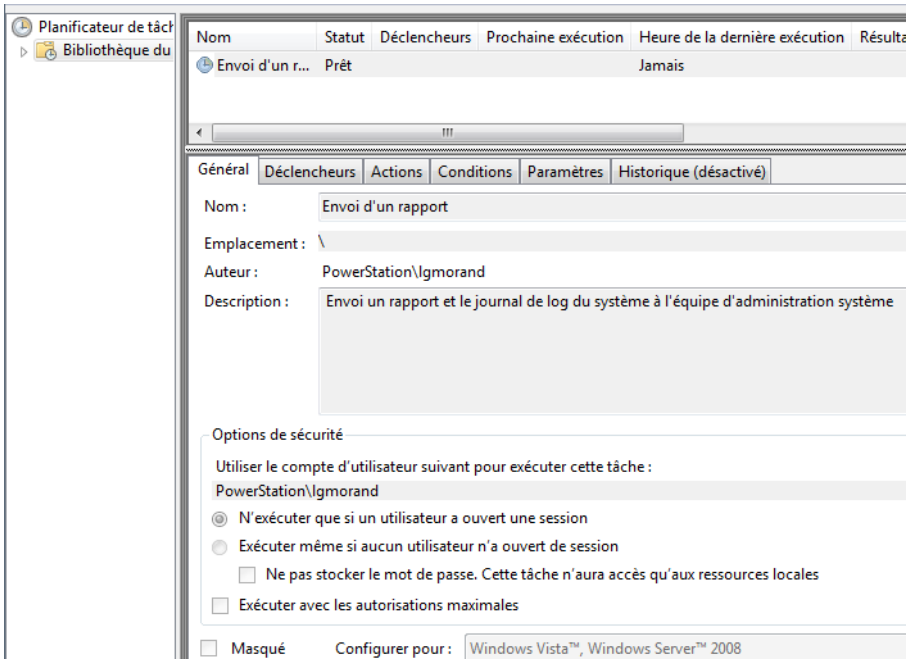


Figure 3–4
Vue d'ensemble des tâches planifiées du système

Le premier onglet, intitulé *Général*, sert à modifier la description de la tâche et à définir si la tâche s'exécutera quand l'utilisateur est déconnecté ou non. Cochez la case *Exécuter avec les autorisations maximales* si votre tâche doit accéder à des ressources nécessitant des privilèges élevés.

L'onglet *Déclencheurs* affiche la liste des événements déclenchant la tâche. Vous pouvez ajouter des déclencheurs supplémentaires ou en supprimer un existant. La fenêtre de création ou de modification d'un déclencheur affiche un grand nombre de possibilités.

La partie supérieure de la fenêtre permet de choisir quand l'action démarrera (par exemple à des dates données ou bien lorsqu'un événement système survient). Choisissez le type de déclencheur dans la liste déroulante en haut de la fenêtre. Spécifiez ensuite les détails dans le cadre *Paramètres*.

Dans la partie inférieure de la fenêtre, vous définissez les options de répétition, d'arrêt et d'expiration de la tâche. La date d'expiration indique le moment à partir duquel la tâche ne sera plus démarrée.

Grâce à l'onglet *Actions*, vous gérez les actions exécutées par la tâche. Vous ajoutez de nouvelles actions ou en supprimez en utilisant les boutons en bas de la liste.

L'onglet *Conditions* permet de définir des conditions qui doivent être réunies pour que la tâche soit exécutée. Ainsi, vous pouvez, dans le cas d'un ordinateur portable, configurer la tâche pour qu'elle démarre uni-

quement si l'ordinateur est branché sur secteur et qu'elle ne s'exécute pas lorsqu'il est alimenté par ses batteries.

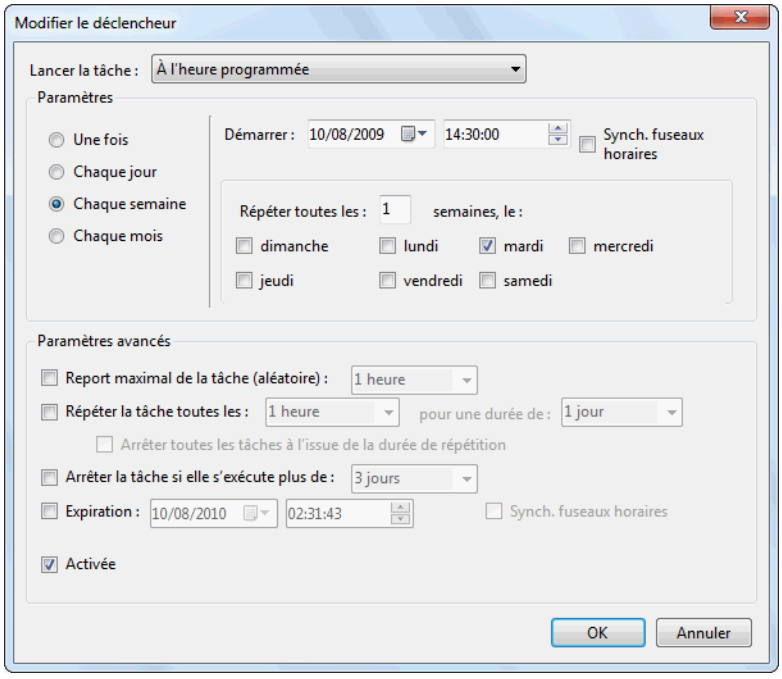


Figure 3–5
Modification d'un déclencheur de tâche planifiée

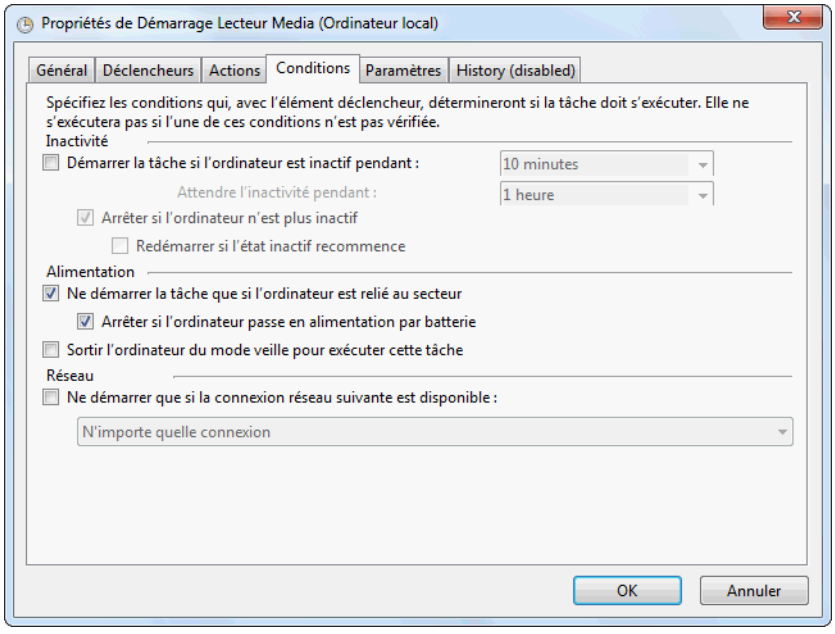


Figure 3–6
Conditions de démarrage d'une tâche planifiée

Dans l'onglet *Paramètres*, spécifiez des options supplémentaires pour le comportement de la tâche. Vous pouvez notamment définir le comportement à adopter en cas d'échec d'exécution de la tâche. Si votre tâche doit expirer un jour, cochez la case *Si la tâche n'est pas programmée pour s'exécuter à nouveau, la supprimer après X jours*. Ainsi, la tâche sera automatiquement supprimée de la bibliothèque du planificateur de tâches quand elle ne sera plus utile.

Régler l'heure et la date de l'ordinateur

La date et l'heure sont des informations que nous utilisons tous les jours sans y prêter attention. Pour un ordinateur, ce sont des éléments fondamentaux. En effet, il les utilise pour savoir si un fichier a été modifié, pour enregistrer les événements système dans des journaux, mais également pour vérifier si de nouvelles mises à jour sont disponibles pour les antivirus, par exemple.

Si l'heure ou la date de votre système sont mal configurées, certaines fonctionnalités risquent de ne plus fonctionner correctement ou bien de se comporter de façon illogique et dangereuse pour votre système. Ces deux paramètres constituant un point critique de votre système, vous devez disposer d'un compte administrateur pour pouvoir les modifier.

1. Cliquez avec le bouton droit de la souris sur l'horloge dans la barre système.
2. Sélectionnez *Ajuster la date/l'heure* dans le menu contextuel.
3. Cliquez ensuite sur le bouton *Changer la date et l'heure*.
4. Effectuez les changements, puis cliquez sur *OK*.

Windows vous donne la possibilité d'afficher les horloges de plusieurs fuseaux horaires simultanément. Pour cela, cliquez avec le bouton droit sur l'heure dans la barre système, sélectionnez *Ajuster la date/l'heure,* puis l'onglet *Horloges supplémentaires*.

Vous pouvez ainsi ajouter jusqu'à deux horloges additionnelles ayant des fuseaux horaires différents. Pour consulter ces horloges, pointez ou cliquez sur l'heure dans la barre système.

Si votre ordinateur est connecté à Internet, mettez à jour votre heure automatiquement à partir de serveurs de temps sur Internet. La procédure est simple :

1. Cliquez avec le bouton droit sur l'heure dans la barre système.
2. Cliquez sur *Ajuster la date/l'heure*.
3. Sélectionnez l'onglet *Temps Internet.*
4. Modifiez les paramètres.

ATTENTION Ajouter une seconde horloge

Le fait d'ajouter une seconde horloge ne modifie pas pour autant l'affichage de la barre des tâches. Pour visualiser les différentes horloges, passez la souris sur l'horloge de la barre des tâches et attendez une seconde. Une infobulle contenant les deux horloges et leur nom s'affiche alors. Vous pouvez également cliquer sur l'heure pour afficher les différentes horloges sous forme analogique.

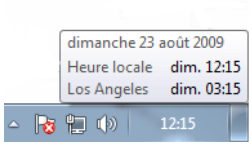


Figure 3–7 Affichage de deux horloges

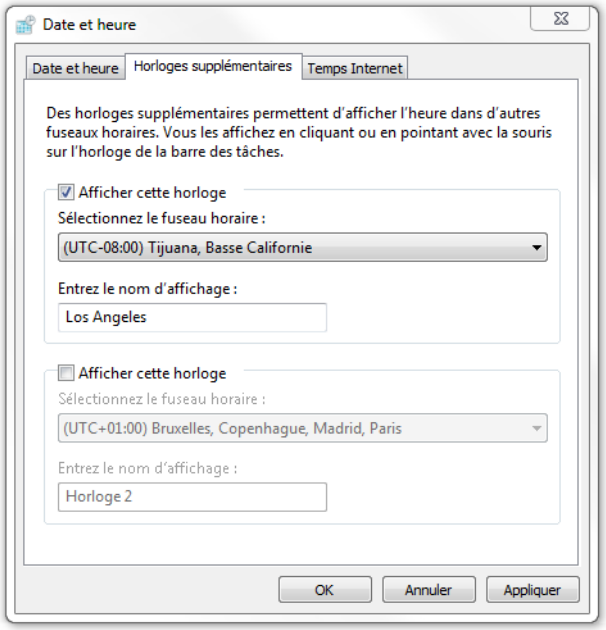


Figure 3–8
Ajout d'une seconde horloge Windows

La console de gestion de l'ordinateur

Cette console donne accès à un certain nombre d'outils permettant de gérer plusieurs aspects du système. Voici comment y accéder :

1. Ouvrez le menu *Démarrer.*
2. Cliquez avec le bouton droit sur *Ordinateur.*
3. Cliquez sur *Gérer* dans le menu contextuel.

Vous avez alors accès aux utilitaires de gestion du système. Ils apparaissent dans la partie gauche de la fenêtre sous la forme d'une arborescence. Lorsque vous y sélectionnez un outil, il s'ouvre dans la partie droite, dédiée au contenu des modules. Les outils de la console de gestion de l'ordinateur sont classés dans trois catégories : *Outils système*, *Stockage* et *Services et applications*. La rubrique *Outils système* donne accès à différents outils importants. Le tableau 3-2 les détaille.

La rubrique *Services et applications* contient le panneau de contrôle des services du système et le contrôle WMI (*Windows Management Instrumentation*). Les services sont des programmes s'exécutant en permanence en tâche de fond du système pour exécuter diverses actions. Certains services sont vitaux et ne peuvent pas être désactivés. N'effectuez pas de modifications dans les réglages des services à moins que vous ne sachiez ce que vous faites. En effet, un mauvais paramétrage peut entraîner le dysfonctionnement de certaines parties du système.

Tableau 3–2 Les outils système

Outil	Action
Planificateur de tâches	Cet utilitaire permet de créer et de gérer des tâches planifiées. Il s'agit d'actions que l'ordinateur exécutera automatiquement à des dates et heures que vous avez spécifiées.
Observateur d'événements	Il permet de visualiser les événements qui se produisent sur le système. Pour en savoir plus, consultez le chapitre 15 « Résoudre les problèmes de Windows 7 ».
Dossiers partagés	Cet outil permet de visualiser les dossiers partagés du système Son fonctionnement est décrit dans le chapitre 11 « Sécurité des fichiers et partage de ressources ».
Utilisateurs et groupes locaux	Ce module donne accès à la liste des utilisateurs et des groupes utilisateur configurés sur le système.
Performances	L'analyseur vous permet de mesurer les performances de votre ordinateur. Consultez le chapitre « Optimiser le système » pour plus d'informations sur cet utilitaire.
Gestionnaire de périphériques	Cet outil permet de visualiser l'ensemble des composants et des périphériques connectés à l'ordinateur. Pour en savoir plus, consultez le chapitre 4 « Configurer le matériel ».
Stockage	Cette rubrique ne contient qu'un seul utilitaire : l'outil *Gestion des disques*. Il permet de visualiser et de gérer les partitions de vos disques durs. Si vous souhaitez avoir plus d'informations sur son fonctionnement, lisez le chapitre 6 « Stocker les données ».

Paramétrage avancé des options de démarrage du système

ATTENTION **Paramétrage à hauts risques**

Ce paramétrage avancé est parfois risqué. N'effectuez de modifications avec cet utilitaire que si vous êtes certain de ce que vous faites.

La fenêtre de configuration du système fait partie des composants d'administration essentiels. Elle sert à personnaliser le démarrage du système, c'est-à-dire les éléments qu'il exécute, mais également les paramètres du noyau de Windows.

Pour utiliser cette fenêtre, ouvrez le menu *Démarrer*, et tapez `msconfig` dans la zone de saisie, puis appuyez sur la touche *Entrée*. Vous devez disposer d'un compte administrateur pour accéder à cette fonctionnalité.

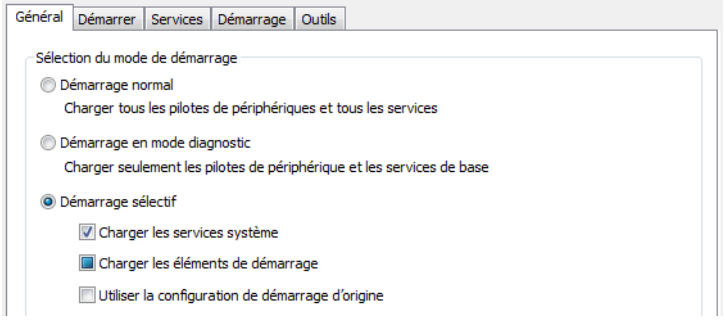


Figure 3–9
Fenêtre Configuration du système

La configuration générale du démarrage Windows s'effectue dans le premier onglet intitulé *Général*. Vous y définissez le mode de démarrage de Windows, un peu comme le menu alternatif affiché lors du *boot*, lorsque vous appuyez sur la touche F8. Vous configurez ainsi un mode diagnostic (*safe mode*) qui permet d'une part d'avoir un système exécutant le minimum d'éléments, et d'autre part de diagnostiquer les éventuels problèmes du système.

Si vous souhaitez paramétrer de façon plus précise les options du bootloader, ouvrez le deuxième onglet, *Démarrer*. Il représente en quelque sorte l'interface graphique de l'utilitaire `bcdedit.exe` (présenté dans le chapitre précédent).

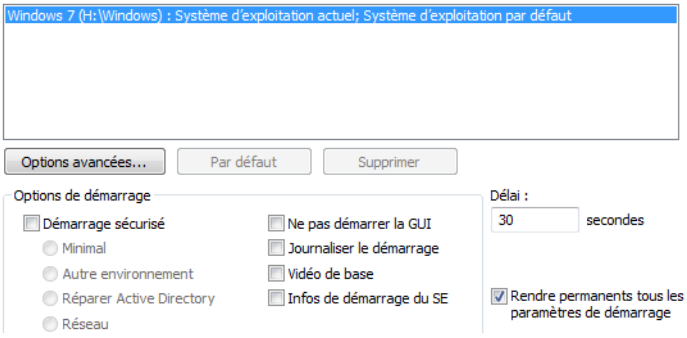


Figure 3–10
Configuration des options de démarrage

Lors du démarrage de Windows, un certain nombre de services démarrent automatiquement. Via le troisième onglet, *Services*, vous contrôlez l'activation et le démarrage des services Windows. Il s'agit d'une version simplifiée de la console Gestion des services (`services.msc`), mais elle autorise la désactivation de tous les services Windows en une seule opération. Si vous rencontrez des problèmes avec un service sans arriver à déterminer lequel est en cause, désactivez les services un à un et vérifiez si le problème est toujours présent au redémarrage du système.

Outre les services Windows, des logiciels supplémentaires peuvent se lancer automatiquement au démarrage de la machine. Il s'agit par exemple de votre logiciel de messagerie instantanée ou bien d'un utilitaire de gestion de la carte graphique, pour ne citer que deux exemples. Le quatrième onglet, *Démarrage*, permet de visualiser et de contrôler tous ces logiciels s'exécutant au démarrage. Qu'ils aient été enregistrés dans la clé `Run` du registre ou dans le dossier *Démarrage* du menu *Démarrer*, vous pouvez les activer ou désactiver à votre guise.

Enfin, le cinquième et dernier onglet, nommé *Outils*, contient des lignes de commandes préconfigurées afin d'ouvrir des interfaces d'administration. Il ne s'agit pour la plupart que de raccourcis vers des éléments du panneau de configuration. Vous y trouvez également l'accès au registre Windows ou à l'invite de commandes.

EN COULISSE

Les logiciels lancés au démarrage

Il existe huit emplacements qui servent à définir les applications qui seront lancées au démarrage du système, certaines avant l'ouverture d'une session Windows, d'autres, après l'ouverture. Ces emplacements sont, dans l'ordre d'exécution :

- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices`
- `<Invite d'ouverture de session>`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
- `Dossier de démarrage`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`

Néanmoins, si vous subissez une attaque virale, certains virus se chargent discrètement en remplaçant les fichiers de certains exécutables et il devient alors difficile de les détecter de cette manière.

Propriétés du système

Pour obtenir des informations importantes sur votre système, consultez le panneau de propriétés du système. Voici comment y accéder :

1. Ouvrez le menu *Démarrer.*
2. Cliquez avec le bouton droit sur *Ordinateur.*
3. Choisissez *Propriétés* dans le menu contextuel. Vous pouvez également y accéder rapidement en utilisant le raccourci clavier *Windows+Pause*.

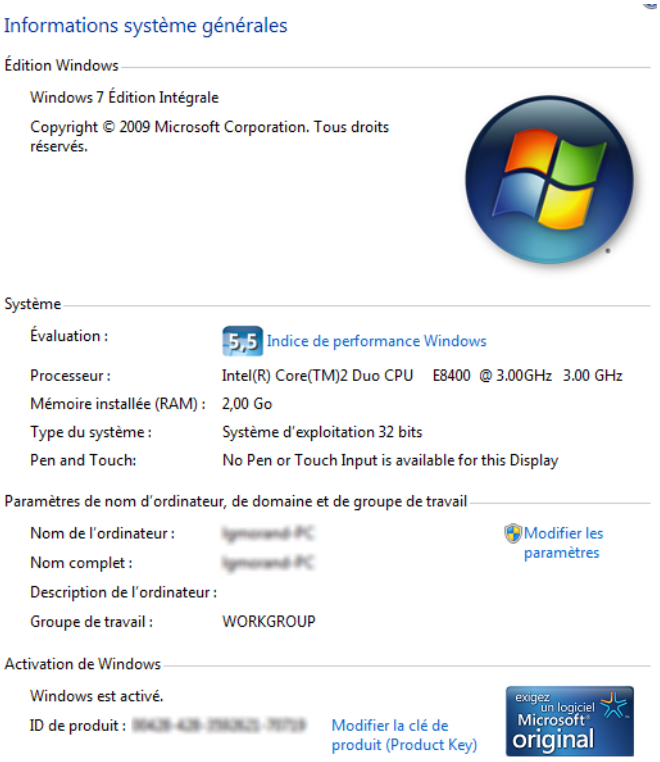


Figure 3–11
Propriétés système

Dans cette fenêtre, le cadre *Édition Windows* indique la version de Windows 7 actuellement installée sur votre ordinateur.

Dans le cadre *Système*, s'affiche l'évaluation de votre ordinateur et ses caractéristiques techniques (processeur, mémoire vive, architecture 32 ou 64 bits).

Le cadre suivant, intitulé *Paramètres de nom d'ordinateur, de domaine et de groupe de travail*, rappelle le nom de l'ordinateur, donne sa description et le nom du groupe de travail auquel il appartient. Modifiez ces informations en cliquant sur le lien *Modifier les paramètres*.

L'évaluation de l'ordinateur

L'évaluation de l'ordinateur est un score calculé par Windows qui évalue votre ordinateur en fonction de plusieurs caractéristiques matérielles. Les éléments matériels évalués sont le processeur, la mémoire, le disque dur et la carte graphique. Les fabricants de jeux vidéo indiquent parfois un score d'évaluation minimal pour utiliser le jeu. Ce chiffre vous permet de savoir si votre ordinateur est compatible avec le jeu sans avoir à étudier toutes les caractéristiques matérielles requises. Pour en savoir plus à ce sujet, consultez le chapitre 12, « Optimiser le système ».

Le dernier cadre de la fenêtre *Système* concerne l'activation de Windows. Ce dispositif vérifie que vous utilisez une version officielle de Windows 7 et non une version piratée.

Certaines paramètres supplémentaires sont accessibles dans la colonne de gauche :

- *Gestionnaire de périphériques* : affiche la liste des périphériques, permet de modifier les paramètres et de mettre à jour les pilotes. Pour en savoir plus, consultez le chapitre 4, « Configurer le matériel ».
- *Paramètres d'utilisation à distance* : active l'Assistance à distance afin d'autoriser un utilisateur distant à se connecter à votre ordinateur pour résoudre un problème. Pour en savoir plus, consultez le chapitre 15, « Résoudre les problèmes de Windows 7 ».
- *Protection du système* : gère les paramètres de la restauration du système. Vous pouvez définir les paramètres des points de restauration pour chacun des disques et déclencher manuellement la création d'un point de restauration.
- *Paramètres système avancés* : donne accès aux paramètres de performances avancées, aux profils utilisateur et de démarrage du système. Il sert également à modifier la configuration de la mémoire virtuelle.

Propriétés avancées du système

Nous venons de le voir, la fenêtre *Système* permet de connaître un certain nombre d'informations concernant le système. Mais Windows 7 dispose d'une fenêtre de paramétrage avancé du système proposant des options avancées de configuration. Pour y accéder, suivez la procédure suivante :

1. Ouvrez le menu *Démarrer*.
2. Cliquez avec le bouton droit sur *Ordinateur*, puis cliquez sur *Propriétés*.
3. Cliquez ensuite sur le lien *Paramètres système avancés* dans la colonne de gauche.

La fenêtre des paramètres système avancés s'affiche. Elle se présente sous la forme d'une boîte à onglets. Voyons les fonctionnalités qu'elle met à notre disposition.

Paramètres système avancés

Le premier onglet donne accès à quatre fenêtres de paramétrages, accessibles via les différents boutons présents.

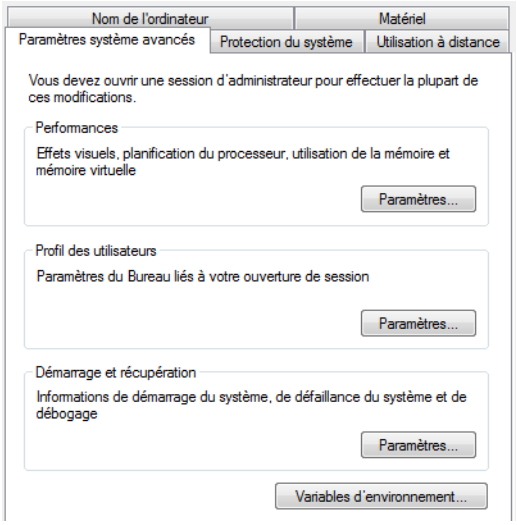


Figure 3–12
Onglet Paramètres système avancés

Le premier cadre intitulé *Performances* donne accès au paramétrage des effets visuels de Windows et à la mémoire virtuelle. Nous traiterons ces aspects au chapitre 12, « Optimiser le système ».

Le bouton *Paramètres...* situé dans le cadre *Profil des utilisateurs* sert à modifier le type de profil pour chaque utilisateur (local ou itinérant), en particulier lorsque votre ordinateur est connecté à un réseau et appartient à un domaine.

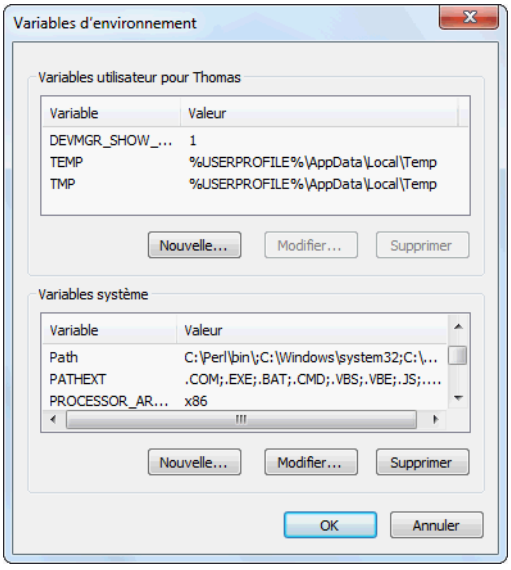


Figure 3–13
Fenêtre de modification des variables d'environnement

Intitulé *Démarrage et récupération*, le troisième cadre donne accès aux options de démarrage de Windows 7 ainsi qu'aux options définissant le comportement de l'ordinateur en cas de plantage de Windows. Pour modifier cette configuration, cliquez sur le bouton *Paramètres...*

Grâce au bouton situé au bas de l'onglet, modifiez les variables d'environnement du système. Définies au niveau du système (variables communes à tous les utilisateurs) ou au niveau de l'utilisateur, elles spécifient un certain nombre de valeurs utiles à plusieurs applications. Nous y trouvons notamment le Path, qui contient la liste des dossiers contenant des programmes exécutables. Pour modifier ces variables, cliquez sur le bouton *Variables d'environnement...*

Utilisation à distance

Avec cet onglet, vous activez l'Assistance à distance, ainsi que le Bureau à distance. La première fonctionnalité permet à un ami de se connecter à votre ordinateur sans se déplacer. Grâce à la seconde, vous pourrez accéder à votre ordinateur, comme si vous vous trouviez devant. Cet onglet vous sera notamment utile pour la résolution de problèmes, comme nous le verrons au chapitre 15, « Résoudre les problèmes de Windows 7 ».

Nom de l'ordinateur

Le nom et la description de l'ordinateur correspondent à son identité sur le réseau local. Pour modifier le nom de l'ordinateur ou le groupe de travail, cliquez sur le bouton *Modifier...* Saisissez ensuite le nouveau nom de l'ordinateur, puis cliquez sur *OK*.

Si vous souhaitez vous connecter à un domaine ou à un groupe de travail, démarrez l'assistant de configuration en cliquant sur le bouton *Identité sur le réseau*.

ALLER PLUS LOIN **Gérer le matériel**

L'onglet *Matériel* vous donne accès au Gestionnaire de périphériques et aux paramètres d'installation des périphériques. Pour en savoir plus à ce sujet, consultez le chapitre 4, « Configurer le matériel ».

Paramétrer les programmes par défaut

Rapidement, vous équipez votre système d'exploitation de dizaines de logiciels différents. Certains sont parfois redondants et il y a fort à parier que vous disposez de plusieurs logiciels capables d'effectuer la même opération, qu'il s'agisse de programmes de retouche d'images ou d'éditeurs de texte. C'est la raison pour laquelle il arrive parfois que le système ouvre un fichier avec un logiciel autre que celui escompté.

Si, dans XP, il fallait définir pour chaque extension de fichier le programme à utiliser, il est possible sous Windows 7, de choisir le programme et de lui attacher les extensions associées.

Associer un programme à un type de fichier

Windows propose une fonctionnalité pour configurer rapidement les programmes utilisés par défaut sur le système et les types de fichiers qu'ils gèrent.

1. Ouvrez le menu *Démarrer*.
2. Cliquez sur *Programmes par défaut*.
3. Cliquez sur *Définir les programmes par défaut*.
4. En cliquant sur l'un des programmes de la liste, vous décidez de l'utiliser par défaut pour tous les types de fichiers qu'il prend en charge ou de choisir manuellement les extensions et les protocoles qui seront ouverts par ce programme.
5. Cliquez ensuite sur *OK* pour enregistrer les changements.

Associer manuellement un type de fichier ou un protocole à un programme

Pour les types de fichiers ou les extensions particulières, il est possible de procéder au cas par cas et donc de prendre les extensions une par une, puis de choisir, parmi la liste de tous les programmes installés, celui qui s'ouvrira par défaut.

1. Ouvrez le menu *Démarrer*.
2. Cliquez sur *Programmes par défaut*.
3. Cliquez sur *Associer un type de fichier ou un protocole à un programme*. Windows 7 affiche alors la liste des extensions et protocoles disponibles. Les extensions se trouvent en tête de liste et les protocoles en bas.
4. Sélectionnez l'extension ou le protocole à associer à votre programme, puis cliquez sur le bouton *Changer le programme*.
5. Choisissez le programme parmi la liste affichée. Les programmes recommandés sont affichés en premier. Pour afficher d'autres programmes, cliquez sur la petite flèche bleue sur la ligne *Autres programmes*. Si votre programme n'est pas listé, cliquez sur le bouton *Parcourir*, puis indiquez le chemin de l'exécutable du programme.

Les modifications que vous réalisez dans cette fenêtre ne s'appliquent qu'à votre compte utilisateur et n'affecteront pas les autres utilisateurs du système.

EN PRATIQUE Programme absent de la liste

Si le programme que vous recherchez n'est pas dans cette liste, utilisez *Associer un type de fichier ou un protocole à un programme*.

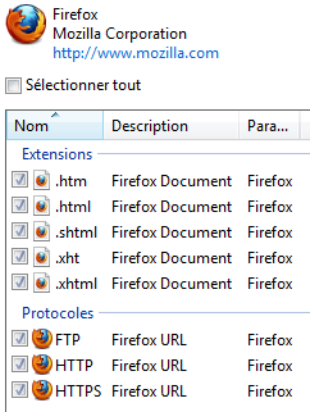


Figure 3–14
Personnalisation des extensions et protocoles qui seront ouverts par Firefox

ATTENTION Extension

Il est impossible de supprimer une association de programme pour une extension : vous devez choisir un nouveau programme à utiliser. Ainsi, la prochaine fois que vous ouvrirez ce type de fichier, le système saura avec quel logiciel l'ouvrir.

Configurer l'exécution automatique

L'exécution automatique est le mécanisme de lancement qui se déclenche lors de l'activation d'un périphérique amovible, qu'il s'agisse d'un CD-Rom, d'une clé USB, d'un lecteur MP3 ou même d'un appareil photo. En effet, lorsque vous introduisez un CD-Rom dans votre ordinateur ou que vous connectez un périphérique sur un port USB, l'exécution automatique affiche une fenêtre pop-up qui propose plusieurs actions, qui dépendent du type de périphérique branché. Ainsi, lorsque vous insérerez un CD-Rom contenant des fichiers musicaux, il vous est proposé de les lire à l'aide du Lecteur Windows Media, ou de tous les autres logiciels installés capables de lire ces fichiers. Sur le même principe, en branchant un appareil photo numérique, il vous est proposé d'ouvrir les photos contenues sur le périphérique, de les importer, d'en afficher un diaporama, etc.

Vous pouvez tout à fait configurer une action par défaut pour chaque type de périphérique. Ainsi, vous n'aurez plus de fenêtre de choix par la suite. De cette façon, il est possible de forcer le système à lire automatiquement les morceaux de musique chaque fois que vous insérez un CD audio dans le lecteur de disques. Cette configuration est très rapide et peut se faire de deux façons.

La première méthode repose sur l'utilisation quotidienne de votre ordinateur. Lorsque la fenêtre d'exécution automatique s'affiche, cochez la case *Toujours utiliser cette action pour ce périphérique*, puis cliquez sur l'action de votre choix.

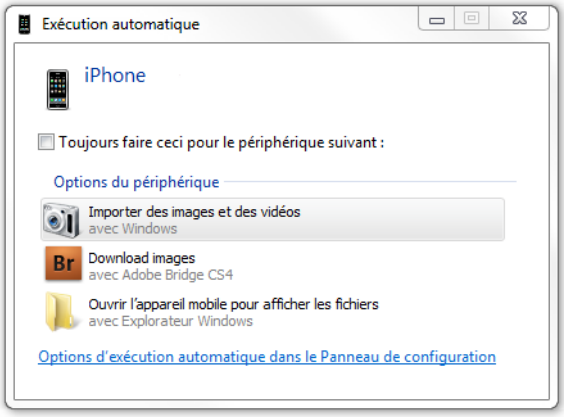


Figure 3–15
Fenêtre d'exécution automatique lors de l'insertion d'un périphérique amovible

Un peu plus longue, la seconde méthode a l'avantage de permettre de configurer d'un seul coup toutes les actions à entreprendre en fonction du type de périphérique.

1 Ouvrez le menu *Démarrer*
2 Saisissez `exécution automatique` dans la zone de recherche.
3 Ouvrez *Exécution automatique*.

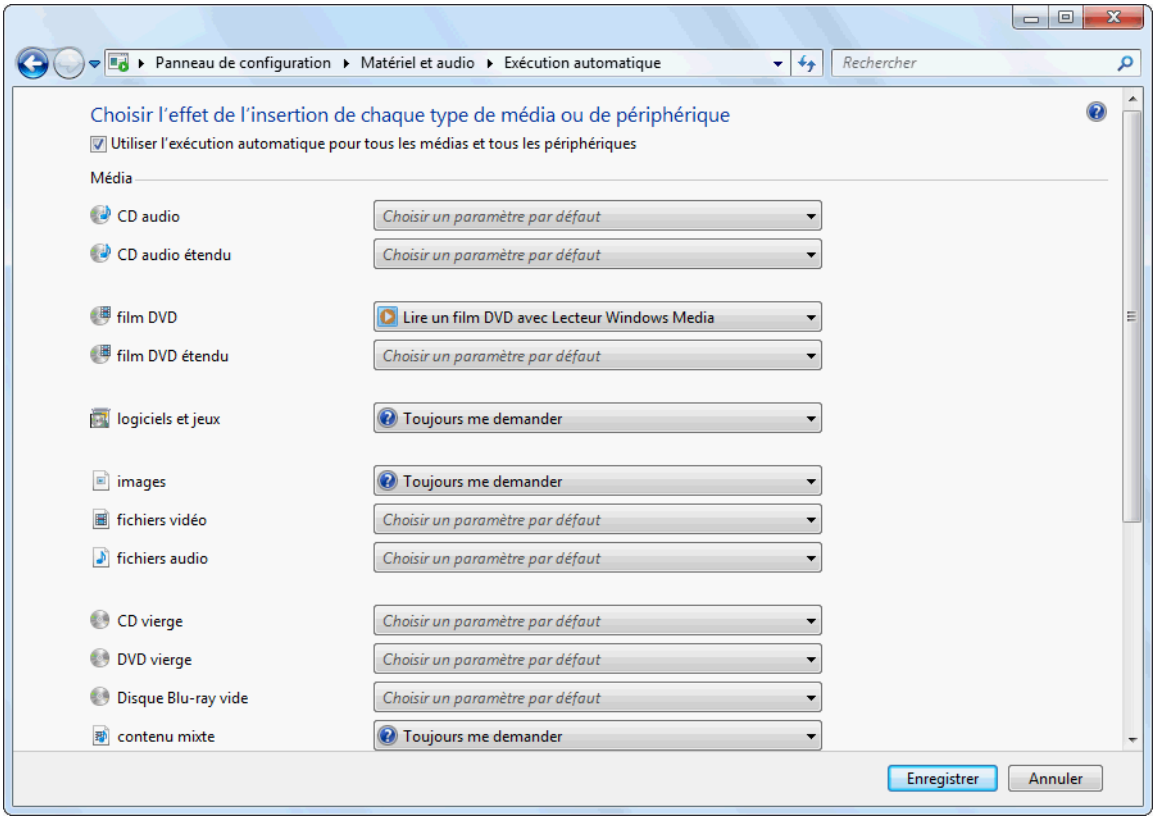


Figure 3–16 Paramétrage de l'exécution automatique

4 Les différents types de médias reconnus par votre système sont alors listés. En face de chacun, une liste d'actions disponibles est proposée. Choisissez pour chaque média ou type de contenu, l'action qui s'effectuera par défaut.
5 Une fois le paramétrage terminé, cliquez sur *Enregistrer*.

ASTUCE Désactiver temporairement l'exécution automatique

Il est possible de désactiver temporairement l'exécution automatique lors de l'insertion de votre périphérique. Pour cela, maintenez la touche *Maj* enfoncée le temps de l'insertion du média ou du périphérique. La fenêtre d'exécution automatique ne devrait alors pas apparaître.

ASTUCE Désactiver entièrement l'exécution automatique

Plutôt que de définir pour chaque périphérique l'option *Ne rien faire*, il est plus rapide de décocher au sein du panneau de paramétrage de l'exécution automatique, la case *Utiliser l'exécution automatique pour tous les médias et tous les périphériques*. L'exécution automatique ne s'exécutera plus jamais, y compris pour l'installation ou le branchement de nouveaux périphériques.

Mettre à jour le système avec Windows Update

Windows Update est le dispositif fourni par Microsoft pour appliquer des mises à jour au système. Lorsque des bogues ou des problèmes de sécurité sont découverts dans le système, Microsoft publie des correctifs et des mises à jour. Il est fondamental pour garder un système sain, optimisé, stable et sécurisé d'effectuer régulièrement ces mises à jour.

Contrairement aux versions antérieures à Windows Vista, les mises à jour Windows Update ne se font plus directement depuis un site Internet. Dans Windows 7, Windows Update s'utilise et se paramètre depuis un module du panneau de configuration. Voici comment y accéder :

1. Ouvrez le menu *Démarrer.*
2. Tapez `update` dans la barre de recherche.
3. Appuyez sur *Entrée* ou cliquez sur *Windows Update*.

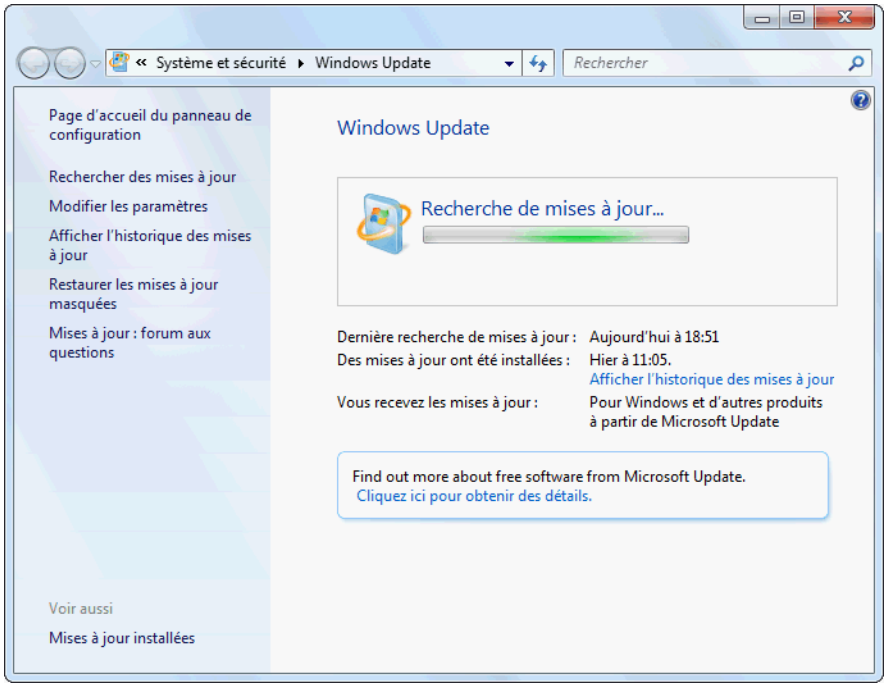


Figure 3–17
Recherche de mise à jour avec Windows Update

La fenêtre qui s'ouvre affiche les mises à jour disponibles. Grâce à elle, vous effectuez manuellement une mise à jour ou définissez les différents paramètres de Windows Update.

Le cadre au centre de la fenêtre indique l'état actuel de Windows Update. Il signale, par exemple, si des mises à jour sont disponibles ou si une recherche ou une installation de mises à jour est en cours.

Dans cette fenêtre, vous retrouvez la date et l'heure des dernières recherches de mise à jour, ainsi que la date des dernières installations de mises à jour. En cliquant sur le lien *Afficher l'historique des mises à jour*, vous consultez la liste des mises à jour installées sur le système ainsi que leurs dates d'installation.

Installer les mises à jour « à la demande »

Pour vérifier si de nouvelles mises à jour sont disponibles, cliquez sur le lien *Rechercher des mises à jour* dans la colonne de gauche. Vous devez, bien sûr, être connecté à Internet pour pouvoir détecter les mises à jour disponibles. Les mises à jour ont plusieurs niveaux d'importance :

- Importante : il est impératif d'installer les mises à jour de ce niveau, car elles corrigent des problèmes de sécurité ou de fiabilité.
- Recommandée : ces mises à jour corrigent des problèmes non critiques. Cependant, leur installation améliore sensiblement l'utilisation de votre système ou ajoute de nouvelles fonctionnalités (par exemple, un jeu Premium ou une nouvelle version du framework .NET).
- Facultative : ces mises à jour apportent des correctifs mineurs ou des fonctionnalités supplémentaires. Par exemple, dans Windows 7 Ultimate, il est possible d'installer d'autres langues pour le système via des mises à jour facultatives.

Culture **Patch Tuesday... Exploit Wednesday**

En règle générale, les mises à jour de Windows sont publiées de manière groupée le deuxième mardi de chaque mois. Cet événement est appelé *Patch Tuesday* (patch du mardi, en français). Cette manière de distribuer les patchs a été mise en place pour faciliter la tâche aux administrateurs de parcs informatiques. En effet, ils doivent mettre à jour un grand nombre de machines et s'assurer que tout le parc fonctionne encore après l'installation du correctif. La date d'arrivée des mises à jour étant connue d'avance, les administrateurs peuvent ainsi prévoir leur installation. Le mardi a d'ailleurs été choisi pour que les mises à jour n'arrivent pas en tout début de semaine et que l'installation se fasse suffisamment loin du week-end afin de pouvoir corriger d'éventuels problèmes.
Cette régularité a amené une autre coutume moins rassurante : en effet, certains hackers profitent de l'arrivée des patchs pour les étudier. Ils déduisent alors la vulnérabilité qui a été corrigée et tentent d'attaquer tous les ordinateurs n'ayant pas encore été mis à jour. Cette « coutume » porte le nom de *Exploit Wednesday* (exploit du mercredi, en français).
Lorsqu'elles sont particulièrement urgentes, certaines mises à jour peuvent être publiées en dehors des dates prévues si la faille de sécurité qu'elles corrigent est critique.

Si des mises à jour importantes ou recommandées sont disponibles, cliquez sur le bouton *Installer les mises à jour* pour mettre à jour votre système. Vous pouvez sélectionner individuellement les mises à jour à installer en cliquant sur les liens indiquant le nombre de mises à jour disponibles. Cochez ensuite les mises à jour que vous souhaitez installer.

Désinstaller une mise à jour

Un système à jour est un système plus sécurisé, plus fiable et plus stable. Il arrive cependant qu'une mise à jour instable endommage le système. Cette défaillance peut provenir de la mise à jour elle-même ou bien, tout simplement, d'une incompatibilité avec un logiciel ou un matériel installé.

Généralement, ce genre de problème est vite repéré, réglé par Microsoft et une nouvelle mise à jour est rapidement disponible. En attendant que ce soit effectivement le cas, il est conseillé de désinstaller la mise à jour incriminée et d'attendre la prochaine. Pour supprimer une mise à jour, rien de plus simple :

1. Ouvrez le *Panneau de Configuration*, cliquez sur *Programmes*.
2. Cliquez sur *Afficher les mises à jour installées*. Un panneau liste alors par type de produits toutes les mises à jour présentes sur le système.
3. Il vous suffit de sélectionner la mise à jour de votre choix et, à l'aide d'un clic droit de la souris, de choisir *Désinstaller* dans le menu contextuel .

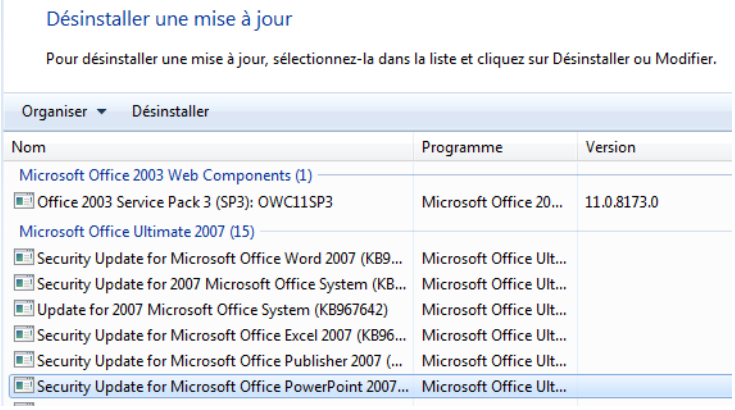


Figure 3–18
Panneau de gestion des mises à jour installées

Paramétrer Windows Update

Plusieurs options sont disponibles pour paramétrer le fonctionnement de Windows Update. Pour y accéder, cliquez sur le lien *Modifier les paramètres* dans la colonne de gauche de Windows Update.

ASTUCE Effacer de la liste une mise à jour

Vous ne souhaitez pas installer l'une des mises à jour et désirez qu'elle n'apparaisse plus dans la liste ? Cliquez avec le bouton droit sur la mise à jour, puis sélectionnez *Masquer cette mise à jour* dans le menu contextuel. La mise à jour n'apparaîtra plus parmi les autres.
Pour la rendre de nouveau visible, cliquez dans la fenêtre *Windows Update* sur le lien *Restaurer les mises à jour masquées*, situé dans la colonne de gauche. Vous pourrez alors choisir les mises à jour que vous ne voulez plus masquer.

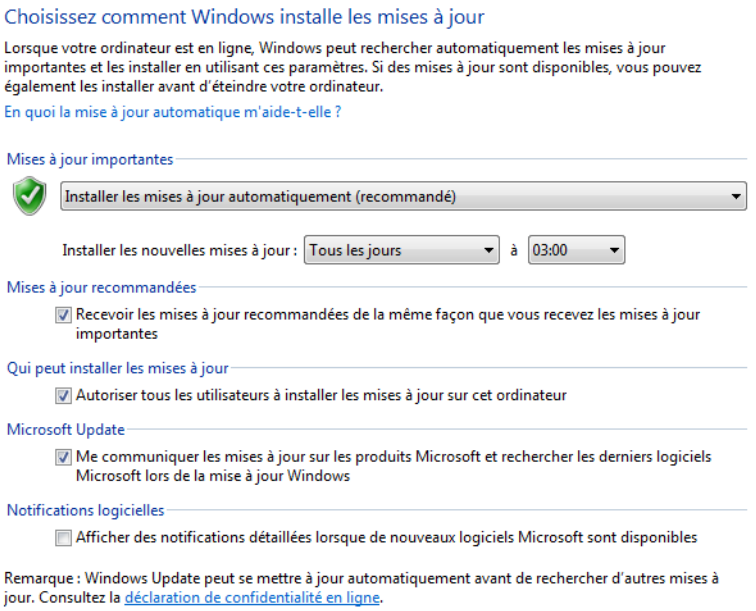


Figure 3–19
Fenêtre de paramétrage de Windows Update

Vous avez la possibilité de choisir la façon dont les mises à jour seront installées sur votre système, mais attention cependant, Windows recommande par défaut d'installer automatiquement les mises à jour. En effet, ceci évite d'oublier de mettre à jour le système et vous permet ainsi de le maintenir stable et sûr. Vous avez le choix des jours et heures de leur installation. Optez de préférence pour un créneau horaire où l'ordinateur est généralement allumé, sans quoi la mise à jour ne se fera pas.

1. Sous le titre *Mises à jour importantes*, choisissez *Installer les mises à jour automatiquement (recommandé)* dans la liste déroulante.
2. Choisissez ensuite les jours où les mises à jour s'installeront. Cette mise à jour peut être quotidienne ou hebdomadaire : sélectionnez le jour de la semaine de votre choix.
3. Sélectionnez dans la dernière liste déroulante l'heure d'installation des mises à jour.

Par défaut, seules les mises à jour importantes sont installées lors d'une installation manuelle ou automatique. Vous installez également les mises à jour recommandées en cochant la case *Recevoir les mises à jour recommandées de la même façon que vous recevez les mises à jour importantes*.

Si vous désirez empêcher les utilisateurs non administrateurs d'installer les mises à jour, décochez la case *Autoriser tous les utilisateurs à installer les mises à jour sur cet ordinateur*. Ainsi, seuls les administrateurs seront habilités à installer les mises à jour Windows.

PRATIQUE

Mise à jour d'autres produits Microsoft

Dans les options, vous pouvez bénéficier de Microsoft Update, qui permet de recevoir des mises à jour pour des produits Microsoft autres que Windows, comme Microsoft Office. Pour l'activer, cochez la case *Me communiquer les mises à jour sur les produits Microsoft et rechercher les derniers logiciels Microsoft lors de la mise à jour Windows*.

En résumé

Dans ce chapitre, nous nous sommes intéressés au panneau de configuration, ainsi qu'au fonctionnement du planificateur de tâches de Windows 7 et de la console de gestion de l'ordinateur. Nous avons également vu comment modifier les paramètres du système et comment le mettre à jour grâce à Windows Update.

chapitre 4

Configurer le matériel

Un ordinateur est constitué de différents composants internes tels que la mémoire vive, les disques durs et les lecteurs de disques optiques (CD-Rom, DVD-Rom, Blu-Ray), ainsi que de nombreux périphériques externes tels que le clavier, la souris, l'imprimante, les haut-parleurs ou encore un vidéoprojecteur. Le système d'exploitation garantit le bon fonctionnement des différents composants et périphériques et assure la communication entre eux mais également avec l'utilisateur.

SOMMAIRE

- Signature des pilotes
- Gestionnaire de périphériques
- Panneau Périphériques et imprimantes
- Paramétrage d'imprimantes
- Configuration du clavier, de la souris, du vidéoprojecteur et des périphériques audio
- Centre de mobilité pour les ordinateurs portables

MOTS-CLÉS

- Pilote
- Signature
- Périphérique
- Plug and play
- Imprimante
- Clavier
- Souris
- Sons système
- Micro
- Volume audio
- Vidéoprojecteur
- Résolution et orientation de l'écran
- Centre de mobilité

Tous les périphériques d'un ordinateur communiquent avec le système d'exploitation via des petits programmes appelés pilotes (*drivers* en anglais). Ces pilotes sont fournis et maintenus par le fabricant du matériel. Certains périphériques importants comme le processeur, la mémoire... sont automatiquement reconnus par le système, ainsi que certains moins importants tels que les clés USB. Pour les autres en revanche, ces pilotes doivent être installés pour permettre au système d'exploitation de les utiliser.

Lorsque Windows 7 détecte la connexion d'un périphérique plug and play, il tente d'installer automatiquement le pilote via Windows Update, le système de mise à jour par Internet. En effet, de nombreux fabricants fournissent des mises à jour de leurs pilotes par ce moyen.

Signature des pilotes

TERMINOLOGIE Signé

L'origine de cette appellation est simple : la validation du pilote par Microsoft est effectuée par une signature numérique infalsifiable.

On dit que certains pilotes de périphériques sont signés. Cela signifie que Microsoft a vérifié que le pilote est compatible avec le système d'exploitation et permet à Windows 7 de savoir si le pilote installé est reconnu ou non par Microsoft. En effet, la signature garantit que le pilote est bien original et n'a pas été modifié par un programme malveillant, par exemple, car toute tentative de modification d'un pilote détruit automatiquement la signature associée.

Cette signature a une incidence sur l'installation du pilote. Si un pilote est signé, tous les utilisateurs de la machine peuvent l'installer. En revanche, seul l'administrateur de la machine peut installer un pilote non signé. Voici comment afficher la liste des pilotes non signés présents sur votre système :

1 Ouvrez le menu *Démarrer*, saisissez `sigverif` dans la barre de recherche, puis appuyez sur *Entrée*.

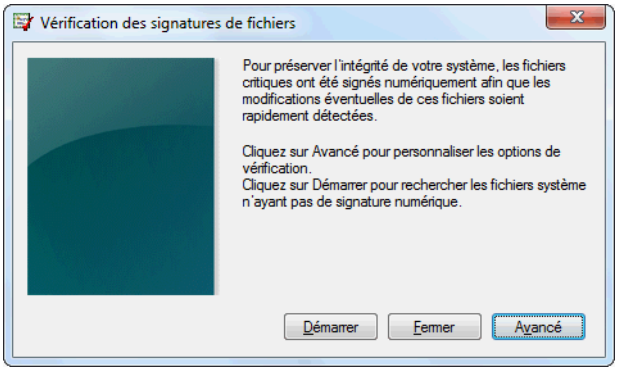


Figure 4–1
Utilitaire de vérification des signatures

2 Utilisez le bouton *Démarrer* pour lancer l'analyse. Avec le bouton *Avancé,* définissez un fichier dans lequel les résultats seront enregistrés.

3 Après l'analyse, l'utilitaire affiche la liste des fichiers non signés qu'il a détectés. Il peut s'agir de pilotes ou de fichiers inclus avec le pilote (par exemple, un fichier d'aide).

4 Si vous trouvez des pilotes non signés, rendez-vous sur le site du constructeur du matériel pour trouver une version signée du pilote.

Gestionnaire de périphériques et pilotes

Le gestionnaire de périphériques sert à installer ou à mettre à jour les drivers, et à gérer les paramètres matériels des composants de votre ordinateur. Celui de Windows 7 se présente sous la même forme que dans les versions antérieures de Windows, c'est-à-dire sous la forme d'une arborescence contenant l'ensemble des périphériques constituant le système regroupés par thème. Les périphériques présents sont les périphériques internes et externes.

Le gestionnaire de périphériques est accessible depuis plusieurs emplacements sur le système. La méthode d'accès la plus rapide est la suivante :

1 Ouvrez le *Panneau de configuration*.

2 Rendez-vous ensuite dans *Système et sécurité*.

3 Cliquez dans la colonne de gauche sur *Gestionnaire de périphériques*.

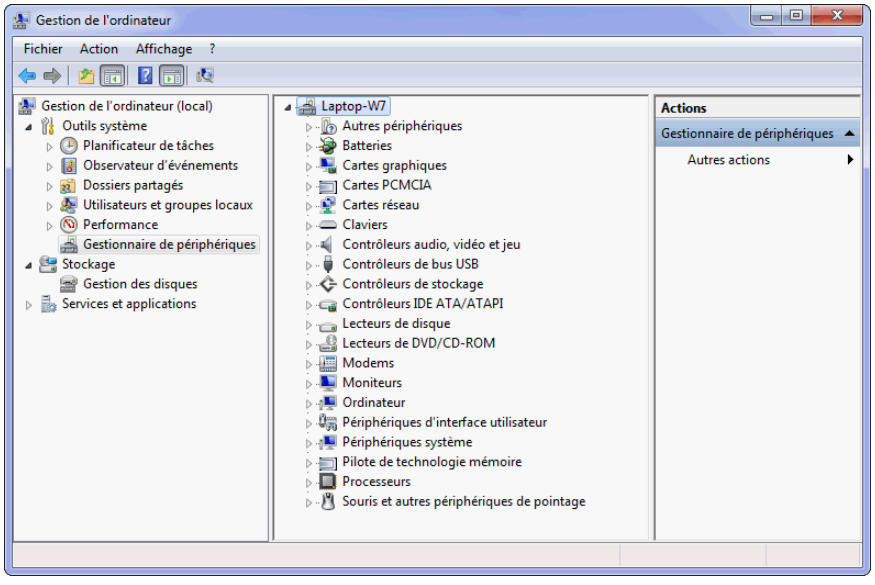


Figure 4–3
Le gestionnaire de périphériques

ALTERNATIVE Ouvrir le gestionnaire de périphériques

D'autres possibilités s'offrent à vous pour accéder au gestionnaire de périphériques :

- utiliser la combinaison de touches *Windows+Pause*, puis cliquer sur *Gestionnaire de périphériques* dans la colonne de gauche ;
- cliquer avec le bouton droit sur *Ordinateur* dans le menu *Démarrer* et choisir *Gérer*. Le gestionnaire de périphériques est ensuite accessible dans la colonne de gauche ;
- taper `gestionnaire de périphériques` dans la zone de recherche du menu *Démarrer*.

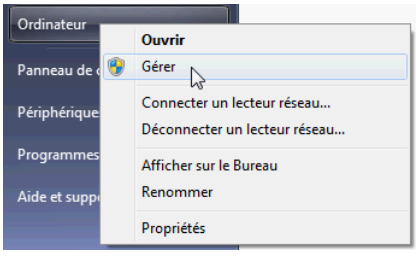


Figure 4–2 Accès au gestionnaire de périphériques par le menu Démarrer

ASTUCE Lancer le gestionnaire de périphériques en ligne de commande

La fenêtre du gestionnaire de périphériques peut s'ouvrir à partir d'une invite de commandes Windows ou d'un fichier batch. Il suffit de saisir la commande suivante : `mmc devmgmt.msc`

Point de raccordement

Le point de raccordement indique le matériel auquel le périphérique est physiquement connecté. Par exemple, si votre ordinateur dispose d'une carte SCSI, les périphériques raccordés à cette carte seront listés sous la carte SCSI dans le gestionnaire de périphériques.

Par défaut, les périphériques sont organisés par types, il est possible de les trier suivant leur point de raccordement à la carte mère. Pour cela, dans le menu *Affichage*, cliquez sur *Périphériques par connexion*.

Le nœud racine (premier élément de la liste, ici *Laptop-W7*) représente l'ordinateur lui-même. Il est possible de lancer une détection du matériel en cliquant avec le bouton droit sur cet élément, puis en choisissant dans le menu contextuel la ligne *Rechercher les modifications du matériel*.

Afficher l'état d'un périphérique

Tous les utilisateurs du système ont accès au gestionnaire de périphériques et peuvent afficher les propriétés. Cependant, seuls les administrateurs peuvent apporter des modifications à la configuration.

Si vous souhaitez vérifier que les pilotes d'un périphérique sont bien installés et que Windows communique correctement avec lui, consultez l'état avancé du matériel en ouvrant la branche correspondant au matériel, puis double-cliquez sur le périphérique dans la liste.

Dans l'onglet *Général*, la zone *État du périphérique* affiche une description de l'état actuel du matériel. Si le périphérique dysfonctionne, le type de problème est indiqué dans cette zone. Un code et un numéro de problème apparaissent également ainsi que des suggestions de solutions.

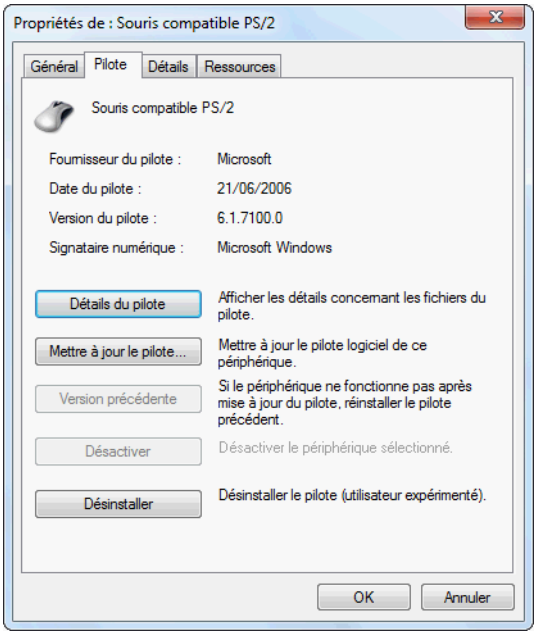


Figure 4–4
Onglet Pilote de la fenêtre de détails d'un périphérique

Pour avoir plus d'informations sur le pilote installé pour ce périphérique, allez dans l'onglet *Pilote*. Cliquez sur le bouton *Détails* du pilote pour visualiser la liste des fichiers constituant le pilote ainsi que leur emplacement sur le disque. En cliquant sur un élément de la liste, vous visualisez un numéro de version ainsi que le nom du fournisseur du pilote.

Le bouton *Mettre à jour le pilote* sert, comme son nom l'indique, à rechercher une version plus récente de pilote pour le périphérique sélectionné. Via l'assistant de mise à jour du pilote, vous pouvez soit rechercher directement un pilote sur Internet en utilisant Windows Update, soit fournir les fichiers du nouveau pilote à partir du disque dur ou d'un périphérique de stockage externe (clé USB, CD-Rom).

Le bouton *Désactiver* permet d'indiquer que ce périphérique ne doit plus être utilisé, mais qu'il doit tout de même rester installé sur le système. Une fois le périphérique désactivé, il apparaît dans le gestionnaire de périphériques en tant que matériel désactivé, mais il n'apparaît plus dans Windows. Par exemple, si vous désactivez le lecteur de DVD-Rom, il disparaîtra de l'explorateur Windows et ne sera plus détecté par les autres logiciels. Pour qu'il soit de nouveau accessible, il suffit de le réactiver via le gestionnaire de périphériques.

LIGNE DE COMMANDE **Lister les pilotes installés**

Windows 7 intègre un utilitaire en ligne de commande qui affiche la liste de tous les pilotes de périphériques installés sur la machine. Lancez-le en saisissant la commande `driverquery` dans une invite de commandes. Elle possède plusieurs options que vous découvrirez en saisissant `driverquery /?`.

Installer un périphérique plug and play

Pour installer un périphérique compatible plug and play, il suffit de le brancher. Certains périphériques tels que les clés USB ou la plupart des souris USB sont détectés et un pilote approprié est chargé par Windows, le rendant immédiatement utilisable. Si Windows ne prend pas en charge nativement le périphérique, la boîte de dialogue *Nouveau matériel détecté* s'affiche et vous propose trois choix :

- *Rechercher et installer le pilote logiciel* : cette option lance le processus d'installation du pilote de périphérique.
- *Me redemander ultérieurement* : ce choix permet de différer l'installation du pilote. Si le périphérique est toujours connecté au système lors de la prochaine ouverture de session, la boîte de dialogue apparaîtra à nouveau.
- *Ne plus afficher ce message pour ce périphérique* : si vous choisissez cette option, Windows n'installera pas de pilote et ne rendra pas ce périphérique opérationnel. Pour installer un pilote pour ce matériel, vous devrez alors débrancher, puis rebrancher le périphérique.

Dans le cas où vous avez choisi d'installer le pilote en sélectionnant l'option *Rechercher et installer le pilote logiciel*, Windows recherche sur Windows Update pour trouver un pilote adéquat.

Installer un périphérique non plug and play

Dans certains cas, notamment pour un matériel un peu ancien, Windows est incapable de le détecter automatiquement. Il est donc nécessaire de cliquer avec le bouton droit sur l'élément racine, puis de choisir l'option *Ajouter un matériel d'ancienne génération*. Il faudra alors fournir le pilote du périphérique.

L'assistant vous propose de tenter de détecter automatiquement le nouveau matériel ou bien d'opérer manuellement. Parfois, la détection automatique échoue et l'assistant propose alors une installation manuelle. Voici comment procéder :

1. Choisissez le type de périphérique dans la liste que vous propose l'assistant.

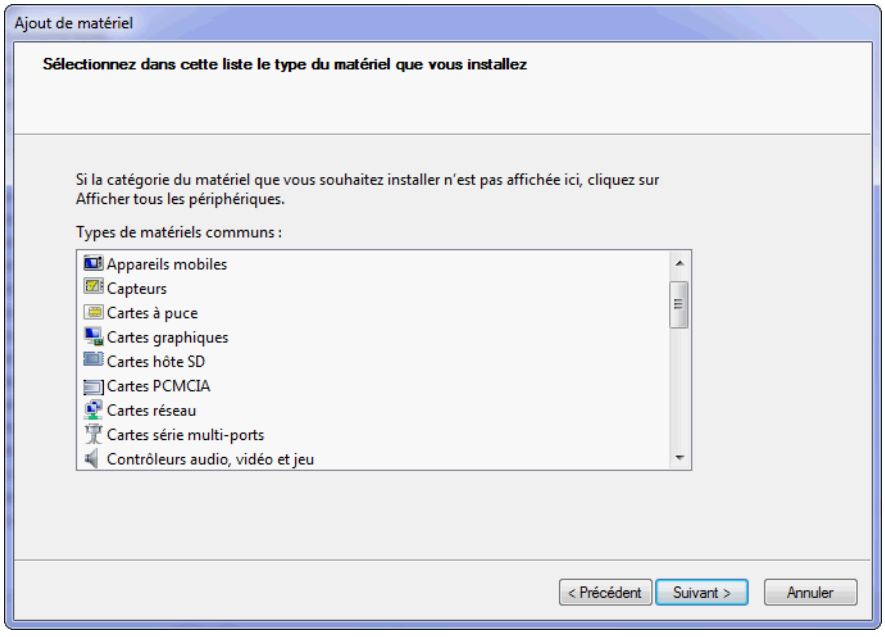


Figure 4–5
Liste des types de périphériques

2. Cliquez ensuite sur *Suivant*, puis choisissez le modèle de périphérique.
3. Si vous ne trouvez pas le modèle correspondant à votre matériel, munissez-vous du pilote fourni par le constructeur, puis cliquez sur le bouton *Disque fourni...* pour indiquer à Windows l'emplacement du pilote pour le périphérique.

Afficher les périphériques déconnectés

Vous l'avez sans doute remarqué, le gestionnaire de périphériques, par défaut, n'affiche que les périphériques actuellement connectés au sys-

tème. Toutefois, il faut savoir que lorsque vous ajoutez un nouveau matériel et que vous installez son pilote, celui-ci reste installé sur le système jusqu'à ce qu'il soit manuellement désinstallé. Ainsi, lorsque vous débranchez un périphérique de votre ordinateur, son pilote reste installé, mais il n'apparaît pas dans le gestionnaire de périphériques. Il est possible d'afficher les périphériques déconnectés dans le gestionnaire de périphériques en effectuant quelques manipulations.

1. Ouvrez tout d'abord le menu *Windows*.
2. Effectuez un clic droit sur *Ordinateur*, puis cliquez sur *Propriétés*.
3. Dans la fenêtre *Système* qui s'ouvre alors, cliquez sur *Paramètres système avancés* dans la colonne de gauche.
4. Cliquez sur *Variables d'environnement* puis, dans *Variables utilisateur*, cliquez sur le bouton *Nouvelle...*
5. Dans la zone *Nom de la variable*, saisissez `DEVMGR_SHOW_NONPRESENT_DEVICES` et dans la zone *Valeur de la variable*, tapez `1`.
6. Validez les trois fenêtres en cliquant sur le bouton *OK*.
7. Ouvrez à présent le gestionnaire de périphériques.
8. Dans le menu *Affichage*, cliquez sur *Afficher les périphériques cachés*. Les périphériques déconnectés du système, mais dont les pilotes sont installés, apparaissent alors en grisé dans le gestionnaire de périphériques.

Pour annuler cette opération et cacher à nouveau les périphériques déconnectés, retournez dans la fenêtre de configuration des variables d'environnement et supprimez la variable `DEVMGR_SHOW_NONPRESENT_DEVICES` que vous avez créée auparavant ou mettez sa valeur à `0`.

Afficher la puissance électrique requise par les périphériques USB

Le gestionnaire de périphériques fournit des informations sur les contrôleurs USB de votre ordinateur. Un contrôleur USB gère l'ensemble des périphériques USB branchés sur son bus. Vous pouvez visualiser l'intensité électrique fournie par le concentrateur et voir l'électricité que consomme chaque périphérique connecté. Voici comment accéder à ces informations :

1. Ouvrez le gestionnaire de périphériques.
2. Dans la liste des types de périphériques, déroulez la branche *Contrôleurs de bus USB*.
3. Double-cliquez sur l'un des concentrateurs USB.

Concentrateur

On appelle concentrateur le composant auquel les ports USB sont raccordés.

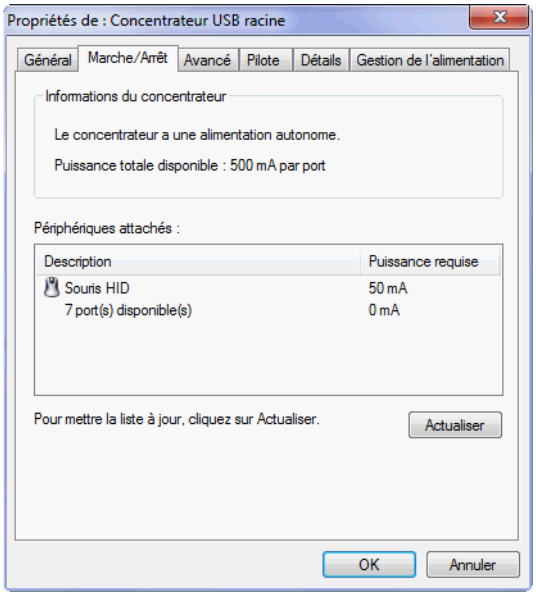


Figure 4–6
Fenêtre de propriétés d'un concentrateur USB – Onglet Marche/Arrêt. Ici, on constate qu'une souris USB est connectée et qu'elle a besoin de 50 mA pour fonctionner.

Vous remarquez que cette fenêtre de propriétés possède un onglet supplémentaire intitulé *Marche/Arrêt*. Dans cet onglet, vous pouvez voir la puissance du courant électrique délivré pour chaque port USB rattaché à ce concentrateur. Vous visualisez également les périphériques actuellement raccordés à ce concentrateur.

ATTENTION
Retirer un périphérique à chaud

Lorsque vous utilisez un périphérique qui prend en charge l'éjection, il est préférable de passer par l'outil *Suppression de matériel en toute sécurité* avant de le débrancher de l'ordinateur. En effet, si vous retirez par exemple une clé USB sans l'avoir « éjectée » auparavant, il est possible qu'au moment du retrait, Windows soit en train de lire ou d'écrire des données dessus. Comme l'opération ne peut alors se terminer correctement, des données peuvent être corrompues, voire perdues.

Débrancher un périphérique amovible

Certains types de périphériques doivent être « démontés » avant d'être débranchés du système, notamment les périphériques de stockage tels que les clés USB ou encore les disques durs externes.

L'éjection d'un périphérique est une procédure simple :

1. Cliquez dans la barre de notification (à côté de l'horloge) sur le bouton *Suppression de matériel en toute sécurité*.

Figure 4–7 Icône de suppression de matériel 

2. La liste des périphériques que vous pouvez alors retirer en toute sécurité s'affiche. Le type de périphérique est indiqué ainsi que la lettre de lecteur dans le cas d'un périphérique de stockage.
3. Cliquez sur le périphérique à éjecter dans la liste qui apparaît. Le message *Le périphérique peut être retiré en toute sécurité* s'affiche, indiquant que l'éjection s'est bien déroulée.

OUPS **Le périphérique n'apparaît pas dans la liste**

Si le périphérique que vous cherchez n'apparaît pas dans la liste, c'est qu'il ne supporte pas ce mode d'éjection, reportez-vous alors au manuel fourni par le constructeur.

Si le message *Problème lors d'éjection du périphérique : le périphérique est en cours d'utilisation* s'affiche, c'est parce que des fichiers présents sur le périphérique sont encore ouverts. Fermez tous les documents pouvant se trouver sur ce périphérique, puis essayez à nouveau de l'éjecter.

Une autre méthode pour éjecter un périphérique consiste à passer par le panneau *Périphériques et imprimantes* :

1. Ouvrez le menu *Démarrer*.
2. Cliquez sur *Périphériques et imprimantes*.
3. Cliquez avec le bouton droit sur le périphérique à éjecter, puis sélectionnez *Éjecter* dans le menu contextuel.

EN COULISSE Cache désactivé pour les médias amovibles

Windows désactive par défaut le cache d'écriture pour les périphériques pouvant être éjectés. Cela permet d'éviter au maximum la perte de données lorsque le périphérique est débranché.

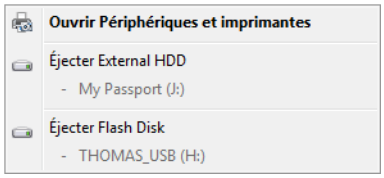


Figure 4–8 Choix du périphérique à éjecter

Gestionnaire de périphériques simplifié : le panneau Périphériques et imprimantes

Le gestionnaire de périphériques Windows est un outil complet et puissant présentant un grand nombre de fonctionnalités. Cependant, il montre rapidement ses limites pour une gestion des périphériques habituels au quotidien (clé USB, disque dur externe, imprimante, webcam, appareil mobile...).

Installer rapidement des périphériques

Dans Windows 7, une nouvelle fonctionnalité est apparue dans le panneau de configuration : *Périphériques et imprimantes*. Pour y accéder, voici la marche à suivre :

1. Rendez-vous dans le *Panneau de configuration*.
2. Dans *Matériel et Audio*, cliquez sur *Périphériques et imprimantes*.
3. Cet écran affiche la liste des principaux périphériques connectés à l'ordinateur : imprimantes, périphériques de stockage (clé USB, disque dur externe...), webcam.

Par défaut, Windows 7 s'efforce de télécharger automatiquement les pilotes depuis Internet ainsi que des images réalistes correspondant réellement au périphérique connecté. Ainsi, l'icône des périphériques apparaissant dans la fenêtre *Périphériques et imprimantes* ressemble à vos périphériques. Toutefois, si vous souhaitez changer ce comportement, voici la procédure à suivre :

1. Ouvrez la fenêtre *Système* avec le raccourci clavier *Windows+Pause*.
2. Dans la colonne de gauche, cliquez sur *Paramètres système avancés*.
3. Sélectionnez l'onglet *Matériel*.

ASTUCE Périphériques et imprimantes

Vous pouvez également accéder à ce menu depuis le menu *Démarrer* dans la colonne de droite.

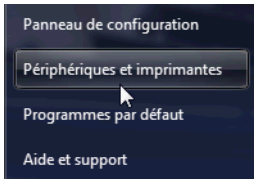


Figure 4–9 Accès aux périphériques par le menu Démarrer

4 Cliquez sur *Paramètres d'installation des périphériques*, puis sélectionnez l'option de votre choix.

5 Validez ensuite par le bouton *OK*.

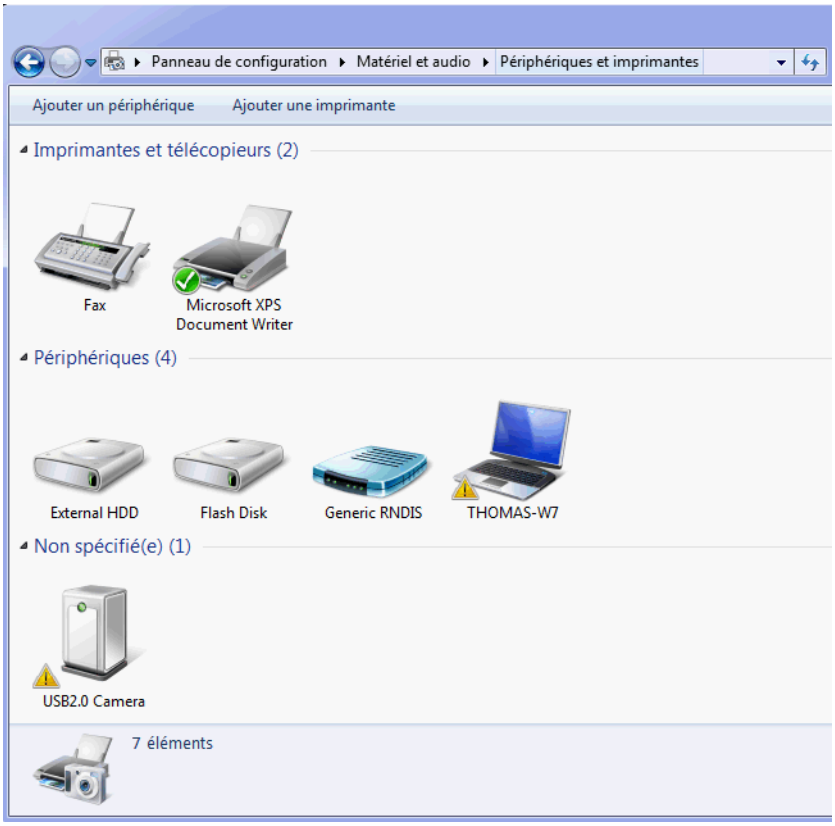


Figure 4–10
Dans le panneau Périphériques et imprimantes, l'imprimante par défaut est indiquée par une coche verte. Les périphériques qui présentent un dysfonctionnement sont indiqués avec un panneau danger jaune. Un pilote manquant peut être la source du problème.

Si l'un de vos périphériques ne fonctionne pas correctement, faites appel à l'utilitaire de résolution de problèmes fourni avec Windows 7. Effectuez un clic-droit sur l'icône du périphérique, puis choisissez dans le menu contextuel l'entrée *Résolution des problèmes*. Suivez ensuite les étapes qui dépendent du type de périphérique.

Comme vous le remarquez sur la figure 4–10, l'ordinateur lui-même apparaît dans la liste des périphériques. Le menu contextuel qui apparaît par clic droit donne accès aux principaux paramètres du système, mais permet également d'explorer les différents disques locaux.

ASTUCE Utiliser le menu contextuel

Pour chaque type de matériel, le menu contextuel permet d'accéder à des options propres au périphérique. Ainsi, sur une imprimante, vous accédez directement aux travaux en cours d'impression, vous définissez l'imprimante par défaut ou accédez aux options de l'imprimante. Pour une souris, vous accédez directement à l'écran de paramétrage avancé de la souris (pointeurs, roulette...). Dans le cas d'une clé USB ou d'un disque dur externe, il est possible de l'éjecter en effectuant un clic droit sur l'icône le représentant.

Installer des imprimantes

L'installation d'un périphérique d'impression sur votre ordinateur est aujourd'hui chose facile. En effet, Windows vous assiste tout au long du processus d'installation.

Pour installer une imprimante USB, branchez-la et puis allumez-la. Windows devrait automatiquement la détecter et installer le pilote adéquat. S'il ne trouve pas le pilote adéquat sur le disque dur, il le recherche sur Windows Update. Après l'installation du pilote, l'imprimante est prête à l'emploi.

Pour installer une imprimante non USB (par exemple, une imprimante utilisant le port parallèle), la procédure à suivre est un peu plus longue :

1. Ouvrez le menu *Démarrer*, puis cliquez sur *Périphériques et imprimantes*.
2. Cliquez sur le bouton *Ajouter une imprimante* en haut de la fenêtre.
3. Cliquez ensuite sur *Ajouter une imprimante locale*.
4. Sélectionnez le type de port à utiliser suivant les instructions fournies par le fabricant de l'imprimante, puis cliquez sur le bouton *Suivant*. L'assistant vous demande ensuite de choisir le pilote à utiliser parmi une liste fournie par Windows 7.
5. Après avoir choisi le pilote, l'assistant vous demande le nom que vous souhaitez donner à l'imprimante. Vous pouvez laisser le nom proposé par défaut ou le personnaliser selon vos souhaits.
6. Cliquez ensuite sur le bouton *Suivant*. L'assistant vous propose alors de partager l'imprimante. Choisissez l'option correspondant à votre choix, puis cliquez sur *Suivant*. Si vous possédez plusieurs imprimantes, l'assistant vous demande si vous voulez utiliser celle-ci par défaut.
7. Cliquez enfin sur *Terminer* pour pouvoir utiliser l'imprimante.

Cas particulier
Ordinateur non relié à Internet

Si vous n'êtes pas connecté à Internet, vous devrez fournir le pilote vous-même à partir du CD-Rom logiquement fourni par le constructeur de l'imprimante.

Bon à savoir
Le pilote n'apparaît pas dans la liste

Si votre pilote d'imprimante ne se trouve pas dans la liste, deux possibilités s'offrent à vous : fournir vous-même le pilote en cliquant sur le bouton *Disque fourni...*, ou cliquer sur le bouton *Windows Update* pour obtenir une liste de pilotes plus complète. Si vous optez pour *Windows Update*, la liste se télécharge via Internet. Cette opération est longue et peut durer plusieurs minutes.

Voir aussi **Installer une imprimante réseau et partager une imprimante**

Si vous souhaitez ajouter une imprimante réseau ou une imprimante partagée, reportez-vous à la section « Partage d'imprimante » du chapitre 11 « Sécurité des fichiers et partage de ressources ».

Modifier les propriétés de l'imprimante

L'imprimante est l'un des périphériques courants le plus fournis en options et en paramétrages. Windows 7 permet de configurer un certain nombre de paramètres et de propriétés pour chacune des imprimantes de votre système. Voyons ces options en détail.

La procédure pour modifier les propriétés d'une imprimante installée sur votre ordinateur est la suivante :

1. Ouvrez le menu *Démarrer* puis cliquez sur *Périphériques et imprimantes*.
2. Cliquez avec le bouton droit sur l'icône représentant l'imprimante à configurer, puis cliquez sur *Propriétés de l'imprimante* dans le menu contextuel.
3. La boîte de dialogue de propriétés s'affiche, vous donnant accès aux différents paramétrages de l'imprimante.

Personnaliser l'imprimante

Dans l'onglet *Général*, vous pouvez personnaliser le nom de votre imprimante. Vous pouvez également indiquer un emplacement (ex : salon, chambre, bureau 210…). Cette information est utile si vous partagez l'imprimante sur le réseau pour que les utilisateurs distants sachent à quel endroit récupérer leurs impressions. Vous pouvez également ajouter des commentaires personnalisés.

Le bouton *Préférences...* vous donne accès aux paramètres d'impression tels que le format de papier utilisé, la couleur, le mode recto verso, etc.

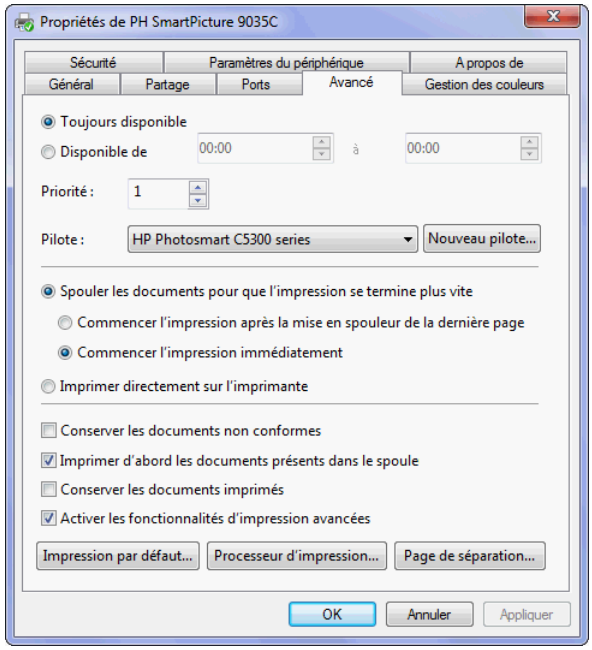


Figure 4–11
Onglet Avancé des propriétés de l'imprimante

L'onglet *Avancé* vous permet de paramétrer plusieurs options avancées pour votre imprimante. Vous avez, par exemple, la possibilité de définir une plage horaire pendant laquelle l'imprimante pourra être utilisée. En dehors de cette plage, les documents seront stockés dans la file d'attente de l'imprimante mais ne seront pas imprimés. La zone *Priorité* sert à définir si une imprimante est prioritaire par rapport à une autre dans le traitement des impressions. La valeur `1` désigne la priorité la plus faible et `99` la priorité la plus haute.

L'option *Activer les fonctionnalités d'impression avancées* permet d'utiliser des fonctions telles que l'ordre des pages ou le nombre de pages imprimées par feuilles. Si vous rencontrez des problèmes de compatibilité avec votre imprimante, essayez de désactiver cette option.

CAS PARTICULIER
Caractéristiques liées à l'imprimante

Suivant le modèle d'imprimante, certaines caractéristiques peuvent également être affichées dans cet onglet comme l'impression en couleur, le recto verso, etc.

BON À SAVOIR
Tester la configuration

Le bouton *Imprimer une page de test* demande l'impression d'une page de diagnostic. Si cette page s'imprime, c'est que votre imprimante est configurée correctement.

VOIR AUSSI **Partage de l'imprimante**

L'onglet *Partage* sert à définir les options de partage de cette imprimante sur le réseau. Nous y reviendrons en détail au chapitre 11, « Sécurité des fichiers et partage de ressources ».

Paramétrer le spool

Toujours dans l'onglet *Avancé*, vous accédez aux paramètres du spool d'impression. Pour activer le spool, cliquez sur *Spouler les documents pour que l'impression se termine plus vite.* Lorsque vous activez le spool, vous pouvez le paramétrer de deux façons : soit le spool attend d'avoir reçu toutes les pages avant de commencer l'impression, soit le spool démarre l'impression dès que la première page est reçue. Cochez le bouton radio correspondant à votre choix et pour le désactiver, cochez *Imprimer directement sur l'imprimante*.

L'option *Imprimer d'abord les documents présents dans le spool* permet d'optimiser les impressions. En effet, la gestion des impressions n'est alors plus basée uniquement sur la priorité, mais également sur le fait qu'un document entièrement présent dans le spool sera prioritaire par rapport à un document qui n'est présent que partiellement.

Si vous activez la case à cocher *Conserver les documents imprimés*, tous les documents imprimés seront conservés dans le spool. Si la case est décochée, les documents imprimés seront effacés du spool.

En coulisse Le spool d'impression

On appelle *spool* (ou file d'attente en français) le lieu de stockage des informations envoyées à l'imprimante. En effet, quand vous imprimez un document volumineux, votre ordinateur traite les pages pour les convertir dans un format compréhensible par l'imprimante.

Quand le spool est activé, les pages sont toutes stockées dans le spool et envoyées à l'imprimante au fur et à mesure de l'impression des pages. Ainsi, une fois que votre application a envoyé toutes les pages au spool, vous pouvez continuer à travailler, le spool se chargeant d'envoyer les pages suivantes au rythme de l'imprimante.

Dans le cas où le spool est désactivé, c'est votre application qui fait office de spool en envoyant les pages une à une directement vers l'imprimante. Dans ce cas, vous devez attendre la fin de l'impression avant de continuer à travailler.

Définir plusieurs imprimantes par défaut

Windows 7 fournit une nouvelle fonctionnalité permettant de sélectionner automatiquement une imprimante par défaut suivant le réseau auquel vous êtes connecté.

1. Ouvrez le menu *Démarrer*, cliquez sur *Périphériques et imprimantes*.
2. Cliquez sur l'une des imprimantes, puis sur le bouton *Gérer les imprimantes par défaut*. Si le bouton n'apparaît pas, cliquez sur le double chevron dans la barre de menus pour le faire apparaître.

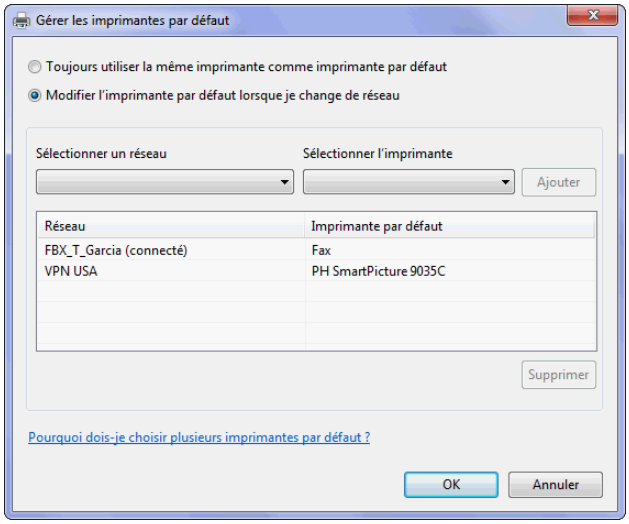


Figure 4–12
Fenêtre de gestion des imprimantes par défaut

3 Dans cette fenêtre vous devez tout d'abord indiquer si vous souhaitez toujours utiliser la même imprimante par défaut ou bien si vous désirez utiliser une imprimante par défaut différente suivant le réseau auquel vous êtes connecté. Dans le second cas, pour chaque réseau pour lequel vous souhaitez personnaliser l'imprimante, sélectionnez-le dans la première liste déroulante et choisissez l'imprimante par défaut à utiliser dans la seconde liste déroulante.

4 Cliquez ensuite sur le bouton *Ajouter*. Pour modifier une ligne, cliquez sur l'une des lignes, apportez le changement souhaité, puis cliquez sur le bouton *Mettre à jour*. Utilisez le bouton *Supprimer* pour enlever la ligne sélectionnée.

Configurer le clavier

Plusieurs paramètres du clavier de votre ordinateur sont personnalisables dans Windows. L'accès aux paramètres du clavier se fait ainsi :

1 Ouvrez le menu *Démarrer*.

2 Saisissez `clavier` dans la barre de recherche.

3 Dans la liste qui s'affiche alors, cliquez sur *Clavier* sous *Panneau de configuration*.

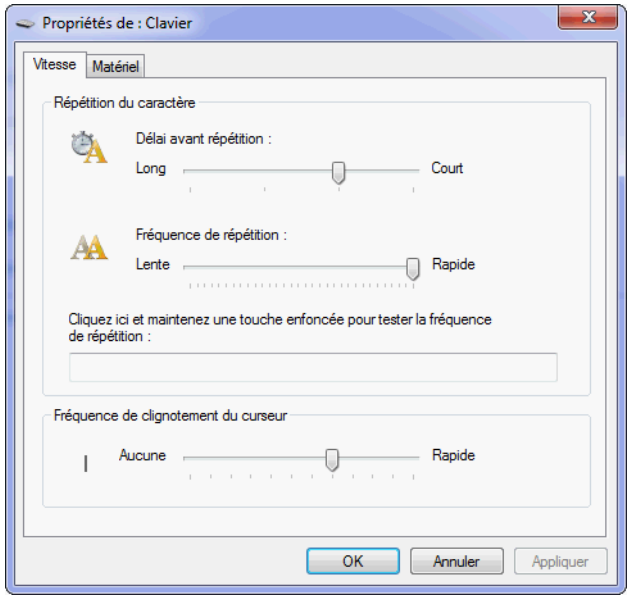


Figure 4–13
Fenêtre de propriétés du clavier

Les deux principaux réglages du clavier pour le système sont le délai de répétition et la vitesse de répétition. La fréquence de répétition (ou

vitesse de répétition) permet d'ajuster le nombre de fois où la lettre sera répétée pendant un certain laps de temps.

C'est toujours dans la boîte de dialogue *Clavier* que vous réglez la vitesse de clignotement du curseur de texte affiché dans toutes les applications de traitement de texte.

Il est également possible de configurer des options d'accessibilité pour le clavier :

1. Ouvrez le menu *Démarrer*, saisissez `ergonomie` dans la barre de recherche.
2. Cliquez sur *Options d'ergonomie* dans la liste qui s'affiche.
3. Cliquez ensuite sur le lien *Rendre le clavier plus facile à utiliser*.

Plusieurs options s'offrent alors à vous. Voyons à quoi elles servent :

- Les *touches souris* permettent de piloter le pointeur de la souris à l'aide du pavé numérique.
- Les *touches rémanentes* vous sont utiles si vous avez des difficultés à presser plusieurs touches en même temps.
- L'option *touches bascules* active un signal sonore lorsque vous utilisez les touches bascules de votre clavier : *Verrouillage Majuscules*, *Verrouillage Numérique* ou *Arrêt Défil*. Activez cette option si vous avez des difficultés à savoir si vous activez ou désactivez chaque touche bascule. En effet, le signal sonore émis est différent suivant si la touche bascule est activée ou désactivée.
- L'option *touches filtres* ignore les pressions brèves ou répétitives sur les touches du clavier.

Configurer la souris

Dans Windows 7, différents types de réglages de la souris sont personnalisables. Pour cela, il vous faut accéder à la fenêtre de propriétés de la souris, en saisissant `souris` dans la barre de recherche du menu *Démarrer*. Dans la liste qui s'affiche, sous *Panneau de configuration*, cliquez sur *Souris* ou *Modifier les paramètres de la souris*.

Régler le comportement des boutons

Dans le premier onglet *Boutons* de la fenêtre de configuration, vous modifiez le comportement des différents boutons de votre souris : inverser le rôle des boutons gauche et droit, personnaliser la vitesse du double-clic ou encore activer le verrouillage du clic.

EN DÉTAIL Verrouillage du clic

Le verrouillage du clic vous sera utile si vous avez des difficultés pour maintenir les boutons de la souris enfoncés pour faire glisser des icônes ou pour sélectionner du texte, par exemple. Lorsque vous activez cette option, vous pouvez verrouiller le clic en maintenant quelques secondes le bouton gauche de la souris enfoncé. Lorsque vous le relâchez, la souris se comportera comme si le bouton était toujours enfoncé. Pour relâcher le bouton, cliquez une fois avec le bouton gauche de la souris.

Modifier l'apparence et le comportement du pointeur

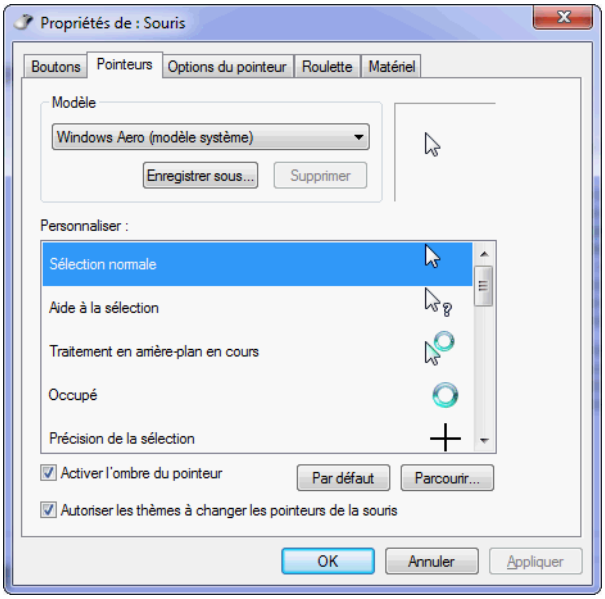


Figure 4–14
Propriétés des pointeurs de la souris

L'onglet *Pointeurs* vous permet de choisir les différentes apparences que prendra le pointeur de la souris à l'écran. Plusieurs modèles de pointeurs vous sont proposés par défaut. Toutefois, vous pouvez personnaliser les pointeurs selon vos goûts. Pour personnaliser l'un des pointeurs, double-cliquez sur celui-ci dans la liste. Une fenêtre vous demande alors de fournir un fichier curseur statique (format `.cur`) ou bien animé (format `.ani`).

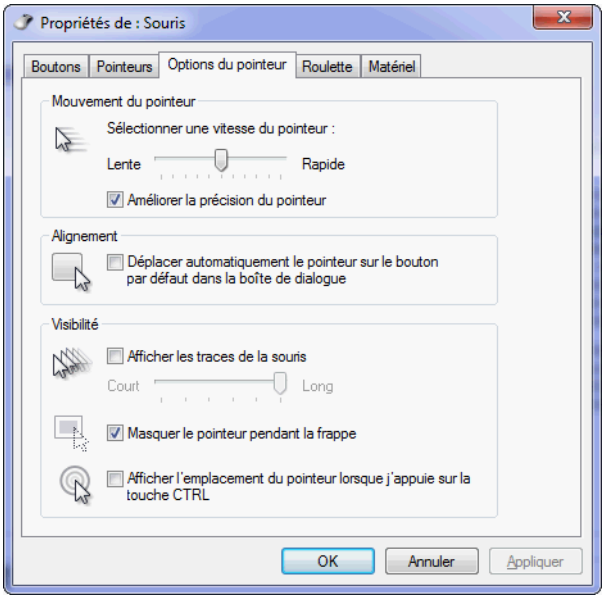


Figure 4–15
Options du pointeur de la souris

L'onglet *Options du pointeur* propose différentes options pour modifier le comportement du curseur à l'écran. Vous pouvez notamment modifier la vitesse à laquelle le pointeur se déplace à l'écran. Plus vous augmentez cette vitesse, moins vous aurez à déplacer votre souris pour faire bouger le pointeur, mais la précision sera alors moins importante. Si vous réduisez la vitesse, vous bénéficierez d'une meilleure précision, mais il vous faudra déplacer votre souris sur de plus grandes distances pour balayer l'écran avec le pointeur.

La case à cocher *Améliorer la précision du pointeur* permet d'activer le comportement suivant : si vous déplacez votre souris lentement, la vitesse de la souris est réduite pour que vous soyez plus précis et lorsque vous bougez rapidement votre souris, la vitesse du pointeur est accélérée pour éviter de devoir faire de grands mouvements de souris.

Les options présentes dans le cadre *Visibilité* en bas de l'onglet proposent différentes fonctionnalités qui permettent de mieux repérer le pointeur si vous avez du mal à le localiser à l'écran.

PORTABLE Pavé tactile

L'option *Déplacer automatiquement le pointeur sur le bouton par défaut dans la boîte de dialogue* est utile notamment sur les ordinateurs portables lorsque vous vous servez du pavé tactile (ou *touchpad*) et que vous n'utilisez pas de souris externe. En effet, vous avez sans doute remarqué qu'il n'est pas évident avec le pavé tactile de parcourir rapidement de grandes distances avec le pointeur. Cette option déplace donc le curseur sur le choix par défaut dans les boîtes de dialogues qui apparaissent à l'écran.

Configurer la roulette

La personnalisation du comportement de la roulette de votre souris se passe dans l'onglet *Roulette*.

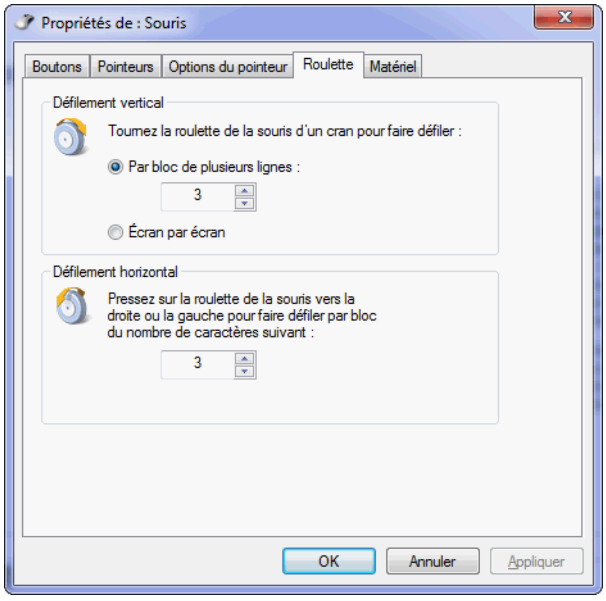


Figure 4–16
Propriétés de la roulette de la souris

Vous définissez dans ce panneau la vitesse de défilement quand vous faites tourner votre roulette vers le haut ou vers le bas. Vous pouvez ainsi choisir de faire défiler le contenu en sautant un certain nombre de lignes ou un écran entier à chaque cran de la roulette.

Certaines souris autorisent également un déplacement horizontal en inclinant la roulette vers la gauche ou vers la droite. La vitesse de défilement horizontal est donc également configurable dans cet onglet, et se définit en nombre de caractères. Si vous choisissez par exemple 3 caractères, chaque fois que vous inclinerez la roulette vers la droite ou la gauche, l'affichage défilera de 3 caractères dans la direction correspondante.

Astuce **Piloter la souris avec le clavier**

Vous utilisez un ordinateur fixe et votre souris a rendu l'âme ? Utilisez alors les raccourcis claviers, même si cela s'avère rapidement fastidieux. Rappelez-vous que la touche *Tab* sert à passer d'un élément à un autre sur l'écran et la touche *Espace* à cocher une case ou activer un élément. Cependant, si cette méthode ne vous convient pas, sachez que Windows intègre un mécanisme permettant de piloter le pointeur de la souris à l'aide du pavé numérique de votre clavier. Voici la marche à suivre pour accéder à cette fonctionnalité :

1. Ouvrez le menu *Démarrer*.
2. Tapez `touches souris` dans la barre de recherche, l'élément *Déplacer le pointeur avec le pavé numérique à l'aide des touches souris* apparaît alors. Tapez *Entrée* pour sélectionner ce choix.
3. Dans la fenêtre qui s'ouvre, cliquez sur *Configurer les touches souris*.
4. Vous pouvez alors choisir d'activer les touches souris et définir leurs paramètres. Un moyen plus rapide pour activer les touches souris est d'utiliser la combinaison de touches *Alt+Maj+Verr. Num*.

Une fois les touches souris activées, vous pilotez le pointeur avec les touches du pavé numérique (*4* et *6* pour se déplacer vers la gauche ou la droite ; *2* et *8* pour haut et bas ; *1*, *3*, *7* et *9* pour se déplacer en diagonale ; *5* pour cliquer ; */* pour choisir le bouton gauche de la souris ; * pour le bouton du milieu et – pour le bouton de droite, enfin utilisez *0* pour laisser le bouton de la souris enfoncé).

Configuration audio

De nos jours, les ordinateurs sont tous équipés d'une carte son à laquelle sont raccordés des périphériques d'entrée (micro, par exemple) et de sortie (haut-parleurs, casque...). Il est donc important de personnaliser le comportement et le volume sonore de ces équipements. Windows 7 propose différentes fenêtres de réglage pour ajuster le volume sonore, pour activer ou désactiver des périphériques audio.

Régler le volume

Le volume général du système s'ajuste rapidement en cliquant une fois sur l'icône en forme de haut-parleur dans la barre de notification à côté de l'horloge. Il suffit alors de déplacer le curseur pour modifier le volume global. Pensez à utiliser la roulette de la souris pour faire varier le volume.

Pour couper tous les sons, cliquez sur le petit haut-parleur bleu affiché sous la jauge. Une coche rouge apparaît, indiquant que le système est maintenant complètement muet. La couleur de la jauge indiquant le niveau sonore passe alors du vert au gris.

Dans les versions antérieures à Windows Vista, le mélangeur de volume permettait de régler le volume pour chaque périphérique. Ce comportement a été modifié dans Windows Vista et Windows 7 et permet maintenant de configurer le volume sonore pour chaque logiciel qui produit du son.

Vous pouvez ainsi ajuster le volume de manière plus précise en le réglant programme par programme :

1. Ouvrez la fenêtre de réglage rapide en cliquant sur le petit haut-parleur dans la barre de notification près de l'horloge.
2. Cliquez sur le lien *Mélangeur*.
3. La fenêtre *Mélangeur de volume* s'ouvre alors. Définissez le niveau sonore maximal pour chaque application. Chaque logiciel émettant du son est affiché dans la partie *Applications* de la fenêtre avec son propre curseur. Il est donc possible de personnaliser les niveaux pour chaque application voire de rendre une application muette en cliquant sur le petit haut-parleur bleu.

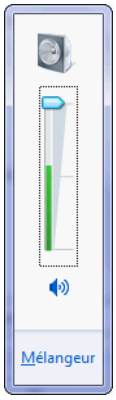


Figure 4–17
Réglage rapide du volume : le niveau sonore est affiché en temps réel par une jauge verte le long du curseur.

ASTUCE Accès rapides

Vous accédez directement à la configuration de vos haut-parleurs en cliquant sur l'icône située au-dessous de *Périphérique*. Vous pouvez aussi accéder à la personnalisation des sons de Windows en cliquant sur l'icône au-dessus de *Sons système*.

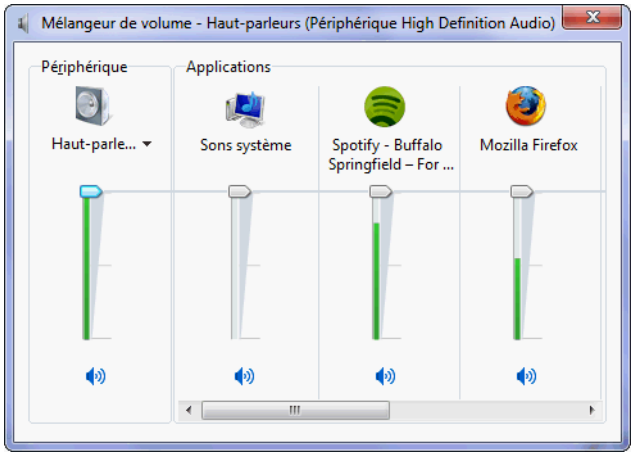


Figure 4–18
Le volume général du système est réglé par le curseur à l'extrême gauche de la fenêtre, dans la colonne Périphérique. Sélectionnez dans cette colonne le périphérique de sortie audio que vous souhaitez régler.

Configurer les périphériques audio

La plupart des ordinateurs sont équipés de périphériques diffusant ou enregistrant le son émis par l'ordinateur. Windows 7 fournit une interface unifiée pour gérer tous les aspects des périphériques audio de votre système. Vous configurez ainsi les différents périphériques audio installés sur votre système en saisissant `son` dans la barre de recherche du menu *Démarrer* puis en cliquant sur *Son* sous *Panneau de configuration* dans la liste qui apparaît au-dessus de la barre de recherche.

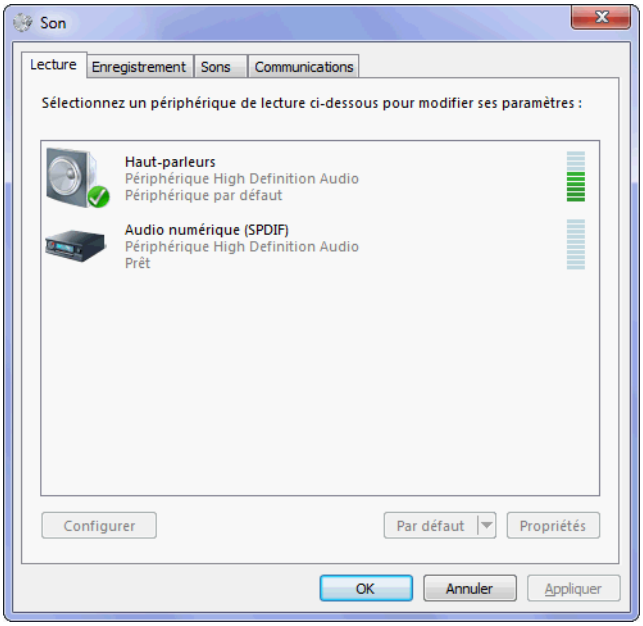


Figure 4–19
Fenêtre de paramétrage des périphériques de lecture audio

Les périphériques de lecture

L'onglet *Lecture* regroupe les paramètres des périphériques de lecture, c'est-à-dire les différents périphériques qui permettent à votre ordinateur de produire du son (des haut-parleurs, par exemple). Chaque périphérique installé sur le système est listé dans la partie centrale de la fenêtre, accompagné d'une jauge de volume indiquant le niveau sonore actuel qu'il produit. En double-cliquant sur l'un des périphériques affichés dans la liste, vous accédez à ses propriétés détaillées.

Pour sélectionner le périphérique de lecture par défaut, cliquez avec le bouton droit sur celui-ci, puis cliquez sur *Définir en tant que périphérique par défaut*. Depuis le menu contextuel, vous pouvez également désactiver l'un des périphériques. Il ne sera alors plus utilisé par Windows.

Si vous désirez le réactiver, cliquez droit dans la liste des périphériques de lecture et vérifiez que la ligne *Afficher les périphériques désactivés* est cochée. Cliquez ensuite avec le bouton droit de la souris sur le périphérique désactivé et sélectionnez *Activer* dans le menu contextuel.

La vérification du bon fonctionnement de l'un des périphériques de lecture s'effectue également depuis cette fenêtre. Effectuez un clic droit sur celui qui vous intéresse, puis sélectionnez *Tester*. Windows émet alors un son dans chacun des haut-parleurs, séparément, pour vérifier leur fonctionnement.

Les périphériques d'enregistrement

Le deuxième onglet affiche la liste des périphériques d'enregistrement, c'est-à-dire ceux qui captent le son.

Il fonctionne de la même façon que l'onglet des périphériques de lecture. Chaque périphérique d'enregistrement apparaît dans la liste accompagné d'une jauge qui affiche le niveau sonore des sons captés.

Comme pour les périphériques de lecture, il est possible de désactiver les périphériques d'enregistrement inutiles. Vous pouvez aussi définir le périphérique à utiliser dans les diverses applications qui ont besoin d'enregistrer du son. Pour effectuer ces actions, cliquez avec le bouton droit sur le périphérique d'enregistrement de votre choix, puis sélectionnez l'action correspondante dans le menu contextuel.

Configurer les sons système

Windows 7 émet des sons lorsque certains événements surviennent : démarrage du système, ouverture de session, message d'information, message d'erreur, etc. Il est bien entendu possible de personnaliser ou de désactiver chacun de ces sons.

1. Effectuez un clic droit sur le Bureau, puis cliquez sur *Personnaliser* dans le menu contextuel.
2. Cliquez ensuite sur l'icône *Sons* au bas de la fenêtre.
3. La fenêtre de personnalisation des sons s'ouvre.

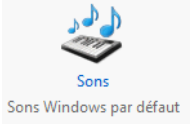


Figure 4–20
Icône de personnalisation des sons Windows

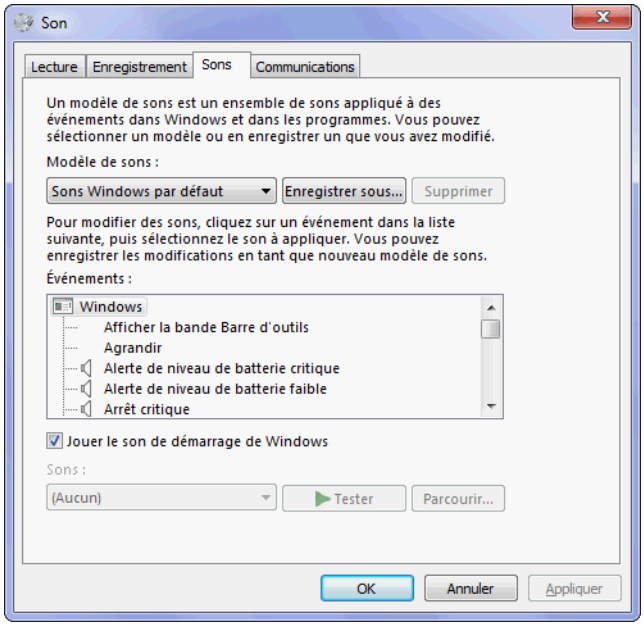


Figure 4–21
Boîte de dialogue de personnalisation des sons Windows

Voici les différents paramétrages qui s'offrent à vous depuis cette fenêtre. Pour commencer, vous pouvez sélectionner ce que l'on appelle un modèle de sons, qui n'est autre qu'une configuration enregistrée de l'ensemble des sons. Windows 7 est fourni avec un certain nombre de modèles de sons accessibles via la liste déroulante *Modèle de son*, mais libre à vous de créer le ou les vôtres !

Si vous ne souhaitez plus conserver l'un de vos modèles, sélectionnez-le dans la liste des modèles, puis cliquez sur *Supprimer*.

Vous pouvez également personnaliser chacun des sons en cliquant sur l'un d'eux dans la liste *Événements*. Sélectionnez ensuite un son dans la liste déroulante *Sons* présente au bas de la fenêtre.

Si aucun son ne vous convient, indiquez un fichier audio à lire en utilisant le bouton *Parcourir...* Cliquez sur le bouton *Tester* pour écouter un aperçu du son.

Une fois que vous avez personnalisé les sons, enregistrez votre personnalisation dans un modèle de sons en cliquant sur le bouton *Enregistrer sous...* Donnez un nom à votre modèle.

BON À SAVOIR

Il est impossible de supprimer les modèles sonores fournis par défaut.

Connecter un vidéoprojecteur

Dans les versions antérieures de Windows, lorsque vous connectiez un vidéoprojecteur, il était nécessaire d'aller dans le panneau de configuration de l'affichage pour définir la façon d'afficher les écrans (mode clone, bureau étendu, etc.).

Configuration rapide

Windows 7 inclut désormais un utilitaire permettant de configurer de manière simple et très rapide un vidéoprojecteur.

1 Après avoir raccordé le projecteur à votre ordinateur, appelez l'utilitaire de configuration rapide par la combinaison de touches *Windows+P*.

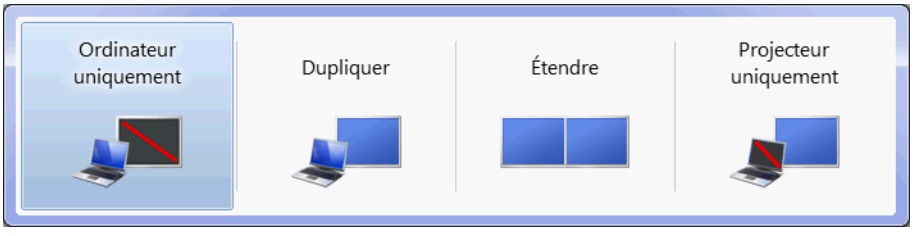


Figure 4–22
Panneau de configuration rapide du vidéoprojecteur

2 Cliquez sur le mode d'affichage de votre choix parmi les quatre modes proposés.

3 Le changement est automatiquement appliqué et l'image s'affiche selon le mode que vous avez choisi.

Regardons de plus près les modes qui vous sont proposés :

- Le mode *Ordinateur uniquement* désactive l'affichage sur le vidéoprojecteur. Dans ce mode, seul l'écran de l'ordinateur affiche une image.
- Le mode *Dupliquer* clone l'affichage de l'écran de l'ordinateur sur le vidéoprojecteur. L'affichage sur le vidéoprojecteur est strictement identique à ce qui est affiché sur l'écran de l'ordinateur.
- L'option *Étendre* affiche la partie gauche du Bureau sur l'écran de l'ordinateur et la partie droite sur le vidéoprojecteur. Cette option est intéressante si vous utilisez un deuxième moniteur à la place d'un vidéoprojecteur, car vous disposez ainsi d'un bureau plus grand. Lorsque vous déplacez votre souris ou une fenêtre au-delà du bord droit du premier écran, elle apparaît sur le bord gauche du deuxième écran.
- Le mode *Projecteur uniquement* désactive l'affichage sur l'écran de l'ordinateur. L'image est alors uniquement affichée sur le vidéoprojecteur ou sur le moniteur raccordé à la carte graphique.

L'option actuellement sélectionnée apparaît sur un fond bleu.

BON À SAVOIR **Ordinateur à double écran**

Le raccourci *Windows+P* sert également à configurer rapidement un ordinateur équipé de deux écrans.

Configuration avancée

L'utilitaire de configuration rapide ne permet pas de paramétrer les réglages avancés tels que la résolution d'écran ou l'orientation de l'affichage.

Pour accéder à des options supplémentaires, cliquez avec le bouton droit de la souris sur une zone libre du Bureau et choisissez *Résolution d'écran* dans le menu contextuel.

Affichage multiple

Si vous avez raccordé un vidéoprojecteur ou un deuxième écran à votre ordinateur et que ce périphérique d'affichage est reconnu, la boîte de dialogue affiche de manière schématique les deux affichages dans la partie supérieure de la fenêtre.

L'écran principal est indiqué par le numéro *1* et le périphérique d'affichage externe par *2*. Pour savoir à quel écran correspond chaque numéro, cliquez sur le bouton *Identifier*. Le numéro correspondant à chaque périphérique s'affiche brièvement sur chaque affichage.

Pour choisir la façon dont seront utilisés l'écran principal de l'ordinateur et le périphérique d'affichage externe, choisissez une option dans la liste déroulante *Affichages multiples*.

Figure 4–23
Schéma affiché dans la fenêtre d'options de résolution pour le mode Dupliquer ces affichages

Figure 4–24
Schéma affiché dans la fenêtre d'options de résolution pour le mode Étendre ces affichages

Les options *Afficher le bureau uniquement sur 1* ou *Afficher le bureau uniquement sur 2* indiquent à Windows quel périphérique est affiché.

Si vous choisissez le mode d'affichage *Dupliquer ces affichages*, l'illustration en haut de la fenêtre affiche un simple moniteur contenant les numéros *1* et *2* comme le montre la figure 4–23. Ce mode de fonctionnement, parfois appelé « mode clone », affiche exactement la même chose sur l'écran principal de l'ordinateur et sur le périphérique d'affichage externe. En utilisant ce mode, les deux affichages auront la même résolution. Si vous souhaitez utiliser une résolution différente sur chaque affichage, utilisez l'option *Étendre ces affichages*.

Si vous choisissez l'option *Étendre ces affichages* dans la liste déroulante *Affichages multiples*, le schéma présent dans la partie supérieure de la fenêtre affiche indépendamment les deux périphériques d'affichage.

Lorsque ce mode est activé, votre Bureau Windows prend la largeur totale des deux affichages. La partie gauche du Bureau est ainsi affichée sur le périphérique principal (numéroté *1*) et la partie droite du Bureau sur le périphérique secondaire (numéroté *2*). Ce mode est particulièrement utile si vous raccordez un deuxième écran à votre ordinateur. En effet, vous travaillez ainsi sur une plus grande surface visuelle. Votre Bureau étant étendu sur deux affichages, vous naviguez avec votre souris d'un écran à l'autre simplement en le faisant glisser vers le bord droit du périphérique principal ou vers le bord gauche du périphérique secondaire. Vous pouvez également déplacer une fenêtre d'un écran à l'autre.

Comme nous venons de le voir, le périphérique principal est celui qui affiche la partie gauche du Bureau ainsi que le menu *Démarrer* et la barre des tâches. Si vous le souhaitez, vous pouvez inverser le rôle des périphériques d'affichage. Pour cela, cliquez sur le moniteur représentant l'affichage secondaire (numéroté *2*) et cochez la case *Faire de cet affichage votre affichage principal*. N'oubliez pas que vous pouvez toujours savoir quel écran est le périphérique principal ou secondaire en cliquant sur le bouton *Identifier*.

Résolution

La résolution correspond au nombre de pixels affichés en largeur et en hauteur sur votre écran. Plus la résolution est élevée, plus il y a d'éléments à l'écran.

Pratique Résolution recommandée

Lorsque vous déroulez la liste *Résolution*, remarquez que l'une des options est suivie de la mention *recommandé* : Windows 7 détecte automatiquement la résolution recommandée pour votre affichage. Il s'agit en général de la plus haute résolution que le périphérique d'affichage peut supporter.

Résolution et orientation

Pour chacun des périphériques d'affichage, il est possible de paramétrer la résolution d'écran.

Voici comment procéder pour changer la résolution :

1. Cliquez sur l'icône représentant le moniteur en haut de la fenêtre.
2. Déroulez ensuite la liste déroulante *Résolution*.
3. Choisissez la résolution en faisant glisser le curseur sur la valeur de votre choix.

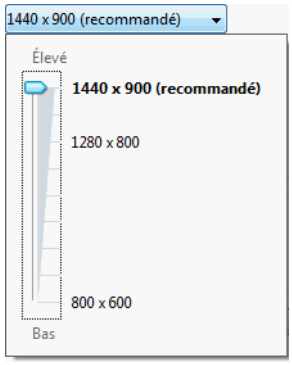


Figure 4–25
Configuration de la résolution de l'affichage

Si vous utilisez un écran dont la dalle peut pivoter à 90° (format portrait), vous apprécierez de pouvoir modifier l'orientation de l'affichage : ouvrez la liste déroulante *Orientation* et sélectionnez l'option de votre choix parmi les quatre orientations possibles.

Écran Format portrait

Cette utilisation des écrans au format portrait est utile pour les personnes qui utilisent beaucoup de traitement de texte. En effet, le format portrait d'une page de traitement de texte A4 s'adapte mieux à l'affichage lorsque l'écran se trouve dans le sens de la hauteur.

Dépannage Mon périphérique d'affichage externe n'est pas détecté

Si un seul périphérique d'affichage est indiqué dans la fenêtre et que vous avez correctement branché votre périphérique, Windows n'a pas réussi à détecter correctement le périphérique utilisé. Cliquez sur le bouton *Détecter* pour que l'ordinateur tente de trouver les caractéristiques du périphérique connecté.
Avec certains téléviseurs, Windows ne détecte pas le périphérique d'affichage et renvoie le message *Autre affichage non détecté*. Forcez alors Windows à envoyer des images vers le périphérique d'affichage :

1. Cliquez sur le cadre *Autre affichage non détecté* en haut de la fenêtre.
2. Dans la liste déroulante *Affichages multiples*, sélectionnez l'option *Essayez de vous connecter quand même*.
3. Cliquez sur *Appliquer*.

Pour annuler cette manipulation une fois que vous aurez terminé d'utiliser le moniteur, cliquez sur l'image représentant le second moniteur (représenté par le chiffre 2) dans la partie supérieure de la fenêtre.

1. Déroulez la liste *Affichages multiples* et choisissez l'option *Afficher le bureau uniquement sur 1* si elle n'est pas déjà sélectionnée.
2. Validez par le bouton *Appliquer*.
3. Sélectionnez l'option *Supprimer cet affichage*.
4. Cliquez sur le bouton *Appliquer* pour que votre choix soit pris en compte.

Centre de mobilité pour les ordinateurs portables

Déjà présent dans Windows Vista, cet outil ne présente pas de nouveauté majeure. Cependant, il n'en demeure pas moins fort utile.

Le centre de mobilité n'est disponible que sur les ordinateurs portables. Il est accessible dans le panneau de configuration sous *Panneau de configuration*>*Matériel et audio*>*Centre de mobilité*. Toutefois, dans son utilisation habituelle, il peut être appelé et fermé en utilisant le raccourci système *Windows+X*.

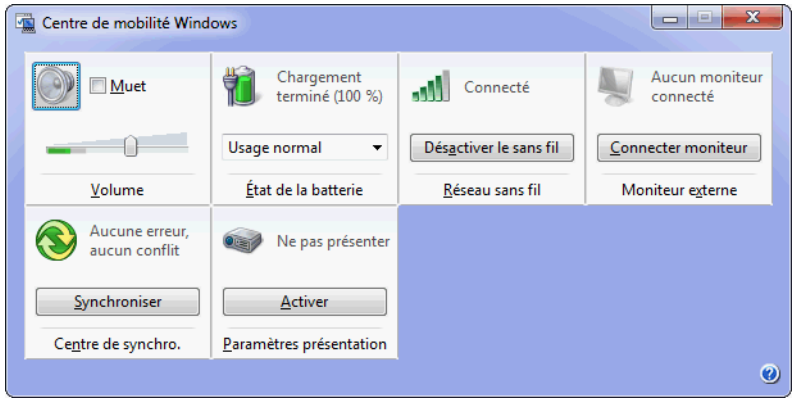


Figure 4–26
Vue du centre de mobilité Windows

Comme vous pouvez le voir sur la figure 4–26, cet outil se décompose en différents modules : volume, batterie, réseau… Ils dépendent du matériel et des pilotes de l'ordinateur. Selon les ordinateurs, vous trouverez donc plus ou moins d'options. Le tableau 4-1 décrit les modules les plus courants du centre de mobilité.

DÉPANNAGE

Le bouton Activer le sans fil est grisé

Si le bouton permettant d'activer le Wi-Fi est grisé dans le centre de mobilité, vérifiez que votre carte Wi-Fi est allumée (votre boîtier possède probablement un interrupteur physique).

Tableau 4–1 Modules indispensables du centre de mobilité

Intitulé	Détail
Luminosité (non présent sur la figure 4–26)	Avec le curseur, variez l'intensité du rétro-éclairage de l'écran. Cliquez sur l'icône pour d'accéder directement aux options d'alimentation.
Volume	Ce module sert à ajuster le volume sonore de vos haut-parleurs et à les rendre muets en cochant la case prévue à cet effet. En cliquant sur l'icône en forme de haut-parleur, vous accèderez au panneau de réglage avancé du son sur votre ordinateur.
État de la batterie	Comme son nom l'indique, ce module affiche l'autonomie de batterie restante. La liste déroulante permet de choisir le mode d'alimentation à utiliser : privilégier les performances, l'autonomie (au détriment des performances) ou encore un état normal intermédiaire. Vous accédez aux options d'alimentation avancées en cliquant sur l'icône en forme de pile.
Réseau sans fil	Via ce module, vous activez ou désactivez votre carte Wi-Fi. Vous pouvez également voir l'état de la connexion sans fil de votre ordinateur (connecté ou non). L'icône donne accès à la liste des réseaux disponibles.
Orientation de l'écran (uniquement sur les tablets PC)	Le bouton présent sur ce panneau permet de faire pivoter l'affichage sur l'écran.
Moniteur externe	Ce module sert à personnaliser l'affichage quand un écran externe est relié à votre ordinateur portable. L'icône donne accès aux paramètres avancés de résolution d'écran.

Tableau 4–1 Modules indispensables du centre de mobilité (suite)

Intitulé	Détail
Centre de synchro.	Ce module affiche l'état de synchronisation des appareils mobiles raccordés à l'ordinateur ou des emplacements réseau synchronisés. Vous pouvez accéder au centre de synchronisation en cliquant sur l'icône.
Paramètres de présentation	Ces paramètres permettent de définir le comportement de l'ordinateur lorsque vous effectuez une présentation. Pour définir les paramètres, cliquez sur l'icône en forme de vidéoprojecteur. Vous pouvez désactiver ou non l'écran de veille, définir le niveau sonore à utiliser et le fond d'écran à afficher lorsque vous êtes en présentation. Lorsque vous souhaitez activer ces paramètres de présentation, cliquez sur le bouton *Activer* du module *Paramètres de présentation* dans le centre de mobilité.

En résumé

Dans ce chapitre, nous nous sommes penchés sur le gestionnaire de périphériques et nous avons vu comment installer de nouveaux périphériques. Nous nous sommes également intéressés au panneau Périphériques et imprimantes, qui est une des nouveautés de Windows 7. Nous savons à présent comment configurer des périphériques incontournables que sont le clavier, la souris, l'imprimante mais également comment paramétrer rapidement un double affichage ou un vidéoprojecteur.

chapitre 5

Installer et gérer les programmes

La vraie force d'un système d'exploitation réside dans la possibilité d'installer des logiciels tiers, un ordinateur se contentant des fonctionnalités de base du système n'ayant aucun intérêt. L'installation de programmes est synonyme non seulement d'ajout de fonctionnalités, mais aussi de gain de productivité et d'amélioration de l'expérience utilisateur. La gestion des programmes est néanmoins une chose délicate et qui peut s'avérer désastreuse si elle n'est pas faite correctement.

SOMMAIRE

- Installation et désinstallation de programmes
- Gestion des composants Windows
- Blocage d'application

MOTS-CLÉS

- Logiciel
- Installation
- Blocage
- AppLocker
- Stratégie
- Fonctionnalité Windows
- Administration
- Restriction logiciel
- Signature

Ce chapitre traite de l'installation et de la désinstallation des programmes. Nous y verrons également comment gérer leurs autorisations d'accès à l'aide de l'outil d'administration AppLocker.

L'ordinateur paramétré, il est temps d'ajouter les programmes. Qu'ils soient vendus par des éditeurs ou Open Source, cette opération peut s'avérer désastreuse pour le système : les programmes peuvent parfois corrompre les fichiers de Windows, installer un virus ou permettre aux utilisateurs de réaliser des actions interdites. Il est donc important de maîtriser le cycle de vie des programmes.

Ajouter un nouveau programme

L'ajout d'un programme se fait dans la plupart des cas par un logiciel d'installation, dit installeur. Il est fourni par l'éditeur du logiciel et permet via un assistant de définir les paramètres d'installation. Ces paramètres concernent tout d'abord le chemin d'installation, qui par défaut est un répertoire situé dans `C:\Program Files`, et demande parfois des informations complémentaires comme un numéro de licence ou des paramétrages pour la création de raccourcis.

L'installation d'un logiciel ne dépend pas réellement du système. Généralement, celui-ci se contente de faire appel au logiciel d'installation. Pour cette raison, nous ne nous attarderons pas sur cette partie, d'autant que les programmes d'installation sous Windows n'ont que très peu évolué au fil des versions.

Désinstaller des programmes

Sur un principe de fonctionnement identique à l'installation de logiciel, la désinstallation ne dépend pas du système, mais du logiciel de désinstallation auquel il fait appel.

Le système nous aide néanmoins à plusieurs choses. Il retrouve la liste complète de tous les programmes désinstallables, s'occupe d'appeler le fichier de désinstallation en lui donnant les informations dont il a besoin, etc. Tout ceci se fait de façon très intuitive via le panneau de configuration.

1. Ouvrez le panneau de configuration et cliquez sur *Programmes*.
2. Cliquez ensuite sur *Désinstaller un programme* afin d'ouvrir le panneau suivant :

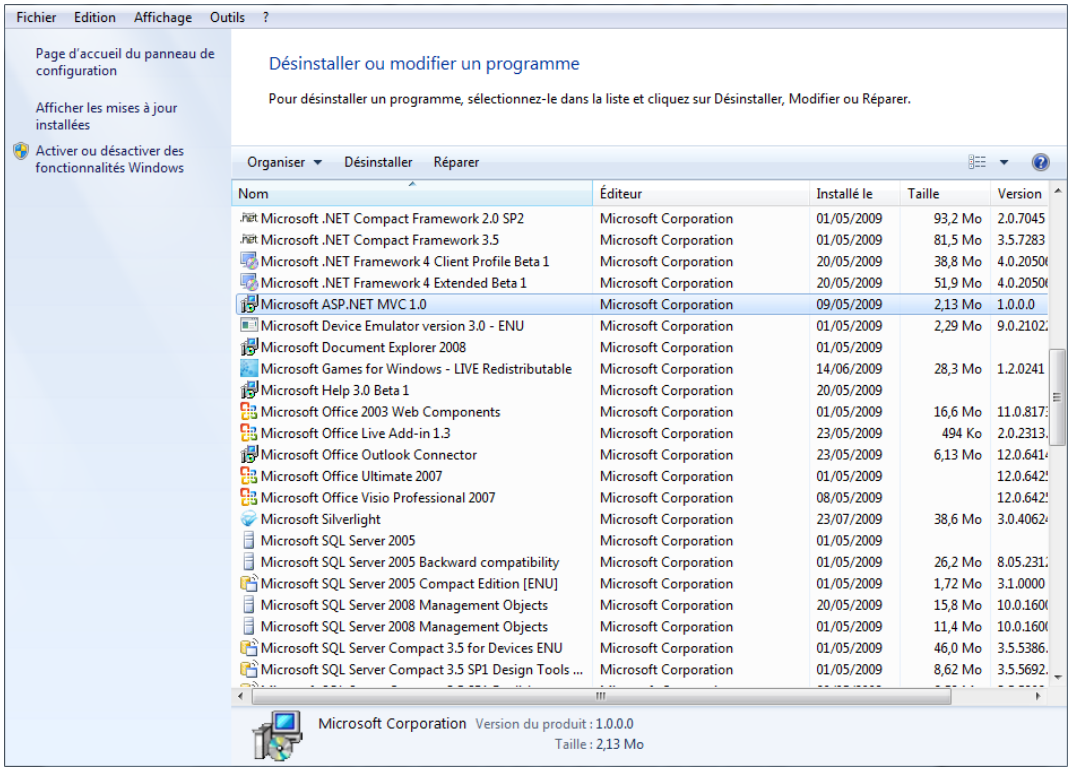


Figure 5–1 Panneau de désinstallation des programmes

3 Ce panneau liste tous les programmes présents sur l'ordinateur pour lesquels un fichier de désinstallation a été enregistré auprès de Windows. Cliquez à l'aide du bouton droit de la souris sur le programme de votre choix et choisissez *Désinstaller*.

Nettoyer le système et le registre

Le temps de son installation sur le système, un programme créé des fichiers et des entrées registre. Tous ces fichiers et données sont nécessaires à son bon fonctionnement et sont donc importants tant que le programme est installé sur le système.

Cependant, une fois le logiciel concerné désinstallé, ces informations n'ont plus aucun intérêt. Si le programme de désinstallation ne les a pas supprimés, il peut arriver que ces données inutiles s'accumulent et posent problèmes.

Astuce Désinstaller un programme non désinstallable

Certains programmes sont coriaces à supprimer. Soit ils n'ont pas enregistré de désinstalleur auprès de Windows, et dans ce cas, il est nécessaire de se rendre dans le répertoire du logiciel pour y supprimer manuellement tous les fichiers. Soit ils apparaissent dans la liste des programmes installés alors qu'ils ne le sont plus. Dans ce cas, il faut ouvrir le registre par `regedit` et ouvrir la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`.

Vous trouvez là tous les désinstalleurs enregistrés, affichés dans le panneau de configuration. Identifiez alors le GUID (identifiant unique) de votre installateur et supprimez sa clé. La modification est immédiate, et le programme n'apparaîtra plus dans le gestionnaire de désinstallation. Assurez-vous de trouver le bon enregistrement dans la base de registre, la suppression involontaire d'une donnée vitale est très vite arrivée.

Le registre Windows ou base de registre

Le registre est la base de données principale de tout système d'exploitation Windows. Elle contient les données de configuration du système mais également des logiciels installés ou encore les paramètres de chaque utilisateur. Ainsi, chaque compte possède son propre fichier `NTUSER.dat` qui contient sa branche de paramètres personnels. L'utilitaire Regedit.exe sert à ouvrir et à éditer les fichiers composant l'ensemble de la base de registre.

Télécharger CCleaner

Pour télécharger CCleaner, rendez-vous sur le site officiel. Ce logiciel est entièrement gratuit, mais certains sites malveillants tentent de vous faire payer ou de vous pousser à faire un don pour y avoir accès. Ne vous faites pas berner.

- http://www.ccleaner.com

C'est là qu'une faiblesse de Windows apparaît. L'OS est totalement incapable de nettoyer les fichiers et de supprimer ceux qui ne sont plus utiles. C'est d'autant plus malheureux que ce besoin existe depuis les toutes premières versions de Windows et que depuis autant d'années, il existe des logiciels, gratuits ou payants, qui réalisent très bien cette tâche. Parmi la multitude de logiciels dédiés qui existent, CCleaner est sans doute l'un des plus efficaces. Il est également important de préciser qu'il est gratuit.

CCleaner pèse quelques mégaoctets et est extrêmement simple à installer. Attention, il vous propose lors de l'installation d'ajouter une barre d'outils *Yahoo!* à vos navigateurs. Il est conseillé de décocher la case pour éviter l'installation de cette barre d'outils, qui est plus un outil de publicité qu'un outil utile. L'interface de CCleaner est simple et réduite au strict minimum comme le prouve la figure 5–2 :

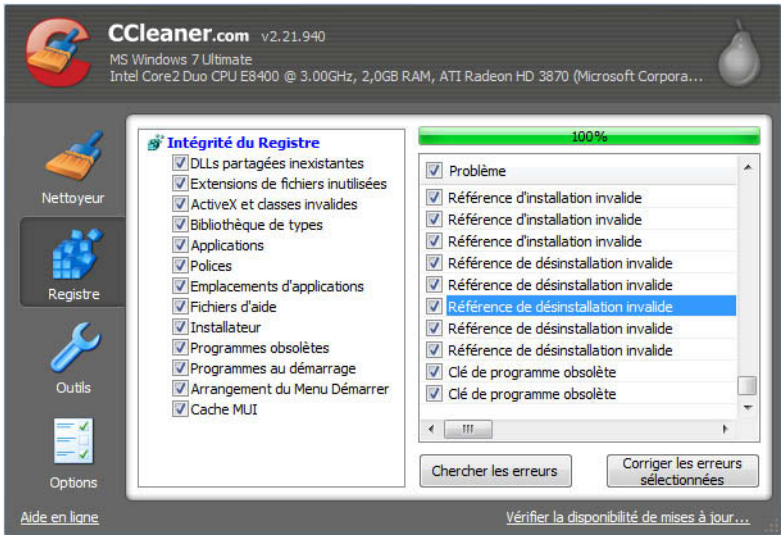


Figure 5–2
Interface du logiciel CCleaner

Bien que CCleaner soit capable de nettoyer beaucoup d'éléments du système, c'est uniquement le nettoyage du registre qui nous intéresse ici :

1. Cliquez sur *Registre*.
2. Cliquez ensuite sur le bouton *Chercher les erreurs*.
3. Une fois l'analyse terminée, cliquez sur *Corriger les erreurs sélectionnées*. L'outil va alors corriger les informations erronées qu'il a trouvées au sein du registre.

Cet outil est particulièrement efficace dans le cas d'une désinstallation logicielle, car il est capable de détecter :

- les références à des fichiers n'existant plus ;
- les références à des fichiers d'installation ou de désinstallation erronées ;

- les entrées registre non utilisées ;
- les DLL partagées inexistantes ou encore les programmes mal installés.

CCleaner ne nettoie pas complètement le système, il sert simplement à le garder aussi propre que possible.

Ajouter des composants Windows

Bien que le module de configuration dont nous allons parler existe depuis bien des années au sein des versions de Windows, il a été complété dans Windows 7. En effet, le gestionnaire de fonctionnalités Windows contrôle encore plus d'éléments que dans les versions précédentes (par exemple, Internet Explorer 8, Plate-forme Microsoft Gadget, etc.).

Windows est de plus en plus modulaire. Si sur ce point il n'est pas au niveau de ses concurrents de type Linux/Unix, il se dirige lentement mais sûrement vers des versions sur lesquelles l'utilisateur pourra décider précisément de ce qui sera installé ou non.

À l'heure actuelle, les fonctionnalités de Windows ne sont pas toutes présentes par défaut. Votre OS est, par exemple, capable de faire office de serveur web si vous le chargez de mettre en place cette fonctionnalité. Un serveur web étant un vecteur potentiel d'attaque pour des hackers, l'activer par défaut ne ferait qu'augmenter la surface d'attaque du système. Il est préférable de limiter les fonctionnalités pour couvrir les besoins d'un maximum d'utilisateurs lambda et de laisser les fonctionnalités avancées aux utilisateurs avertis.

À SAVOIR Surface d'attaque d'un système d'exploitation

On parle de surface d'attaque d'un système d'exploitation lorsque l'on évoque la totalité des fonctionnalités qui sont activées sur ce dernier. Un système se veut sécurisé, mais des failles de sécurité peuvent néanmoins être découvertes bien après la sortie du produit. En multipliant les fonctionnalités du système, vous multipliez par la même occasion la probabilité qu'un attaquant trouve une faille de sécurité dans votre système. Ainsi, plus la surface attaquable est grande, plus il est possible d'y trouver un trou de sécurité. Il n'est pas pour autant nécessaire d'être pessimiste et de refuser d'ajouter la moindre fonctionnalité. N'installez que ce qui vous est nécessaire.

Ajouter une fonctionnalité Windows

L'ajout de fonctionnalités se fait de deux manières :

- par l'installation d'un outil tiers comme nous l'avons évoqué au début de ce chapitre ;
- par l'activation d'une fonctionnalité Windows déjà présente.

C'est le deuxième cas de figure qui nous intéresse ici. Il suffit d'utiliser un module bien spécifique du panneau configuration.

1. Ouvrez le panneau de configuration.
2. Cliquez sur *Programmes*.
3. Sélectionnez *Ajouter ou désactiver des fonctionnalités Windows*.
4. Une fenêtre s'ouvre et charge une liste de toutes les fonctionnalités Windows de votre version. Soulignons qu'une version Intégrale présentera une liste bien plus complète qu'une version Familiale.

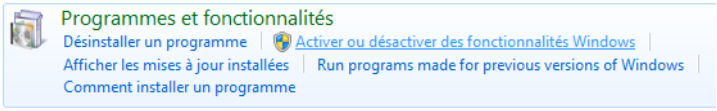


Figure 5–3
Panneau de configuration – Les différents modules de gestion des programmes

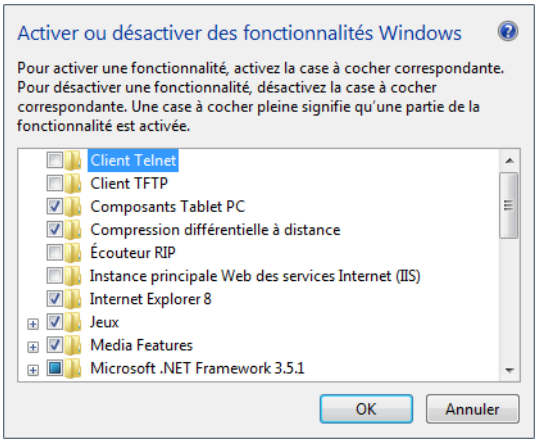


Figure 5–4
Gestionnaire de fonctionnalités Windows

5 Cochez alors les fonctionnalités de votre choix, puis cliquez sur *OK*. Leur installation peut durer plusieurs minutes.

Supprimer une fonctionnalité Windows

Le module *Ajouter ou désactiver des fonctionnalités Windows* permet également de désactiver des fonctionnalités actuellement présentes sur le système. Qu'il s'agisse de supprimer les jeux Windows ou simplement de retirer une fonctionnalité que vous aviez précédemment installée, il vous suffit d'ouvrir le gestionnaire de fonctionnalités Windows, de décocher les cases se situant devant les éléments à supprimer, puis de cliquer sur le bouton *OK*. Il sera bien entendu possible de réactiver ces fonctionnalités par la suite, et ce, autant de fois que vous le jugerez nécessaire.

Contrôle d'application avec AppLocker

Installer des programmes permet de décupler les fonctionnalités d'un ordinateur, mais entre de mauvaises mains, ces mêmes programmes peuvent devenir une source de problèmes. Prenons l'exemple simple d'un logiciel de *peer-to-peer*, permettant d'échanger des fichiers à travers Internet. En installant ce type de logiciel, il est possible que l'un des utilisateurs en fasse un usage illégal et qu'il s'agisse d'une utilisation professionnelle ou personnelle de l'ordinateur, l'administrateur du système doit, autant que possible, empêcher cela.

Les enjeux du blocage de logiciel

Jusqu'à maintenant, un administrateur avait à sa disposition les stratégies de restriction logicielle (SRP pour *Software Restriction Policy*), apparues avec Windows XP et Windows Serveur 2003. Ces stratégies de restriction logicielle permettent de contrôler l'utilisation des applications des ordinateurs se trouvant dans un domaine. Ces SRP permettent, entre autres, de :

- définir les ActiveX qui peuvent être téléchargés sur le navigateur web ;
- exécuter des scripts signés ;
- verrouiller un ordinateur ;
- s'assurer que seuls certains logiciels autorisés peuvent être installés sur les ordinateurs.

L'inconvénient des SRP est d'être long à configurer pour des protections malheureusement faciles à outrepasser.

Avec Windows 7 et Windows Serveur 2008 R2, Microsoft intègre AppLocker, un nouveau module de gestion d'exécution d'application, fonctionnant aussi bien via des stratégies de groupe que des stratégies locales. Avec un fonctionnement sensiblement identique aux stratégies de restriction logicielle, AppLocker a pour but de dépasser ces deux inconvénients.

Néanmoins, il existe des différences entre les configurations de ces deux solutions. Pour les stratégies de restriction logicielle de Windows 7, nous disposons :

- de plusieurs niveaux de sécurité (Non autorisé, Utilisateur Standard, Non Restreint) ;
- des règles supplémentaires (surcharge des règles par défaut soit par certificat, hash, zone réseau ou chemin d'accès) ;
- du contrôle obligatoire (type de logiciel auquel les règles s'appliquent) ;
- des types de fichiers désignés (extension de fichier) ;
- des éditeurs approuvés.

Tandis que pour AppLocker, nous avons :

- les règles de l'exécutable ;
- les règles de Windows Installer ;
- les règles de scripts.

Certes, les deux solutions se complètent. Cependant, avec une stratégie bien réfléchie, il est possible de n'utiliser qu'AppLocker pour arriver à ses fins, c'est pourquoi nous nous focaliserons sur cette solution.

À SAVOIR AppLocker et les versions de Windows 7

AppLocker n'est pas disponible sur toutes les versions de Windows 7 et vous ne le trouverez que sur les versions Intégrale, Entreprise et Professionnelle. Néanmoins, même s'il est possible d'appliquer des stratégies locales AppLocker sur Windows Professionnel, vous ne pourrez pas forcer l'application de règles sur des ordinateurs d'un domaine tournant sous Windows 7 Professionnel.

POUR ALLER PLUS LOIN Documentation SRP

Si vous souhaitez recourir aux stratégies de restriction logicielle au lieu d'AppLocker, lisez la documentation officielle se trouvant à l'adresse suivante :

- http://technet.microsoft.com/en-us/library/cc507878.aspx

ou recherchez « *Using Software Restriction Policies to Protect Against Unauthorized Software* » sur le site :

- http://technet.microsoft.com

À SAVOIR AppLocker et les stratégies de groupe

Vous pouvez passer par AppLocker pour des stratégies de sécurité locales, mais également pour des stratégies de groupe. La console pour les stratégies de groupe n'étant pas toujours disponible par défaut, il vous faudra :

1. Télécharger les *Remote Server Administration Tools for Windows 7* (RSAT).
2. Vous rendre dans l'outil *Ajouter ou désactiver des fonctionnalités Windows.*
3. Cocher la case devant *Outils d'administration de serveur distant* et particulièrement devant le nœud enfant se nommant *Outils de gestion des stratégies de groupe*.

RSAT est téléchargeable depuis l'adresse suivante :

- http://www.microsoft.com/downloads/details.aspx?displaylang=fr&FamilyID=7d2f6ad7-656b-4313-a005-4e344e43997d

Une autre manière de se procurer RSAT consiste à vous rendre sur le site MSDN.fr et à saisir `Outils d'administration de serveur distant pour Windows 7` dans la zone de recherche.

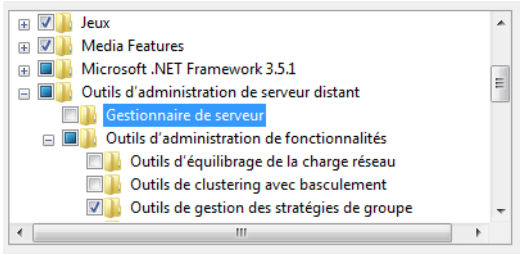


Figure 5–5 Ajout des outils d'administration de serveur distant

Configurer AppLocker

AppLocker est le nom donné aux stratégies de contrôle de l'application. Tout comme les stratégies de restriction logicielle, il s'agit de stratégies de sécurité accessibles via la console de gestion des stratégies de sécurité locale.

1. Saisissez `secpol.msc` dans la zone de saisie du menu *Démarrer*.
2. Dépliez l'arborescence jusqu'à *Stratégies de contrôle de l'application*.

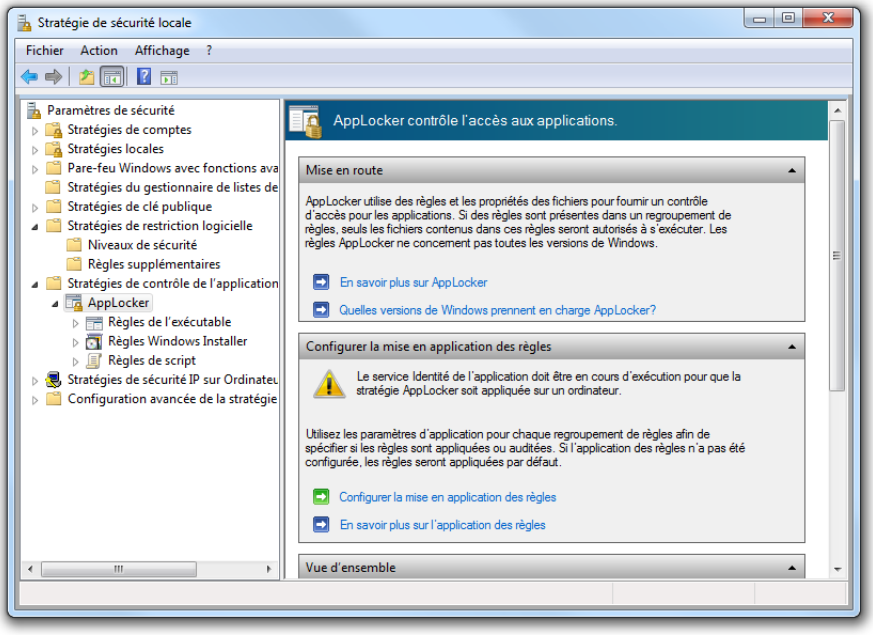


Figure 5–6
Console de gestion des stratégies locales

Les règles AppLocker s'appliquent à quatre types d'objets :

- les exécutables, correspondant aux fichiers `.exe` ou `.com` ;
- les fichiers d'installation, correspondant aux fichiers Windows Installer (`.msi`) et correctifs (`.msp`) ;
- les scripts, correspondant aux fichiers PowerShell (`.ps1`), batchs (`.bat`), commandes (`.cmd`), VBScript (`.vbs`) et JavaScript (`.js`) ;
- les fichiers DLL.

Pour chacun de ces objets, AppLocker définit une règle autorisant ou non l'objet en fonction de trois critères :

- L'éditeur : renseigner ce paramètre permet de vérifier que l'exécutable a bien été signé numériquement par l'éditeur du logiciel.
- Le chemin d'accès : il s'agit de pointer directement vers un fichier ou un dossier particulier.
- Le hachage du fichier : il s'agit ici d'utiliser la signature du hash du fichier.

Les deux critères recommandés sont le certificat éditeur et le hachage. En effet, pour un exécutable bloqué depuis un chemin donné (par exemple, `C:\appli.exe`), il suffit de déplacer ou de renommer l'exécutable pour que celui-ci soit éventuellement autorisé, s'il répond aux critères d'une autre règle d'autorisation. Il nous reste maintenant à définir nos propres règles.

Créer des règles d'application

La création d'une règle d'application est simple et ne requiert que quelques clics. Nous allons ici mettre en place une règle d'application afin de n'autoriser qu'un seul utilisateur à lancer Daemon Tools, un outil de disque virtuel.

1. Dans la fenêtre des stratégies locales, cliquez à l'aide du bouton droit sur l'élément *Règles de l'exécutable* et choisissez le menu *Créer une règle*. Un assistant s'ouvre alors. La première étape consiste à définir s'il s'agit d'une règle d'autorisation ou une règle de blocage. Pour notre exemple, cliquez sur *Autoriser*, puis sur le bouton *Sélectionner* pour choisir le groupe *Administrateurs*.
2. À l'écran suivant, il vous est demandé de choisir les conditions de votre règle. Dans notre cas, nous allons prendre la condition recommandée par Microsoft, à savoir l'éditeur. Cliquez sur le bouton *Suivant*. L'écran de l'éditeur permet deux choses :
   - choisir un exécutable signé par un éditeur donné ;
   - le niveau des critères pour reconnaître l'application signée.

ASTUCE AppLocker et les DLL

Par défaut, AppLocker ne gère que les trois premiers types d'objets. Pour activer la gestion des DLL, suivez la procédure suivante :

1. Cliquez avec le bouton droit sur l'élément *AppLocker* et choisissez le menu *Propriétés*.
2. Dans l'onglet *Avancé*, cochez la case *Activer le regroupement de règles DLL*.
3. Cliquez sur le bouton *Appliquer*.

Le hachage de fichier

Il s'agit d'une méthode particulière qui, pour une chaîne de données précise, donne une signature unique. Par exemple, le hash MD5 de Louis-Guillaume Morand est, immuablement, b997e521d4309ad8fe1791f66402b686. L'intérêt du hash est que la signature (dite aussi empreinte) est unique pour chaque chaîne d'entrée.

Dans le cas d'AppLocker, ou d'un fichier en général, les informations binaires du fichier sont placées bout à bout pour former une chaîne. Un hash est effectué sur cette chaîne. Cela signifie que si vous renommez le fichier, son hash sera toujours identique. Cependant, si vous prenez le même exécutable, mais dans une version différente, même s'il fait la même taille à l'octet près, l'empreinte hash sera différente.

Bien que des cas de collisions (deux chaînes ayant la même signature) aient été démontrés, il s'agit ici d'une façon très fiable de certifier qu'un fichier est formellement identique au fichier qui a été autorisé.

COMPRENDRE Règle d'autorisation ou règle de blocage ?

Ce choix dépend généralement du nombre de règles parallèles qui relèvent de cette même règle. Il est en effet plus facile de définir une règle pour bloquer un programme que des règles pour autoriser tous les autres.

ATTENTION Configurer une règle par défaut pour les programmes système

Lorsque AppLocker est activé, tout logiciel qui ne correspond pas à une règle d'autorisation sera refusé. Ceci concerne tous les exécutables de l'ordinateur y compris les exécutables système. Dans notre cas, toutes les applications autres que Daemon Tools seront bloquées, y compris certaines consoles d'administration système ! Il est donc impératif de configurer une règle par défaut pour autoriser les programmes système.

3 Lorsque vous optez pour un applicatif signé, différents champs d'informations sont proposés. Le premier décrit la signature de l'éditeur, le second le nom du produit. Vient ensuite le nom du fichier exécutable et enfin son numéro de version. Définissez ensuite à l'aide du curseur les éléments qui serviront de critères pour la règle que vous êtes en train de configurer. Vous pouvez définir une règle qui accepte tous les programmes d'un éditeur donné. Il faut pour cela monter le curseur et le placer face au champ éditeur. Ou alors, comme le montre la figure 5–7, vous pouvez créer une règle qui autorise l'exécution du logiciel Daemon Tools Lite, quel que soit son numéro de version. Ainsi, si l'utilisateur met à jour son logiciel, celui-ci pourra toujours être exécuté.

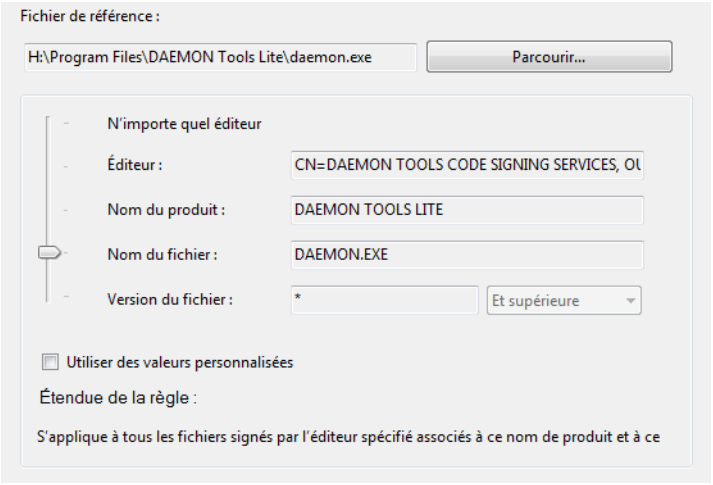


Figure 5–7
Définition du paramétrage de l'éditeur

4 Continuez en créant un service par défaut pour les programmes système. Cliquez à l'aide du bouton droit sur la partie centrale et choisissez le menu *Créer des règles par défaut*.

Trois règles génériques sont alors créées :

- La première indique que tous les programmes situés dans le répertoire `Windows` peuvent être exécutés par n'importe qui.
- La deuxième fait de même, mais pour tous les programmes se trouvant dans le répertoire `Programmes` (`%ProgramFiles%`).
- La troisième et dernière précise quant à elle que les administrateurs locaux peuvent exécuter toutes les applications de l'ordinateur, où qu'elles se trouvent.

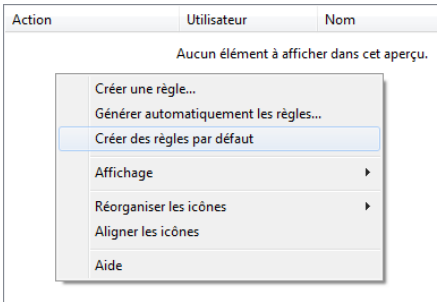


Figure 5–8
Menu de création des règles par défaut

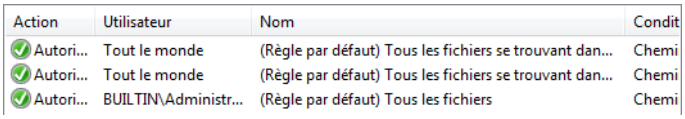


Figure 5–9
Les trois règles par défaut d'AppLocker

Les stratégies sont prêtes, mais pourtant, elles ne seront pas appliquées. Cela provient du fait que le service *Identité de l'application* qui s'occupe d'identifier les applications n'est pas démarré.

5 Ouvrez le menu *Démarrer* et tapez `services.msc` dans la zone de saisie, afin d'ouvrir la console de gestion des services.

6 Cherchez alors le service *Identité de l'application* et démarrez-le.

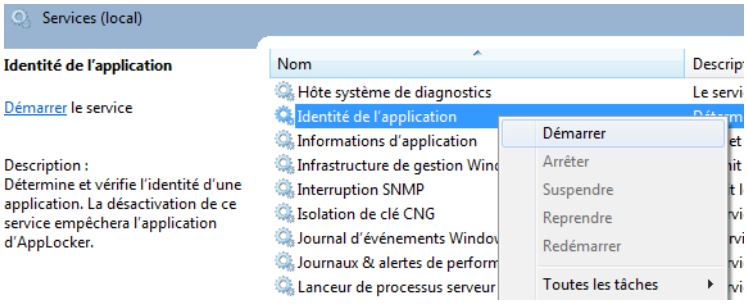


Figure 5–10
Console de gestion des services Windows

7 AppLocker est maintenant configuré et actif. Lorsque vous tenterez de réaliser une action non autorisée par l'une des règles de contrôle d'application, un message d'avertissement vous le signalera.

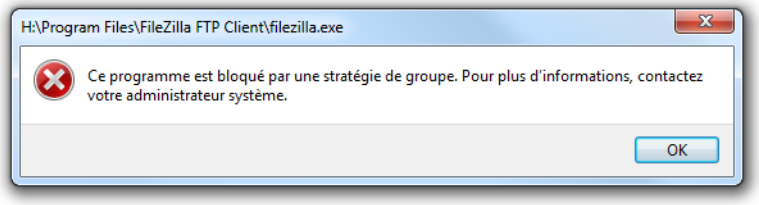


Figure 5–11
Fenêtre d'avertissement en cas de blocage par AppLocker

En résumé

Au cours de ce chapitre, nous avons étendu les fonctionnalités de Windows 7 à l'aide de logiciels et grâce à des fonctionnalités Windows désactivées par défaut. Nous nous sommes ensuite intéressés à la manière de mieux contrôler les applications installées sur le système. Nous savons à présent prévenir l'utilisation de logiciels qui pourraient s'avérer dangereux pour le système.

chapitre 6

Stocker les données

Le stockage des données n'est pas qu'une question de disposition organisée de fichiers et de dossiers, il résulte de stratégies destinées à répondre à des besoins très précis. Qu'il s'agisse de duplication, de compression ou encore de chiffrement de données, il faut choisir la solution la plus adaptée à vos besoins.

SOMMAIRE

- Espace disque et partitions
- Indexer les fichiers
- Compresser les fichiers
- Chiffrer les données
- Virtualiser les fichiers

MOTS-CLÉS

- Partition
- Disque dynamique
- Système de fichiers
- NTFS, FAT32, RAID
- Étendre
- Indexation
- Chiffrement
- EFS
- BitLocker
- Mot de passe
- Compression
- Virtual Store

Mirroring

Aussi appelé agrégation par bande ou RAID-1, le *mirroring* améliore les performances d'écriture des données. De plus, il accroît la pérennité des données car elles sont écrites en double.

Optimiser les partitions et les disques durs

Le stockage des données et la configuration d'un disque dur ne sont pas des opérations aussi anodines qu'il y paraît. Tout choix que vous ferez à ce niveau a des conséquences, tant sur les performances que sur la pérennité des données, mais aussi sur la facilité d'utilisation de l'espace disque.

Un ordinateur possède un ou plusieurs disques durs. La façon de les configurer et/ou de les partitionner a un impact sur l'utilisation que vous pourrez en faire. Il en va de même pour le système de fichiers que vous choisissez.

On distingue entre les disques durs dits « de base » et les disques dynamiques. Un disque de base est un disque simple sur lequel vous créez des partitions principales ou étendues. Les disques dynamiques, quant à eux, servent à mettre en place des mécanismes de *mirroring* à l'aide de volumes.

Culture **Systèmes de fichiers**

Windows ne gère que trois systèmes de fichiers : FAT32 et NTFS pour les disques durs, et exFAT destiné à l'origine aux supports de stockage externes et mémoire flash. Chacun de ces systèmes de fichiers a ses avantages et inconvénients. Le système FAT32 est le plus ancien d'entre tous, il est plus limité, tant en taille maximale de fichier (4 Go) qu'en taille de partition (32 Go sous Windows, 8 To en théorie). Le nombre de fichiers est limité à 268 000 000 et il n'est pas possible de définir des droits d'accès de groupe.
Évolution de FAT32, exFAT permet de gérer de bien plus gros fichiers, sans limite de taille de partition. Il gère les autorisations d'accès (ACL) ainsi que la lecture/écriture via des transactions TFAT (*transaction-safe FAT*), système permettant de garantir la non-corruption des données en cas de retrait brusque du support de stockage amovible.
Enfin, le système NTFS est destiné à corriger les inconvénients de FAT32. Il propose la gestion des droits sur les fichiers ou les dossiers, mais permet aussi, et surtout, d'établir des quotas utilisateur pour limiter l'utilisation de l'espace disque. Il permet également la compression à la volée des fichiers (gain de place) et surtout de chiffrer les fichiers avec EFS (*Encrypting File System*).
Il est néanmoins possible d'utiliser un système de fichiers supplémentaire, Ext2, en installant un pilote tiers :

- http://www.fs-driver.org/

Toutes les opérations de gestion et de choix de système de fichiers se font via la console de gestion des disques. Pour la lancer :

1. Ouvrez le menu *Démarrer*.
2. Cliquez avec le bouton droit sur le menu *Ordinateur*.
3. Choisissez l'option *Gérer*.
4. Dans la console *Gestion de l'ordinateur*, utilisez l'extension *Gestion des disques* qui se trouve sous le libellé *Stockage*.

Gérer les disques de base

La partie supérieure de la fenêtre liste les partitions et volumes actifs. C'est dans la partie inférieure de la console qu'auront lieu les opérations de configuration. Chaque disque dur physique y est représenté par une ligne sur laquelle sont représentées les partitions.

Il existe deux types principaux de partitions :

- Les partitions principales (un disque de base ne peut en contenir que quatre au maximum). Pour démarrer un système d'exploitation, il est nécessaire d'avoir au moins une partition principale active.
- Les partitions étendues (qui peuvent contenir un très grand nombre de partitions logiques).

Chaque type de partition possède une couleur particulière permettant de les différencier :

- Bleu foncé : partition principale.
- Bleu clair : partition logique.
- Vert clair : espace non partitionné.
- Encadré vert foncé : partition étendue.

Puisque vous êtes actuellement connecté sous Windows, cela signifie que votre disque dur principal possède au moins une partition principale. Vous pouvez donc créer trois partitions principales supplémentaires ou alors en créer deux autres, puis créer une partition étendue au sein de laquelle il sera possible d'ajouter autant de partitions logiques que nécessaire. Voici comment ajouter une partition principale :

1. Cliquez avec le bouton droit sur un espace non alloué et sélectionnez *Nouveau volume simple*.
2. Un assistant de création s'affiche et vous demande en premier lieu la taille en mégaoctets de la partition que vous voulez créer. Pensez à toujours laisser 1 Mo non utilisé. En effet, si vous souhaitez un jour convertir un disque de base en disque dynamique, le mécanisme de conversion nécessitera un espace non alloué d'environ 1 Mo pour y stocker les informations de conversion.
3. L'écran suivant de l'assistant permet de définir le moyen d'accès à la partition. L'option *Attribuer une lettre spécifique* permet d'indiquer la lettre par laquelle la partition sera disponible via l'explorateur. Avec *Monter dans un dossier NTFS vide*, la partition n'aura pas de lettre attribuée mais sera accessible comme s'il s'agissait d'un simple dossier. Enfin, si vous cochez *Ne pas attribuer de lettre de lecteur ni de chemin d'accès de lecteur*, la partition sera présente mais inaccessible. Vous pourrez néanmoins lui attribuer une lettre plus tard.

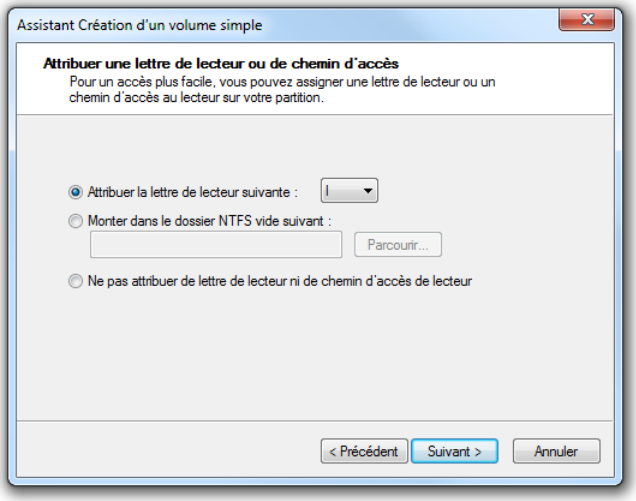


Figure 6–1
Assistant de création de partition

ATTENTION Le système exFAT et les versions antérieures de Windows

L'assistant permet de choisir la taille d'unité d'allocation (zone minimale peut prendre un fichier sur le disque dur) de la partition et choisir une valeur allant jusqu'à 64 Ko. Par défaut, sur un système FAT, la taille d'allocation par défaut est de 16 Ko, tandis qu'elle est de 4 Ko pour NTFS. Néanmoins, si vous configurez une partition en FAT utilisant une unité d'allocation supérieure à 32 Ko, la partition ne sera pas utilisable par certaines versions antérieures de Windows (95, 98, 2000 et XP). Augmenter la taille d'unité d'allocation améliore très sensiblement les performances d'accès aux fichiers mais entraîne une perte d'espace disque. En effet, sur une partition possédant une unité d'allocation de 4 Ko, un fichier de 5 Ko occupe alors un espace de 8 Ko (2 x 4 Ko).

BON À SAVOIR
Éléments modifiables a posteriori

Si la manière dont est configurée la partition ne correspond plus à vos besoins, le nom, la lettre d'accès ou encore la taille seront modifiables par la suite.

ASTUCE L'extension de volume est désactivée

Il arrive que le menu *Étendre le volume* soit désactivé pour certaines partitions. Cela est dû au fait qu'une partition ne peut être étendue que sur un espace contigu de clusters. Ainsi, selon la position du volume sur le disque dur physique, il est possible que cette option ne soit pas disponible. Il ne reste alors que la solution de mettre en œuvre un outil tiers, tel que DiskPart, dont la documentation se trouve à l'adresse suivante :

- http://support.microsoft.com/kb/325590

4 Le dernier écran de l'assistant permet de définir le formatage de la partition. Vous pouvez ainsi choisir le système de fichiers NTFS pour avoir un système de fichiers avancé ou choisir le format exFAT (version améliorée de FAT/FAT32) pour obtenir une partition pleinement compatible avec d'autres systèmes d'exploitation tels Linux ou Mac OS X.

La partition est alors fin prête et directement utilisable par le système.

La création d'une partition étendue se fait de la même façon et avec les mêmes options.

Réduire ou augmenter la taille d'une partition

- Comme son prédécesseur Windows Vista, Windows 7 permet le redimensionnement des partitions. Cette fonctionnalité est utile lorsqu'une partition possède trop d'espace disque inutilisé ou à l'inverse, lorsqu'une partition manque visiblement d'espace libre.

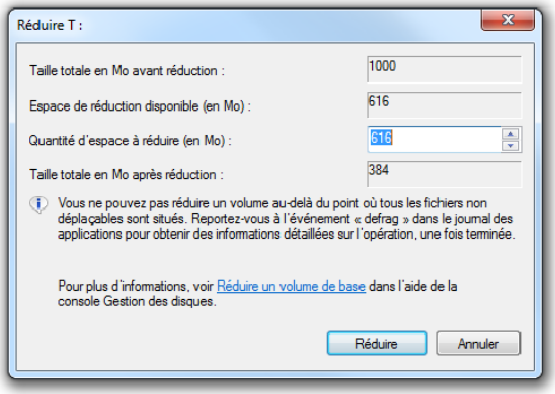


Figure 6–2
Assistant de réduction de partition

- Après avoir cliqué avec le bouton droit sur l'une des partitions, vous avez le choix entre les menus *Réduire le volume* et *Étendre le volume*. Dans chacun des cas, un assistant vous permet de définir la nouvelle taille de partition que vous souhaitez obtenir.

Changer le système de fichiers

Il est également possible de changer le système de fichiers d'une partition par la suite. Néanmoins, selon le type de conversion choisi, la façon de faire et les conséquences ne seront pas les mêmes. Ainsi, pour convertir une partition FAT32 en NTFS, il suffit d'ouvrir une invite de commandes et de saisir :

```
Convert X: /fs:NTFS
```

où `X` représente la lettre de la partition à convertir. Dans ce sens, la conversion se fait sans perte de données.

Il n'en va pas de même pour convertir une partition NTFS en FAT32. La conversion nécessite un reformatage complet de la partition ce qui entraîne une perte des données. Il est donc nécessaire d'effectuer une sauvegarde des données avant d'exécuter la commande suivante dans une invite de commandes :

```
format X: /fs:fat32
```

B.A.-BA L'invite de commandes

L'invite de commandes est une interface qui permet une communication directe entre l'utilisateur et son système d'exploitation. Elle sert à lancer des programmes en lignes de commandes ou bien à exécuter directement des commandes MS-DOS. Voici comment l'ouvrir :

1. Ouvrez le menu *Démarrer*.
2. Saisissez `cmd` dans la zone de saisie.
3. Appuyez sur la touche *Entrée*.

La gestion des disques dynamiques

L'utilisation de disques dynamiques n'a d'intérêt que si votre ordinateur possède plusieurs disques durs physiques. Les manipulations suivantes nécessitent que le disque dur ait été préalablement converti en disque dynamique :

1. Rendez-vous dans la partie inférieure centrale de la console de gestion.
2. Cliquez à l'aide du bouton droit sur le disque de votre choix.
3. Choisissez l'option *Convertir en disque dynamique*.

Posséder des disques dynamiques vous permet de profiter de différentes solutions de volume :

- volume simple ;
- volume fractionné ;
- volume agrégé par bande ;
- volume en miroir ;
- volume RAID-5.

ATTENTION Conversion disque de base vers disque dynamique

Si la conversion d'un disque de base vers un disque dynamique se fait sans perte de données, l'inverse n'est pas vrai. Le fait de repasser en disque de base nécessite la suppression de tous les volumes et les données qui s'y trouvent. Pensez donc à effectuer des sauvegardes préalables.

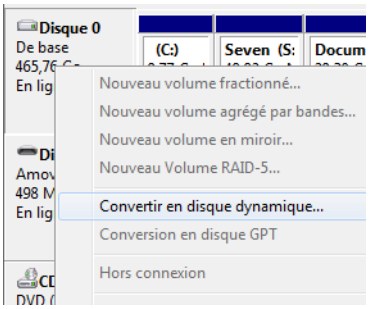


Figure 6–3 Menu contextuel pour la conversion dynamique

Chacune de ces possibilités correspond à un besoin particulier et possède ses propres avantages.

Les volumes simples

Un volume simple est l'équivalent dynamique des partitions principales d'un disque de base. Cependant, leur nombre n'est pas limité au sein d'un même disque dur. Créer un volume simple revient à créer une partition sur un disque de base.

Les volumes fractionnés

Un volume fractionné (ou réparti) est composé de l'espace disque se trouvant sur plusieurs disques durs (jusqu'à 32). Le système considère ce volume comme un volume unique. Ses données sont inscrites sur le premier disque, puis lorsque celui-ci est plein, sur le disque suivant, et ainsi de suite.

Cette méthode permet d'étendre très facilement un volume en lui ajoutant de l'espace disque au fur et à mesure que les premiers disques se remplissent. Malheureusement, cette solution comporte un inconvénient majeur : si un disque devient défectueux, les données qu'il contenait sont perdues. Pour créer un volume fractionné :

1. Cliquez sur un espace non alloué et choisissez le menu *Nouveau volume fractionné*.
2. Sélectionnez ensuite au moins deux disques dynamiques.
3. Définissez ensuite taille, système de fichiers et lettre à attribuer (ou le point de montage).

S'il est possible d'étendre un volume fractionné, il est en revanche impossible de récupérer une partie d'un volume fractionné sans défaire entièrement le volume et perdre les données qui s'y trouvent.

Les volumes agrégés par bande

Les volumes agrégés par bande (RAID-0) sont des volumes liés au sein de plusieurs disques durs physiques (entre 3 et 32) pour ne former qu'un seul et unique volume logique visible par le système. Au sein de ce volume, les données sont écrites alternativement sur les différents disques, ce qui améliore les performances d'écriture. Lorsqu'un fichier est crée, il est découpé en petits blocs de 64 Ko qui sont écrits sur le premier disque, puis sur le deuxième, et ainsi de suite. Le fichier se retrouve ainsi morcelé sur différents disques durs. La vitesse d'écriture est améliorée puisque plusieurs têtes de lecture de disque dur sont utilisées simultanément.

Comme les données sont réparties équitablement sur les différents disques, l'agrégat est basé sur la taille du disque ayant le moins d'espace

disque. Ainsi, si vous possédez deux disques de 500 Go et un disque de 200 Go, et que vous décidez de les agréger, alors l'agrégat sera de 200 Go et l'espace restant ne sera pas utilisé. Voici la procédure à suivre pour créer un volume agrégé par bande :

1. Cliquez sur un espace non alloué et choisissez le menu *Nouveau volume agrégé par bandes*.
2. Sélectionnez ensuite au moins deux disques dynamiques.
3. Définissez la taille, le système de fichiers et la lettre à attribuer (ou le point de montage).

Bien que performante, cette méthode ne tolère aucune panne de la part d'un des disques durs. Elle est donc très peu usitée.

Les volumes en miroir

Appelé aussi RAID-1, le *mirroring* est un mécanisme qui, à l'aide de deux disques durs physiques distincts, écrit les données sur deux volumes différents. Les deux volumes en miroir sont alors identiques à l'octet près. En cas de défaillance de l'un des deux disques, les données sont conservées sur l'autre disque. La mise en miroir apporte donc une tolérance de panne et améliore les performances de lecture et d'écriture des données.

Voici comment mettre en place des volumes en miroir :

1. Sélectionnez un volume simple.
2. À l'aide du bouton droit, choisissez *Ajouter un volume miroir*.
3. Suivez l'assistant pour sélectionner un espace non alloué qui servira de volume jumeau.

ATTENTION **Extension impossible**

Les volumes miroirs ne peuvent être étendus.

Les volumes RAID-5

Le RAID-5 est l'une des techniques de RAID les plus utilisées. Il s'agit d'un système de volumes agrégés par bande à parité répartie. Cela signifie que les données sont découpées et placées sur les différents disques du RAID et les données de parité sont elles aussi réparties sur les différents disques (à l'inverse du RAID-4 qui possède un disque dédié à la parité).

La création d'un volume RAID-5 se réalise de la même manière que précédemment : après avoir cliqué sur un disque non alloué, choisissez l'option *Nouveau volume RAID-5*. Il est important que l'ordinateur soit muni d'une carte mère sachant gérer le RAID. Pour bénéficier de tous les avantages de cette méthode, il est important de mettre à jour le contrôleur RAID de cette dernière en se rendant régulièrement sur le site du constructeur.

Chiffrer les données

Tous les utilisateurs, professionnels et particuliers, ont pris l'habitude de stocker de plus en plus d'informations sur leurs ordinateurs. Qu'il s'agisse de simples courriers électroniques, des photographies ou des relevés bancaires, toutes ces informations se retrouvent à la portée de tout attaquant en quête de données sensibles. Que ce soit via un accès distant ou via un accès physique (l'attaquant est présent près de l'ordinateur), il est relativement aisé pour quelqu'un d'expérimenté de s'introduire sur un ordinateur et d'y dérober les précieuses informations. Il ne s'agit pas forcément d'une vulnérabilité de Windows, mais bien souvent d'une erreur de configuration de la part de l'utilisateur.

L'une des solutions les plus efficaces contre le vol d'informations demeure encore et toujours le chiffrement des données. Il s'agit-là de rendre illisibles les données pour toute personne qui n'aurait pas la clé du « coffre virtuel » les contenant. Dans ce coffre, le chiffrement se propose de modifier les données à l'aide d'un algorithme qui, tant que la bonne clé de décryptage n'est pas utilisée, restera étanche à toute tentative d'accès à la donnée d'origine.

Windows 7 prend en compte ce problème de sécurité et propose trois fonctionnalités permettant d'améliorer de manière significative la protection des données confidentielles. Ce sont ces trois fonctionnalités que nous allons maintenant voir de plus près, afin de découvrir laquelle utiliser selon chaque cas de figure.

Encryption File System

Système de fichiers propre à Windows, EFS permet de stocker les informations dans un format chiffré. C'est, avec BitLocker, la protection la plus élevée que propose Windows sans installer de programmes additionnels.

Compatible avec EFS, le système de fichiers NTFS permet de définir des autorisations d'accès aux fichiers ACL (*Account Control List*) qui sont chargés de contrôler les accès de tel ou tel utilisateur aux données de l'ordinateur. Cette méthode de sécurisation est très efficace lorsque le système est en état de marche, mais peut facilement être contournée si l'attaquant a un accès physique au disque dur et essaie d'y accéder depuis un système d'exploitation alternatif (Linux, live CD Windows, disque dur branché sur un autre ordinateur, etc.). Une solution consiste alors à chiffrer les fichiers sur le disque dur. Ces fichiers seront déchiffrés au moment de l'exécution du système.

ATTENTION
EFS et les versions de Windows 7

Le système de fichiers EFS n'est pas entièrement géré par les versions Starter, Familiale Basique et Familiale Premium. Sur ces versions, le chiffrement et déchiffrement se fait en ligne de commande à l'aide de l'outil intégré à Windows `Cipher.exe`. Tapez la commande `cipher.exe /?` pour apprendre comment utiliser cet outil sur ces versions de Windows.

CULTURE **Le live CD ou CD autonome**

Le live CD est un CD-Rom (ou un DVD-Rom) contenant un système d'exploitation entièrement fonctionnel qui ne nécessite aucune installation. Il suffit en effet d'insérer le CD-Rom dans l'ordinateur au moment du démarrage, le système d'exploitation est alors entièrement chargé en mémoire et est capable de réaliser l'intégralité des fonctionnalités de base de tout système d'exploitation : navigation sur Internet, envoi d'e-mails, visionnage de vidéos, utilisation d'une suite bureautique, etc. Soulignons qu'aucune information n'est sauvegardée (sauf si l'on possède un disque dur de stockage ou une clé USB) et il faudra réinsérer le CD-Rom au prochain démarrage pour recharger le système d'exploitation.
Pour créer des live CD Windows, il suffit d'utiliser les OS minimalistes tels que Windows PE ou BartPE. Pour en savoir plus, consultez l'article suivant :

- http://www.svmlemag.fr/pratique/03156/creez_votre_live_cd_windows_vista

Chiffrer un fichier vous garantit que les fichiers ne seront exploitables et lisibles que sur votre ordinateur. Voici comment chiffrer un fichier ou un dossier :

1. Ouvrez à l'aide du bouton droit les propriétés du dossier (ou du fichier).
2. Cliquez sur le bouton *Avancé* de l'onglet *Général*.
3. Cochez la case *Chiffrer le contenu* pour sécuriser les données.
4. Cliquez sur *OK*.

Votre dossier ou fichier est alors automatiquement chiffré et apparaît en vert dans l'explorateur Windows.

Figure 6–4
Les fichiers chiffrés dans l'explorateur Windows

VERSIONS Chiffrement et Windows XP

La première version de Windows XP (et versions antérieures de Windows) utilisait le cryptage DES (*Data Encryption Standard*) qui n'utilisait alors que des clés de chiffrement de 56 bits clés devenues trop peu sécurisées avec les systèmes actuels. Le Service Pack 1 de Windows XP remplaça alors DES par EFS avec des clés de 128 bits.

EN COULISSE Le fonctionnement d'EFS

EFS utilise le chiffrement AES (*Advanced Encryption Standard)*, dit aussi chiffrement Rijndael, du nom de son créateur (prononcez « rinedeul »). Cet algorithme de chiffrement symétrique a été choisi par le gouvernement des États-Unis pour chiffrer les données des applications qu'il utilise. Simple à mettre en place, il est très sécurisé et permet l'utilisation de clé de cryptage allant jusqu'à 256 bits.

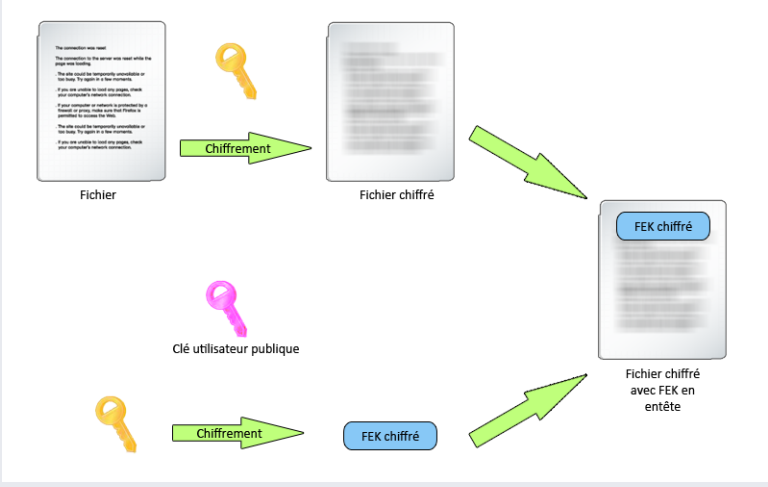


Figure 6–5 Fonctionnement du chiffrement EFS

EFS utilise une clé symétrique générale (FEK pour *File Encryption Key*, mécanisme plus performant pour le chiffrement de fichier de grande taille) pour chiffrer chaque fichier, puis chiffre cette même clé avec la clé publique de l'utilisateur. Enfin, elle place la clé FEK chiffrée dans l'entête du fichier ce qui lie fortement un fichier à un utilisateur donné.

ATTENTION EFS et perte de la clé de déchiffrement

La clé de déchiffrement est liée à chaque utilisateur et principalement à son mot de passe. La réinitialisation du mot de passe par un outil tiers ou la réinstallation du système empêche la récupération de la clé et rend totalement impossible la récupération des données. Les données sont perdues à jamais. Néanmoins, sur Windows 7, il est possible d'exporter la clé sur une *Smart Card*, ce qui permet d'externaliser la reconnaissance de l'utilisateur par un autre élément que son mot de passe. La *Smart Card* fonctionne alors comme une sorte d'empreinte digitale et sera requise à chaque fois qu'un accès à un fichier chiffré sera demandé.

Dans le cadre d'une utilisation professionnelle au sein d'une entreprise, il est recommandé de définir, au niveau du domaine, des agents de récupération, c'est-à-dire des utilisateurs ayant une clé passe-partout permettant de déchiffrer les fichiers chiffrés, même lorsque la clé a été perdue.

Référence Cryptographie symétrique

Pour en savoir plus sur le mécanisme du chiffrement symétrique et ses différences avec le chiffrement asymétrique, reportez-vous à l'article suivant :

▸ http://fr.wikipedia.org/wiki/Cryptographie_symétrique

Au moment du déchiffrement, la clé FEK est exportée depuis l'en-tête du fichier, puis déchiffrée à l'aide de la clé utilisateur et sert enfin à déchiffrer le fichier.

Il est intéressant de noter que l'algorithme de chiffrement est différent en fonction de la version de Windows utilisée et de la configuration du système, puisque EFS permet d'utiliser différents algorithmes.

Tableau 6–1 Versions de Windows et algorithmes de chiffrement

Système d'exploitation	Algorithme par défaut	Autres algorithmes
Windows 2000	DESX	aucun
Windows XP	DESX	3DES
Windows XP SP1	AES	3DES, DESX
Windows Serveur 2003	AES	3DES, DESX
Windows Vista	AES	3DES, DESX
Windows Serveur 2008	AES	3DES, DESX

Dans Windows 7, la nouveauté par rapport à ses prédécesseurs est donc l'apparition des ECC (*Elliptic Curve Cryptographic*), algorithmes de toute dernière génération et considérés comme les plus sécurisés. Bien entendu, Windows 7 reste compatible avec les anciens algorithmes sauf si l'administrateur configure une stratégie de groupe (GPO, *Group Policy Object*) afin de forcer l'utilisation d'ECC.

Dès lors qu'un dossier est marqué avec un attribut de chiffrement, les fichiers et dossiers qu'il contient seront alors automatiquement chiffrés. Tant que ces fichiers sont déplacés sur des volumes NTFS, le chiffrement est conservé ; mais, s'ils sont déplacés sur un système de fichiers ne gérant pas EFS (par exemple, une partition contenant un système de fichiers FAT32), alors ils seront déchiffrés avant d'être copiés.

BitLocker

BitLocker Drive Encryption, plus simplement appelé BitLocker, est une fonctionnalité apparue avec Windows Vista, qui sert à protéger les données en chiffrant entièrement le disque dur.

Contrairement à EFS qui ne chiffre que certaines données, BitLocker chiffre non seulement les données, mais aussi les fichiers système et la totalité des informations d'un disque dur. En effet, il chiffre :

- les données utilisateurs ;
- les fichiers système (dossier Windows, etc.) ;
- le fichier de veille prolongée (copie de la mémoire lors du dernier lancement pouvant contenir des informations sensibles) ;

- le fichier d'échange (dit de swap) ;
- les fichiers temporaires (souvent source d'informations pour un attaquant).

La seconde protection se situe au niveau de l'amorçage du système dont l'intégrité est vérifiée par plusieurs mécanismes :

- À l'aide de chiffrement et de fonctions de hachage, il vérifie si les fichiers servant au démarrage n'ont pas été modifiés par un virus de secteur d'amorçage ou de kit racine.
- Il empêche le système de démarrer si les fichiers système ont été modifiés par malveillance.
- Il empêche tout accès aux données via des applications tierces ou systèmes d'exploitation alternatifs, en bloquant l'accès aux clés racines du disque dur.

EN COULISSE Le fonctionnement de BitLocker

BitLocker se base idéalement sur une puce matérielle de la carte mère nommée TPM (*Trust Plateform Module*) afin de chiffrer une clé volume FVEK (*Full Volume Encryption Key*) ayant servi à chiffrer les données. Néanmoins, ce type de puce est peu courant et nécessite également un BIOS compatible TCG 1.2, ce qui rendait BitLocker difficilement utilisable si une solution alternative n'était pas incluse au sein du système.
BitLocker propose ainsi trois protections en fonction du matériel que contient l'ordinateur :

- Protection via le TPM seulement : la puce TPM est utilisée pour chiffrer la clé et participe lors de la vérification des fichiers système.
- Protection via code PIN : au démarrage, un code PIN vous est demandé. Cette méthode requiert tout de même une puce TPM.
- Protection via une clé USB : au démarrage, BitLocker exige le branchement d'une clé USB sur laquelle est stockée une clé secrète. Sans cette clé USB, le système ne démarre pas. Il s'agit de la seule fonctionnalité disponible si votre ordinateur ne possède pas de puce TPM.

Attention, en cas de perte de la clé de chiffrement ou du mot de passe de récupération, les données sont définitivement irrécupérables.
Le processus de chiffrement est simple. Le disque est chiffré à l'aide d'une clé FVEK, qui est ensuite chiffrée à l'aide de la clé publique du volume VMK (*Volume Master Key*) qui est ensuite, lorsque c'est possible, chiffré grâce à la puce TPM.

Activer BitLocker

Les opérations de gestion de BitLocker se réalisent depuis deux endroits bien distincts du système. Son activation et la configuration de chiffrement s'effectue grâce à un module du panneau de configuration tandis que le paramétrage avancé se fait via le composant enfichable MMC de gestion des stratégies locales (GPO).

COMPRENDRE Virus de secteur d'amorçage et de kit racine

Ces virus infectent le MBR (*Master Boot Record*), élément chargé en mémoire lors du lancement du système d'exploitation.

RÉFÉRENCE Les fonctions de hachage (hash)

Pour tout savoir sur le processus des fonctions de hachage, consultez l'article suivant :

- http://fr.wikipedia.org/wiki/Fonction_de_hachage

RÉFÉRENCE Tout savoir sur les TPM

Si l'utilisation des TPM vous intéresse, n'hésitez pas à lire les documents officiels disponibles sur le portail du groupe de développement de ce mécanisme hardware :

- http://www.trustedcomputinggroup.org/

Pour lancer le panneau de contrôle de BitLocker :

1. Ouvrez le menu *Démarrer.*
2. Saisissez `BitLocker` dans la zone de saisie.
3. Cliquez sur *Chiffrement de lecteur BitLocker*.
4. L'interface de gestion de BitLocker s'affiche et liste les volumes de l'ordinateur pour lesquels il peut être activé ou désactivé.
5. Choisissez le volume de votre choix et cliquez sur le bouton *Activer BitLocker* correspondant. Un assistant d'activation s'ouvre.

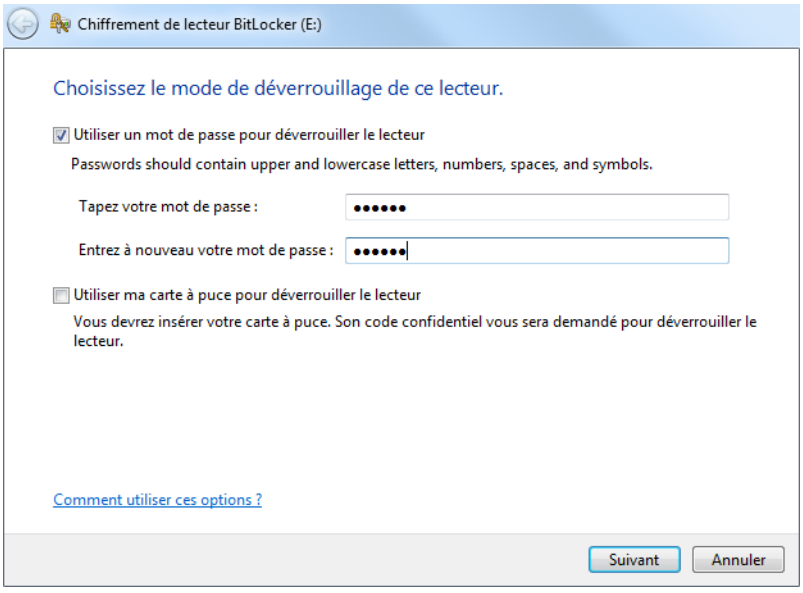


Figure 6–6
Assistant d'activation de BitLocker

ATTENTION BitLocker To Go Reader

BitLocker To Go Reader sert à déverrouiller les lecteurs chiffrés sur les systèmes Windows XP et Vista. Si les Smart Cards constituent une bonne solution de sécurité pour les lecteurs BitLocker, il est important de savoir qu'elles ne sont pas compatibles avec cette fonctionnalité. Si vous souhaitez connecter le lecteur à un autre système, optez pour la solution du mot de passe. Dernière précision, BitLocker To Go Reader requiert que le lecteur soit formaté avec le système de fichiers FAT.

6. Choisissez parmi les trois options de déverrouillage proposées celle qui correspond à vos besoins :
   - *Déverrouillage par mot de passe* : le mot de passe est demandé lors de l'accès au disque. Cela permet de partager le disque avec d'autres utilisateurs, s'ils en connaissent le mot de passe.
   - *Déverrouillage par Smart Card* : le système vous demandera d'insérer la carte à puce pour accéder au lecteur. Cette carte à puce aura préalablement été configurée à l'aide d'un certificat de sécurité.
   - *Déverrouillage automatique* : le lecteur est déchiffré au moment où vous vous connectez sous votre compte Windows.

   Cliquez ensuite sur le bouton *Suivant*.
7. Une dernière confirmation vous est alors demandée. Cliquez sur *Démarrer le chiffrement* pour activer BitLocker. Une fenêtre de progression apparaît alors. Le chiffrement peut prendre plusieurs minutes et il est très important de ne pas éteindre l'ordinateur pen-

dant l'opération. Un message vous informe lorsque le traitement est terminé. Votre lecteur s'orne alors d'une nouvelle icône dans l'interface de gestion de BitLocker, tout comme dans le poste de travail.

Figure 6–7
Affichage d'un lecteur chiffré dans l'interface de gestion BitLocker

Le chiffrement n'est pas irréversible : il peut être désactivé ou modifié à tout moment, tant que le lecteur est déverrouillé. Ainsi, à l'aide du panneau de contrôle de BitLocker, vous pouvez soit déchiffrer un lecteur en cliquant sur le bouton *Désactiver BitLocker*, soit cliquer sur le bouton *Gérer BitLocker* qui vous permet d'effectuer différentes opérations relatives au lecteur :

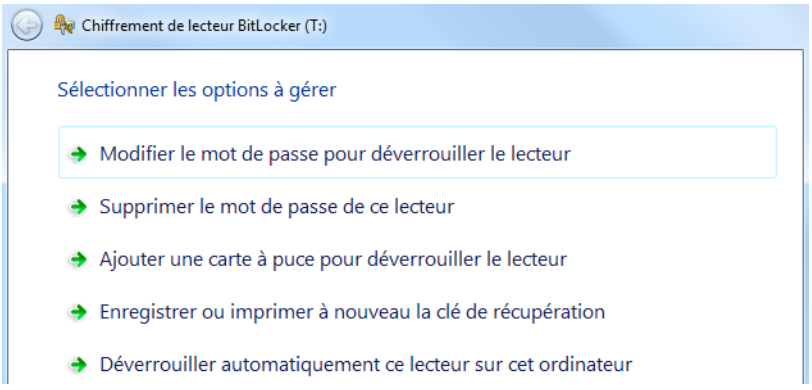


Figure 6–8
Opérations de maintenance d'un lecteur chiffré avec BitLocker

BitLocker To Go

Dans Windows 7, la protection BitLocker est étendue aux périphériques amovibles tels que les clés USB et les disques durs externes grâce à BitLocker To Go.

L'avantage est de pouvoir mettre en œuvre une *passphrase* (phrase servant de mot de passe) afin de déchiffrer les données au moment où l'on tente d'y accéder. Pas besoin de matériel spécifique (comme une puce TPM) ou de mettre à jour son BIOS, il suffit de posséder Windows 7 (version Entreprise ou Intégrale) et d'utiliser un périphérique de stockage USB. Tous vos lecteurs externes peuvent ainsi être protégés contre la récupération des données qu'ils contiennent, et ceci sans vous gêner dans leur utilisation de tous les jours.

Le chiffrement d'un périphérique de stockage externe est sensiblement identique à l'utilisation de BitLocker pour un disque dur interne :

À SAVOIR BitLocker et le déverrouillage automatique

Si vous cochez l'option *Déverrouiller automatiquement ce lecteur*, le lecteur sélectionné sera déverrouillé dès que vous vous connectez à Windows. Ce mécanisme de déverrouillage automatique requiert que le volume contenant le système soit lui aussi chiffré.

ATTENTION BitLocker To Go et les clés USB

Pour pouvoir activer BitLocker sur une clé USB, il faut que la taille de cette dernière soit au minimum de 128 Mo.

1. Ouvrez le panneau de configuration.
2. Saisissez `BitLocker` dans la zone de recherche pour ouvrir le panneau *Gérer BitLocker*.
3. Repérez votre périphérique et cliquez sur le bouton *Activer BitLocker*. Choisissez soit la sécurité par mot de passe, soit par carte à puce. Lorsque vous y êtes invité, effectuez une sauvegarde de la clé de récupération.

Lors de la première tentative d'accès au périphérique, une fenêtre vous demandant de saisir votre mot de passe (ou d'insérer votre Smart Card) s'affiche. Si le mot de passe saisi est correct, le périphérique est déverrouillé jusqu'à ce que vous quittiez votre session Windows.

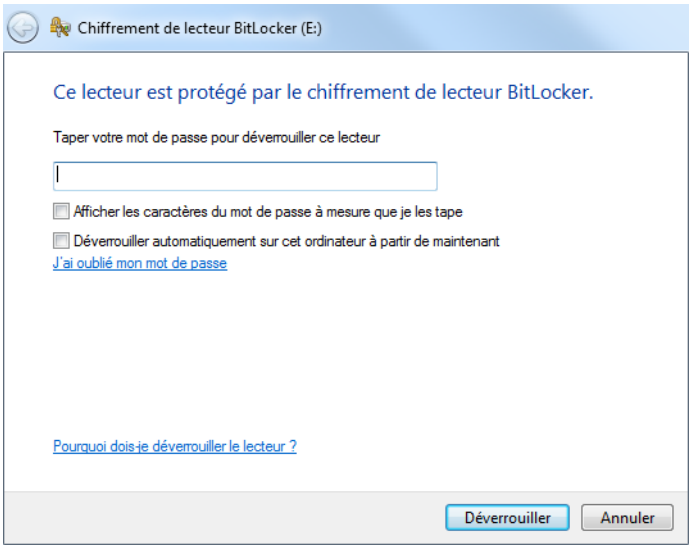


Figure 6–9
Tentative d'accès à un périphérique protégé par BitLocker

Paramétrer BitLocker

Il est possible de paramétrer finement tant le comportement de BitLocker que la façon de l'utiliser. Vous pouvez ainsi forcer, via les stratégies de groupe, tous les utilisateurs du domaine ou de l'ordinateur à chiffrer les périphériques amovibles lorsqu'ils tentent de copier des données depuis leur ordinateur vers les périphériques. Il est également possible de configurer le niveau de vérification de BitLocker lors du préchargement du système.

1. Dans le menu *Démarrer*, saisissez *gpedit.msc* dans la zone de recherche, puis appuyez sur la touche *Entrée*.
2. Dans les stratégies locales, *Configuration ordinateur*, dépliez l'arborescence pour trouver les stratégies relatives à BitLocker : *Modèles d'administration*/*Composants Windows*/*Chiffrement de lecteur BitLocker*.

Un grand nombre de stratégies locales permettent alors de paramétrer l'utilisation de BitLocker. Vous pouvez, par exemple :

- Choisir le niveau de chiffrage utilisé (AES 128 bits ou 256 bits), ainsi que la méthode de chiffrement.
- Forcer le chiffrement des lecteurs externes pour y copier des données de l'ordinateur.
- Empêcher la désactivation de BitLocker sur les lecteurs chiffrés.
- Configurer le niveau de complexité requis pour les mots de passe : caractères spéciaux, longueur minimale, etc.
- Autoriser l'activation d'un agent de récupération qui pourra accéder à tous les lecteurs sans posséder les clés de déchiffrage.
- Configurer le profil de validation du système par le TPM, c'est-à-dire paramétrer les verrous de vérification de BitLocker, allant de la vérification du secteur d'amorçage jusqu'à la vérification du constructeur de l'ordinateur.

En cas de perte de mot de passe

Lorsque le moyen de déverrouillage d'un disque chiffré avec BitLocker (mot de passe ou carte à puce) est perdu, il est impossible de récupérer les données. Il ne reste qu'un seul recours : avoir préalablement sauvegardé la clé de récupération sur un support externe. Cette clé de récupération se présente généralement sous la forme d'un simple fichier texte contenant différentes informations.

Contenu d'un fichier d'export de clé BitLocker

```
Clé de récupération du chiffrement de lecteur BitLocker.

La clé de récupération permet de récupérer les données sur un lecteur protégé par BitLocker.

Pour vérifier qu'il s'agit de la bonne clé de récupération, comparez l'identification avec ce qui est
proposé sur l'écran de récupération.

Identification de la clé de récupération : 1F17D9A1-2721-49
Identification complète de la clé de récupération : 1F17D9A1-2721-4997-9755-E921D6BCCADC

Clé de récupération BitLocker :
027940-635503-618838-501468-419529-352462-574167-245487
```

Voici comment procéder dans ce cas :

1. Lorsque vous tentez d'accéder à un disque chiffré, un assistant vous demande la saisie du mot de passe. L'assistant propose un bouton *J'ai oublié mon mot de passe*. Cliquez sur ce bouton, un moyen de récupération vous est proposé :

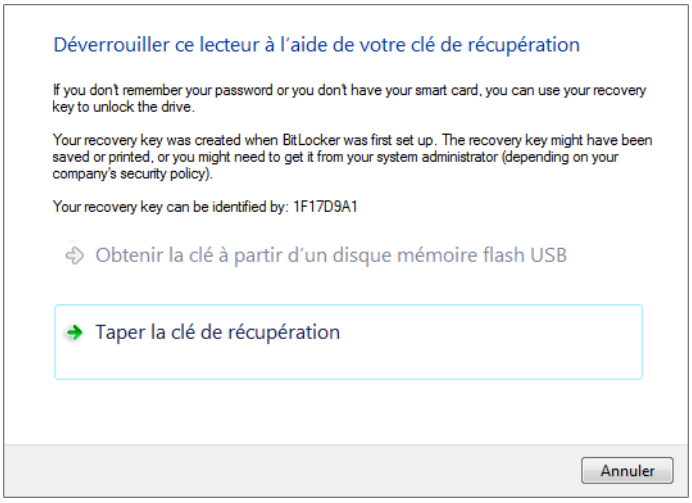


Figure 6–10
Assistant de récupération de périphérique chiffré

2 L'écran suivant vous permet, dans le cas d'une saisie manuelle de la clé, de déverrouiller le lecteur. C'est alors à vous de modifier les options du lecteur pour changer le mot de passe.

BitLocker est donc une manière simple et efficace de protéger ses données. Néanmoins, elle nécessite tout de même de prendre quelques précautions, notamment d'avoir toujours de côté des clés de récupération, sous peine de voir les données disparaître à jamais.

Personnaliser l'indexation des fichiers

L'indexation est un mécanisme transparent qui permet de référencer certains fichiers du disque dur afin d'y accéder plus rapidement en effectuant une recherche qui sera alors optimisée par l'utilisation d'un index, sorte de table des matières des fichiers du disque dur. Elle permet de retrouver non seulement des fichiers et des programmes, mais également des e-mails stockés sur votre ordinateur. Elle est avantageuse du point de vue du temps d'exécution : là où une recherche standard (non indexée) sur un répertoire contenant un très grand nombre de fichiers prend plusieurs dizaines de secondes, la recherche indexée retourne les résultats voulus en quelques secondes seulement.

Ce référencement utilise un catalogue dit d'index unique, dans lequel sont stockées les informations qui seront utilisées par le moteur de recherche du système. Pour éviter que ce catalogue ne prenne trop de place, seuls les dossiers *Utilisateurs* (`C:\Utilisateurs`) et le menu *Démarrer* (`C:\ProgramData\Microsoft\Windows\Start Menu`) sont indexés par défaut.

ALLER PLUS LOIN Guide d'utilisation expert de BitLocker

Si vous souhaitez déployer BitLocker sur un réseau local ou en entreprise, ou tout simplement étudier en profondeur les différentes manières de l'utiliser, il existe deux guides rédigés en anglais qui répondront à toutes vos interrogations. Ces guides sont accessibles à l'adresse suivante :

- http://www.microsoft.com/downloads/details.aspx?familyid=41BA0CF0-57D6-4C38-9743-B7F4DDBE25CD&displaylang=en

ou en cherchant le document nommé « Windows BitLocker Drive Encryption Design and Deployment Guides » sur le centre de téléchargement de Microsoft :

- http://www.microsoft.com/downloads/en/default.aspx

LOGICIEL Indexer Status Gadget

Brandon Paddock, l'un des membres de l'équipe de développement de Windows 7 a créé un petit gadget qui sert à contrôler l'état du service d'indexation et à surveiller le nombre d'éléments indexés par le système. Pour télécharger gratuitement ce gadget, rendez-vous à l'adresse suivante :

- http://brandontools.com/content/IndexerStatusGadget.aspx

RÉFÉRENCE
Les commandes de Windows Search

Pour une liste plus complète des commandes disponibles dans Windows Search, rendez-vous en annexe de cet ouvrage.

POUR ALLER PLUS LOIN Développement avec Windows Search

Si vous souhaitez implémenter la recherche Windows au sein de l'une de vos applications, lisez l'article technique situé à l'adresse suivante :

- http://lgmorand.developpez.com/dotnet/wds/

EN COULISSE **Fonctionnement de Windows Search**

Contrairement aux idées reçues, le service d'indexation de Windows 7 ne consomme que très peu de ressources système et s'autorégule pour ne pas dépasser 2 % des ressources processeur. Bon nombre d'utilisateurs se trompent en pensant améliorer sensiblement la réactivité de leur système en désactivant ce service. En effet, le service d'index a été optimisé pour être le plus léger possible :

- Il est exécuté en tant que service système plutôt que service utilisateur. Cela a pour conséquence de réduire la taille des index puisque les contenus/fichiers ne sont alors référencés qu'une seule fois.
- Il utilise des accès disque à faible priorité (apparus avec Windows Vista), ce qui permet de réduire leur nombre et surtout de ne pas gêner la réactivité du système.

Dans la version 4 de Windows Search (incluse dans Windows 7), différentes évolutions ont été effectuées au niveau des filtres, mais également au niveau des fonctionnalités comme le tri et les regroupements.

Par rapport à la version 3 comprise dans Windows Vista, les performances sont nettement meilleures :

- Le temps de recherche des requêtes complexes a été amélioré de 38 %.
- L'utilisation processeur a été réduite de 80 %.
- L'utilisation mémoire a été réduite de 20 %.

La recherche devient ainsi très précise, car il est possible de l'affiner par des critères (plus de 300 critères de recherche différents sont disponibles) afin de filtrer les résultats et retrouver rapidement le ou les fichiers recherchés. Ces recherches se font à l'aide d'une syntaxe AQS (*Advanced Query Syntax*) et permettent, entre autres, d'élargir le filtre de recherches aux propriétés des fichiers comme l'auteur du fichier, sa date de création ou encore sa taille.

Le format de la syntaxe est toujours composé d'une propriété séparée de sa valeur par deux points (« : »). Voici quelques exemples de recherches pratiques qu'il est possible d'effectuer :

Tableau 6–2 Exemples de syntaxe de recherche utilisant AQS

Propriété	Syntaxe	Résultat
`author : name`	`author : louis-guillaume`	Retrouve les fichiers dont l'auteur contient `louis-guillaume`.
`from name`	`from : louis-guillaume`	Retrouve les éléments comme des e-mails dont les propriétés `fromName` ou `fromAddress` contiennent `louis-guillaume`.
`has : attachment`	`devoir hs : attachment`	Retrouve les e-mails contenant le mot `devoir` et comportant une pièce jointe.
`author : name OR has : attachment`	`author : louis-guillaume OR has : attachment`	Retrouve les fichiers qui ont soit `louis-guillaume` comme auteur, soit une pièce jointe.

Il est également possible d'affiner les résultats en filtrant par date ou taille de fichier.

Tableau 6–3 Exemples de filtre de recherche

Syntaxe	Résultat
`size :>20KB`	Cherche les fichiers ayant une taille supérieure à 20 Ko.
`size :>=20KB <=70KB`	Cherche les fichiers ayant une taille comprise entre 20 Kko et 70 Ko.
`date :>2/1/09 <2/7/09`	Cherche les fichiers ayant une date située entre le 2 janvier 2009 et le 2 juillet 2009.

L'indexation des fichiers est une fonctionnalité fort utile pour l'utilisateur averti qui souhaite utiliser efficacement son système. Étant donné qu'elle ne s'applique par défaut qu'à certains dossiers et ne prend en compte qu'un certain nombre d'extensions de fichiers, il est préférable de la configurer pour qu'elle réponde aussi précisément que possible aux besoins de l'utilisateur.

ATTENTION
Indexation et répertoire Démarrer

S'il est possible de modifier les emplacements indexés, sachez qu'il est fortement déconseillé de supprimer le répertoire du menu *Démarrer* de l'indexation, cela aurait pour conséquence de ralentir l'utilisation que vous faites du menu.

Plusieurs paramétrages sont à votre disposition dans l'interface de gestion de l'indexation. Pour y accéder :

1 Lancez la commande *Panneau de configuration* dans le menu *Démarrer*.

2 Tapez le mot-clé `index` dans la zone de recherche et appuyez sur *Entrée*.

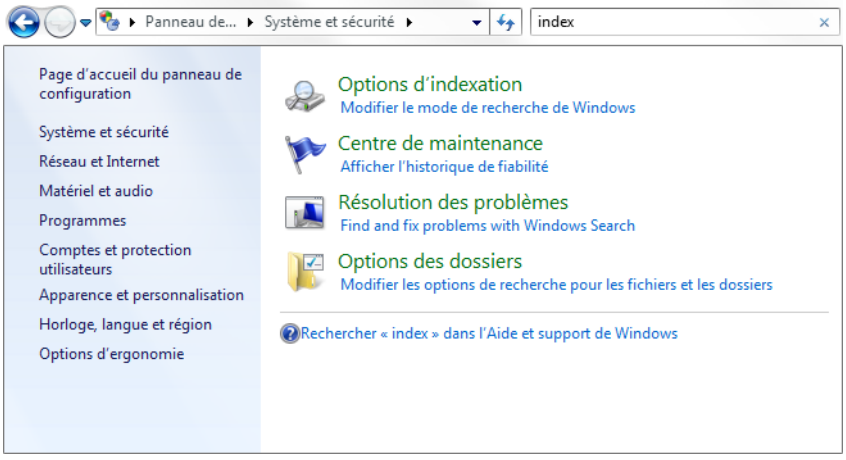


Figure 6–11
Les options d'indexation dans le panneau de configuration

3 Sélectionnez alors *Options d'indexation.*

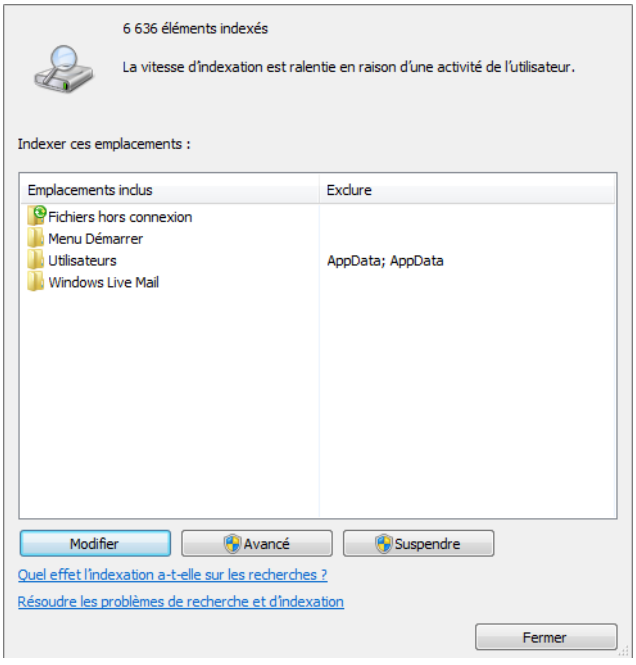


Figure 6–12
Interface des options d'indexation

À partir de cette interface, vous avez le choix entre configurer les dossiers à indexer et paramétrer la façon dont se fait l'indexation.

Définir les dossiers à indexer

Voici comment ajouter un nouveau répertoire à indexer :

1 Cliquez sur le bouton *Modifier*.

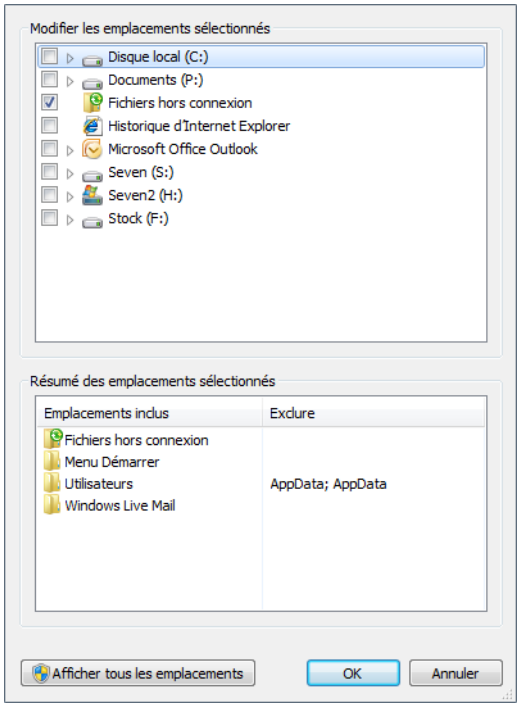


Figure 6–13
Interface de gestion des emplacements indexés

2 Cochez les répertoires dont vous souhaitez indexer le contenu.

3 Cliquez sur *OK*.

Ajouter trop de répertoires (donc indexer plus de fichiers) a pour effet de démultiplier les résultats de recherche, réduisant de fait la possibilité de retrouver rapidement un fichier précis. Préférez donc la qualité à la quantité en ne choisissant que les répertoires contenant les fichiers de travail auxquels vous accédez plus ou moins régulièrement.

Si votre arborescence de fichiers n'est pas optimisée et qu'elle contient des dossiers contenant à la fois des dossiers utiles et des dossiers remplis de fichiers inintéressants, pensez à exclure les répertoires inutiles en les décochant dans la liste des répertoires à inclure.

ASTUCE Réparer l'index

Lorsque l'index ne fonctionne pas convenablement et que la recherche ne permet pas de trouver certains fichiers, videz et reconstruisez l'index en vous rendant dans les paramètres avancés des *Options d'indexation*, puis en cliquant sur le bouton *Reconstruire* dans la rubrique *Dépannage*.

À RETENIR **Chiffrement et indexation**

S'il est possible de crypter vos données à l'aide de logiciels tiers et de chiffrements propriétaires, il est important de noter que seuls les fichiers chiffrés avec EFS peuvent être indexés.

ATTENTION **Indexation et sécurité**

Lorsque le volume (ou la partition) n'est pas chiffré entièrement et que vous indexez certains fichiers qui ont été chiffrés avec EFS, le service d'indexation référence ces fichiers en copiant une partie de leur contenu dans l'index à l'aide d'un chiffrement faible. Il est ainsi possible à un attaquant d'extraire des données depuis l'index.

ATTENTION **Signes diacritiques et langue de l'utilisateur**

Par défaut, Windows 7 utilise la langue système que l'utilisateur a choisie pour détecter les signes diacritiques. En revanche, concernant des mots venant d'une autre langue contenant des signes diacritiques particuliers (grec, espagnol, etc.), il est nécessaire d'activer la gestion des accents pour que ces caractères spéciaux soient pris en compte.

EXPERT **Filtres d'indexation personnalisés**

Pour les utilisateurs les plus avertis et/ou les administrateurs qui ont besoin d'indexer le contenu de certains fichiers particuliers comme une extension propre à l'un de leurs logiciels, il est possible d'ajouter un filtre personnalisé afin de l'associer à l'extension voulue. Sur ce sujet, lisez la documentation technique Microsoft :

- http://msdn.microsoft.com/fr-fr/library/ms692577(en-us,VS.85).aspx

Paramétrage avancé

Il est possible de configurer plus finement le service d'indexation afin d'élargir la quantité d'informations à indexer ou, au contraire, de la réduire. Trois fonctionnalités permettent de personnaliser l'indexation des données pour que les recherches soient efficaces et précises, tout en répondant parfaitement à vos attentes :

- L'indexation des fichiers cryptés : ceux-ci sont donc inclus dans les résultats de recherche.
- La gestion des accents dans les noms de fichiers : cette fonctionnalité autorise la recherche à prendre en compte les accents pour différencier les mots. Si elle semble intéressante de prime abord, elle comporte un inconvénient majeur. En effet, si vous cherchez le terme `mémo`, les fichiers contenant le mot `memo` (sans accent) n'apparaîtront pas dans les résultats.
- La sélection des extensions de fichiers et des propriétés d'extension qui seront indexés. Windows 7 permet de choisir les fichiers que vous désirez voir ressortir rapidement lors d'une recherche. Il est ainsi possible d'exclure des extensions de fichiers que vous jugez inutile d'inclure à vos recherches. Pour les fichiers que vous souhaitez inclure, il est possible de définir si l'indexation se fait uniquement sur le nom du fichier ou, de façon plus complète, sur son contenu ainsi que sur ses propriétés.

Ces trois fonctionnalités sont accessibles via l'élément *Options d'indexation* du *Panneau de Configuration* :

1. Ouvrez le *Panneau de configuration* depuis le menu *Démarrer*.
2. Saisissez le mot-clé `index` dans la zone de recherche et appuyez sur *Entrée*.
3. Sélectionnez alors l'élément *Options d'indexation*.
4. Cliquez sur le bouton *Avancé*.
5. Cochez ou décochez la case *Indexer les fichiers chiffrés*.
6. Cochez ou décochez la case *Traiter les mots avec accents et signes diacritiques en tant que mots différents*.
7. Pour la gestion des extensions, ouvrez l'onglet *Type de fichier*.
8. Décochez les extensions que vous ne souhaitez pas indexer.
9. Dans la partie inférieure de la fenêtre, ajoutez la nouvelle extension et précisez le comportement de filtrage que le service doit lui associer.

Déplacer les fichiers d'indexation

L'indexation liste dans une micro base de données les fichiers et leur emplacement. Les fichiers qui interviennent dans ce processus se trouvent par défaut dans les sous-répertoires du dossier `C:\ProgramData\Microsoft\Search\Data\Applications\Windows\Projects\SystemIndex`.

Pour des raisons d'espace disponible sur le disque système ou tout simplement pour améliorer les performances de recherche, il faut parfois déplacer ces fichiers d'indexation sur une partition d'un deuxième disque dur.

1. Ouvrez le *Panneau de configuration* depuis le menu *Démarrer*.
2. Saisissez le mot-clé `index` dans la zone de recherche et appuyer sur la touche *Entrée*.
3. Sélectionnez alors *Options d'indexation*.
4. Cliquez sur le bouton *Avancé*.
5. Dans l'onglet *Paramètres d'indexation*, choisissez *Indexer l'emplacement*. Cliquez ensuite sur le bouton *Nouveau*.
6. Choisissez alors le répertoire qui contiendra les fichiers d'index. Les modifications seront prises en compte au prochain démarrage du service à la prochaine ouverture de session.

ATTENTION Performances et disques durs physiques

On parle ici de deux disques durs physiques différents. Utiliser deux partitions différentes du même disque n'apporterait aucune amélioration de performance sachant qu'une seule tête de lecture est capable de lire les données du disque dur.

Compresser les fichiers

Autre avantage d'utiliser un système de fichiers NFTS, la compression native des fichiers permet de compresser et de décompresser à la volée les fichiers d'un dossier ou d'une partition, afin de gagner de l'espace disque.

La compression NTFS apporte un gain de place compris entre 20 et 40 % en fonction du type de fichier compressé. Contrairement à d'autres mécanismes de compression (ZIP, RAR, tarball, Gzip, 7z, etc.), une fois l'option de compression activée, plus aucune manipulation n'est requise : tout se fait de manière parfaitement transparente et avec une infime perte de performance.

La compression peut avoir lieu soit sur un volume disque entier, soit sur des dossiers particuliers. Pour compresser une partition entière, il suffit d'ouvrir les propriétés de cette dernière, puis de cocher la case *Compresser ce lecteur pour augmenter l'espace disque*.

Au contraire, pour ne compresser que certains dossiers – par exemple, ces fichiers que vous utilisez peu et qui occupent une quantité d'espace disque importante –, il est nécessaire d'effectuer les opérations suivantes :

1. Cliquez droit sur le dossier ou le fichier de votre choix pour accéder à ses propriétés.

ATTENTION Compression d'une partition

Évitez cette manipulation sur les partitions système car le système ne cessera de compresser/décompresser des fichiers auquel il essaie constamment d'accéder .

ATTENTION Compression et chiffrement

Pour des raisons de sécurité et de performance, il est impossible d'utiliser à la fois le chiffrement (EFS) et la compression sur un même fichier. Le système vous empêche d'activer la compression s'il détecte un fichier chiffré. Si vous avez réellement besoin de mettre en œuvre ces deux méthodes simultanément, créez une archive ZIP protégée par un mot de passe. La compression est certes moindre et son niveau de sécurité moins efficace, mais reste tout à fait valable.

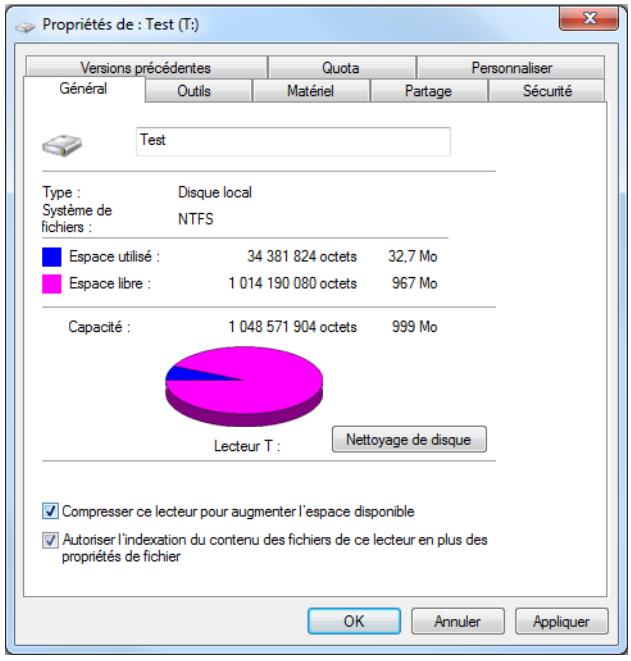


Figure 6–14
Options de compression de volume disque

2 Dans la fenêtre qui s'ouvre, cliquez sur le bouton *Avancé* situé dans l'onglet *Général*.

3 Cochez la case *Compresser le contenu* pour libérer de l'espace disque.

4 Cliquez sur *OK*, et de nouveau sur *OK*.

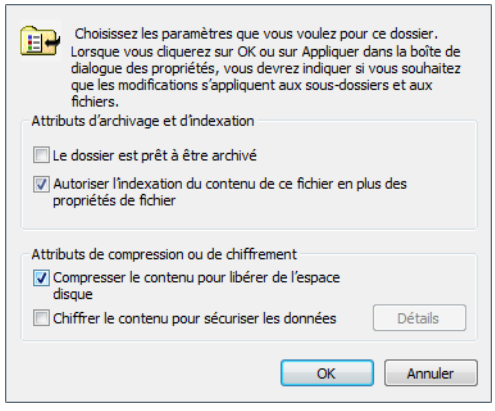


Figure 6–15
Options de compression avancées

Sur XP, Vista et Windows 7, il est facile d'identifier les fichiers et dossiers qui sont compressés, car leur nom apparaît en bleu.

Astuce Compression et couleur de fichier

Il est possible de désactiver cet affichage en couleur ou de changer la couleur par celle de votre choix. Pour désactiver l'ajout de couleur sur les fichiers compressés :

1. Ouvrez l'explorateur Windows.
2. Appuyez sur la touche *Alt* pour faire apparaître les menus.
3. Cliquez sur le menu *Outils>Options des dossiers*.
4. Ouvrez l'onglet *Affichage*.
5. Décochez la case *Afficher les dossiers et les fichiers NFTS chiffrés ou compressés en couleur*.
6. Cliquez sur *OK*. La modification est appliquée immédiatement.

Si vous souhaitez remplacer la couleur des fichiers par celle de votre choix :

1. Via le menu *Démarrer*, saisissez `regedit` pour ouvrir l'éditeur de registre.
2. Ouvrez la clé `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer`.
3. Ajoutez une nouvelle valeur binaire : cliquez avec le bouton droit, puis sélectionnez *Nouveau>Valeur binaire*. Donnez-lui le nom `AltColor`.
4. Modifiez la valeur par la valeur hexadécimale de la couleur. Par exemple `FF 00 00 00` pour le rouge. La modification ne sera effective qu'au prochain démarrage.

Plusieurs points importants sont à prendre en compte lorsque vous compressez des données :

- La compression peut prendre plusieurs heures selon la quantité de données à traiter, mais elle ne vous empêche pas de continuer à utiliser le système normalement pendant ce temps.
- Si vous créez ou copiez un fichier dans un dossier compressé, il le sera lui aussi.
- Si vous déplacez un fichier compressé dans un dossier non compressé d'une même partition, il reste compressé. Si vous le déplacez dans un dossier décompressé d'une autre partition, il perd alors son attribut de compression.

Virtualiser les fichiers avec le virtual store

Comme Windows Vista, Windows 7 est équipé d'un mécanisme destiné à améliorer la sécurité et la stabilité du système, il s'agit de la virtualisation des fichiers.

L'une des sources d'instabilité d'un système provenait du fait que certains logiciels mal conçus écrivaient un peu partout sur le disque et dans le registre. Pour pallier ces désagréments, Microsoft a défini un ensemble d'emplacements protégés sur le disque dur. Aucun utilisateur (qu'il s'agisse d'un utilisateur standard au compte limité ou d'un administrateur) ne peut écrire dans les dossiers protégés sans élévation de pri-

vilèges. Ces dossiers, comme `Windows`, `Programmes` (ou `Program Files`) sont donc protégés et les logiciels n'y accèdent pas en écriture.

Afin d'éviter les bogues lorsque un logiciel mal conçu tente d'écrire dans l'un de ces emplacements, Windows 7 intègre le mécanisme de virtualisation des fichiers. Ainsi, si le logiciel essaie, par exemple, de créer un fichier dans `\Program Files\Le logiciel\`, Windows ne provoquera pas d'erreur et simulera l'écriture dans ce dossier. En réalité, comme il est interdit d'y écrire réellement, le système stocke le fichier dans un emplacement appelé situé dans *`virtual store`* `C:\Users\{nom_utilisateur}\AppData\Local\VirtualStore\`.

Grâce à ce mécanisme, le logiciel continue de fonctionner sans erreur critique. Cependant, le virtual store étant stocké dans le profil utilisateur, il sera donc différent pour chaque utilisateur. Cela entraînera alors probablement des comportement étranges lorsqu'un logiciel est partagé par plusieurs utilisateurs.

Vous pouvez observer ce mécanisme dans l'explorateur Windows en allant dans le dossier correspondant dans `Program Files`. Si des fichiers ont été stockés dans le virtual store, un bouton *Fichiers de compatibilité* apparaît et renvoie vers le dossier correspondant dans le virtual store. Si un logiciel effectue ses sauvegardes dans un emplacement protégé du système, vous saurez maintenant où chercher l'emplacement réel des fichiers...

En résumé

Le stockage de fichiers ne se limite pas à déposer les données sur un disque en attendant de les utiliser un jour. Le choix de la méthode de stockage influe sur la future utilisation des fichiers.

La sécurité étant une question incontournable, le meilleur moyen de vous prémunir contre le vol de données est de les chiffrer.


7
TM

chapitre 7

Les comptes utilisateur

Un grand nombre de personnes pensent, à tort, qu'il suffit d'un seul compte utilisateur pour utiliser un ordinateur. Cependant, posséder plusieurs comptes permet de définir des droits et des autorisations propres à chaque utilisateur et donc de contrôler leurs actions tout en protégeant au mieux le système d'éventuels comportements inadaptés ou risqués.

SOMMAIRE

- Créer des comptes utilisateur
- Administrer les groupes
- Contrôle parental
- Contrôle utilisateur

MOTS-CLÉS

- UAC
- Contrôle
- Privilège
- Utilisateur
- Profil
- Groupe
- Moindre privilège
- Contrôle parental
- Création, modification, suppression
- Mot de passe
- Ouverture de session
- Élévation de privilège
- Sécurité

Ce chapitre insiste sur l'intérêt de la gestion des utilisateurs et explique la mise en place de stratégies pour contrôler finement l'accès à l'ordinateur ou à certaines ressources en fonction des personnes connectées au système.

Créer et gérer les comptes utilisateur

Un système d'exploitation ne montre pleinement l'étendue de ses fonctionnalités qu'en présence de plusieurs comptes utilisateur. En effet, en définissant différents profils, vous améliorez la fiabilité du système en mettant en place des quotas d'espace disque ou encore en contrôlant l'installation de logiciels susceptibles de se révéler néfastes pour la stabilité, tout en accroissant la sécurité.

La console d'administration des comptes

La gestion des utilisateurs se réalise via le panneau de configuration. Vous pouvez soit recourir à l'assistant, soit utiliser la console d'administration si vous désirez des paramétrages fins. Pour lancer la console d'administration :

1. Ouvrez le menu *Démarrer*.
2. Cliquez à l'aide du bouton droit sur le lien *Ordinateur*, puis choisissez le menu *Gérer*.
3. Dépliez l'arborescence pour sélectionner le menu *Utilisateurs et groupes locaux*.

La partie centrale charge alors le composant MMC (*Microsoft Management Console*) enfichable de gestion des utilisateurs. Comme le panneau de configuration de gestion des utilisateurs, ce composant d'administration se contente de lister les utilisateurs de l'ordinateur. Néanmoins, il affiche également les comptes désactivés, reconnaissables à leur icône présentant une flèche vers le bas. Il est intéressant de désactiver un compte lorsque vous voulez empêcher l'utilisation d'un profil pendant une période donnée, sans supprimer le compte et les données qui lui sont liées.

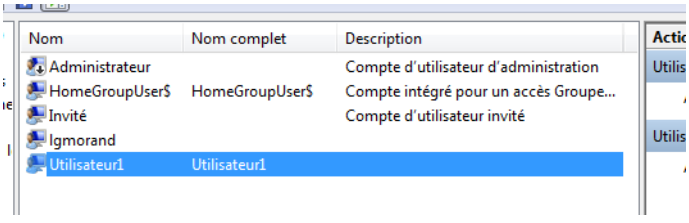


Figure 7–1
Interface de la console MMC de gestion des utilisateurs et des groupes locaux

Créer et modifier les profils

Plusieurs autres fonctionnalités sont disponibles au sein de cette interface. Les plus importantes sont la création d'un profil utilisateur et la modification de ses propriétés.

Voici comment créer un nouveau profil :

1. Cliquez sur le menu *Action*.
2. Cliquez sur *Nouvel utilisateur*.
3. Renseignez les propriétés principales, dont le nom du compte.

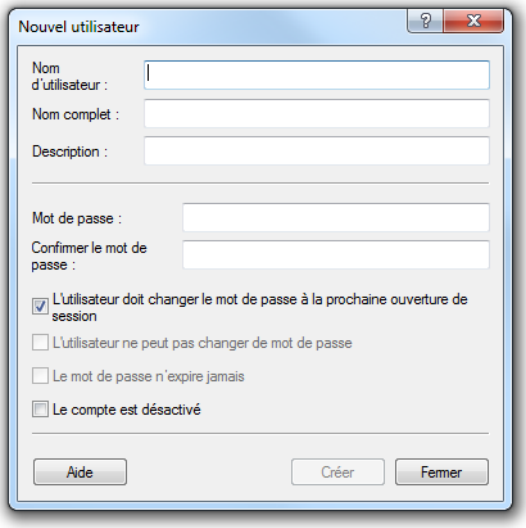


Figure 7–2
Fenêtre de création de profil utilisateur

Lorsque vous créez un compte administrateur avec le panneau de configuration, n'oubliez pas de l'ajouter au groupe administrateur dans la gestion des groupes.

Pour modifier un profil existant, double-cliquez sur le nom d'un utilisateur pour accéder à sa fenêtre de propriétés.

L'onglet *Général* de cette fenêtre permet de définir le nom du compte, une description (qui ne sera affichée que dans cette interface d'administration) et de configurer les groupes auxquels l'utilisateur appartient. La fenêtre propose également cinq options, décrites dans le tableau 7-1.

POUR ALLER PLUS LOIN Stratégie de groupe locale et profil utilisateur

Plusieurs stratégies locales permettent de configurer finement l'utilisation de comptes utilisateur, de la complexité du mot de passe à sa péremption, en passant par les stratégies de verrouillage. Tout ceci se configure via la console de stratégie locale. Pour la lancer :

1. Ouvrez le menu *Démarrer*.
2. Tapez `secpol.msc` dans la zone de saisie.
3. Appuyez sur *Entrée*.

Pour plus de détails sur l'utilisation des stratégies, reportez-vous au chapitre 9.

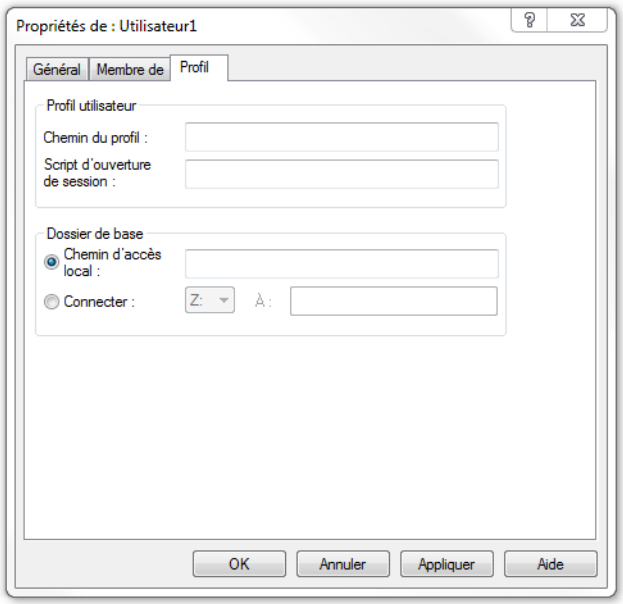


Figure 7–3
Propriétés d'un compte utilisateur

Tableau 7–1 Options disponibles depuis l'onglet Général

Libellé	Détail
L'utilisateur doit changer le mot de passe à la prochaine ouverture de session	Cette option est utile lorsque l'administrateur vient de redéfinir le mot de passe de l'utilisateur en question et souhaite ne pas connaître le nouveau.
L'utilisateur ne peut pas changer le mot de passe	Cette option est utilisée pour les comptes partagés dont vous ne souhaitez pas qu'on modifie les mots de passe d'accès.
Le mot de passe n'expire pas	Cette option est liée à la stratégie locale qui, par défaut, force l'utilisateur à changer son mot de passe tous les 42 jours.
Le compte est désactivé	Bloque un compte et empêche son utilisation sans pour autant le supprimer.
Le compte est verrouillé	Certaines stratégies locales verrouillent un compte lorsque plusieurs tentatives de connexion ont échouées (mauvais mot de passe). Cette sécurité évite la technique dite de la force brute (*brute force* dans la langue de Shakespeare), qui consiste à essayer des centaines de mots de passe jusqu'à trouver le bon.

Définir les répertoires utilisateur

Certaines propriétés comme le répertoire qui contiendra le profil utilisateur ou encore le chemin d'un script d'ouverture de session se définissent via l'onglet *Profil*. Rappelons que les scripts d'ouverture permettent, par exemple, à l'utilisateur de se connecter automatiquement aux lecteurs réseau, de mettre à jour le système d'exploitation, de connecter une imprimante, etc. Ils ont l'avantage d'éviter à l'utilisateur d'effectuer certaines tâches redondantes à chaque ouverture de session, et de lui donner directement accès à un système pleinement exploitable.

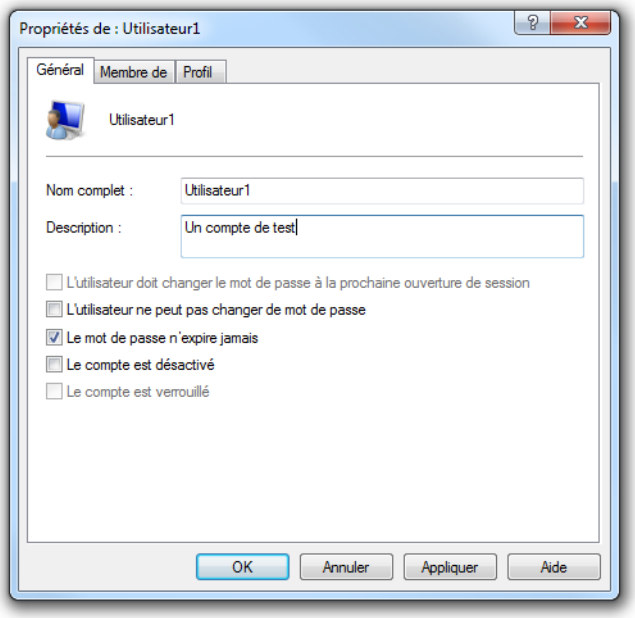


Figure 7–4
Paramétrage du profil d'un utilisateur

Dans la seconde partie de la fenêtre, définissez l'emplacement du répertoire *Home* de l'utilisateur. Ce répertoire contient les dossiers *Mes Documents*, *Mes Images*, *Ma Musique* ainsi que tous les autres répertoires propres à l'utilisateur que l'on retrouve dans toutes les versions de Windows depuis XP. L'option *Connecter* permet de placer le répertoire *Home* sur un lecteur réseau.

Changer le mot de passe utilisateur

Accessible uniquement par les administrateurs, cette console permet également de redéfinir le mot de passe d'un utilisateur, dans le cas où celui-ci l'aurait perdu. Pour cela :

1. Cliquez avec le bouton droit sur le nom de l'utilisateur.
2. Dans le menu contextuel, sélectionnez *Toutes les tâches*, puis *Définir le mot de passe*.
3. Une fenêtre d'avertissement vous rappelle que modifier le mot de passe utilisateur peut entraîner la perte de données.
4. La console qui s'ouvre alors vous permet de gérer l'ensemble des utilisateurs, et les groupes rattachés, d'un seul coup selon la technique du *batch processing* ou traitement par lots.

POUR ALLER PLUS LOIN
Clé de déchiffrement des données

Comme nous le verrons au chapitre 14 dans la section consacrée à EFS, la clé de déchiffrement des données est liée à un compte et principalement au mot de passe utilisateur. Le changer rend le déchiffrage impossible.

BONNE PRATIQUE
Compte administrateur et sécurité

Une bonne pratique consiste à posséder un unique compte administrateur pour les tâches dites administratives (gestion des utilisateurs, etc.). Le propriétaire de l'ordinateur doit autant que possible utiliser un compte limité pour les tâches quotidiennes. Ainsi, en cas de corruption du compte utilisateur (virus, piratage informatique), celui-ci n'aura pas de droits suffisants pour endommager gravement le système.

Les groupes utilisateur

Réunissant plusieurs comptes utilisateur sous le même label, les groupes utilisateur servent à définir des habilitations à un ensemble de personnes rapidement. Si elle paraît triviale, cette fonctionnalité fait gagner un temps considérable dans l'administration de très grands parcs informatiques.

Créer un groupe

Par défaut, un certain nombre de groupes sont présents. Bien entendu, il est tout à fait possible, et même recommandé, de créer des groupes supplémentaires adaptés à vos besoins.

1. Dans la console de gestion de l'ordinateur, cliquez sur l'élément *Outils système*.
2. Sélectionnez ensuite *Utilisateurs et groupes locaux*, puis *Groupes*.
3. La partie centrale de la console affiche alors tous les groupes locaux de l'ordinateur.

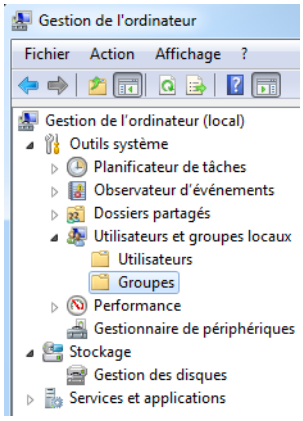


Figure 7–5
Console de gestion des groupes

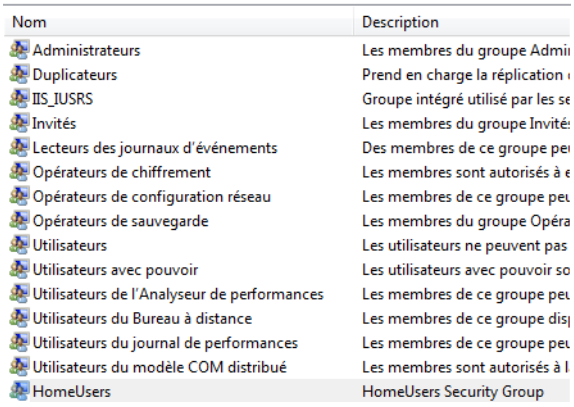


Figure 7–6
Liste des groupes locaux

4. Cliquez sur le menu *Action>Nouveau Groupe*.
5. Saisissez un nom, une description et cliquez sur le bouton *OK*. Vous pourrez par la suite ajouter les utilisateurs de votre choix au groupe.

En procédant ainsi, l'ajout de nouveaux groupes n'endommage pas le système en éditant potentiellement de façon incorrecte les groupes par défaut.

Modifier les propriétés d'un groupe

Pour configurer les utilisateurs appartenant à un groupe, il suffit de double-cliquer sur son nom.

EXEMPLE

Lorsque nous aborderons au chapitre 11 les droits d'accès aux ressources, nous apprécierons de pouvoir donner accès à un répertoire à plusieurs personnes d'un seul coup.

ATTENTION

Suppression de groupe utilisateur

Tous les groupes présents par défaut sont utilisés par telle ou telle fonctionnalité du système, comme IIS, le logiciel de serveur web de la plate-forme NT, ou pour des services de maintenance. Leur suppression entraînerait leur défaillance. Créer un nouveau groupe possédant le même nom ne suffirait pas à résoudre les troubles ainsi provoqués, car les droits sont basés sur des identifiants uniques, différents du nom de chaque groupe. Évitez donc de supprimer des groupes, même inutilisés.

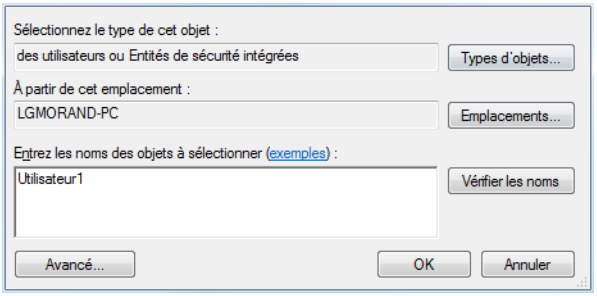


Figure 7–7
Propriétés d'un groupe local

Pour ajouter un utilisateur, cliquez sur le bouton *Ajouter* :

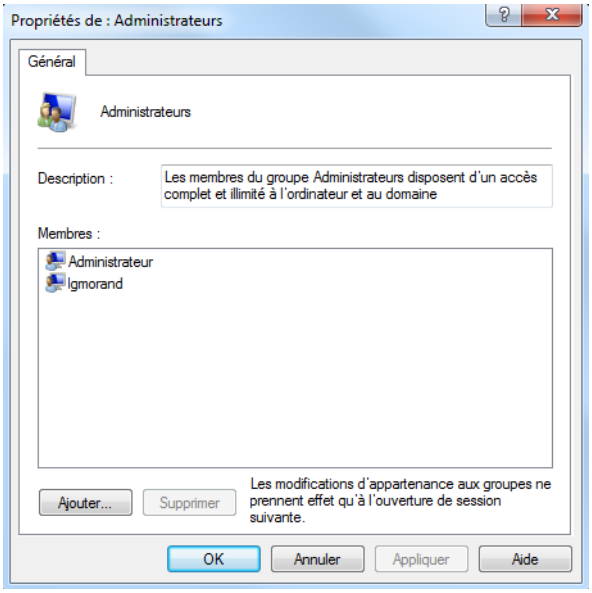


Figure 7–8
Ajout d'un utilisateur à un groupe local

L'assistant vous permet alors d'ajouter un utilisateur ou un groupe. Les modifications sont immédiates et ainsi les autorisations d'accès qui étaient propres à ce groupe sont disponibles pour le ou les utilisateurs qui ont été ajoutés.

BONNE PRATIQUE Création de groupe vs autorisations spécifiques

Nous verrons dans le chapitre consacré au partage des ressources qu'il est bien souvent plus intéressant de passer par la création d'un groupe que par la mise en place d'autorisations spécifiques pour chaque utilisateur concerné.

Le contrôle parental

Cette fonctionnalité permet à un administrateur de contrôler les autres comptes de son ordinateur. Comme son nom l'indique, elle peut servir à un parent pour contrôler les actions de ses enfants sur le système. Par contrôle, nous sous-entendons deux choses :

- Limiter les actions utilisateur (jeux, horaires d'utilisation, applications autorisées).
- Surveiller les actions des utilisateurs (journal d'événements).

Configurer le contrôle parental

Contrairement à ce que l'on pourrait croire, le contrôle parental s'applique tout à fait aux comptes d'utilisateurs adultes : une fois activé, il propose quelques fonctionnalités qui vous permettront de mieux maîtriser les actions des différents utilisateurs de votre système.

Activer le contrôle parental

Voici la procédure à suivre pour mettre en place un contrôle parental :

1. Ouvrez le menu *Démarrer* et saisissez `parental` dans la zone de recherche.
2. Cliquez sur l'élément *Contrôle parental*.
3. La fenêtre d'administration liste alors tous les comptes actifs du système.

EN PRATIQUE Compte administrateur et contrôle parental

Un message d'alerte s'affiche lorsque le compte administrateur n'est pas protégé par un mot de passe. En effet, il est inutile de configurer un contrôle parental si n'importe quel utilisateur peut se connecter sous le compte administrateur et désactiver les limitations mises en place.

Figure 7–9
Fenêtre principale du contrôle parental

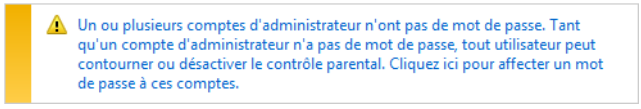


Figure 7–10
Message d'avertissement en cas de mauvaise configuration du compte administrateur

4 Le contrôle parental ne se configure qu'au cas par cas. Il vous faut donc, pour chaque utilisateur, définir les restrictions que vous souhaitez mettre en place. Cliquez sur l'utilisateur de votre choix afin d'ouvrir sa fiche de contrôle. Le contrôle parental intégré à Windows permet trois contrôles :
   – *Limites horaires* : définissez les horaires d'ouverture de session. Impossible de se connecter en dehors de ces horaires et en cas de dépassement, le compte est déconnecté.
   – *Jeux* : cette option sert à contrôler les jeux autorisés pour l'utilisateur en fonction de leur catégorisation (violence, -12 ans, etc.).
   – *Autoriser et bloquer des programmes spécifiques* : définissez les applications que l'utilisateur a le droit d'exécuter.

Voyons en détail comment mettre en place chacun de ces types de contrôles.

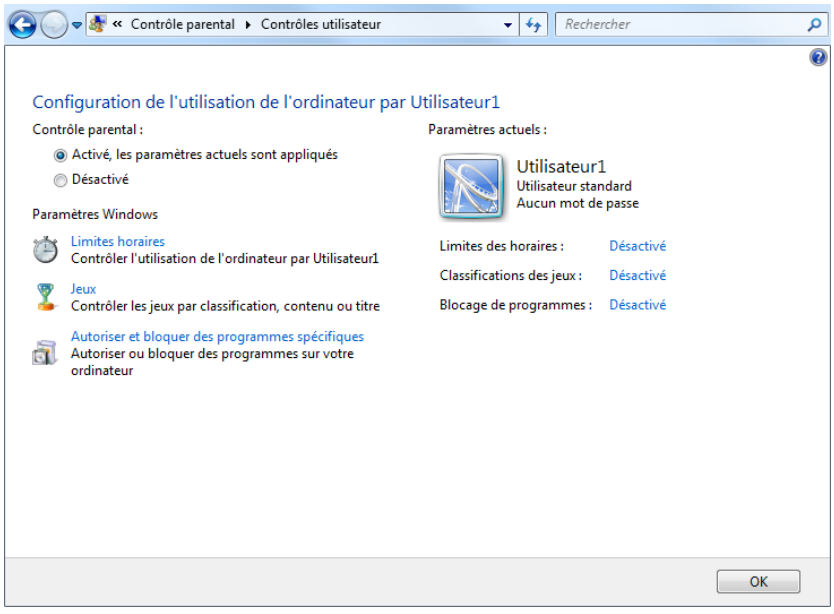


Figure 7–11
Fiche de contrôle parental d'un utilisateur

Définir des horaires de connexion

La mise en place d'horaires de connexion pour les utilisateurs d'un ordinateur répond à différents besoins : limiter l'utilisation de l'ordinateur pour un enfant, empêcher l'utilisation de l'ordinateur en dehors des horaires de présence de l'administrateur ou assurer que l'ordinateur n'est pas utilisé lorsque l'administrateur en a besoin à son retour à la maison.

L'interface de gestion des horaires de connexion est intuitive. Il suffit d'activer les cases, correspondant aux heures, qui définissent l'emploi du temps d'utili-

sation autorisée du système. Dès lors qu'un horaire est sélectionné, le contrôle des horaires est alors considéré comme actif pour l'utilisateur.

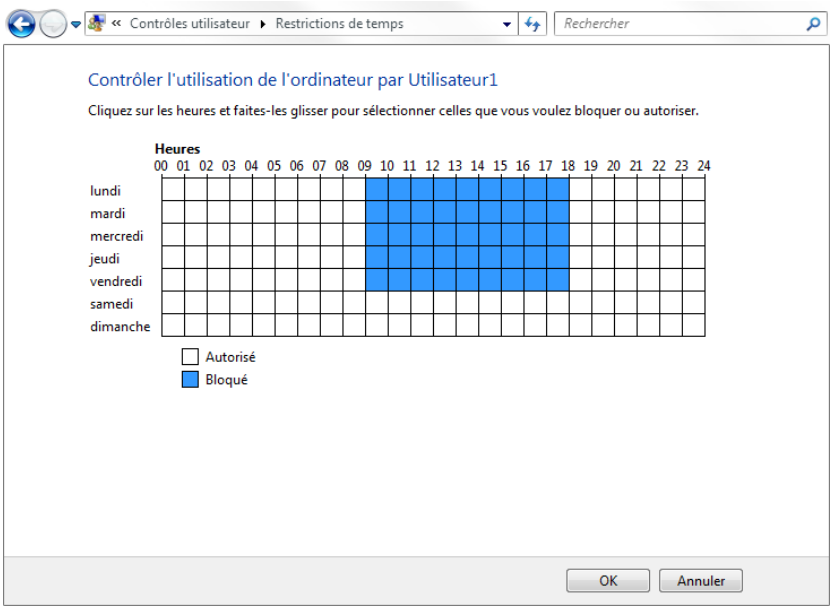


Figure 7–12
Interface de gestion des horaires du contrôle parental

Définir les jeux autorisés

Comme son nom l'indique, grâce à cette interface, vous autorisez ou non l'utilisation des jeux sur l'ordinateur. Ceci concerne aussi bien les jeux installés par l'utilisateur que les jeux système comme le Démineur, Jeux de cartes, etc. Cette fonctionnalité est donc fort utile pour limiter l'utilisation oisive de l'ordinateur.

Pour des profils utilisés par des enfants, il est possible de configurer le niveau des jeux autorisés. Ce niveau se base sur le sujet (violence, sexe, drogue) ou sur la classification PEGI (*Pan European Game Informations*) du jeu (interdit aux moins de 12 ans, 16 ans, etc.).

Bloquer ou autoriser certaines applications

En règle générale, les applications installées sont disponibles pour tout utilisateur du système. Si la configuration du logiciel est propre à chaque utilisateur car stockée dans le répertoire personnel du profil (`USERDATA`), l'utilisation même du logiciel est par défaut autorisée pour tous.

Ce fonctionnement s'avère parfois gênant si vous souhaitez, par exemple, qu'un profil utilisateur ne puisse lancer que certains logiciels bien définis et bloquer tous les autres (messagerie instantanée, peer-to-peer, etc.). C'est là un des avantages du contrôle parental, qui ne s'appliquera pas exclusivement à un contexte familial, mais, pourquoi pas, à une entreprise.

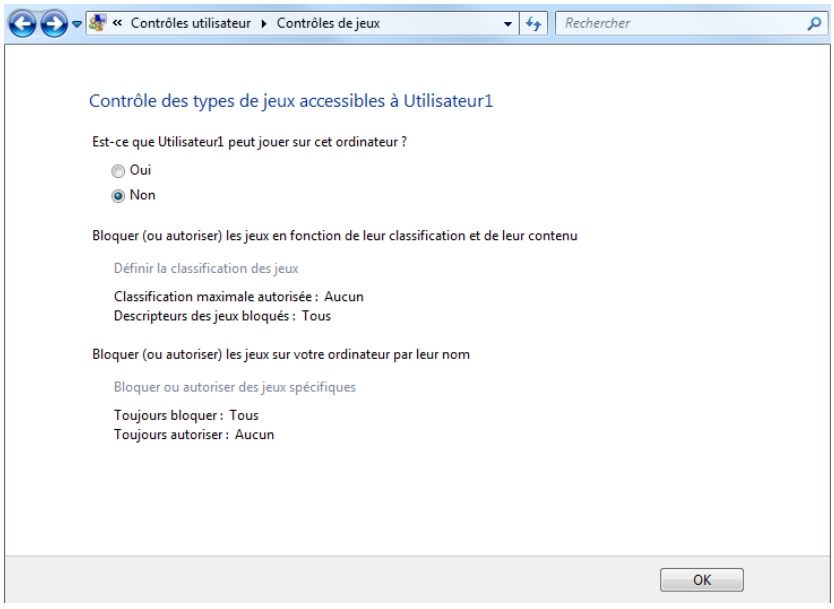


Figure 7–13
Interface de gestion
du contrôle parental des jeux

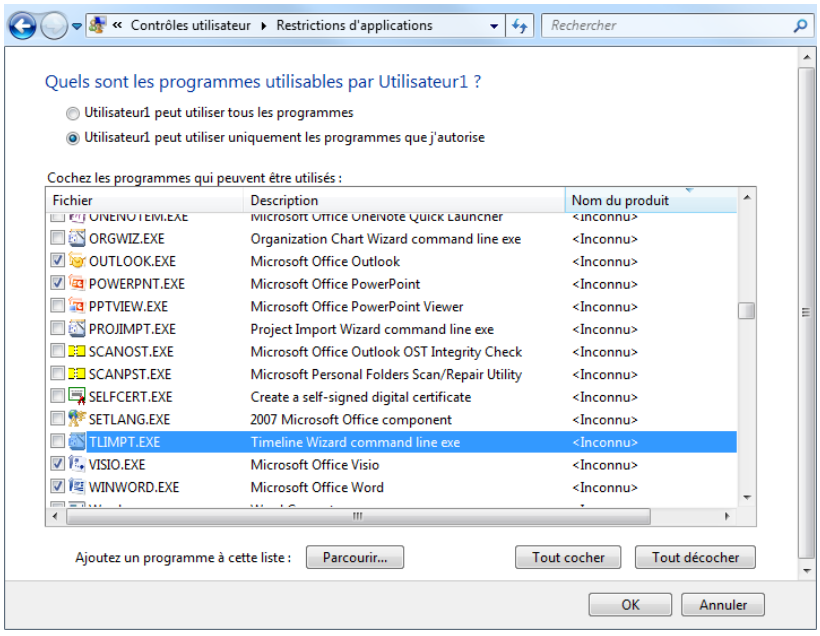


Figure 7–14
Interface de configuration
des applications autorisées et bloquées

Le contrôle des applications se fait via une simple liste d'applications bloquées ou autorisées. La liste des applications se met à jour à chaque lancement en parcourant le disque dur pour y trouver tous les fichiers exécutables. Si vous souhaitez contrôler une application qui ne s'y trouve pas, ajoutez l'application manuellement en utilisant le bouton *Parcourir* et en allant chercher son exécutable.

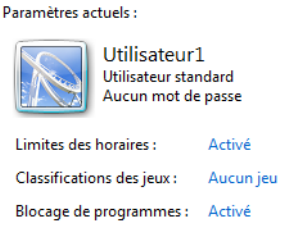


Figure 7–15
Résumé des limitations actives

EN DÉTAIL Le contrôle parental et bien plus encore

L'exécutable que vous venez de télécharger permet d'installer, tous les modules de la suite Windows Live. Vous y trouverez notamment :

- la barre d'outils Windows Live (traduction, recherche, etc.) ;
- Messenger (messagerie instantanée) ;
- Mail (client de messagerie électronique) ;
- Galerie de photos (outils permettant de trier et partager ses photos) ;
- Writer (outil de bureautique pour écrire sur les blogs) ;
- le contrôle parental ;
- Microsoft Office Live Add-in (module permettant d'ouvrir en local des documents Office Live).

Il vous reste alors à choisir les applications que l'utilisateur ne pourra pas utiliser, en choisissant l'option *L'utilisateur peut utiliser uniquement les programmes que j'autorise* et en cochant les applications concernées.

Une fois vos paramètres configurés, un résumé des limitations activées apparaît dans la partie droite de la fiche utilisateur.

Ajouter le filtrage web

Contrairement à Vista qui contient par défaut tous les contrôles disponibles, Windows 7 s'est vu amputé de deux contrôles majeurs, à savoir le filtrage web et les rapports d'activité. Ces fonctionnalités sont toujours disponibles gratuitement, mais en tant que modules Windows Live, téléchargeables depuis Internet.

Le module de contrôle parental avancé est un applicatif s'exécutant au démarrage du système et nécessitant l'utilisation d'un compte Live ID. Voici comment télécharger le module de contrôle parental avancé complet :

1. Rendez-vous à l'adresse http://fss.live.com .
2. Saisissez les identifiants de votre compte Live.
3. Téléchargez l'exécutable d'installation.

L'administration du contrôle parental se fait non pas sur le système, mais via une interface web à laquelle seuls les comptes habilités pourront se connecter. Toute personne non connectée verra sa navigation web bloquée.

Figure 7–16
Navigation web bloquée par le contrôle parental

Via cette interface d'administration, vous définissez les pages que chaque utilisateur a le droit de visiter, mais également les contacts de messagerie instantanée (*Windows Live Messenger*) que le profil peut avoir et avec lesquels il peut communiquer.

Cet outil de contrôle permet non seulement de garantir, autant que possible, la sécurité des enfants sur Internet, mais aussi de configurer à distance l'ordinateur grâce à l'interface en ligne.

Le contrôle utilisateur

La dernière pierre angulaire de la sécurité utilisateur est le contrôle de l'utilisateur par l'utilisateur lui-même. En effet, de par les droits qui lui sont attribués, les dégâts possibles sur le système et provoqués par un utilisateur peuvent être considérables.

Pendant de très nombreuses années, un utilisateur ne pouvait avoir que l'un des trois rôles suivant : utilisateur, utilisateur avec pouvoir ou administrateur. Pour se faciliter la vie, la majorité des personnes s'attribuaient automatiquement les droits administrateur. Si l'on ajoute à cela que le point faible d'un ordinateur se situe entre le clavier et la chaise (comme le dit l'adage informatique), on comprend aisément l'importance de limiter les actions de l'utilisateur. En effet, il arrive encore trop souvent qu'un utilisateur effectue sans le faire exprès une action système qui aura des conséquences fâcheuses (suppression d'un fichier système vital, etc.).

De leur côté, les virus deviennent des programmes de plus en plus complexes. Ils parviennent même à simuler la présence d'un utilisateur et sont capables d'effectuer des actions d'administration complexes.

Il était donc grand temps de trouver une parade tant pour les virus, que pour les mauvaises habitudes utilisateur ! Microsoft a alors proposé UAC (*User Account Control*) au sein de Vista et a implémenté le principe dit de moindre privilège. Ce principe consiste à toujours donner à l'utilisateur, qu'il soit administrateur ou non, le moins de droits possible, et à les compléter uniquement lorsqu'il en a besoin.

Le principe de moindre privilège

Avec le mécanisme du moindre privilège, un utilisateur doit logiquement, lors de sa connexion au système, recevoir des jetons (ou badges, en anglais *tokens*) définissant les rôles qu'il possède. Avec le mécanisme du moindre privilège, il reçoit uniquement les jetons qui correspondent à des rôles ne comportant que peu de risques pour le système (incapables de modifier le registre ou les fichiers système, par exemple).

Ainsi, lorsque l'utilisateur tente d'accéder à une console d'administration système telle que la console de stratégies locales, le système vérifie ses jetons. Comme l'utilisateur ne porte avec lui qu'une partie de ses jetons d'accès, s'il ne possède pas les jetons nécessaires à l'exécution d'une tâche ou d'un programme, le système vérifie dans la liste complète des jetons de l'utilisateur s'il possède celui qui permet d'utiliser la console. Dans le cas où l'utilisateur possède un jeton directement valide, le système lui demande juste de valider s'il souhaite réellement accéder à cette console.

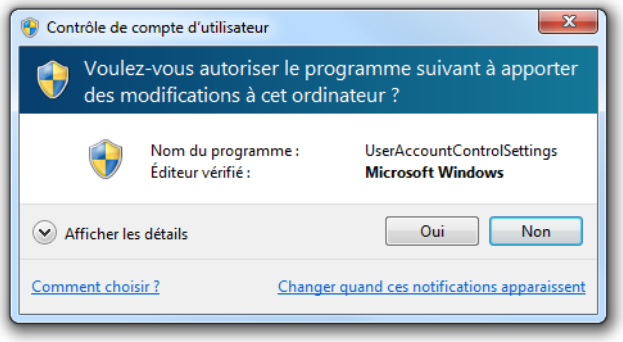


Figure 7–17
Boîte de dialogue de confirmation UAC

Si l'utilisateur ne possède pas le jeton nécessaire, une boîte de dialogue lui demande de saisir les identifiants de connexion administrateur.

Configurer le contrôle utilisateur

Ajouté dans Windows Vista pour parer aux mauvaises habitudes utilisateur, UAC a donc été présenté comme *la* solution pour la sécurité de l'utilisateur contre lui-même. Malheureusement, ses fenêtres de confirmation intempestives gênaient les utilisateurs qui ont pris pour habitude de désactiver complètement cette fonctionnalité. Elle perdait ainsi tout son intérêt.

EN COULISSE Le fonctionnement du contrôle utilisateur

Le contrôle utilisateur fonctionne comme une surcouche système. Il est suffisamment séparé du système pour qu'aucun programme ou virus ne puisse y accéder et seuls les messages envoyés légitimement depuis la souris ou le clavier sont autorisés à lui parvenir, afin de bloquer les virus simulant l'appui sur les touches.
Le mécanisme du contrôle utilisateur pour les applications est simple mais efficace. Pour chaque application, une méthode de détection heuristique (algorithme permettant de rapidement trouver une solution) est utilisée pour détecter si :

- L'application est bloquée par une stratégie de sécurité ou si son éditeur est bloqué.
- L'éditeur est le système lui-même.
- L'éditeur est un éditeur vérifié.
- L'éditeur n'est pas connu.

Pour chacune de ces vérifications, une fenêtre d'alerte s'affiche, demandant à l'utilisateur de valider.

Afin de persister dans cette solution, Windows 7 propose un compromis en proposant à l'utilisateur de définir le niveau d'alerte qu'il souhaite recevoir, sans pour autant avoir à désactiver cette sécurité complémentaire. Si les fenêtres de confirmation vous gênent et que vous êtes sûr de vos actions, vous pouvez ainsi réduire le nombre des confirmations nécessaires. La procédure à suivre est la suivante :

1. Ouvrez le *Panneau de Configuration* et cliquez sur *Comptes et protection utilisateur*.
2. Cliquez sur *Comptes utilisateur*, puis sur *Modifier les paramètres de contrôle de compte utilisateur*.
3. Une interface très simple vous permet alors de définir l'un des quatre niveaux disponibles, allant d'une sécurité maximale avec confirmation à chaque opération système jusqu'à la désactivation complète des alertes (ce qui, bien entendu, n'est pas recommandé).

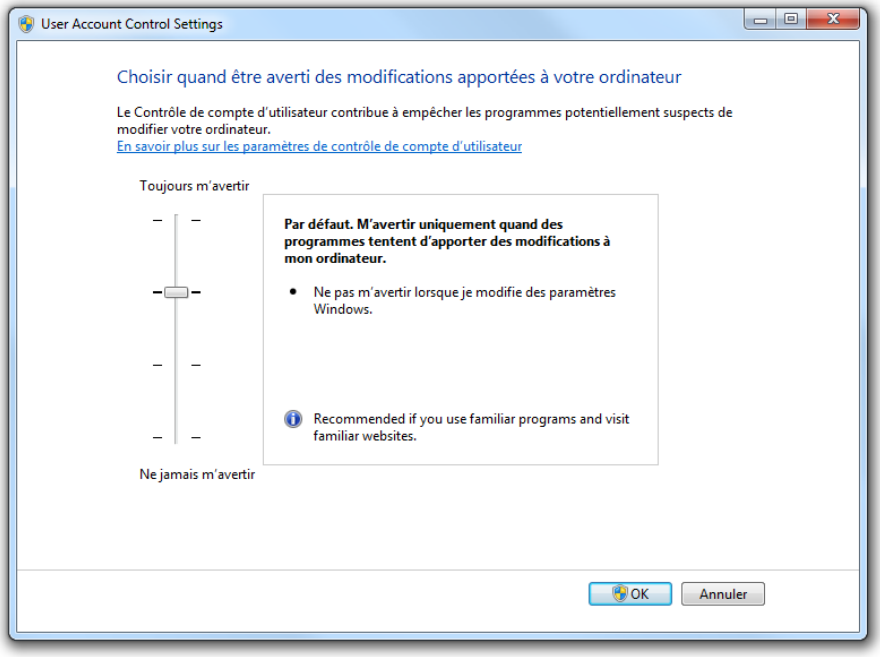


Figure 7–18
Interface de configuration du contrôle utilisateur

Configuration avancée

Malgré cet assistant, si vous souhaitez configurer finement le contrôle utilisateur, il vous faut passer par les stratégies de sécurité locales.

1. Ouvrez la console de gestion des stratégies de sécurité : lancez le menu *Démarrer*, puis saisissez `gpedit.msc`.
2. Dépliez l'arbre latéral en choisissant *Stratégie Ordinateur local>Configuration ordinateur>Paramètres Windows>Paramètres de sécurité*.
3. Cliquez ensuite sur *Stratégies locales>Options de sécurité*.
4. Neuf stratégies sont alors à votre disposition afin de répondre à des cas d'utilisation bien particuliers du contrôle utilisateur.

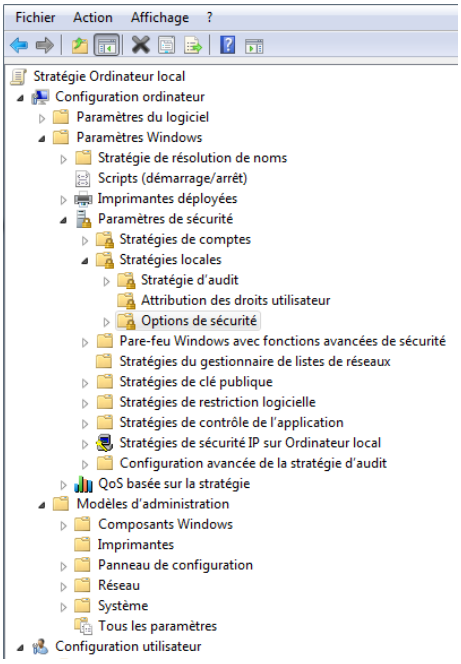


Figure 7–19
Console de gestion des stratégies de groupe locales.

Pour comprendre ces stratégies, il faut savoir que les droits utilisateur sont stockés dans un jeton, mais que vous démarrez toujours une session avec les droits minimaux, y compris si vous êtes administrateur de la machine. Les droits complémentaires ne vous sont octroyés qu'à la demande.

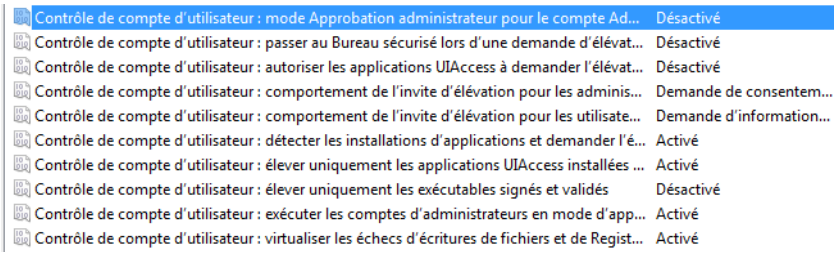


Figure 7–20
Stratégies de sécurité locales du contrôle utilisateur

Tableau 7–2 Liste des stratégies locales du contrôle utilisateur

Stratégie	Description
Mode Approbation administrateur pour le compte Administrateur intégré	Si cette stratégie est désactivée, l'administrateur utilise toujours un jeton complet ne nécessitant jamais d'élévation de droits.
Passer au Bureau sécurisé lors d'une demande d'élévation	Lorsque cette stratégie est activée, un rideau noir semi-transparent s'affiche au moment de la demande d'élévation de privilèges pour montrer de façon explicite qu'aucune opération n'est possible tant que la fenêtre d'élévation est ouverte.
Autoriser les applications UIAccess à demander l'élévation sans utiliser le bureau sécurisé	Le Bureau sécurisé est l'écran noir s'affichant au moment de la demande d'élévation. Cette stratégie permet, lorsqu'elle est activée, de ne pas bloquer le fonctionnement des applications ayant besoin d'accéder à des composants de l'interface.

Tableau 7–2 Liste des stratégies locales du contrôle utilisateur (suite)

Stratégie	Description
Comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	Cette stratégie concerne l'élévation de privilèges pour un utilisateur qui est déjà administrateur. Trois options sont disponibles : • *Aucune invitation* : l'élévation se fait en mode silencieux et sans demande particulière. • *Demande de consentement* : l'administrateur doit confirmer l'élévation de privilèges. • *Demande d'informations d'identification* : le mode le plus sécurisé, qui demande, à chaque action sensible, l'identifiant et le mot de passe administrateur.
Comportement de l'invite d'élévation pour les utilisateurs standards	Lorsque le paramètre de cette stratégie est positionné sur *Demande d'informations d'authentification*, une fenêtre d'authentification (identifiant/mot de passe) s'affiche. Si le paramètre *Aucune invite* est activé, l'utilisateur doit choisir à chaque exécution l'option *Exécuter en tant qu'administrateur*.
Détecter les installations d'applications et demander l'élévation	Lorsque cette stratégie est activée, le système tente de détecter soit par le nom de l'exécutable, soit par son manifeste, si ce dernier requiert une élévation de droits. Dans le cas où cela est nécessaire pour le bon fonctionnement de l'application, une demande d'élévation est alors proposée à l'utilisateur.
Élever uniquement les applications UIAccess installées à des emplacements sécurisés	Cette stratégie limite l'accord de droits UIAccess (accès aux interfaces) aux applications installées dans le répertoire `Programmes` (`%ProgramFiles%`) et `Windows` (`%Windir%`). Dans le cas où un applicatif UIAccess est démarré depuis un autre emplacement, il obtiendra les droits de la personne qui l'exécute (niveau asInvoker).
Élever uniquement les exécutables signés et validés	Lorsque cette stratégie est activée, seuls les fichiers exécutables signés peuvent s'exécuter. Elle se base sur une vérification de signature utilisant une PKI (*Public Key Infrastructure*) pour chaque exécutable nécessitant une élévation de privilèges. L'administrateur peut définir la liste des applications autorisées via le *magasin d'éditeurs approuvés* des ordinateurs locaux.
Exécuter les comptes administrateur en mode d'approbation d'administrateur	Lorsque cette stratégie est désactivée, le contrôle utilisateur est quasiment éteint. Les comptes ayant des droits administrateur ne reçoivent plus de demandes d'élévation de privilèges. Le centre de sécurité indique d'ailleurs que le système est potentiellement faillible si jamais une application malintentionnée est exécutée sous la session du compte administrateur. Celle-ci pourra alors agir à sa guise sans qu'aucun contrôle ne soit disponible.

Certaines de ces stratégies nécessitent un redémarrage complet du système pour s'appliquer. Quoi qu'il en soit, elles vous permettent de définir très précisément le niveau de notifications que vous souhaitez recevoir sans désactiver complètement le contrôle utilisateur.

En résumé

Dans ce chapitre, nous nous sommes intéressés aux rouages de l'administration des profils et groupes utilisateur, qu'il s'agisse de les contrôler par leurs propriétés, par les droits attribués ou encore en utilisant le contrôle parental. Nous nous sommes également penchés sur le paramétrage avancé du contrôle utilisateur (UAC) qui contrôle l'élévation de privilèges lors d'opérations sensibles sur le système.

chapitre 8

Gérer les fichiers : sauvegardes, quotas et mode hors connexion

Qu'il s'agisse de données personnelles ou publiques, que ce soit en local ou via le réseau, l'accès aux fichiers doit être à la fois contrôlé mais surtout garanti à tout instant.

SOMMAIRE

- Mécanisme de sauvegarde des données
- Mise en place de quotas disque
- Versions de fichiers
- Fichiers hors connexion

MOTS-CLÉS

- Sauvegarde
- Quota
- Fichier hors connexion
- Image disque
- Limite de quota
- Restauration
- Récupération

Ce chapitre aborde les différentes fonctionnalités inhérentes au contrôle des données, c'est-à-dire la sauvegarde ou la restauration, mais également des plus avancées telles que la gestion des quotas disque ou l'accès aux fichiers lorsque l'ordinateur n'est pas connecté au réseau. L'ensemble de ces fonctionnalités ayant pour but de vous permettre d'utiliser l'espace disque intelligemment afin de garantir un accès aux données en tout temps.

Sauvegarde de fichiers

Personne n'est à l'abri d'une panne matérielle ou d'une suppression, accidentelle ou volontaire, d'un ou de plusieurs fichiers. Dans les deux cas, les données sont perdues et deux solutions s'offrent alors à l'utilisateur qui souhaiterait les récupérer :

- L'utilisation d'un outil de récupération de données. À l'exception de Recuva, ce genre d'outil est bien souvent payant, mais la fiabilité et les résultats ne sont pas toujours au rendez-vous et dépendent de beaucoup de critères. Par exemple, un fichier ne sera pas récupérable si une application quelconque écrit sur un secteur du disque dur sur lequel se trouvait un fichier à récupérer. De fait, ces outils ne sont pas des plus fiables et restent à utiliser uniquement en dernier recours.
- La mise en place de sauvegardes automatiques.

La seconde solution est de loin la plus pertinente et doit être mise en place dès l'installation du système. Un mécanisme de sauvegarde automatique permet à l'utilisateur de disposer d'une copie de sûreté de l'ensemble de ses données. Dans l'idéal, ces données devraient être conservées physiquement dans un endroit éloigné de l'ordinateur, ainsi en cas d'intempéries tels qu'un incendie ou une inondation, les données ne seront pas touchées. Bien entendu, si vous n'avez pas le choix, une sauvegarde sur un périphérique externe devrait suffire (une sauvegarde, même proche, vaut toujours mieux que pas de sauvegarde du tout). Enfin, l'avantage des sauvegardes automatiques est qu'elles n'ont pas à être déclenchées par l'utilisateur. De cette manière, vous ne vous retrouverez pas avec des données obsolètes parce que vous n'aurez pas pris le temps de les sauvegarder.

UTILITAIRE

Recuva et récupération de données

Recuva est un outil entièrement gratuit qui scanne les clusters du disque dur afin de tenter de récupérer des fichiers qui auraient été supprimés et qui ne seraient plus accessibles par le système d'exploitation. Il récupère également les fichiers sur les cartes mémoire des appareils photo et sur les lecteurs MP3.

▸ http://www.recuva.com/

Les différentes solutions de sauvegarde

Windows 7 propose quatre fonctionnalités de sauvegarde :

- La première consiste en l'utilisation de points de restauration. Il s'agit de clichés instantanés du disque, effectués régulièrement (lors de procédures importantes telles que la mise à jour du système, par

exemple), permettant de restaurer les fichiers système du disque en cas de problème.

- La deuxième consiste à versionner les fichiers, c'est-à-dire sauvegarder régulièrement les modifications apportées à un fichier. De cette manière, il est possible de remonter dans le temps et de revenir à une version précise d'un fichier. Cette fonctionnalité va de pair avec la suivante.
- La sauvegarde de fichiers est le troisième outil à votre disposition. Il met en place des tâches automatisées qui copieront certaines données sur un autre périphérique.
- La dernière solution disponibles dans Windows 7 est la sauvegarde du disque sous forme d'image, dont la taille sera légèrement inférieure à la celle du système sauvegardé. Elle permet de restaurer l'ensemble du système d'un seul bloc, aussi aucun cas par cas n'est permis.

Configurer des sauvegardes automatiques

Pour mettre en place une sauvegarde automatique, il est nécessaire de passer par le panneau de configuration dédié accessible via le menu *Démarrer*.

1 Une fois le panneau de configuration ouvert, tapez `sauvegarder` dans la zone de saisie et cliquez sur *Sauvegarder l'ordinateur*.

Figure 8–1
Le panneau Sauvegarder ou restaurer des fichiers est divisé en deux parties. La partie supérieure est dédiée à la sauvegarde et la partie inférieure est consacrée aux options de restauration.

2 Cliquez sur le lien *Modifier les paramètres*. Le premier écran sert à définir l'emplacement dans lequel seront effectuées toutes les futures sauvegardes.

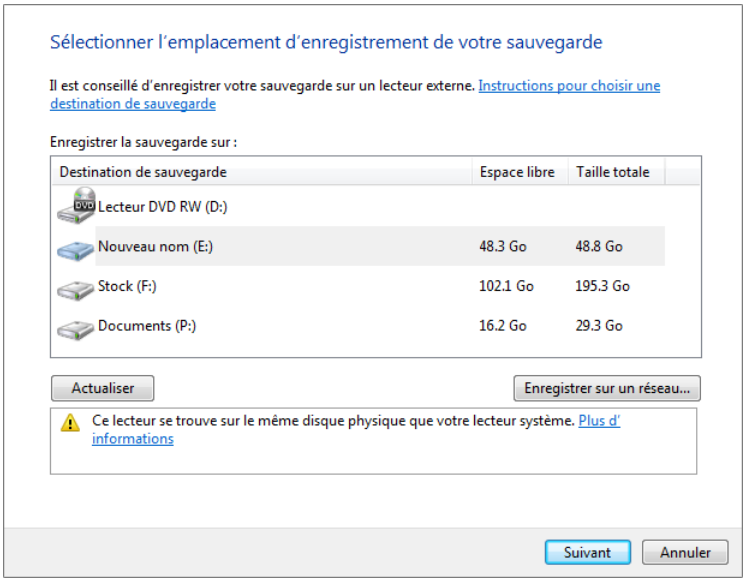


Figure 8–2
Sélection de l'emplacement de sauvegarde

3 À l'étape suivante, vous pouvez soit laisser Windows définir lui-même les données à sauvegarder, soit préciser ce qui mérite d'être sauvegardé. Une sauvegarde personnalisée vous assure de conserver vos données sensibles en cas de défaillance matérielle. Elle accélère également les différents processus de sauvegarde et diminue l'espace disque qu'elle occupe, en choisissant moins de fichiers que Windows ne l'aurait fait.

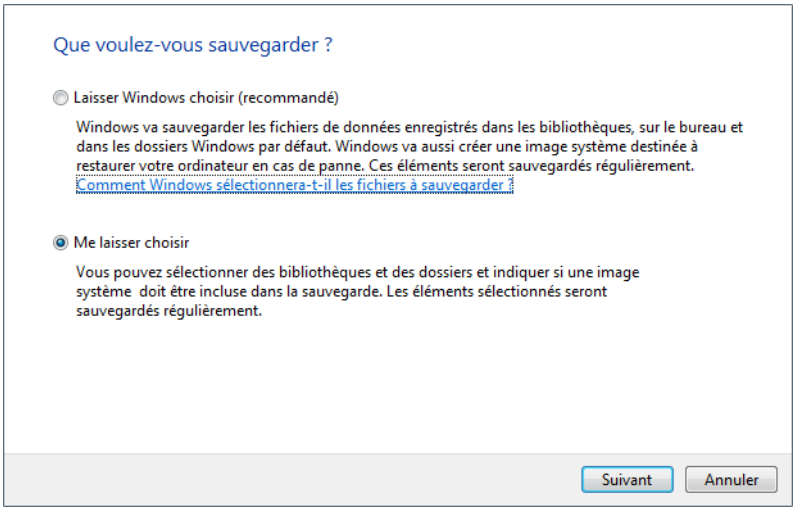


Figure 8–3
Choix du type de sauvegarde

Cochez alors les partitions ou les dossiers que vous voulez sauvegarder. Bien entendu, il est possible de cocher toutes les cases, mais assurez-vous de disposer de suffisamment d'espace disque. Les sauvegardes ne s'écra-

sent pas les unes les autres, aussi sauvegarder un dossier de 1 Go finira par représenter plusieurs gigaoctets sur votre disque dur.

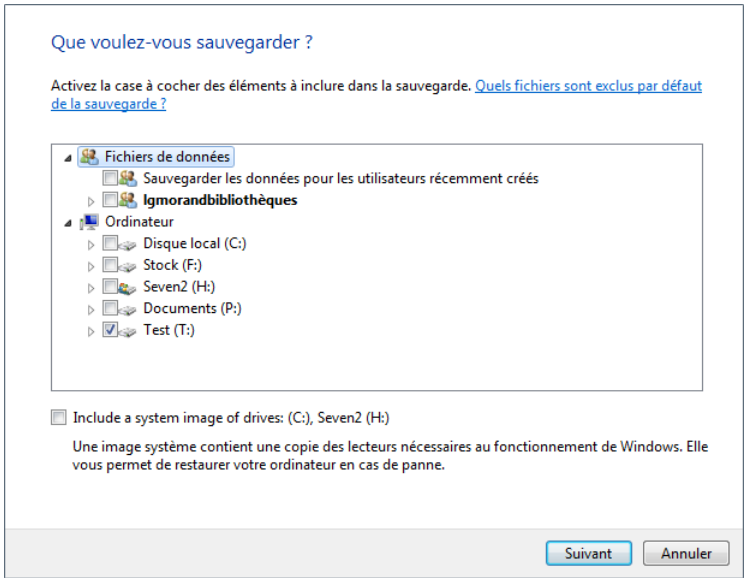


Figure 8–4
Choix des données à sauvegarder

Il est possible de déclencher la création d'une image disque des partitions système au moment de la sauvegarde. Sachant que ces deux procédés ne visent pas les mêmes fichiers, cette solution est très pertinente et vous permettra de restaurer d'autant plus facilement un système fonctionnel en cas de défaillance.

4 Pour finir, l'écran de résumé affiche les détails de la sauvegarde qui vient d'être configurée. Il ne reste qu'à configurer la planification éventuelle de la sauvegarde en cliquant sur le lien *Modifier la planification*.

Selon les paramètres que vous choisissez, la sauvegarde s'exécute entre une et trente fois par mois. La durée entre chaque sauvegarde dépend de plusieurs critères :

- Plus les données sont critiques, plus les sauvegardes doivent être fréquentes.
- Plus l'espace disponible pour le fichier de sauvegarde est limité, plus les sauvegardes doivent être espacées.
- La durée entre deux sauvegardes doit correspondre à l'utilisation qui est faite de la partition. Il ne sert à rien d'effectuer une sauvegarde quotidienne d'un disque sur lequel les données sont peu modifiées.

5 Pour finir, cliquez sur *Enregistrer les paramètres et quitter*. Une fois sur l'écran principal du panneau *Sauvegarder ou restaurer des fichiers*, cliquez sur *Sauvegarder maintenant*, afin d'effectuer une première sauvegarde si vous le souhaitez.

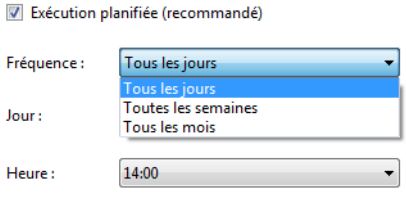


Figure 8–5
Planification de la sauvegarde

Vos données sont à présent sécurisées et vous ne serez plus démuni en cas de défaillance matérielle. Voyons maintenant comment protéger le système grâce aux images disque.

Exploiter les images disque

Les images disque sont des copies parfaites d'une partition : tout ce qui est présent sur la partition est copiée au bit près. Ceci permet de restaurer entièrement un disque et de le rétablir à un état antérieur estimé comme sain. En général, on génère des images disque à partir des disques système. Ainsi, en cas de crash de la machine, on pourra restaurer le système à l'identique. Voyons comment gérer les images disque.

1. Ouvrez le panneau *Sauvegarder ou restaurer des fichiers* du *Panneau de configuration*.
2. Dans la partie gauche, cliquez sur *Créer une image système* pour lancer l'assistant de création. La première étape consiste à définir l'emplacement de destination. Si vous en avez la possibilité, choisissez le partage réseau. Bien que plus lente, il s'agît de la meilleure solution. Les DVD sont plus coûteux, mais ont l'avantage d'être facilement transportables pour être mis en lieu sûr. Enfin, la sauvegarde sur disque reste la solution de dernier recours.

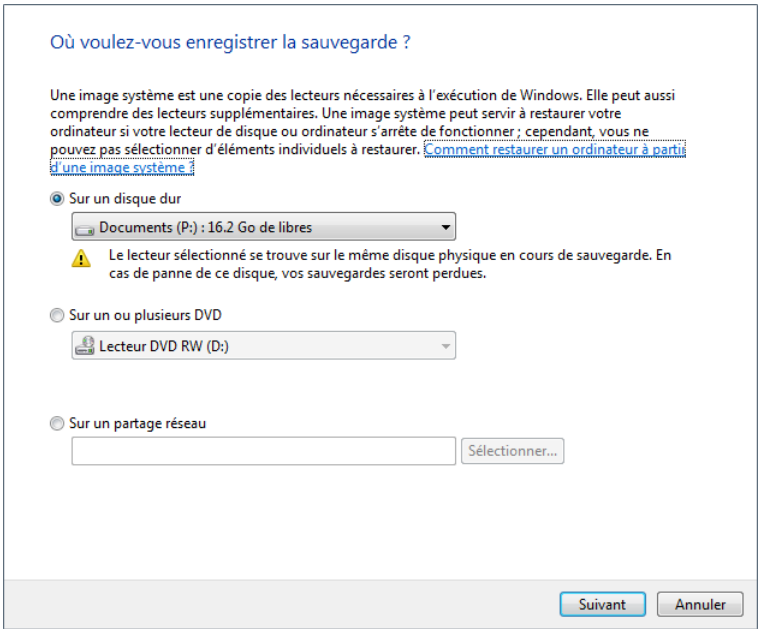


Figure 8–6
Sélection du périphérique de sauvegarde

3. Spécifiez ensuite les disques pour lesquels une image système doit être créée. Par défaut, tous les disques contenant un système d'exploitation Windows (y compris XP ou Vista) sont automatiquement

cochés. Cochez *Plus de disques* si vos données sensibles sont réparties sur différents disques. Gardez cependant à l'esprit que plus de disques seront sauvegardés, plus la création de l'image système sera longue et plus l'image ainsi créée prendra de place.

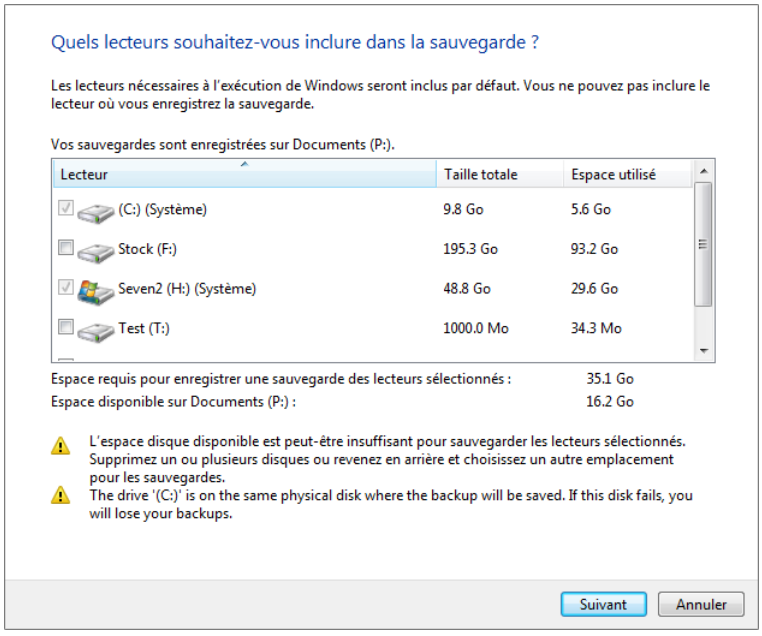


Figure 8–7
Sélection des disques à sauvegarder

4 Le dernier écran récapitule les partitions sauvegardées ainsi que l'espace estimé de l'image disque. Dans notre cas, on observe que faire une image disque d'un Windows XP et d'un Windows 7 pèse déjà 36 Go. C'est pour cette raison qu'il est intéressant de déplacer les données utilisateur en dehors des disques système, afin de diminuer la taille des images générées.

Fichiers hors connexion

Professionnels ou domestiques, les réseaux sont de plus en plus complexes et il n'est pas rare de voir les données réparties au sein de plusieurs périphériques réseau. Malheureusement, cette répartition a pour inconvénient de ne pas être en mesure de fournir un accès continu aux ressources. Que ce soit parce que le réseau est inconsistant (problème matériel, bande passante surchargée, etc.) ou parce que le périphérique distant passe en mode hors ligne (déconnecté du réseau), les ressources deviennent tout bonnement inaccessibles.

C'est ici qu'entrent en jeu les fichiers hors connexion. Ils permettent d'accéder aux fichiers contenus dans un dossier réseau même si le dossier

EN PRATIQUE Comment restaurer une image disque si le système ne démarre plus ?

Ce problème arrive plus souvent que l'on ne le croit ! En effet, s'il est extrêmement facile d'utiliser l'assistant de restauration pour revenir à un état précédent, encore faut-il pouvoir accéder à cet assistant... ce qui n'est pas forcément le cas lorsque le système est défaillant. Pour cela, il est nécessaire de créer un disque de réparation système. Ce disque, qui peut être utilisé sur plusieurs ordinateurs, est un disque sur lequel l'ordinateur pourra démarrer et surtout, qui contient tous les outils nécessaires, soit pour réparer le système lorsque c'est possible, soit pour restaurer une image disque qui aurait été réalisée préalablement. Voici comment le créer :

1. Ouvrez *Sauvegarder ou restaurer des fichiers* dans le *Panneau de configuration*.
2. Dans la partie latérale, cliquez sur *Créer un disque de réparation système*. Le graveur de CD-Rom que vous utilisez doit être sélectionné dans l'assistant.
3. Cliquez sur *Créer un disque*.

Nous vous conseillons de le conserver précieusement.

Conflit

Lorsque deux utilisateurs modifient un même fichier au même moment, on dit qu'il y a conflit. S'ils travaillent en mode hors connexion, lorsque les utilisateurs se reconnectent, seul le fichier modifié en dernier sera conservé et les données du second fichier seront perdues.

est indisponible. Il est donc possible de travailler à tout moment sur les fichiers d'un dossier pourtant inaccessible. Lors de la prochaine connexion du dossier en question, Windows se chargera de synchroniser les modifications apportées.

Configurer un répertoire en mode hors ligne

Le point fort des fichiers hors ligne est leur simplicité de mise en place. Pour les créer, deux méthodes s'offrent à vous.

La solution la plus simple est d'accéder à un partage réseau comme vous le faites habituellement (`\\serveur-distant\nom-du-partage`). Il suffit alors de cliquer avec le bouton droit sur le dossier partagé et de choisir le menu *Toujours disponible hors connexion*.

La seconde solution consiste à créer un lecteur réseau :

1. Ouvrez le *Poste de travail (Ordinateur)*.
2. Cliquez sur le menu *Outils* et sélectionnez *Connecter un lecteur réseau*.
3. Utilisez l'assistant pour préciser le chemin du dossier partagé distant.
4. Cliquez sur le bouton *Terminer*, votre nouveau lecteur réseau apparaît dans le poste de travail.
5. Cliquez dessus avec le bouton droit et choisissez le menu *Toujours disponible hors connexion*.

Astuce **Le menu Toujours disponible hors connexion n'est pas présent**

Lorsque vous tentez de rendre disponible un lecteur réseau alors que vous n'y êtes pas connecté, le menu *Toujours disponible hors connexion* n'apparaît pas. En effet, il est nécessaire d'être connecté afin qu'une première synchronisation des fichiers ait lieu.
Ceci se produit également lorsque la fonctionnalité des fichiers hors connexion est désactivée sur votre système. Voici comment la réactiver :

1. Ouvrez le menu *Démarrer* et saisissez `synchronisation` dans la zone de saisie.
2. Cliquez sur l'élément *Centre de synchronisation*.
3. Cliquez sur le bouton situé dans la barre latérale *Gérer les fichiers hors connexion*.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton *Activer les fichiers hors connexion*.
5. Redémarrez pour rendre la modification effective.

D'un simple coup d'œil, vous pouvez savoir si la synchronisation est complète ou non. Dans le cas d'une synchronisation complète, un logo vert apparaîtra :

Si jamais l'un des fichiers n'a pas pu être rapatrié pour le mode déconnecté, une croix rouge s'ajoute par-dessus l'icône du répertoire.

Lecteur réseau

On appelle lecteur réseau un dossier réseau distant qui s'affiche sur votre poste de travail comme s'il était une partition de votre système.

Figure 8–8 Les dossiers hors connexion sont reconnaissables à cette icône. Elle est utilisée pour tous les éléments synchronisables du système (périphériques, dossiers, etc.).

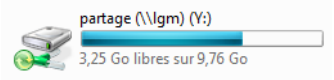


Figure 8–9
Dossier hors ligne entièrement synchronisé

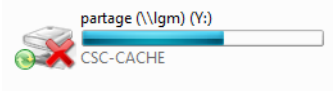


Figure 8–10
Dossier hors ligne partiellement disponible

Configurer les documents hors connexion

Ce mécanisme d'accès à des copies locales des fichiers qui se trouvent sur un répertoire distant est simple d'utilisation : il crée sur l'ordinateur une copie de chaque fichier distant. Bien entendu, la création de ce fichier de sauvegarde prend de l'espace sur le disque de l'utilisateur. Étant donné que le contrôle du contenu du répertoire réseau n'est pas garanti, les données répliquées pourraient très bien remplir le disque dur local.

Plusieurs solutions sont alors possibles. La première consiste à ne synchroniser que les fichiers que vous souhaitez sauvegarder. Ceci se configure directement dans les propriétés du dossier marqué comme étant disponible hors ligne. Pour exploiter cette première solution, utilisez la console de management de l'ordinateur :

1. Ouvrez le menu *Démarrer*. Cliquez avec le bouton droit sur *Ordinateur* et sélectionnez le menu *Gérer*.
2. Dans l'arborescence, cliquez sur *Outils système*>*Dossiers partagés*>*Partages*.
3. Double-cliquez sur le répertoire pour lequel vous souhaitez définir les options de synchronisation hors ligne.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton *Paramètres hors connexion* et choisissez le premier des trois modes de synchronisation, à savoir *Seuls les fichiers et les programmes spécifiés par les utilisateurs sont disponibles hors connexion*.
5. Rendez-vous dans le partage réseau, puis définissez un par un les fichiers et dossiers à synchroniser.

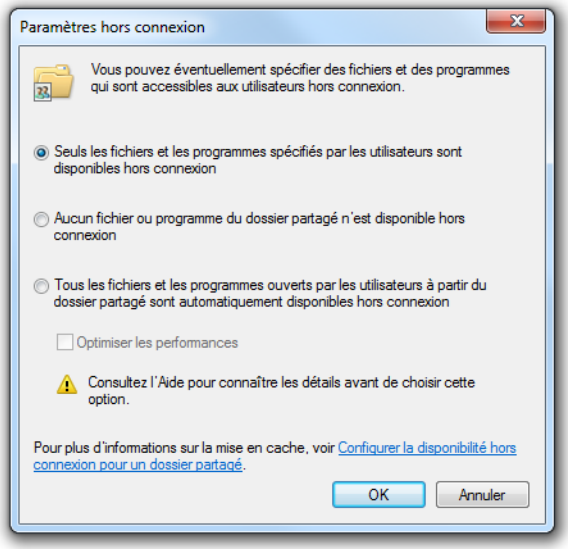


Figure 8–11
Fenêtre de configuration des paramètres hors connexion

La seconde solution consiste à définir une limite générale pour l'espace disque utilisé par les fichiers hors connexion :

1. Ouvrez le *Centre de synchronisation.*
2. Dans la partie latérale du panneau, cliquez sur le lien *Gérer les fichiers hors connexion*.
3. Ouvrez l'onglet *Utilisation du disque*, puis cliquez sur *Modifier les limites*.
4. Utilisez alors le curseur pour définir la taille que vous souhaitez allouer aux fichiers hors connexion.

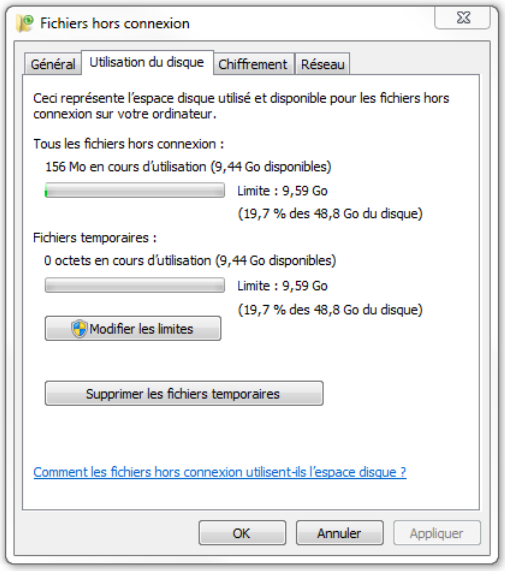


Figure 8–12
Configuration de la limite d'espace disque des fichiers hors connexion

Forcer les synchronisations de fichiers hors connexion

La synchronisation des fichiers et répertoires hors ligne est automatique. Cependant, elle n'a pas lieu de façon continue. Ainsi, si un fichier est ajouté à un répertoire réseau distant, il peut se passer plusieurs minutes avant que celui-ci ne soit mis à disposition en mode hors ligne sur votre ordinateur. Voici comment procéder pour effectuer une synchronisation dans la seconde :

1. Ouvrez le menu *Démarrer*.
2. Tapez `synchronisation` dans la zone de saisie.
3. Cliquez sur le menu *Centre de synchronisation*.
4. Cliquez sur le bouton *Synchroniser tout*.

Pour ne synchroniser qu'un seul dossier hors ligne, cliquez sur ce dernier à l'aide du bouton droit de la souris et choisissez le menu *Synchroniser*>*Synchroniser les fichiers hors connexion sélectionnés*.

Utilitaire Windows Live Mesh

Depuis peu, un nouvel utilitaire gratuit nommé Live Mesh propose des fonctionnalités sensiblement identiques aux fichiers hors connexion. Cet outil synchronise des dossiers partagés entre votre ordinateur et différents périphériques que vous aurez préalablement configurés. Il permet de partager des fichiers et d'y accéder depuis n'importe quel ordinateur, y compris un ordinateur sur lequel vous avez des droits limités. Avantage de taille, la synchronisation peut se faire via Internet, sans nécessiter la mise en place de connexions sécurisées de type tunnel comme les VPN.

▸ http://www.mesh.com

Versionning de fichiers

Généralement appelé copie fantôme (*shadow copy* ou *ghost*), ou versions précédentes dans Windows 7, le *versionning* de fichiers sert à conserver plusieurs versions d'un même fichier. Ainsi, en cas d'écrasement malencontreux d'un fichier par un autre, il est possible de revenir à un état initial. Il permet également dans certains cas de récupérer un fichier qui aurait été supprimé par erreur.

Ces différentes versions de fichiers sont tirées des sauvegardes réalisées par les outils de point de restauration de Windows. Il est donc nécessaire d'activer ces sauvegardes si l'on souhaite pouvoir avoir un suivi des modifications apportées à un ou plusieurs fichiers. Par la suite, il sera alors possible de comparer les fichiers pour en restaurer une version bien précise.

Pour accéder aux précédentes versions d'un fichier :

1. Cliquez avec le bouton droit sur le fichier et dans le menu contextuel choisissez *Propriétés*.
2. Cliquez ensuite sur l'onglet *Versions précédentes* afin d'afficher toutes les versions existantes. Pour chaque version affichée, il est possible d'effectuer trois actions :
   - *Ouvrir* le fichier, ce qui affiche le fichier sans pour autant le restaurer.
   - *Copier* le fichier, qui permet de restaurer le fichier à un autre emplacement.
   - *Restaurer* le fichier, qui écrase le fichier actuellement sur le disque par l'ancienne version sélectionnée.

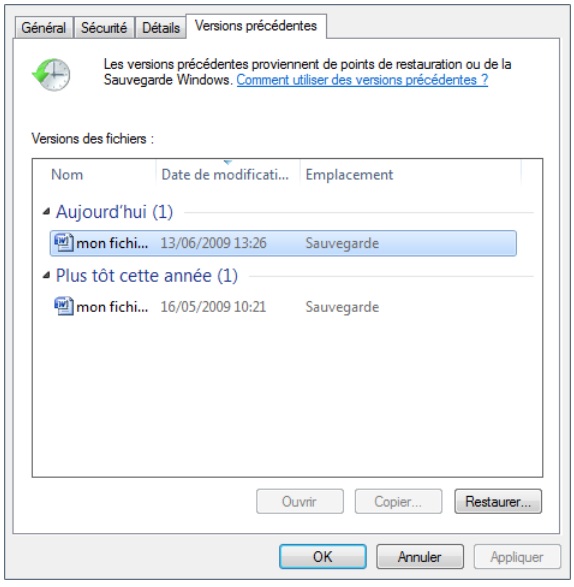


Figure 8–13
Interface de gestion des versions précédentes d'un fichier

AU PRÉALABLE

Les manipulations suivantes supposent que vous avez mis en place des sauvegardes comme indiqué dans la première partie de ce chapitre.

ASTUCE Prévisualisation de fichiers versionnés

Avant de restaurer un fichier, prenez le temps d'ouvrir l'ancienne version pour vérifier qu'elle correspond bien à ce que vous souhaitez récupérer. Néanmoins, le bouton *Ouvrir* qui ouvre cette ancienne version n'est disponible que pour les versions générées par les points de restauration. Si la version du fichier a été créée lors d'une sauvegarde, seule l'option restauration est disponible.

Mettre en place des quotas utilisateur

Bien que la capacité de stockage des disques durs actuels soit de plus en plus importante (plusieurs téraoctets pour certaines configurations), si aucune stratégie particulière n'est mise en œuvre, il est possible qu'un utilisateur monopolise, volontairement ou non, tout l'espace disque, empêchant ainsi les autres d'utiliser convenablement leur poste. Une bonne stratégie consiste alors à limiter les comptes utilisateur à un espace de stockage maximal, de manière à ce que l'espace disque soit partagé équitablement entre les différents utilisateurs.

Simple et paramétrable, la fonctionnalité de quotas n'est pas contraignante. Elle mérite donc d'être mise en place dès que possible, même s'il s'agit de définir un espace de stockage illimité pour certains utilisateurs. Sa configuration ne peut malheureusement pas se faire de façon globale, mais uniquement pour chaque volume ou partition et requiert que le disque utilise le système de fichiers NTFS.

1. Sélectionnez le disque à configurer sachant qu'il est préférable d'avoir déplacé les espaces utilisateur sur un disque différent du disque système.
2. Une fois votre disque choisi dans le poste de travail, cliquez avec le bouton droit et sélectionnez le menu *Propriétés*.
3. Dans la fenêtre des propriétés, placez-vous alors dans l'onglet *Quota* et cliquez sur le bouton *Afficher les paramètres de quota*.

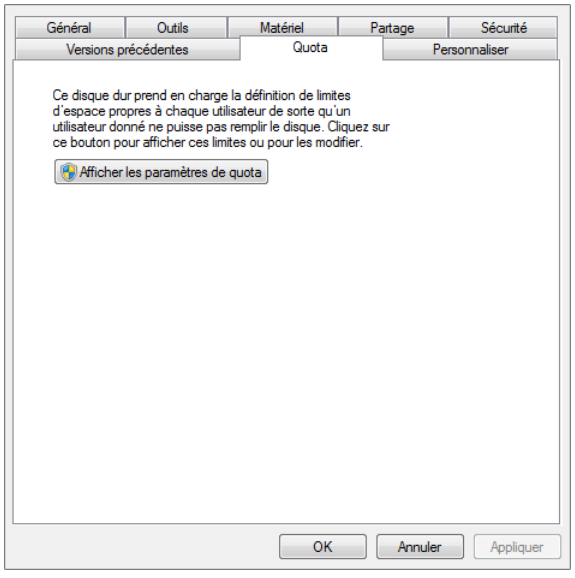


Figure 8–14 Fenêtre de propriétés d'une partition

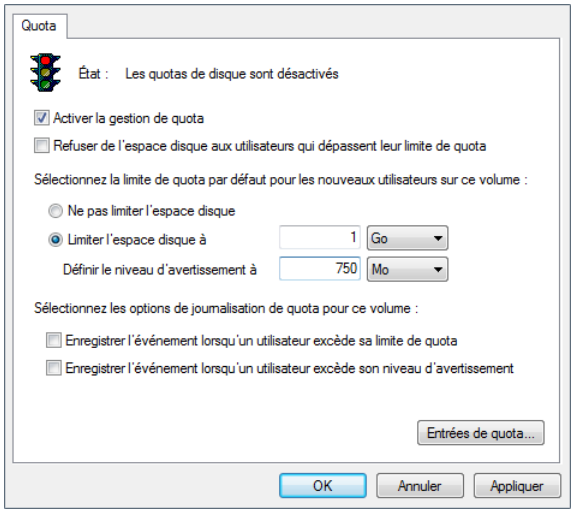


Figure 8–15 Fenêtre de propriétés de gestion des quotas

4. Cochez la case *Activer la gestion de quota*. Ceci vous permet de configurer les quotas, ou des avertissements, mais n'applique pas pour

autant la limite de chaque quota. Cela signifie que l'utilisateur peut dépasser l'espace qui lui est attribué. Pour l'empêcher de dépasser cette limite, cochez la case *Refuser de l'espace disque aux utilisateurs qui dépassent leur limite de quota*.

5 Cochez *Limiter l'espace disque à*, afin de configurer un quota pour chaque nouvel utilisateur du système. Ainsi, vous n'aurez pas reconfigurer un quota la prochaine fois que vous créerez un nouveau profil utilisateur.

Pour configurer des entrées de quotas personnalisées pour un ou plusieurs utilisateurs, cliquez sur le bouton *Entrées de quota*.

1 Cliquez sur le menu *Quota>Nouvelle entrée de quota*. Choisissez alors l'un des utilisateurs de l'ordinateur, puis configurez les limites de disque et d'avertissement que vous souhaitez lui attribuer. En cas de dépassement, l'utilisateur sera averti par le système et bloqué par ce dernier pour la création de fichiers, tant qu'il n'aura pas au préalable regagné de l'espace disque.

2 Cliquez sur le bouton *OK* pour retourner à la vue d'ensemble des entrées de quota de ce disque.

BONNES PRATIQUES

Bien utiliser les quotas disque

Voici plusieurs bonnes pratiques qui vous aideront à gérer les quotas dans la durée et vous permettront ainsi une utilisation contrôlée de l'espace sur votre ordinateur :

- Définir les limites par défaut : paramétrez les limites par défaut pour les utilisateurs et configurez ensuite les utilisateurs ayant besoin d'un quota particulier.
- Supprimer les entrées de quota non utilisées : lorsqu'une entrée n'est plus utile, supprimez-la.
- Quotas et comptes administrateur : les administrateurs doivent avoir un quota illimité et sont les seuls à pouvoir installer des applications sur la partition système.
- Configurer des entrées de quota appropriées : les entrées de quota doivent répondre à un besoin particulier et être ni trop grandes, ni trop petites. Si vous activez la limite de quota, prévoyez alors un espace suffisamment large pour que l'utilisateur ne soit pas gêné.

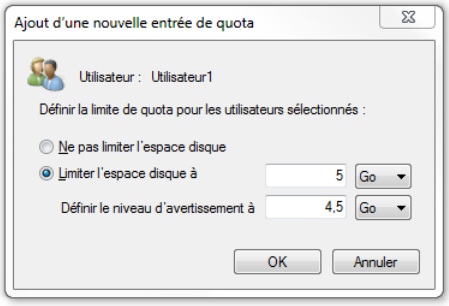


Figure 8–16 Configuration du quota d'un utilisateur

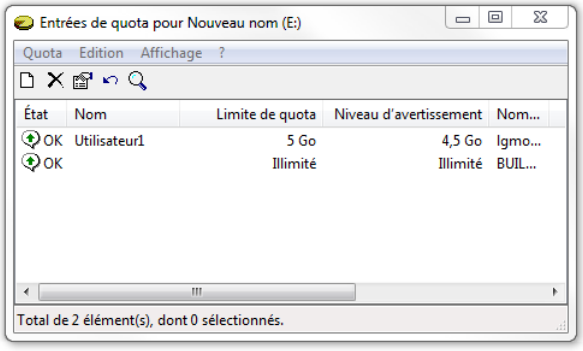


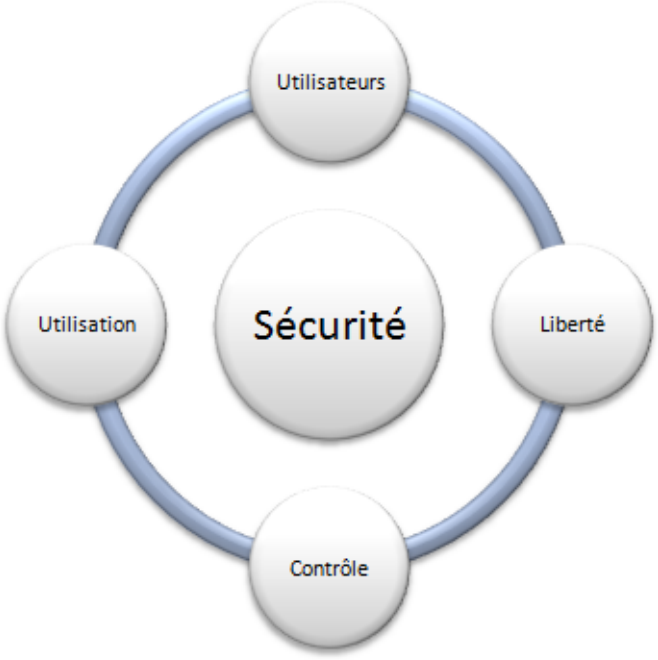
Figure 8–17 Vue d'ensemble des entrées de quota d'un disque spécifique

3 Pour finir, si vous souhaitez surveiller via les journaux d'événements les dépassements de quotas, cochez dans la fenêtre de gestion des quotas, les cases *Enregistrer l'événement lorsqu'un utilisateur excède sa limite de quota* et *Enregistrer l'événement lorsqu'un utilisateur excède son niveau d'avertissement*.

En résumé

Maintenant que nous avons vu comment mettre des méthodes de contrôle des données en place, intéressons-nous aux différentes stratégies de sécurité. Grâce à elles, nous allons instaurer une stratégie de fonctionnement précise sur différentes parties du système.

chapitre 9



Les stratégies de sécurité

La sécurité d'un ordinateur ne se limite pas à mettre en place un pare-feu et un antivirus. Il faut également configurer avec soin son système d'exploitation afin d'éviter les intrusions et les mauvaises manipulations.

SOMMAIRE

- Politique de sécurité
- Stratégies de sécurité
- Modèles de stratégies
- Bonnes pratiques

MOTS-CLÉS

- Stratégie
- Sécurité
- Secpol
- Modèle
- Audit
- MMC
- Snap-in
- Droits
- AppLocker
- Srp

Ce chapitre explique comment mettre en place une politique de sécurité et détaille les outils à votre disposition. Nous nous intéressons principalement aux stratégies de sécurité, à leur répartition et à leur mise en œuvre, mais également à l'utilisation de modèles de sécurité afin de mettre en place une stratégie globale sur différents ordinateurs.

Qu'est-ce qu'une stratégie de sécurité ?

Le mot stratégie vient du grec *stratos* (armée) et *hégéomai* (conduire) et représente à l'origine l'art de diriger les soldats pour vaincre un ennemi. Dans son acception informatique, le terme est resté proche de son étymologie. En effet, il s'agit de l'art de diriger un ensemble d'éléments contre un ennemi : le *hacker*.

Une stratégie de sécurité digne de ce nom ne s'arrête pas à quelques paramétrages dans une console. Il s'agit en réalité d'effectuer certaines actions pour se protéger des risques ou du moins, les limiter. Certes, il est impossible de rendre son ordinateur parfaitement inviolable sans le couper du réseau ou le laisser dans son emballage, mais il existe cependant des risques connus dont voici une courte liste :

- risques liés à un piratage interne ou externe ;
- risques liés à l'utilisation de virus/malware*s ;*
- risques liés à une erreur de manipulation de la part d'un utilisateur ;
- risques liés à la station de travail elle-même ;
- risques liés à la négligence.

Nous traitons de leur prévention dans différents chapitres de ce livre et notamment dans le chapitre 13 dédié à la sécurité du système. Pour les autres risques, une grande partie peut être limitée grâce à l'utilisation de stratégie de sécurité Windows (*Windows Security Policy*).

Les différents types de stratégies

Il existe différents types de stratégies, notamment les stratégies de comptes, de droits utilisateur et d'audit.

Les stratégies de comptes

Les stratégies de comptes concernent l'ouverture de session des utilisateurs. Elles portent sur la gestion des mots de passe et sur les conditions de verrouillage de compte. À l'origine des failles de sécurité, se trouve

bien souvent un mot de passe trop simple ou inchangé depuis trop longtemps. Il est alors facile pour une personne malintentionnée d'usurper l'identité de l'utilisateur négligeant. Les stratégies de comptes sont donc particulièrement importantes :

- Elles définissent une durée de validité d'un mot de passe afin de forcer l'utilisateur à en changer régulièrement.
- Elles définissent une durée minimale pour éviter que l'utilisateur ne le change trop souvent et l'oublie.
- Elles activent le stockage des mots de passe de façon réversible afin qu'un administrateur puisse retrouver ce mot de passe et le redonner à l'utilisateur.
- Elles obligent à utiliser des mots de passe complexes afin d'éviter les mots de passe trop simples.
- Elles définissent la longueur minimale d'un mot de passe.
- Elles conservent l'historique des mots de passe pour éviter qu'un utilisateur n'en emploie un ancien.

Pour se prémunir de tentative d'accès par force brute, les stratégies de comptes permettent également de définir une politique de verrouillage de compte utilisateur en cas d'échec de connexion. À vous de définir au bout de combien d'essais le compte est verrouillé et pour combien de temps. Par défaut, les comptes ne se verrouillent jamais et une attaque par force brute est tout à fait possible.

BONNE PRATIQUE

Stockage réversible des mots de passe

Il n'est pire stratégie que celle-ci ! En effet, avec cette stratégie activée, si un attaquant venait à prendre le contrôle en tant qu'administrateur, il aurait accès à tous les mots de passe de tous les utilisateurs. Sa capacité d'action s'en trouverait démultipliée. Lorsqu'un utilisateur a perdu son mot de passe, optez pour la génération d'un mot de passe temporaire en cochant la case *L'utilisateur doit changer son mot de passe à la prochaine connexion*. De cette façon, l'utilisateur pourra accéder à son compte et une boîte de dialogue lui permettra de définir un nouveau mot de passe, sans que l'administrateur le connaisse.

Les stratégies de droits utilisateur

Plus nombreuses mais plus simples d'utilisation, les stratégies de droits utilisateur permettent de gérer les permissions et les actions possibles de chaque utilisateur ou groupe d'utilisateurs.

Vous pouvez y configurer qui des utilisateurs ou des groupes :

- peut modifier les pilotes de périphériques ;
- peut changer l'heure du système ;
- peut créer d'autres comptes utilisateur ;
- peut modifier les droits d'accès d'autres utilisateurs ;
- peut changer les variables d'environnement, etc.

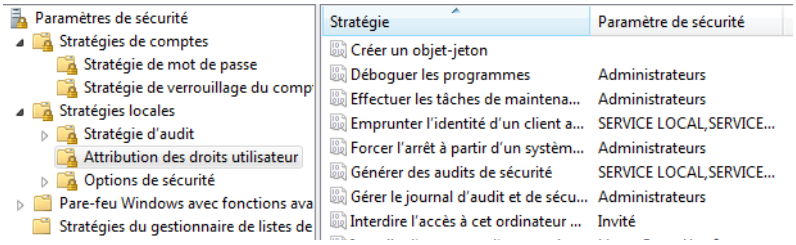


Figure 9–1
Stratégies de droits utilisateur

Les stratégies d'audit

Les stratégies d'audit servent à mettre en place ce que l'on appelle des journaux d'audit afin d'enregistrer les actions effectuées sur le système. Ces audits concernent principalement les ouvertures de session et les accès aux fichiers.

Pour chacune des stratégies d'audit, deux options sont disponibles : les réussites et les échecs. Chaque fois qu'un accès a réussi ou à l'inverse, chaque fois qu'il a échoué, une entrée est générée dans le journal. Bien qu'il soit possible d'enregistrer à la fois les réussites et les échecs, vous ne devriez normalement n'avoir besoin que de l'un ou l'autre. Soulignons également que le fait d'activer les deux options a comme effet d'augmenter de façon considérable les enregistrements d'audit et rend leur analyse plus difficile, puisque l'information intéressante est noyée au milieu d'enregistrements inutiles.

Pensez également à regarder le nœud *Configuration avancée de la stratégie d'audit* qui propose des stratégies plus fines pour des besoins très précis, comme l'audit du verrouillage de session ou l'audit des modifications de stratégie de sécurité par auteur.

BONNE PRATIQUE Audit et tentative d'intrusion

Les audits détectent très efficacement les tentatives d'intrusion sur votre système. Il est possible d'activer des audits enregistrant les échecs de connexion pour repérer un éventuel attaquant cherchant à forcer la combinaison identifiant/mot de passe. De même, si un de vos répertoires contient des données sécurisées, un audit sur les tentatives d'accès à l'objet vous permettra de vérifier que les droits d'accès ont bien été configurés.

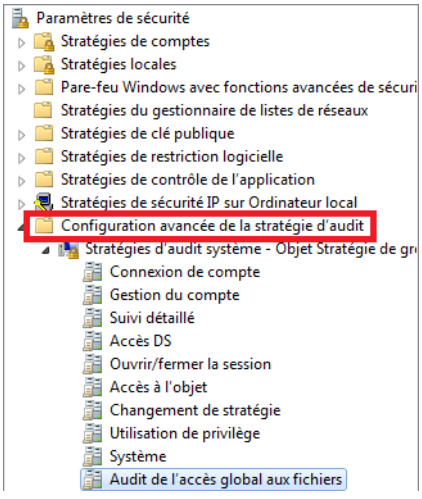


Figure 9–2
Configuration avancée de la stratégie d'audit

Les stratégies complémentaires

Plusieurs autres groupements de stratégies sont également disponibles depuis la console de gestion. Le tableau 9-1 de la page suivante les détaille.

CULTURE Nombre de stratégies disponibles

Au fil des années, plusieurs utilisateurs avancés nous ont affirmé, au cours d'échanges informels, que les stratégies de sécurité étaient trop peu nombreuses et pas assez précises. Si ceci était vrai pour les toutes premières versions de Windows, il existait déjà du temps de Vista pas moins de 2 747 stratégies de sécurité disponibles. Ce nombre a encore augmenté avec Windows 7. Rien que pour Internet Explorer 8, près de 1 300 stratégies de sécurité sont disponibles.

Tableau 9–1 Liste des stratégies complémentaires

Libellé	Description
Pare-feu Windows avec fonctions avancées de sécurité	Configure très finement les règles de trafic entrant et sortant de l'ordinateur. Établit également des connexions sécurisées entre plusieurs ordinateurs du réseau.
Stratégies du gestionnaire de liste de réseaux	Personnalise l'affichage et le comportement du système lors de la détection d'un réseau local.
Stratégies de clé publique	Configure les sécurités de chiffrement du système comme BitLocker ou EFS.
Stratégies de restriction logicielle	Définit les applications autorisées sur le système.
Stratégies de contrôle de l'application	Remplaçantes des stratégies de restriction logicielle, elles correspondent à AppLocker, l'outil de gestion d'exécution des applications. Celui-ci permet d'autoriser ou de refuser l'exécution ou l'installation de certains programmes par certains utilisateurs.
Stratégie de sécurité IP sur Ordinateur Local	Contrôle l'utilisation d'IPSec, en tant que surcouche pour les communications IP de l'ordinateur.

Mettre en place une stratégie de sécurité

Appliquer une ou plusieurs stratégies de sécurité n'est pas tant une question d'utilisation technique de l'ordinateur, mais bien une question de méthodologie. La majorité des stratégies ont pour objectif de garantir la disponibilité et la sécurité des données, mais également l'intégrité du système.

Il ne faut pas voir un ordinateur juste comme un simple outil mécanique, mais plutôt comme un média servant de système IT (*Information Technology*), c'est-à-dire un système centralisé traitant toutes sortes d'informations, dont certaines s'avèrent critiques et/ou sensibles. Il est donc important d'aborder ce point en prenant du recul et en se posant d'autres questions que simplement le fait de répondre à des besoins. Quelles sont les données à protéger ? Quel est l'impact sur l'utilisation de l'ordinateur ? Préférons-nous laisser une grande liberté aux utilisateurs ou garantir la sécurité du système ? Quels sont les éléments critiques à auditer ? Auditons-nous pour détecter des attaques ou pour nous assurer que les utilisateurs accèdent correctement aux ressources ?

Avant même d'ouvrir la console de sécurité locale, munissez-vous d'un papier et d'un crayon et écrivez les grandes lignes de votre politique de sécurité. Différenciez ensuite les points importants et ceux qui le sont moins. C'est seulement lorsque vous aurez mené cette phase de réflexion que vous pourrez faire efficacement le tour des stratégies de sécurité locales. Grâce à elles, vous mettrez en pratique vos principes et votre vision de la sécurité du système.

CONSEIL Dans la peau de l'administrateur et de l'utilisateur

Lors de votre phase de réflexion, mettez-vous à la place de l'administrateur, mais également à la place de l'utilisateur. Vous combinerez ainsi tous les besoins avec vos préceptes.

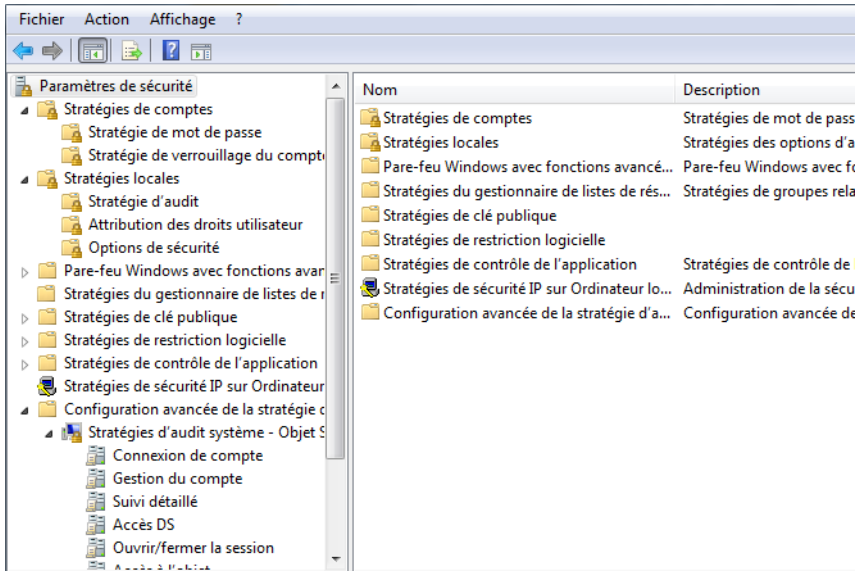


Figure 9–3
Console de stratégie de sécurité locale

Ouvrez le menu *Démarrer*, saisissez `secpol.msc` dans la zone de saisie, puis appuyez sur la touche *Entrée*. Il ne reste alors plus qu'à trouver la ou les stratégies de sécurité de votre choix, de double-cliquer dessus et d'en modifier si besoin les paramètres. Les modifications sont instantanées. Néanmoins, avant de foncer tête baissée dans la configuration longue et fastidieuse des stratégies de sécurité, intéressons-nous de plus près aux modèles de stratégies de sécurité.

Les modèles de stratégies

Au sens large, une stratégie de sécurité est une philosophie de sécurité que l'on souhaite appliquer à l'aide d'une multitude d'autres stratégies (règles) sur un ordinateur précis. Mettre en place cette stratégie pour la première fois peut être d'autant plus chronophage que le nombre d'ordinateurs sur lesquels on souhaite appliquer les mêmes règles de sécurité augmente.

Dans cette optique, Microsoft propose des modèles de stratégies, configurations complètes applicables d'un seul clic à un ordinateur. Ils sont d'autant plus intéressants que vous pouvez créer vos propres modèles de stratégies correspondant exactement à ce que vous souhaitez configurer. Ainsi, avant de vous jeter à corps perdu dans la configuration de la stratégie de votre ordinateur, nous vous recommandons de passer par la case modèle. Cela ne peut que vous faire gagner du temps, même si le modèle ne s'applique qu'à un seul ordinateur.

Créer son modèle de sécurité

La création des modèles de sécurité se fait via un snap-in MMC nommé Modèles de sécurité.

1. Ouvrez le menu *Démarrer*, entrez `mmc.exe` dans la zone de saisie et tapez sur la touche *Entrée*.
2. Cliquez sur le menu *Fichier*, puis *Ajouter>Supprimer un composant logiciel enfichable*.
3. Dans la liste qui s'ouvre, double-cliquez sur *Modèles de sécurité* pour qu'il apparaisse dans la colonne de droite, puis appuyez sur le bouton *OK*.

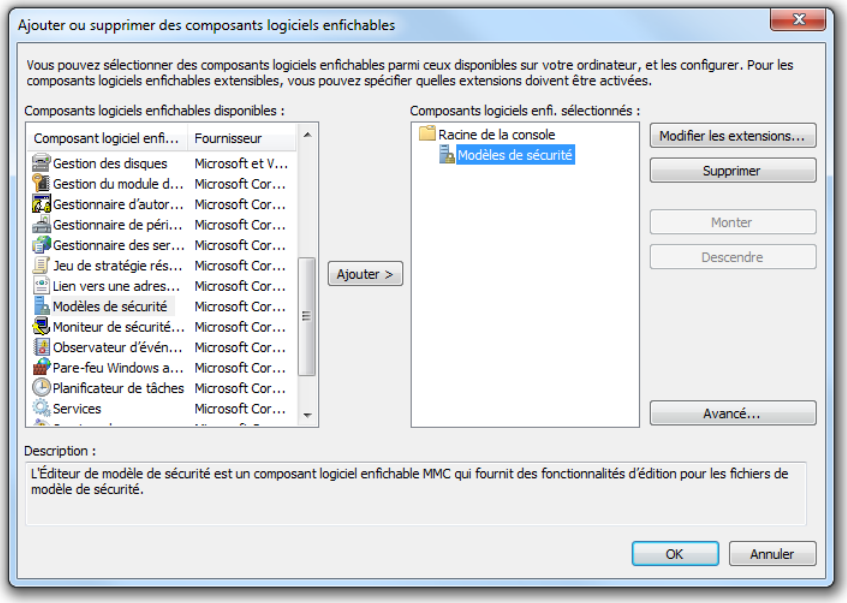


Figure 9–4
Ajout d'un composant enfichable

4. Cliquez ensuite sur *Modèles de sécurité* et sur le chemin de recherche qui doit exister par défaut. Il s'agit normalement du chemin `C:\Users\<nom utilisateurs>\Documents\Security\Templates`. Dans la partie centrale, cliquez avec le bouton droit et choisissez *Nouveau modèle*. Donnez-lui le nom de votre choix et cliquez sur *OK*.

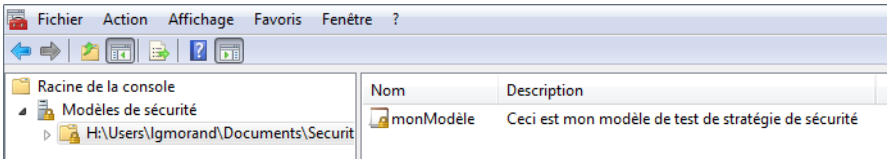


Figure 9–5
Fenêtre de gestion des modèles de sécurité

5. Votre modèle créé, vous pouvez éditer toutes les stratégies de sécurité disponibles sur votre ordinateur sans que celles-ci ne soient appliquées. Soulignons qu'il s'agit bien ici d'éditer un modèle et non pas les stratégies courantes.

Snap-in MMC

La console MMC (*Microsoft Management Console*) est une interface de contrôle système dont le rôle est de charger des composants enfichables, nommés *snap-in*. Ces composants sont des petits panneaux de configuration qui s'affichent au sein même de la console et adressent le paramétrage d'une partie spécifique du système. Ainsi, il existe des snap-in de gestion des services, des stratégies de sécurité, des certificats, des périphériques, des utilisateurs, etc. Soulignons enfin qu'il est également possible de télécharger des composants enfichables supplémentaires sur Internet.

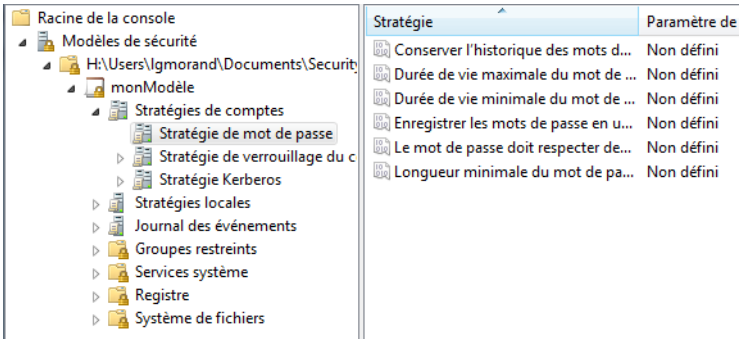


Figure 9–6
Stratégies du modèle de stratégie de sécurité

EN DÉTAIL Fichier .inf

Ce fichier est de taille minime. En effet, il ne contient que la configuration des stratégies qui ont été modifiées. Ceci a son importance, car cela signifie que vous pouvez créer autant de modèles que vous le souhaitez et que si les modèles ne définissent pas les mêmes stratégies, ils vont pouvoir être appliqués à un même ordinateur sans créer de conflits de paramétrage.

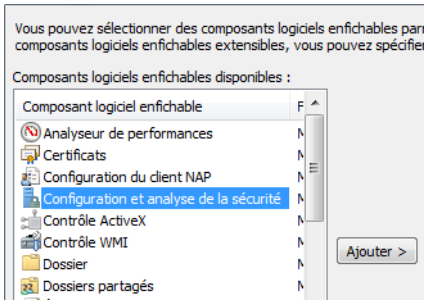


Figure 9–7
Ajout d'un composant MMC enfichable

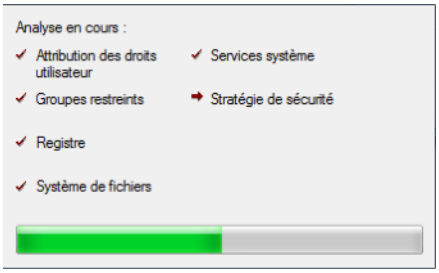


Figure 9–8
Analyse de la configuration de l'ordinateur

6 Prenez alors le temps de configurer toutes les stratégies dont vous avez besoin. Chaque fois qu'une stratégie est configurée, son statut ne sera plus *Non défini*.

7 Vos paramétrages terminés, il est temps d'enregistrer tout cela. Cliquez avec le bouton droit sur le nom de votre modèle et choisissez *Enregister*. Un fichier portant l'extension `.inf` se place alors dans le chemin de recherche affiché au-dessus du modèle.

Passons maintenant au déploiement de notre modèle.

Tester son modèle de sécurité

Avant de déployer le modèle à grande échelle, mais également avant de le tester sur la machine de test (dite maître), il convient de tester le modèle et de voir si sa configuration correspond bien à ce que vous souhaitez.

1 Toujours dans la console MMC utilisée pour créer le modèle, cliquez sur le menu *Fichier>Ajouter/Supprimer un composant enfichable* et choisissez cette fois l'élément *Configuration et analyse de la sécurité*.

2 Commençons par créer une base de données, celle-ci va servir à comparer le modèle à la configuration actuelle de l'ordinateur. Dans la console MMC, cliquez avec le bouton droit sur *Configuration et analyse de la sécurité*, puis choisissez *Ouvrir une base de données*. Comme celle-ci n'existe pas encore, tapez un nom dans la zone *Nom du fichier* et cliquez sur *Ouvrir*. Ceci a pour effet de créer la base de données. Il vous est ensuite demandé de choisir un modèle de sécurité. Prenez celui que nous venons de créer.

3 Le modèle est alors chargé dans la base de données, en parallèle de la configuration existante. Cliquez maintenant, toujours avec le bouton droit, sur *Configuration et analyse de la sécurité* et choisissez *Analyser l'ordinateur maintenant*.

4 Le composant compare alors la configuration de chaque stratégie afin de détecter les différences entre le modèle et les stratégies locales.

Une fois l'analyse terminée, vous visualisez les différences détectées. Chaque stratégie configurée obtient soit une coche verte lorsqu'elle est identique à la stratégie locale, soit une coche rouge en cas de différence. Vous identifiez ainsi rapidement les éléments qui seront modifiés lors de l'importation.

Sur la figure suivante, vous voyez dans la partie supérieure l'analyse du modèle, et dans la partie inférieure l'affichage de la console de stratégies de sécurité locales. Les différences et les points communs ont été parfaitement détectés lors de l'analyse. Le modèle est prêt, il ne reste plus qu'à l'importer.

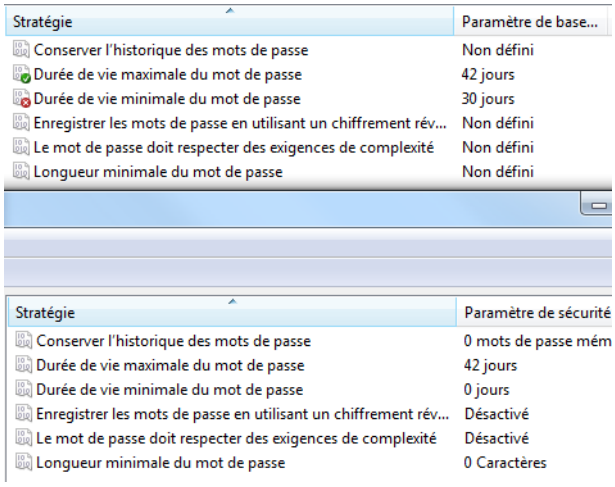


Figure 9–9
Mise en parallèle des deux consoles pour confirmer le test

Appliquer un modèle de sécurité

Pour appliquer le modèle, rien de plus simple. Cliquez sur *Configuration et analyse de la sécurité* et choisissez le menu *Configurer l'ordinateur maintenant*. Si tout se passe bien, la base de données est détruite et la configuration locale de l'ordinateur contient alors les modifications importées par le modèle.

Bonnes pratiques

Les bonnes pratiques lors de l'utilisation des stratégies de sécurité sont assez simples :

- Recourez autant que possible aux modèles et n'hésitez pas à en créer plusieurs afin de gérer plusieurs configurations possibles.
- Les stratégies de sécurité peuvent être mises en œuvre pour configurer pratiquement tout le système. Qu'il s'agisse de paramètres de compte, de paramètres de démarrage de services Windows ou encore de droits d'accès à une clé registre particulière, elles constituent le moyen le plus simple pour configurer à partir d'une seule interface différentes parties du système et permettent surtout, de copier une configuration d'un ordinateur à un autre.

En résumé

Dans ce chapitre, vous avez appris comment sécuriser différents points clés du système grâce à une console principale. Vous avez également vu les principes et la méthodologie nécessaires à la mise en œuvre de stratégies de sécurité pour adapter les besoins utilisateur aux contraintes de sécurité.

Nous avons détaillé comment exporter toute une configuration de stratégies au travers de modèles qui permettent ensuite soit de déployer vos stratégies sur différents ordinateurs, soit d'effectuer une sauvegarde que vous pourrez recharger si vous venez à réinstaller votre système.

chapitre 10

Configurer le réseau

De nos jours, les réseaux sont partout. Si, à une époque pas si lointaine, seuls les ordinateurs se connectaient à Internet, les évolutions technologiques amènent de plus en plus de périphériques mobiles à y accéder, améliorant ainsi l'interconnectivité ordinateur/ordinateur, mobile/mobile, mais également ordinateur/mobile.

SOMMAIRE

- Centre réseau et partage
- Connexion à un réseau sans fil
- Connexion à un réseau VPN
- Modifier les paramètres de partage
- Le groupe résidentiel d'ordinateurs

MOTS-CLÉS

- Connexion
- Réseau
- Wi-Fi
- Ad hoc
- VPN
- Statut de connexion
- Carte réseau
- Adresse IP
- Groupe résidentiel

Ce chapitre présente les différents outils fournis par Windows 7 pour configurer la connectivité de votre ordinateur.

Le centre réseau et partage, centre névralgique de la configuration réseau

Le centre réseau et partage est le cœur de la gestion des connexions aux différents réseaux. En un coup d'œil, vous visualisez l'état de toutes vos connexions. Pour y accéder, vous avez comme toujours le choix entre plusieurs méthodes :

- saisir `centre réseau et partage` dans la barre de recherche du menu *Démarrer* ;
- via le panneau de configuration dans la catégorie *Réseau et Internet* ;
- cliquer droit sur l'icône réseau dans la barre de notification de Windows (à côté de l'horloge) et sélectionner *Centre Réseau et partage*.

Effectuons le tour du propriétaire de la fenêtre du centre réseau et partage.

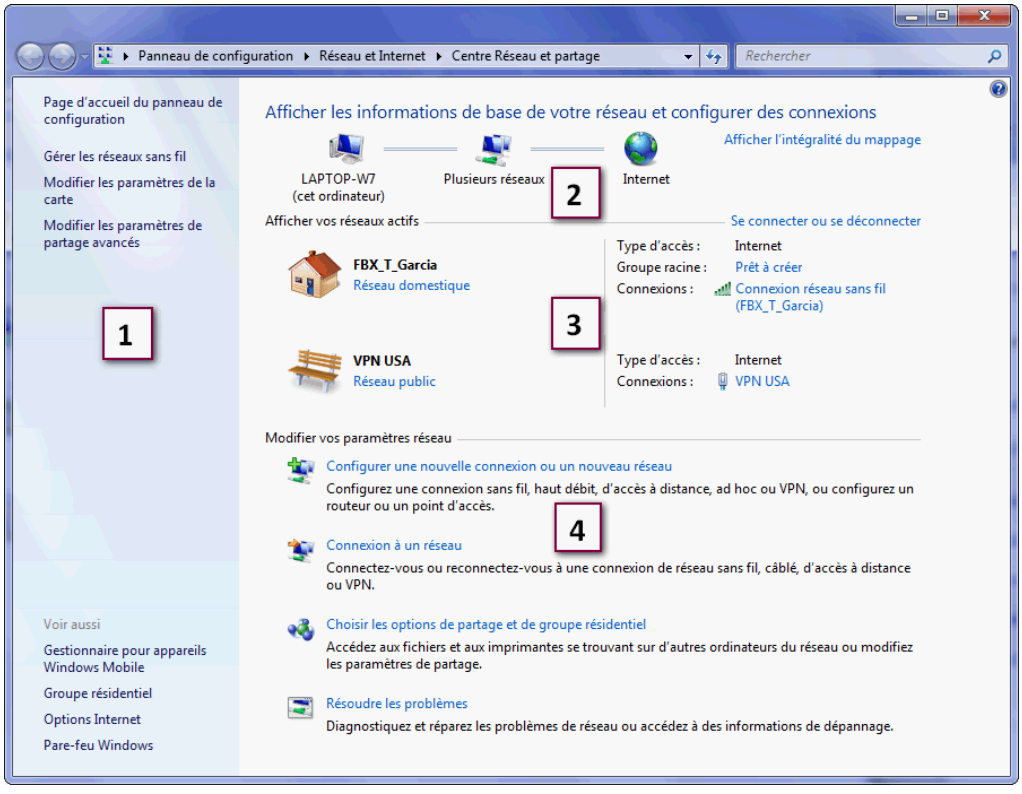


Figure 10–1
Vue du centre réseau et partage de Windows 7

Comme toutes les fenêtres liées au panneau de configuration, le centre réseau et partage est structuré en deux parties : la barre verticale sur la gauche contient la liste des actions possibles concernant les réseaux, et le reste de la fenêtre affiche l'état de la connectivité ainsi que des actions complémentaires comme la connexion à un nouveau réseau ou la réparation d'une connexion défaillante. Regardons tout cela de plus près.

La colonne d'actions 1 permet de revenir en un clic au panneau de configuration, mais également d'accéder à la fenêtre de gestion des réseaux sans fil, d'accéder aux paramètres des différentes cartes réseau ainsi qu'à des options avancées concernant le partage.

La partie supérieure 2 de la fenêtre affiche de manière schématique et simplifiée la façon dont vous êtes connecté au réseau. Le schéma permet de visualiser d'un coup d'œil si l'ordinateur a accès à Internet ou non. Le lien *Afficher l'intégralité du mappage* affiche une vue plus détaillée listant les points d'accès Wi-Fi, les routeurs ou les passerelles présents sur votre réseau.

La partie centrale de la fenêtre 3 dresse la liste des connexions actuellement établies. Sur la figure 10-1, vous remarquez que deux connexions sont établies : l'une à un point d'accès sans fil et l'autre à un réseau VPN.

Les liens *Réseau domestique* et *Réseau Public* servent à définir le niveau de sécurité pour chaque connexion. Lorsque vous choisissez *Réseau public*, la sécurité augmente : votre ordinateur ne partage plus de ressources (imprimante ou fichier) et n'est plus visible sur le réseau. Ce mode est préconisé dans des lieux publics (*hot spots*). Lorsque vous configurerez votre réseau à domicile, vous souhaiterez certainement accéder à tous vos autres ordinateurs et éventuellement partager des fichiers. Pour cela, choisissez le mode *Réseau domestique*.

Au bas de la fenêtre 4, se trouvent des liens vers des tâches courantes permettant de créer une nouvelle connexion, gérer les options de partage ou encore de résoudre les problèmes éventuels.

ASTUCE Raccourcis

Un clic sur l'icône représentant l'ordinateur ouvre directement la fenêtre *Ordinateur* (anciennement *Poste de travail*). Si vous cliquez sur l'icône symbolisant le réseau, la liste des périphériques (ordinateurs, imprimantes…) du réseau s'affiche. Enfin, un clic sur l'icône Internet ouvre votre navigateur web par défaut.

Les connexions sans fil

Incontournable, la technologie Wi-Fi est aujourd'hui utilisée autant à domicile que dans des lieux publics en point d'accès libre (*hot spot*). Windows 7 permet de configurer votre connexion aux ressources du réseau ou à Internet en quelques clics.

Se connecter à un réseau Wi-Fi

Windows 7 est à l'écoute permanente des réseaux sans fil autour de votre ordinateur. Tous les points d'accès Wi-Fi visibles détectés à proximité sont indiqués dans la mini-fenêtre *Réseau* qui apparaît lorsque vous cliquez sur l'icône réseau située près de l'horloge dans la barre des tâches.

Pour vous connecter à un réseau spécifique, il vous suffit de cliquer dessus. Il est possible d'indiquer à Windows que vous souhaitez vous connecter automatiquement à ce réseau lorsque votre ordinateur est à portée. Selon le type de sécurité du réseau, vous serez amené à saisir des informations d'identification. Une fois que vous vous serez identifié, la connexion s'établit et vous pourrez l'utiliser.

Figure 10–2
Points d'accès Wi-Fi à proximité

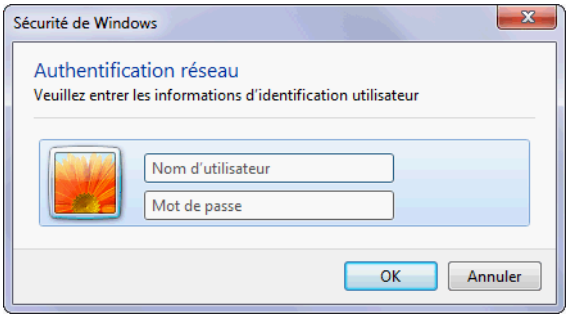


Figure 10–3
Fenêtre d'identification à un réseau sans fil

COMPRENDRE Les différents types de sécurité Wi-Fi

Les réseaux Wi-Fi diffusant des données de manière immatérielle à travers les airs, il est plus facile pour une personne malintentionnée de s'introduire dans votre réseau. Il existe trois types de sécurité principaux pour les réseaux sans fils.

- Le premier, appelé Open, ne nécessite aucune identification pour se connecter au réseau. C'est le niveau de sécurité le moins sûr de tous.
- Le deuxième type de sécurité est baptisé WEP (*Wired Equivalent Privacy*). Un peu ancienne, cette sécurité est conservée dans Windows 7 pour des raisons de compatibilité avec certains périphériques. Quand vous vous connectez à un réseau protégé par clé WEP, vous devez saisir cette clé lors de la connexion au réseau. Cette clé chiffre les informations qui sont échangées au sein du réseau. Cependant, la protection WEP peut être facilement crackée et des personnes malintentionnées pourraient s'introduire dans votre réseau. Mais, si vous possédez des appareils non compatibles tels que certaines consoles de jeu portables ou autres appareils utilisant le Wi-Fi, vous serez certainement contraint d'utiliser une protection WEP. En raison du faible niveau de sécurité de la protection, il est recommandé d'utiliser plutôt WPA ou WPA2. Une clé WEP est constituée, au choix, de 5 ou 13 caractères alphanumériques ou de 10 ou 26 caractères hexadécimaux (chiffres de 0 à 9 ou lettres de A à F).
- Le troisième type de sécurité est la protection WPA (*Wi-Fi Protected Access*). Le WPA chiffre les informations échangées sur le réseau Wi-Fi et s'assure que la clé du réseau n'a pas été modifiée. Ce type de sécurité exige des utilisateurs qu'ils s'identifient pour accéder au réseau. Ceci permet de vérifier que seules les personnes autorisées s'y connectent. Il existe deux types d'authentification : WPA et WPA2. Certains routeurs n'acceptent que l'un des deux systèmes. Dans certains cas, une même clé est fournie à tous les utilisateurs du réseau (cette clé est appelée *passphrase*). Dans Windows 7, ce type de protection est appelé WPA-Personnel ou WPA2-Personnel. Une passphrase WPA se compose au choix de 8 à 63 caractères alphanumériques respectant la casse ou de 64 caractères hexadécimaux (chiffres de 0 à 9 et lettres de A à F). Si chaque utilisateur dispose d'identifiants personnels, il faut alors choisir WPA-Entreprise ou WPA2-Entreprise. Les identifiants seront demandés lors de la connexion.

Si vous souhaitez vérifier l'état de la connexion, ouvrez à nouveau la mini-fenêtre *Réseau*. Votre connexion Wi-Fi est indiquée en gras suivie de la mention *Connecté* et du niveau de puissance du signal. La partie supérieure de la mini-fenêtre vous précise le type d'accès au réseau actuel (réseau local uniquement ou accès à Internet).

Une fois connecté, l'icône réseau dans la barre de notification Windows affiche la puissance du signal Wi-Fi sous la forme de petites barres blanches.

Figure 10–4
La barre de notification système affiche le niveau de réception du Wi-Fi.

Créer une connexion Wi-Fi ad hoc

Si vous ne possédez pas de point d'accès Wi-Fi par routeur ou box ADSL, vous pouvez tout de même relier deux ordinateurs équipés de cartes Wi-Fi directement entre eux. Ce type de connexion est appelé Wi-Fi ad hoc.

1. Ouvrez le *Centre Réseau et partage* et cliquez sur *Configurer une nouvelle connexion ou un nouveau réseau*.
2. Dans la liste qui s'affiche, choisissez *Configurer un réseau sans fil ad hoc (ordinateur à ordinateur)*.
3. L'assistant vous présente alors rapidement le principe de la connexion ad hoc et vous précise que vous serez déconnecté de votre connexion sans fil actuelle si vous ne possédez qu'une seule carte Wi-Fi.
4. Donnez ensuite un nom à votre réseau ad hoc.
5. Choisissez le type de sécurité que vous souhaitez utiliser, si bien entendu vous envisagez d'en appliquer une.
6. Une fois la connexion configurée, vous devez paramétrer la même configuration sur l'ordinateur auquel vous souhaitez vous connecter. En effet, les deux ordinateurs formant une connexion ad hoc partagent les mêmes paramètres de sécurité.

Modifier les paramètres des réseaux Wi-Fi configurés

Windows 7 conserve les paramètres de tous les réseaux sans fil auxquels vous vous êtes connecté. Ces paramètres sont accessibles via le centre réseau et partage.

Ouvrez le centre, puis cliquez sur *Configurer les réseaux sans fil*. Windows ouvre alors une fenêtre contenant la liste des connexions Wi-Fi que vous avez configurées. Grâce à cette fenêtre, vous pouvez :

- Ajouter manuellement un nouveau réseau sans fil, même si celui-ci ne se trouve pas à portée de votre ordinateur, via le bouton *Ajouter* présent en haut de la fenêtre.

DÉPANNAGE En cas de problème de connexion au Wi-Fi

Si vous rencontrez des difficultés pour vous connecter à un réseau Wi-Fi, vérifiez les points suivants :

- Assurez-vous que vous êtes suffisamment près du point d'accès : plus le signal est fort, plus stable sera la connexion.
- Vérifiez vos informations d'identification : si vous indiquez une mauvaise clé ou si vous n'utilisez pas les bons identifiants, la connexion au réseau Wi-Fi vous est refusée.
- Assurez-vous qu'il n'y a pas de parasites autour de vous. Certains équipements électroniques brouillent les ondes du signal Wi-Fi, rendant la connexion instable, voire impossible à établir. Vérifiez que vous n'avez pas, dans l'entourage de votre ordinateur ou de votre point d'accès, d'équipements de type transmetteur audio/vidéo sans fil, téléphone sans fil ou gros haut-parleurs.

INFO Un seul réseau à la fois

Une carte Wi-Fi ne se connecte qu'à un seul réseau à la fois. Cela signifie que si vous disposez d'une connexion à Internet par Wi-Fi, vous ne pourrez pas l'utiliser pendant que vous serez connecté à un autre ordinateur via un réseau ad hoc. Pour vous connecter à Internet, utilisez alors une connexion Ethernet.

EN PRATIQUE Spécificités de nommage

Le nom de votre réseau doit comporter au maximum 32 caractères. Soulignons également que la casse (majuscules/minuscules) est respectée.

ATTENTION Connexion Open

Avec une connexion de type Open, l'ordinateur avec lequel vous souhaitez établir une connexion n'a pas besoin de s'identifier pour se connecter. N'étant rien d'autre qu'une faille de sécurité, il vaut mieux éviter cette solution, surtout en milieu professionnel ou si vous vous trouvez dans un lieu public.

- Modifier les paramètres d'un réseau précédemment configuré en double-cliquant sur son nom dans la liste. La fenêtre qui s'ouvre alors affiche dans un premier onglet les informations générales sur ce réseau sans fil : son nom logique (que vous choisissez, par exemple `Wi-Fi travail`, `Wi-Fi maison`, etc.), son nom réel (SSID), son type (ad hoc ou point d'accès) et enfin la disponibilité du réseau aux utilisateurs de l'ordinateur.
- Choisir que l'ordinateur se connecte au réseau dès qu'il le capte en cochant la case *Me connecter automatiquement lorsque ce réseau est à portée*.

BON À SAVOIR Pas de nom SSID

Certains réseaux ne diffusent pas leur nom SSID par mesure de sécurité. Pour vous connecter à ce type de point d'accès, cochez la case *Me connecter même si le réseau ne diffuse pas son nom (SSID)*.

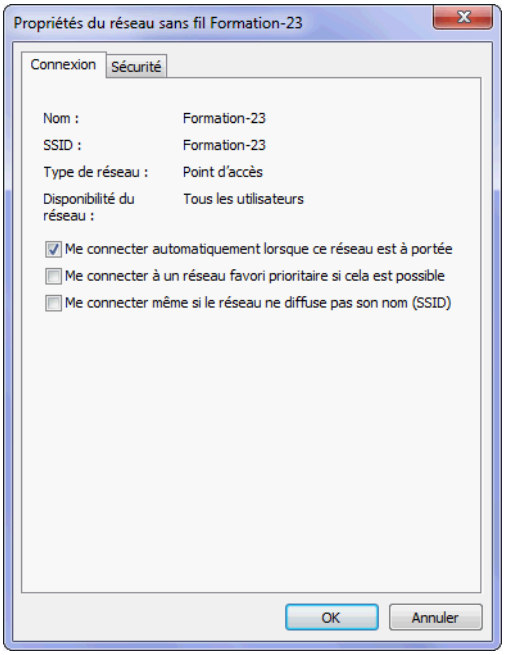


Figure 10–5 Fenêtre de configuration des propriétés du réseau Wi-Fi

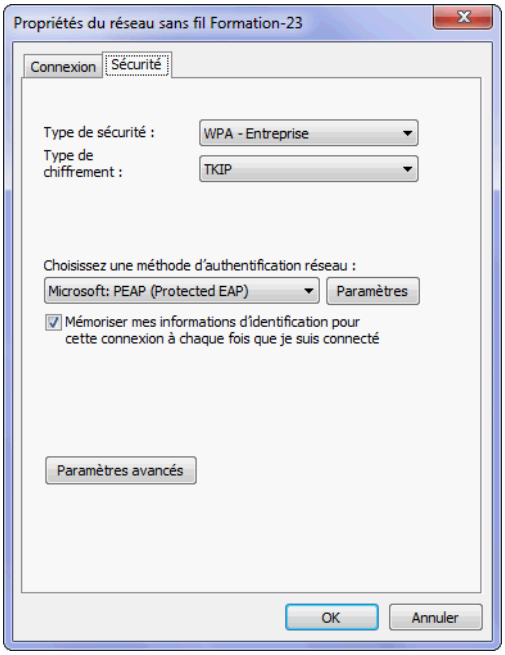


Figure 10–6 Paramètres de sécurité du réseau Wi-Fi

La configuration des options de sécurité du réseau sans fil se déroule dans l'onglet *Sécurité* de la fenêtre de propriétés. Le contenu de cet onglet change suivant le type de sécurité choisi. C'est dans cet onglet que vous pourrez saisir la clé de sécurité de votre réseau Wi-Fi.

Connexion à un réseau VPN

Infrastructure logique, un réseau privé virtuel (ou VPN pour *Virtual Private Network*) relie entre eux plusieurs réseaux locaux distants. Cette liaison s'effectue le plus souvent via le réseau Internet.

En pratique Connexion via modem analogique

Fortement utilisés il y a quelques années comme moyen d'accès à l'Internet bas débit, les modems analogiques sont aujourd'hui bien moins utilisés. Il est toutefois toujours possible d'établir une connexion à l'aide de votre modem. Pour vous connecter à l'aide de votre modem analogique, vous devez le raccorder à une prise téléphonique classique (c'est-à-dire une ligne France Télécom pour la France). En effet, si vous souhaitez établir une connexion via la ligne téléphonique associée à votre box ADSL, il est probable qu'il soit impossible d'établir la liaison. Généralement, les fournisseurs d'accès à Internet via une box ne garantissent pas le fonctionnement d'une connexion modem sur la ligne téléphonique associée à la box.

1. Ouvrez le *Centre Réseau et partage*, puis cliquez sur *Configurer une nouvelle connexion ou un nouveau réseau*.
2. Dans la fenêtre qui s'ouvre alors, choisissez *Configurer une connexion par modem à accès à distance*, afin d'ouvrir la fenêtre affichée ci-à la figure 10–7.
3. Indiquez le numéro de téléphone que vous a remis votre fournisseur de service. Le lien *Règles de numérotation* vous permet de définir des paramètres généraux de numérotation, notamment si vous devez utiliser un préfixe devant tous les numéros. Ceci est intéressant si vous êtes derrière un standard téléphonique d'entreprise et que vous devez composer le zéro avant tout appel vers l'extérieur.
4. Renseignez ensuite les informations de connexion également communiquées par votre fournisseur d'accès. En cochant la case *Mémoriser ce mot de passe*, vous n'aurez plus besoin de le saisir à chaque fois que vous utiliserez cette connexion.
5. Le champ *Nom de la connexion* vous permet de nommer cette connexion pour pouvoir la retrouver plus facilement par la suite.
6. Si vous êtes administrateur de la machine, vous pouvez rendre cette connexion disponible à tous les autres utilisateurs sans configuration supplémentaire en cochant simplement la case *Autoriser d'autres personnes à utiliser cette connexion*.
7. Cliquez sur le bouton *Connecter*. L'assistant tente alors d'établir la connexion. En cas d'échec, il vous en indique la cause et vous propose d'effectuer une nouvelle tentative de connexion. Si vous souhaitez simplement configurer la connexion mais ne pas l'utiliser immédiatement, indiquez-le en cliquant sur *Configurer quand même la connexion*.

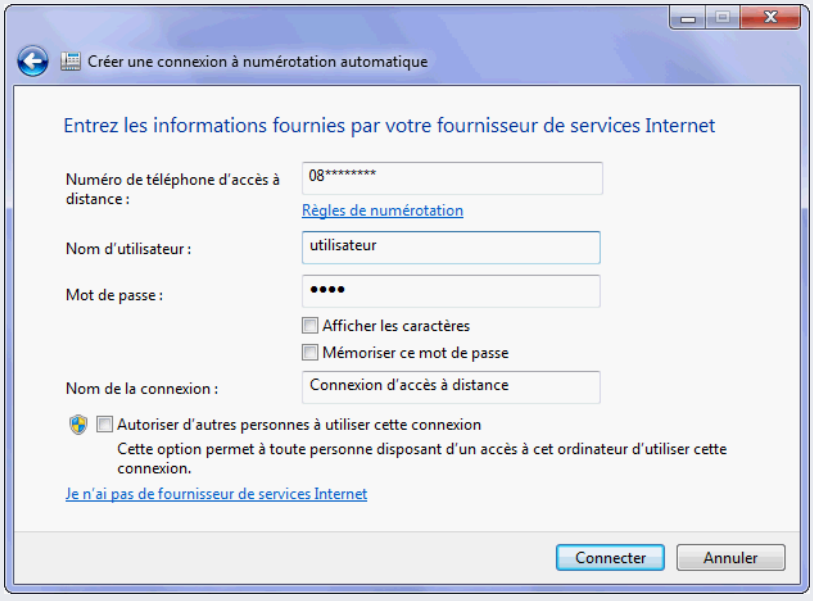


Figure 10–7 Informations de connexion via le modem

On utilise les VPN dans différents cas de figure : certaines entreprises permettent à leurs employés de connecter à distance leur ordinateur au réseau interne de l'entreprise ; les VPN sont parfois utilisés aussi pour se connecter à des proxys.

Dans Windows 7, la configuration d'un VPN est simple et rapide. Il suffit de connaître l'adresse du serveur VPN auquel vous souhaitez vous connecter et de posséder un compte utilisateur sur ce serveur. Ces prérequis remplis, voici comment vous connecter :

1 Cliquez sur l'icône réseau dans la barre de notification Windows (à côté de l'horloge), puis cliquez sur *Ouvrir le Centre Réseau et partage*.

2 Cliquez ensuite sur le lien *Configurer une nouvelle connexion ou un nouveau réseau*. La fenêtre représentée à la figure 10–8 s'affiche.

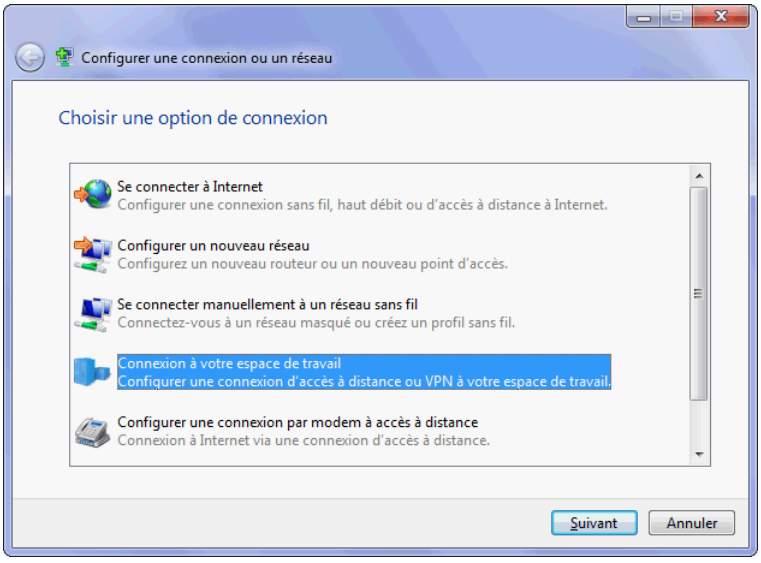


Figure 10–8
Choix du type de connexion à créer

3 Sélectionnez l'option *Connexion à votre espace de travail*.

4 L'assistant vous demande ensuite comment vous souhaitez vous connecter au réseau VPN. Dans la plupart des cas, choisissez *Utiliser ma connexion Internet*. L'assistant vous propose ensuite la fenêtre ci-dessous.

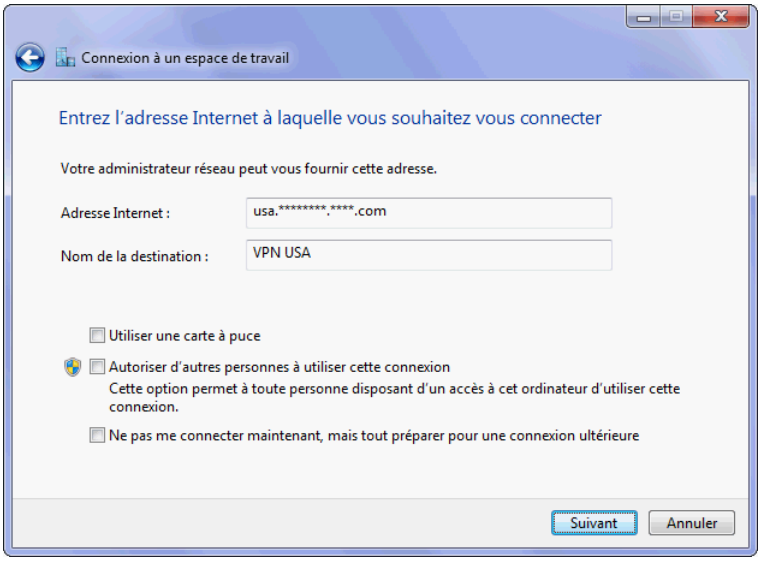


Figure 10–9
Informations de connexion au VPN

5 Indiquer l'adresse Internet du serveur VPN auquel vous souhaitez vous connecter. La zone *Nom de la destination* vous permet de donner à cette connexion un nom de votre choix.

6 Indiquez si cette connexion pourra être utilisée par d'autres utilisateurs de votre ordinateur en cochant la case *Autoriser d'autres personnes à utiliser cette connexion*.

7 Si vous désirez configurer des options avancées ou que vous ne souhaitez pas vous connecter immédiatement à la fin de l'assistant mais tout préparer pour une connexion ultérieure, cochez la case *Ne pas me connecter maintenant*.

8 Ces informations précisées, saisissez vos informations d'identification, ainsi que le domaine de connexion si le VPN auquel vous vous connectez en nécessite un. Choisissez *Mémoriser le mot de passe* pour ne pas avoir à le ressaisir à chaque connexion à ce VPN.

9 La configuration de base étant maintenant achevée, l'assistant vous connecte au réseau VPN.

BON À SAVOIR Vérifier la connexion

Une fois la connexion établie, vous pouvez vérifier son état en affichant la mini-fenêtre *Réseaux* en cliquant sur l'icône réseau dans la barre de notification Windows.

Figure 10–10
Établissement de la connexion au réseau VPN

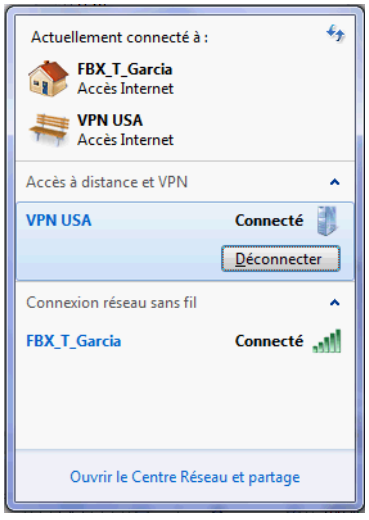


Figure 10–11
L'ordinateur est connecté à un point d'accès sans fil (FBX_T_Garcia) ainsi qu'au VPN configuré précédemment (VPN USA).

Figure 10–12
Réseau VPN configuré mais non connecté

BON À SAVOIR **Supprimer une connexion VPN**

1. Ouvrez le *Centre Réseau et partage*.
2. Dans la colonne de gauche, cliquez sur *Modifier les paramètres de la carte*.
3. Dans la liste qui s'affiche, vous trouvez les différentes connexions que vous avez créées.
4. Cliquez avec le bouton droit sur la connexion à supprimer, puis sélectionnez *Supprimer* dans le menu contextuel. Elle n'apparaîtra plus dans la liste des connexions réseau, ni dans la mini-fenêtre *Réseau*.

Toutes les connexions VPN que vous avez configurées restent accessibles dans la mini-fenêtre *Réseaux*, même si vous n'y êtes pas connecté. Ainsi, sur la figure 10–13, le réseau VPN est toujours visible bien que nous ne soyons plus connectés. Il suffit de double-cliquer sur son nom pour nous y connecter de nouveau.

Afficher l'état de la connexion

En vous intéressant à l'état de la connexion et à ses informations de statut, vous pouvez d'une part résoudre des problématiques de connexion, et d'autre part améliorer le fonctionnement de certains logiciels lorsque vous devez vérifier les adresses IP ou les protocoles utilisés.

Statut de la connexion

Si vous souhaitez avoir des détails sur une connexion établie à un moment donné :

1. Ouvrez la mini-fenêtre *Réseau* en cliquant sur l'icône réseau de la barre de notification (à coté de l'horloge).
2. Repérez votre connexion dans la liste (elle est normalement suivie de la mention *Connecté*) et effectuez un clic droit sur la ligne, puis choisissez *État* dans le menu déroulant. Vous accédez alors à la fenêtre représentée à la figure 10–13.

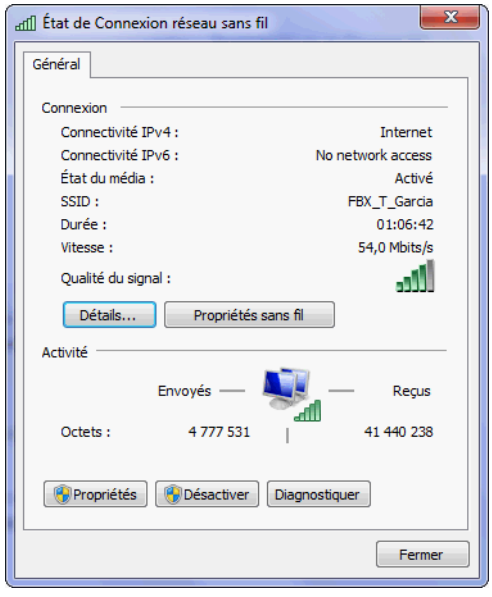


Figure 10–13
La fenêtre État d'une connexion indique si vous utilisez l'IPv4 ou l'IPv6, quel est l'accès dont vous disposez (réseau local uniquement ou accès à Internet), ainsi que la durée d'activité de la connexion.

Les différents boutons présents sur cette fenêtre donnent accès à plusieurs actions intéressantes :

- Le bouton *Détails...* permet de visualiser de nombreuses informations complémentaires sur la connexion : le nom de la carte réseau, son adresse physique (MAC), l'adresse IP de votre ordinateur sur le réseau et le masque de sous-réseau correspondant. Vous trouverez également ici l'adresse IP de la passerelle de votre réseau et du serveur DHCP, si vous en utilisez un. Vous verrez également les serveurs DNS utilisés avec cette connexion.
- Le bouton *Propriétés* donne accès à la fenêtre de propriétés de la carte.
- Le bouton *Désactiver* sert à désactiver la carte réseau en un clic.
- Le bouton *Diagnostiquer* démarre l'utilitaire de diagnostic réseau, si votre connexion ne fonctionne pas ou incorrectement. L'utilitaire analyse votre configuration à la recherche d'éventuels problèmes. S'il identifie un problème, il tente de le résoudre, par exemple, en réinitialisant la carte réseau.
- Dans le cas d'un réseau Wi-Fi, le nom du réseau (SSID), la vitesse de la liaison ainsi que la qualité du signal sans fil sont indiqués.

> **Attention**
> **Désactiver n'est pas déconnecter**
>
> Il ne faut pas utiliser le bouton *Désactiver* pour se déconnecter du réseau : désactiver une carte réseau équivaut à l'éteindre pour l'ordinateur.

En ligne de commande

Il est également possible d'obtenir rapidement toutes les informations sur les connexions établies via la ligne de commande :

1. Ouvrez une invite de commandes en saisissant `invite` dans le menu *Démarrer*.
2. Cliquez sur *Invite de commandes.*
3. Saisissez ensuite `ipconfig`, puis tapez sur la touche *Entrée*. Les informations principales concernant les connexions s'affichent.

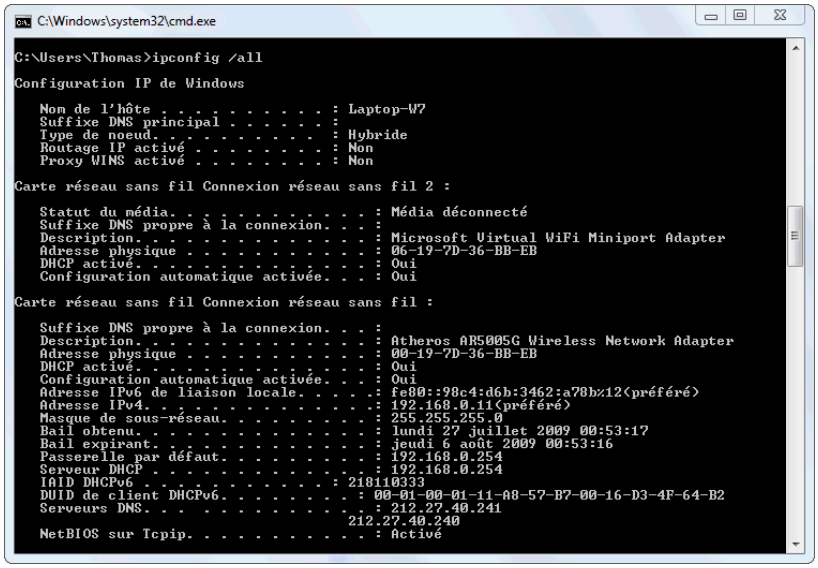


Figure 10–14
Résultat de la commande ipconfig/all

Pour visualiser des informations supplémentaires telles que l'adresse MAC de la carte réseau et les serveurs DNS utilisés, par exemple, saisissez la commande `ipconfig /all`.

Modifier les paramètres des cartes réseau

Les cartes réseau jouent un rôle essentiel dans la connexion aux différents réseaux car ce sont elles qui assurent la connexion physique au réseau.

Fenêtre Connexions réseau

Votre ordinateur est équipé d'une ou plusieurs cartes réseau. Un certain nombre de paramètres sont configurables pour chacune d'entre elles. Windows 7 vous permet d'afficher la liste des cartes réseaux installées sur votre ordinateur. À partir de cette liste, modifiez ensuite à votre guise un certain nombre de réglages sur les cartes.

1. Ouvrez le *Centre Réseau et partage*.
2. Cliquez dans la colonne de gauche sur le lien *Modifier les paramètres de la carte*.
3. Windows affiche alors la liste des connexions réseau de l'ordinateur. Les connexions représentées dans la liste sont soit des cartes physiques (carte Ethernet, carte Wi-Fi...), soit des connexions logiques (connexion VPN).

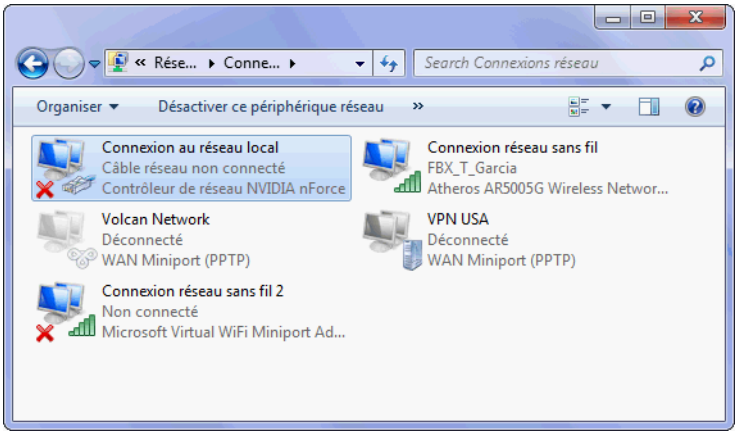


Figure 10–15
Liste des connexions

Chaque connexion est représentée par une icône et est accompagnée par 3 lignes de description :

- La première information est le nom de la connexion.

EN PRATIQUE Renommer une connexion

Les connexions portent des noms logiques par défaut : *Connexion au réseau local* pour une carte Ethernet et *Connexion réseau sans fil* pour une carte Wi-Fi. Si vous souhaitez renommer une connexion, cliquez avec le bouton droit sur l'une des connexions, puis choisissez *Renommer* dans le menu déroulant.
Pour aller encore plus vite, appuyez sur la touche *F2* après avoir sélectionné la connexion à renommer.

- Sous le nom logique du réseau, la ligne suivante indique l'état de la connexion. C'est ici que vous pourrez détecter si le câble est débranché (pour une connexion Ethernet) ou si le réseau est connecté. Dans le cas d'une carte Wi-Fi, le nom du réseau (SSID) auquel la carte est connectée s'affiche (ici, *FBX_T_Garcia*).
- Enfin, la troisième ligne indique le nom du périphérique physique. Ce nom inclut généralement le nom du constructeur et parfois le modèle de la carte.

Il est possible d'activer ou de désactiver une interface réseau directement depuis cette fenêtre. Pour cela, cliquez avec le bouton droit sur la connexion de votre choix, puis sur *Activer* ou sur *Désactiver*.

RAPPEL

Lorsque vous désactivez une carte réseau, Windows 7 la considère comme éteinte et n'établit plus de connexions sur cette carte. Pour vous en servir à nouveau, vous devez l'activer.

Propriétés de la carte réseau

L'accès aux propriétés d'une carte réseau se fait à partir de la fenêtre *Connexions Réseau* que nous venons de voir :

1 Cliquez avec le bouton droit sur le nom de votre carte réseau, puis choisissez *Propriétés* dans le menu contextuel.

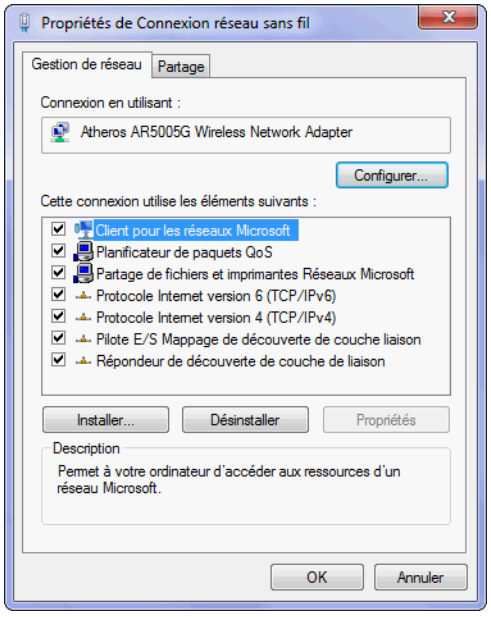


Figure 10–16
Propriétés d'une carte réseau

2 La fenêtre de propriétés affiche le nom du périphérique réseau utilisé. Vous accédez au paramétrage avancé du périphérique en cliquant sur le bouton *Configurer...*. Vous obtenez alors la même fenêtre que si vous étiez passé par le gestionnaire de périphériques.

COMPRENDRE Fonctionnalités réseau de la connexion

Un élément de type *Client* donne accès à des ordinateurs et fichiers sur le réseau. Par exemple, client pour les réseaux Microsoft.
Un élément de type *Service* sert à ajouter des fonctionnalités supplémentaires au réseau. Citons comme exemple le partage de fichiers et imprimantes réseau Microsoft.
Un élément de type *Protocole* permet de prendre en charge un protocole sur le réseau, comme le protocole Internet version 4 (TCP/IPv4).

3 La fenêtre dresse la liste des fonctionnalités réseau utilisées par la connexion. Ces éléments peuvent être de type *Client*, *Service* ou *Protocole*.

Vous avez la possibilité d'installer ou de désinstaller des fonctionnalités à l'aide des boutons situés au bas de la liste. Certains éléments de la liste, par exemple les protocoles IPv4 et IPv6, disposent de propriétés supplémentaires, notamment pour configurer l'adresse IP de votre ordinateur. Ces options sont décrites à la section suivante.

Le deuxième onglet de cette fenêtre est dédié aux options de partage de la carte réseau. Si votre ordinateur dispose de plusieurs cartes réseau, vous pouvez partager une connexion Internet avec d'autres périphériques du réseau en cochant la case *Autoriser d'autres utilisateurs du réseau à utiliser la connexion Internet de cet ordinateur*. N'oubliez pas alors d'indiquer l'interface réseau sur laquelle se connecteront les ordinateurs du réseau local souhaitant accéder à Internet via la carte réseau dont vous modifiez les paramètres.

Modifier les options d'adresse IP

RAPPEL Adresse IP

L'adresse IP est une suite de chiffres qui identifie de manière unique votre ordinateur sur un réseau. La version la plus couramment utilisée jusqu'à présent est la version 5. Elle se compose de 4 chiffres compris entre 1 et 254, séparés par des points (par exemple, 192.168.0.10). Toutefois, en raison du risque de pénurie d'adresses dans les prochaines années, la version 6 du protocole IP a été mise au point et de nouvelles adresses, composées désormais de caractères hexadécimaux, ont fait leur apparition. Toutefois, peu de réseaux implémentent IPv6 aujourd'hui.
Pour se connecter à un réseau local ou à Internet, tout ordinateur doit donc posséder une adresse IP. Cette adresse est définie soit manuellement en la saisissant dans les propriétés de la carte réseau, soit attribuée automatiquement par un serveur DHCP. Rappelons qu'un serveur DHCP est un équipement réseau qui attribue automatiquement une adresse IP unique à tout ordinateur souhaitant se connecter au réseau.

Intéressons-nous à présent au paramétrage IP d'une carte réseau. En règle générale, cette action n'est pas nécessaire pour la plupart des réseaux, puisque la majorité des réseaux domestiques et d'entreprise sont configurés automatiquement par DHCP.

Vous pouvez être amené à modifier les paramètres IP si vous utilisez un adressage IP statique dans votre réseau et que vous souhaitez définir manuellement les adresses IP. Voyons la procédure à suivre pour effectuer ce paramétrage :

1 Ouvrez le *Centre Réseau et partage*.
2 Dans la colonne de gauche, cliquez sur *Modifier les paramètres de la carte*.
3 Cliquez avec le bouton droit sur la carte réseau que vous souhaitez configurer, puis choisissez *Propriétés* dans le menu contextuel.
4 Dans la liste des fonctionnalités installées, cliquez sur le protocole dont vous voulez gérer l'adresse (IPv4 ou IPv6), puis cliquez sur le bouton *Propriétés* au bas de la liste.

Dans la fenêtre de propriétés d'IPv4, vous pouvez choisir la configuration automatique de l'adresse IP (si vous disposez d'un serveur DHCP sur votre réseau) ou bien la configuration manuelle de l'adresse.

Si vous choisissez d'obtenir une adresse IP automatiquement, un onglet *Configuration alternative* s'affichera. Définissez dans celui-ci une configuration IP fixe qui sera utilisée si le serveur DHCP est injoignable.

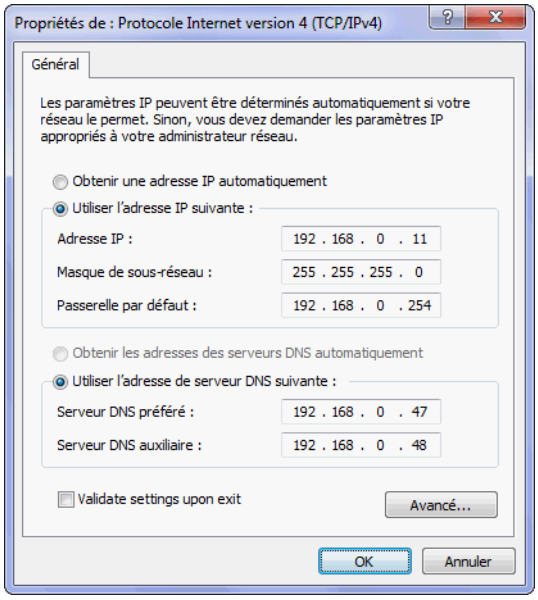


Figure 10–17
Configuration d'adresse IPv4 pour une connexion

Le bouton *Avancé...* permet de définir des paramètres supplémentaires. Vous pouvez notamment définir plusieurs adresses IP pour la même connexion (uniquement si vous n'utilisez pas la configuration automatique de l'adresse IP), vous pouvez également indiquer plusieurs passerelles et d'autres serveurs DNS. Si nécessaire, il est possible de définir les adresses des serveurs WINS et de configurer les options LMHOSTS et NetBIOS.

Modifier les paramètres de partage

Lorsque votre ordinateur est connecté à un réseau, il est intéressant de définir son comportement vis-à-vis des autres machines du réseau. Ainsi, vous pouvez paramétrer les différentes options pour rendre visibles ou non les ressources de votre ordinateur.

Pour définir la façon dont vous souhaitez que votre ordinateur apparaisse sur le réseau ainsi que les ressources que vous partagez, vous devez vous rendre dans le centre réseau et partage. Dans la colonne de gauche, cliquez sur le lien *Modifier les paramètres de partage avancés*. Cet écran vous permet de définir les options de partage réseau de votre ordinateur.

Vous pouvez définir des paramètres distincts suivants si vous êtes raccordés à un réseau de type public ou un réseau privé (« résidentiel ou professionnel »). Windows 7 vous indique le type de réseau auquel vous êtes connecté actuellement en affichant la mention *(profil actuel)* en face du paragraphe correspondant.

ATTENTION **Invisible ? Pas tout à fait...**

Lorsque vous désactivez l'option *Découverte du réseau*, votre ordinateur n'est plus visible dans l'explorateur des autres machines du réseau. Cependant, cela ne signifie pas que vous êtes complètement anonyme. En effet, vous restez détectable par tout utilitaire de monitoring du réseau de type WireShark.

Découverte du réseau

Cette fonctionnalité permet à votre ordinateur d'apparaître aux yeux des autres ordinateurs du réseau et permet réciproquement de visualiser la liste des matériels connectés au réseau.

Si vous activez cette option, vous pourrez visualiser la liste des machines connectées au réseau via l'explorateur Windows sous *Réseau*. En double-cliquant sur l'une des machines, vous verrez la liste des ressources qu'elle partage.

Partage de fichiers et d'imprimantes

Comme son nom l'indique, cette option permet de configurer Windows 7 pour qu'il autorise le partage de fichiers et d'imprimantes avec les autres ordinateurs du réseau. Lorsque vous désactivez cette option, l'accès aux dossiers et imprimantes partagés de votre ordinateur devient impossible depuis tous les autres ordinateurs du réseau.

Partage de dossiers publics

Si vous ne voulez pas perdre de temps à définir des options de partage pour les dossiers que vous souhaitez rendre accessibles sur le réseau, vous pouvez choisir d'activer l'option de partage des dossiers publics. Lorsque cette option est activée, tout le monde sur le réseau peut lire et écrire dans vos dossiers publics. Si cette option est désactivée, seuls les utilisateurs disposant d'un compte sur la machine pourront accéder aux dossiers publics.

Les dossiers publics sont intégrés par défaut aux bibliothèques de Windows. Par exemple, la bibliothèque `Documents` combine les fichiers de votre dossier `Document` ainsi que ceux contenus dans le dossier `Documents publics`. Les dossiers publics sont stockés sur le disque dur système dans `\Users\Public`.

SÉCURITÉ **Contenu**

Vous ne pouvez pas utiliser la diffusion de contenu multimédia sur des réseaux de type public pour des raisons évidentes de sécurité.

Diffusion de contenu multimédia

Lorsque votre ordinateur est connecté à un réseau domestique, vous pouvez utiliser le Lecteur Windows Media comme serveur de diffusion (*streaming*) de fichiers multimédias tels que les photos, musiques ou vidéos.

Pour activer cette option, cliquez sur le lien *Choisir les options de diffusion du contenu multimédia*. Cliquez ensuite sur le bouton *Autoriser la diffusion multimédia en continu*. Vous accéderez alors à un écran vous permettant de personnaliser la diffusion en choisissant le contenu à diffuser. Pour désactiver cette option, cliquez sur le bouton *Bloquer tout*, puis sur *OK*.

Des options supplémentaires sont disponibles dans le Lecteur Windows Media via le menu *Diffuser en continu* présent sur la barre de menus située en haut de la fenêtre.

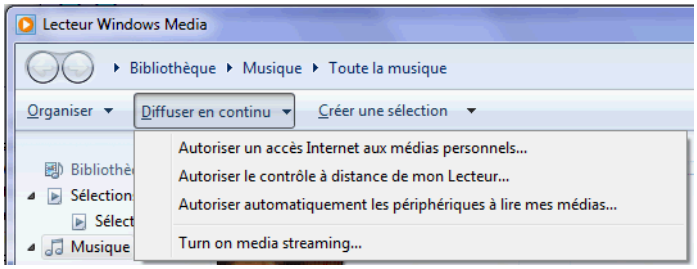


Figure 10–18
Options de diffusion multimédia dans le Lecteur Windows Media

Sécurité des connexions de partage de fichiers

Windows 7 vous permet de chiffrer les connexions établies lors de l'accès à des fichiers partagés. Windows active donc par défaut une protection 128 bits. Cependant, certains périphériques réseau ne sont pas capables de prendre en charge ce type de chiffrement. Vous devrez alors choisir l'option de chiffrage en 40 ou 56 bits.

Partage protégé par mot de passe

Lorsque vous activez cette option, seuls les utilisateurs disposant d'un compte sur l'ordinateur pourront accéder aux fichiers et imprimantes partagés. Si vous souhaitez que d'autres personnes puissent accéder à ces ressources, vous devrez désactiver cette option.

Voir les ordinateurs du réseau

Pour voir la liste des ordinateurs de votre réseau, il suffit d'ouvrir l'explorateur Windows, puis de cliquer sur *Réseau* dans la colonne de gauche. La liste des machines connectées au réseau diffusant leur nom s'affiche alors. Double-cliquez sur l'une d'entre elles pour accéder aux ressources (dossiers ou imprimantes) qu'elle partage.

Parmi les ressources les plus partagées, on trouve les imprimantes. Si vous souhaitez installer une imprimante partagée, il suffit de double-cliquer sur son nom dans la liste des ressources partagées de l'ordinateur distant.

Suivant la façon dont la machine a été configurée, il se peut que vous deviez vous identifier lorsque vous essayez d'accéder à l'ordinateur distant. Vous devez alors disposer d'un compte utilisateur sur la machine à laquelle vous accédez.

Le groupe résidentiel d'ordinateurs

Une nouvelle fonctionnalité est apparue dans Windows 7 pour partager plus facilement documents, imprimantes ou fichiers multimédias.

Créer un groupe résidentiel

SÉCURITÉ Mot de passe du groupe résidentiel

Le groupe résidentiel est protégé par un mot de passe. Ainsi, seules les machines que vous spécifiez ont le droit d'y accéder. Soulignons que ce mot de passe peut être changé à tout moment.

Un groupe résidentiel réunit un ensemble d'ordinateurs. Pour constituer un groupe résidentiel, la première manipulation consiste à créer le groupe sur un unique ordinateur. Ensuite, les autres ordinateurs viendront se joindre au groupe créé. Voici les différentes étapes à suivre pour créer le groupe :

1. Ouvrez l'explorateur Windows, puis cliquez sur *Groupe résidentiel d'ordinateurs* dans la colonne de gauche.
2. Cliquez sur le bouton *Créer un groupe résidentiel*. L'assistant vous demande quelles bibliothèques vous souhaitez partager avec le groupe. Cochez les cases de votre choix, puis cliquez sur *Suivant*.

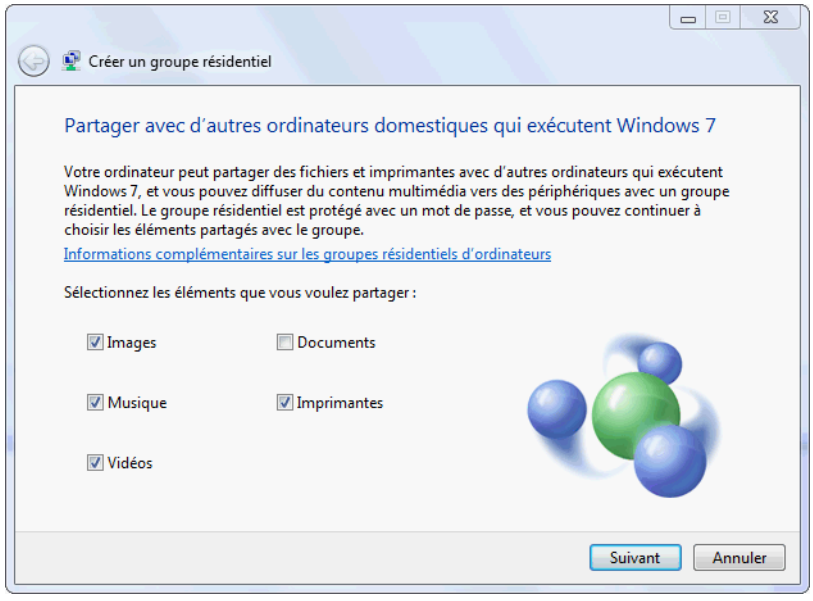


Figure 10–19
Choix des éléments à partager avec le groupe résidentiel

3. Une fois que vous avez sélectionné les éléments à partager, le groupe résidentiel est créé. Windows 7 fournit le mot de passe du groupe.
4. La configuration du groupe étant effectuée sur votre ordinateur, cliquez sur le bouton *Terminer*.

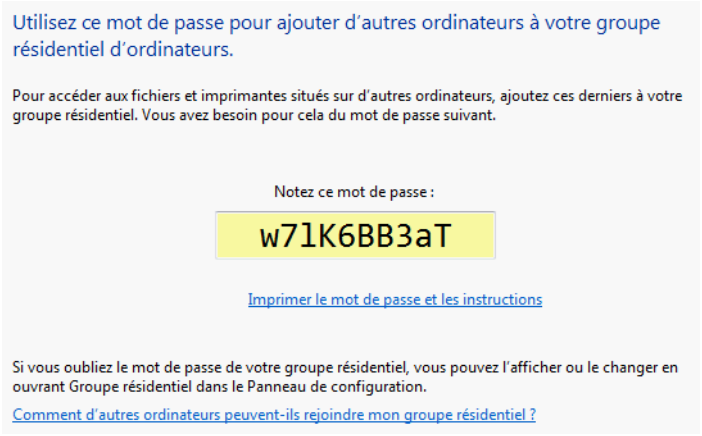


Figure 10–20
Ce mot de passe vous permettra d'ajouter d'autres ordinateurs à ce groupe résidentiel. Notez-le ou imprimez-le en cliquant sur Imprimer le mot de passe et les instructions.

5 Rendez-vous à présent sur les autres ordinateurs de votre réseau pour leur faire rejoindre ce groupe résidentiel. Pour cela, suivez la procédure indiquée à la section suivante.

Rejoindre un groupe résidentiel existant

Si vous avez déjà créé un groupe résidentiel sur un autre ordinateur et que vous souhaitez rejoindre ce groupe, les étapes à suivre sont les suivantes :

1 Ouvrez le menu *Démarrer*, puis cliquez sur *Panneau de configuration*.
2 Sous *Réseau et Internet*, cliquez sur le lien *Choisir les options du groupe résidentiel et de partage*.
3 Cliquez ensuite sur *Rejoindre*, puis suivez les instructions pour entrer le mot de passe du groupe. L'ordinateur fait maintenant partie du groupe résidentiel.

EN PRATIQUE Ordinateurs sous Windows 7 uniquement

Cela peut sembler une évidence, mais soulignons que seuls les ordinateurs sous Windows 7 peuvent profiter des fonctionnalités qu'apporte le groupe résidentiel.

Modifier les paramètres du groupe résidentiel

Si vous souhaitez modifier les ressources partagées dans votre groupe résidentiel, qu'il s'agisse d'activer ou de désactiver les fonctions de diffusion multimédia ou de modifier le mot de passe du groupe résidentiel, vous devez en modifier les paramètres. Voici comment procéder :

1 Ouvrez l'explorateur Windows, puis choisissez *Groupe résidentiel d'ordinateurs* dans la colonne de gauche.
2 Cliquez ensuite sur *Modifier les paramètres du groupe résidentiel*.
3 La fenêtre présentée à la figure 10–21 s'ouvre. Modifiez-y les éléments que vous souhaitez partager ou non avec votre groupe résidentiel.

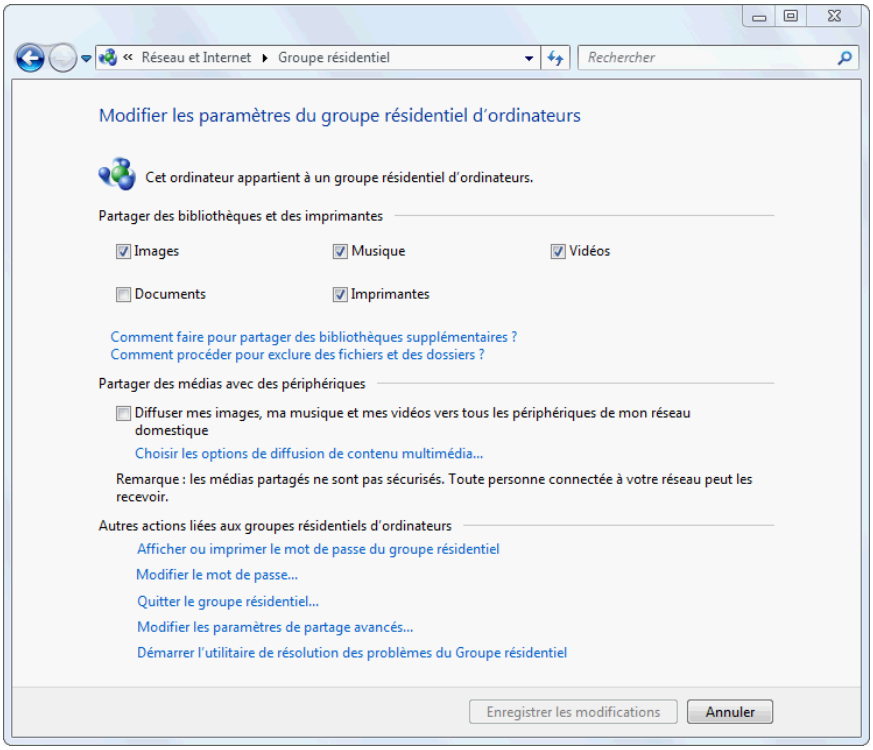


Figure 10–21
Fenêtre de modification des paramètres du groupe résidentiel. Seules les bibliothèques principales et les imprimantes sont visibles.

PRÉCISION Paramètres du dossier à partager

Il est possible de partager le dossier en lecture seule ou en lecture/écriture.

OPTION Fichiers multimédias

Si vous souhaitez partager des fichiers multimédias avec le groupe résidentiel, cochez la case *Diffuser mes images, ma musique et mes vidéos vers tous les périphériques de mon réseau domestique*.

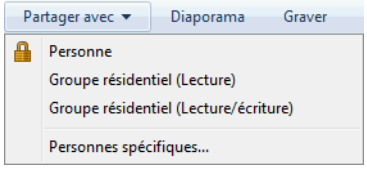


Figure 10–22
Partage d'un dossier du disque dur avec le groupe résidentiel

4 Pour partager d'autres dossiers du disque dur, rendez-vous dans le dossier que vous souhaitez partager, puis cliquez sur le bouton *Partager avec...*

En bas de la fenêtre se trouve un ensemble de liens. Ils vous permettent d'effectuer des actions supplémentaires sur votre groupe résidentiel :

- Vous pouvez ainsi afficher le mot de passe du groupe résidentiel et imprimer les instructions pour rejoindre le groupe. Cliquez sur le lien *Afficher ou imprimer le mot de passe du groupe résidentiel* si vous souhaitez ajouter un nouvel ordinateur à votre groupe.
- Pour modifier le mot de passe du groupe, cliquez sur le lien *Modifier le mot de passe...* Si vous changez le mot de passe, vous devrez aussi le changer sur toutes les autres machines appartenant au groupe résidentiel.
- Grâce au lien *Quitter le groupe résidentiel...*, vous retirez immédiatement un ordinateur du groupe. Vous pourrez le reconnecter de nouveau en indiquant le bon mot de passe.
- Si vous souhaitez accéder directement aux paramètres avancés de partage que nous avons présentés précédemment, cliquez sur le lien *Modifier les paramètres de partage avancés...*

- Un utilitaire de résolution de problèmes est à votre disposition si vous rencontrez des dysfonctionnements dans votre groupe résidentiel. Pour y accéder, cliquez sur le lien *Démarrer l'utilitaire de résolution des problèmes du groupe résidentiel*.

EN PRATIQUE Lancer le diagnostic de l'utilitaire de résolution des problèmes du groupe résidentiel

1. Cliquez sur le lien *Démarrer l'utilitaire de résolution des problèmes du groupe résidentiel*.
2. Cliquez sur le bouton *Suivant*. L'assistant de résolution de problèmes analyse alors la configuration de votre réseau.
3. Il vérifie ensuite les paramètres du groupe résidentiel. S'il détecte un problème ou une incohérence durant le processus, l'assistant vous propose une solution.

En résumé

Dans ce chapitre, nous avons appris à établir une connexion réseau que ce soit à un réseau sans fil ou à un VPN. Vous savez également modifier les paramètres des cartes réseau et afficher l'état de la connexion sur chacune d'elles.

Nous nous sommes également penchés sur le partage simplifié de fichiers et d'imprimantes à l'aide de la fonctionnalité groupe résidentiel intégrée à Windows 7. Nous approfondirons le partage de fichiers et d'imprimantes à la section « Partage de dossiers sur le réseau » et « Partage d'imprimantes » du chapitre suivant.

chapitre 11

Sécurité des fichiers et partage de ressources

La sécurité des fichiers est un sujet sensible dans l'informatique moderne. Chaque utilisateur souhaite conserver de manière privée ses informations personnelles. Cependant, il arrive que certaines informations aient besoin d'être partagées, que ce soit pour diffuser des photos sur le réseau domestique ou bien travailler sur des documents communs.

SOMMAIRE

- Gestion des autorisations des fichiers
- Partage de fichiers sur le réseau
- Partage d'imprimantes

MOTS-CLÉS

- Autorisations NTFS
- Permissions
- Dossiers et fichiers partagés
- Partage
- Serveur d'impression
- Imprimante partagée

Ce chapitre décrit les mécanismes de sécurité intégrés au système de fichiers NTFS sur lequel est basé Windows 7, notamment l'attribution de droits sur les fichiers et les répertoires. Ce chapitre aborde également le partage de fichiers, de dossiers et d'imprimantes sur le réseau.

Les autorisations NTFS

Le système de fichiers NTFS, utilisé par Windows 7, intègre un mécanisme de sécurité au niveau des fichiers. Ce mécanisme est appelé ACL (*Access Control List*) c'est-à-dire liste de contrôle d'accès en français. Cette liste permet de déterminer les actions que les utilisateurs ont le droit d'effectuer sur chaque fichier et répertoire.

Tableau 11–1 Détail des autorisations disponibles

Libellé	Explication
Parcours d'un dossier	Autorise ou non à afficher le contenu du répertoire pour accéder à un fichier ou un sous-répertoire.
Liste du dossier	Donne l'autorisation de visualiser le contenu d'un dossier
Lecture des attributs	Permet de consulter les attributs du fichier ou du répertoire. Ces attributs sont définis par le système de fichiers NTFS (exemple : lecture seule, archive...).
Lecture des attributs étendus	Ces attributs sont définis par des logiciels : tags sur une photo, information sur l'artiste, l'album, la durée etc. à propos d'un fichier musical, etc.
Création de fichier *Écriture de données*	Permet d'ajouter des éléments dans un répertoire (pour les répertoires uniquement) et de modifier le contenu d'un fichier ou écraser le contenu existant (pour les fichiers uniquement).
Création de dossier *Ajout de données*	Sert à créer un dossier à l'intérieur d'un répertoire. Autorise l'ajout de données à la suite du contenu d'un fichier existant.
Écriture d'attributs	Autorise ou non la modification des attributs NTFS d'un élément.
Écriture d'attributs étendus	Permet ou non de modifier les attributs étendus d'un fichier ou d'un répertoire.
Suppression	Donne le droit de supprimer l'élément.
Lire les autorisations	Permet de visualiser les paramètres de sécurité (détail de l'ACL pour un fichier ou un répertoire).
Modifier les autorisations	Donne l'autorisation de modifier les paramètres de sécurité d'un élément.
Appropriation	Donne le droit de modifier le propriétaire de l'élément.

ATTENTION **Droits de l'utilisateur Système**

Ne modifiez pas les autorisations associées à l'utilisateur *Système* : en cas de mauvaise manipulation, cela vous empêcherait totalement d'accéder aux éléments via l'explorateur.

Les droits d'accès s'appliquent soit à tous les utilisateurs de l'ordinateur (*Tout le monde*), soit à un groupe utilisateur (par exemple, *Administrateurs*), soit à un utilisateur en particulier. Vous pouvez rencontrer des noms d'utilisateurs particuliers comme *Système* qui représente Windows lui-même ou *Propriétaire* qui représente le propriétaire de l'élément.

Les autorisations NTFS sont gérées de manière hiérarchique. Vous pouvez ainsi choisir d'hériter les paramètres d'autorisation du dossier parent ou encore d'appliquer les permissions définies pour le dossier

courant à tous ses sous-dossiers. De même, lorsque vous créez des fichiers ou des dossiers, les autorisations de l'objet nouvellement créé seront héritées du dossier parent.

Modifier les autorisations standards

La gestion des autorisations NTFS s'effectue dans la fenêtre de propriétés du fichier ou du dossier. Pour y accéder :

1. Cliquez avec le bouton droit sur l'élément de votre choix.
2. Cliquez sur *Propriétés* dans le menu contextuel.
3. Sélectionnez l'onglet *Sécurité*.

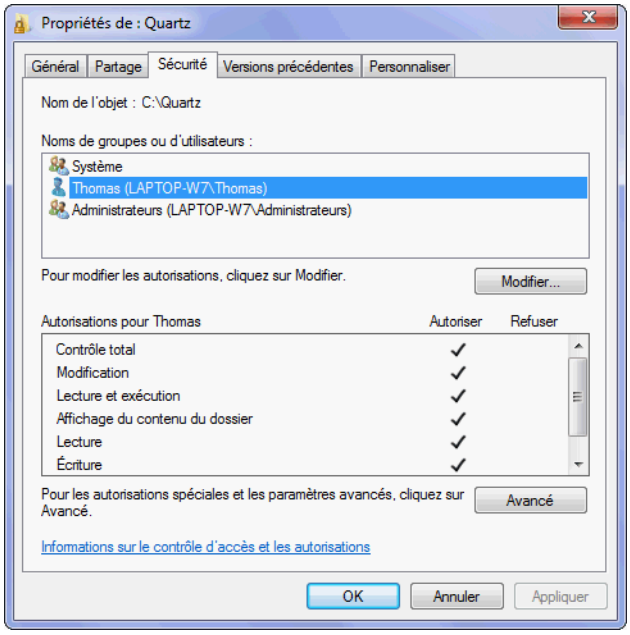


Figure 11–1
Onglet Sécurité des permissions d'un dossier

Dans la partie supérieure de la fenêtre, vous trouvez la liste des utilisateurs ou des groupes utilisateur pour lesquels des droits ont été définis. Les groupes sont signalés par une icône représentant deux personnages alors qu'un simple utilisateur est indiqué par un seul personnage. En sélectionnant un utilisateur ou un groupe, vous accédez à la partie inférieure de la fenêtre qui liste les autorisations standards attribuées ou prohibées.

Cette première fenêtre est en lecture seule et n'est donc accessible qu'en consultation. Pour apporter des changements aux autorisations, cliquez sur le bouton *Modifier...* Si ce bouton n'est pas affiché, c'est parce que vous ne disposez pas de permissions suffisantes pour modifier cet objet. Si vous êtes administrateur, définissez-vous comme propriétaire de l'élé-

ATTENTION Chaque utilisateur est unique

Les ACL de NTFS sont gérés à l'aide du SID (*Security IDenfifier*) de l'utilisateur. Le SID est un identifiant unique utilisé par Windows pour désigner les utilisateurs de la machine. Ces SID sont différents d'une installation de Windows à une autre. C'est pourquoi, si vous définissez des propriétés de sécurité de fichiers pour un utilisateur appelé « Thomas » dans une installation de Windows, un utilisateur appelé « Thomas » mais sur une autre installation de Windows ne sera pas reconnu au niveau de ces fichiers, car les SID seront différents. Les SID sont également utilisés dans la base de registre pour désigner les utilisateurs.

ment pour pouvoir modifier ses propriétés (reportez-vous à la section « Modifier le propriétaire d'un dossier ou d'un fichier » de ce chapitre).

La fenêtre de modification est organisée de la même façon que précédemment : les utilisateurs en haut et les droits en bas de la fenêtre.

Dans la partie supérieure, vous avez la possibilité d'ajouter ou de supprimer des éléments. Lorsque vous ajoutez un utilisateur ou un groupe, la fenêtre représentée sur la figure 11–2 s'ouvre.

Figure 11–2
Sélection d'utilisateur ou de groupe

Dans la zone de texte, saisissez un nom d'utilisateur ou de groupe utilisateur. Ce nom doit être « exact » et correspondre au nom précis d'un profil utilisateur existant pour être reconnu, mais la casse (minuscule/majuscule) n'a pas besoin d'être exacte. Vous pouvez entrer plusieurs noms en les séparant par un point-virgule. Une fois votre saisie effectuée, cliquez sur le bouton *Vérifier les noms*. Windows vérifie alors l'existence des noms que vous avez saisis et ajoute le domaine devant les noms (pour les utilisateurs locaux, c'est le nom de l'ordinateur qui est ajouté avant le nom de l'utilisateur).

Une fois que vous avez ajouté les utilisateurs de votre choix, cliquez sur l'un des utilisateurs dans la liste, puis définissez ses droits dans la partie inférieure de la fenêtre intitulée *Autorisations pour <nom-de-l'utilisateur>*. Cochez les cases appropriées pour lui accorder ou lui refuser chacune des autorisations.

Lorsque vous autorisez ou refusez la permission *Contrôle total*, toutes les autres autorisations prennent la même valeur. La case *Autorisations spéciales* désigne des privilèges avancés qui sont accessibles via une autre fenêtre que nous allons aborder dans le paragraphe suivant.

ASTUCE Effectuer une recherche de nom d'utilisateur

Si vous ne savez pas exactement quels sont les noms d'utilisateurs ou de groupes disponibles, Windows propose un outil de recherche d'utilisateur. Pour y accéder, suivez la procédure suivante :

1. Cliquez sur le bouton *Avancé...* Vous accédez alors à une fenêtre de recherche.
2. Cliquez sur le bouton *Rechercher* pour visualiser les choix possibles. Une liste d'utilisateurs et de groupes disponibles s'affiche en bas de la fenêtre.
3. Effectuez votre sélection (utiliser la touche *Ctrl* pour sélectionner plusieurs lignes), puis cliquez sur *OK*. Les éléments choisis sont alors ajoutés à la zone de texte.
4. Cliquez sur *OK* pour valider la liste des utilisateurs à ajouter à la liste de contrôle d'accès.

Modifier les paramètres d'autorisation avancés

L'onglet *Sécurité* de la fenêtre de propriétés des fichiers ne propose pas de définir avec précision toutes les autorisations NTFS possibles. Pour accéder à plus d'options, cliquez sur le bouton *Avancé* à partir de l'onglet *Sécurité*.

L'onglet *Autorisations* dresse la liste des utilisateurs et de leurs droits sur le fichier ou le répertoire. Cette fenêtre est en lecture seule par défaut. Pour visualiser les autorisations plus en détail, double-cliquez sur l'une des lignes. La colonne *Héritée de* vous indique si l'autorisation est définie au niveau de l'élément ou si elle a été définie dans un dossier parent.

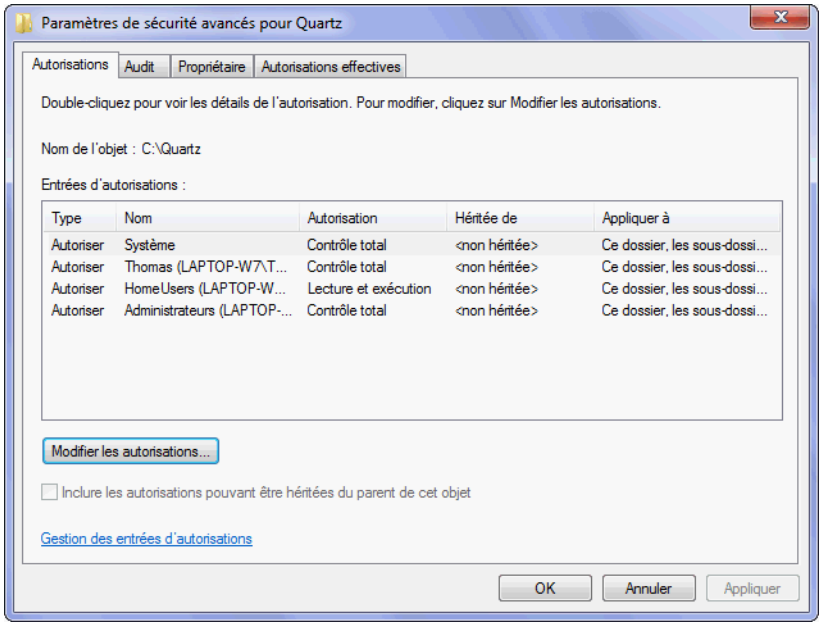


Figure 11–3
Fenêtre dressant la liste des autorisations pour un répertoire

Si vous désirez modifier les autorisations, cliquez sur le bouton *Modifier les autorisations...* présent au bas de la liste. Vous avez la possibilité de gérer les autorisations à l'aide des boutons *Ajouter*, *Modifier* et *Supprimer*.

Si vous voulez définir les mêmes autorisations que le dossier parent, cochez la case *Inclure les autorisations pouvant être héritées du parent de cet objet*. En activant cette option, vous aurez bien sûr la possibilité de définir des autorisations supplémentaires spécifiques à l'objet courant.

Pour que les permissions que vous avez définies pour un dossier soient également appliquées à ses fichiers et sous-dossiers, cochez la case *Remplacer toutes les autorisations des objets enfants par des autorisations pouvant être héritées de cet objet*.

Pour définir des permissions pour un utilisateur qui n'est pas encore présent dans la liste, cliquez sur le bouton *Ajouter...* Vous devez ensuite indiquer à quel utilisateur ou groupe utilisateur va s'appliquer la règle d'autorisation. Saisissez le nom exact ou utilisez le bouton *Avancé* pour rechercher des utilisateurs ou groupes. Validez ensuite votre saisie par le bouton *OK*.

ATTENTION Utilisateur non présent

Vous ne pouvez saisir qu'un seul nom d'utilisateur ou de groupe à la fois. Si vous souhaitez définir des autorisations similaires pour plusieurs utilisateurs, vous devrez ajouter une ligne pour chaque utilisateur.

Pour chacune des permissions NTFS, vous pouvez choisir de l'accorder ou non. Si vous optez pour l'autorisation *Contrôle total*, toutes les cases de la colonne seront alors sélectionnées automatiquement. Si vous désirez décocher toutes les cases de la fenêtre, utilisez le bouton *Effacer tout* présent au bas de la liste.

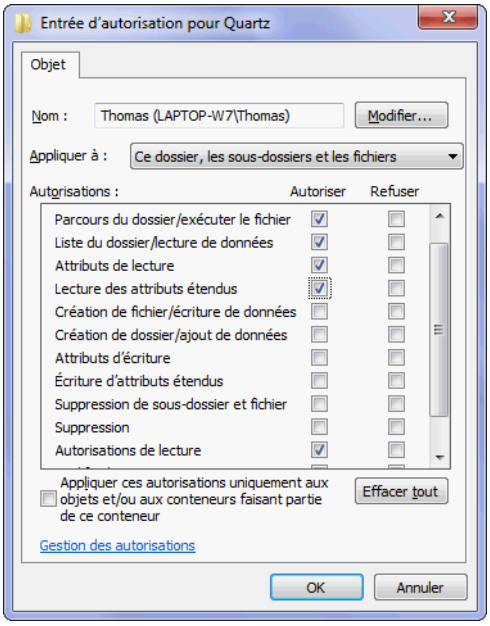


Figure 11–4
Détails d'autorisations pour un utilisateur sur un dossier

Modifier le propriétaire d'un fichier ou d'un dossier

Dans le système de fichiers NTFS, chaque fichier ou répertoire a un propriétaire. Le propriétaire peut définir les permissions sur cet objet et choisir quels utilisateurs y ont accès. Il pourra toujours modifier les permissions sur un objet, même si celles-ci sont définies pour lui refuser tout accès.

Par défaut, le propriétaire est l'utilisateur qui a créé l'objet. Il peut être modifié soit par un administrateur, soit par un utilisateur possédant le privilège NTFS Appropriation sur l'élément (par défaut, les utilisateurs du groupe *Administrateurs* disposent de ce privilège).

1. Avant de chercher à modifier le propriétaire d'un fichier ou d'un dossier, assurez-vous d'utiliser un compte administrateur ou bien le compte du propriétaire du fichier.
2. Cliquez avec le bouton droit sur le fichier ou le dossier et choisissez *Propriétés* dans le menu contextuel.
3. Sélectionnez l'onglet *Sécurité* et cliquez sur le bouton *Avancé*.

4 Dans l'onglet *Propriétaire,* la fenêtre affiche alors le propriétaire actuel de l'objet sélectionné.

5 Pour changer le propriétaire, cliquez sur le bouton *Modifier...* La fenêtre qui s'affiche est similaire à la précédente, mais vous permet cette fois de définir un nouveau propriétaire pour l'objet. Le propriétaire peut être un utilisateur spécifique ou un groupe utilisateur. Sélectionnez le nouveau propriétaire dans la liste, puis validez en cliquant sur le bouton *OK*.

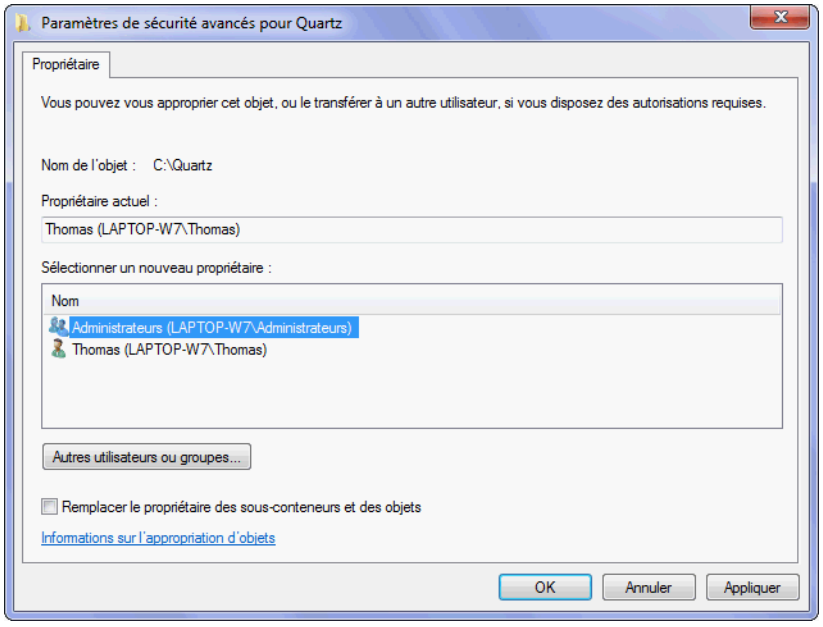


Figure 11–5
Fenêtre de changement de propriétaire d'un répertoire

EN PRATIQUE Propriétaires des éléments enfants d'un dossier

Si vous changez le propriétaire d'un dossier, vous avez la possibilité de changer le propriétaire des éléments enfants en cochant la case *Remplacer le propriétaire des sous-conteneurs et des objets*.

SÉCURITÉ NTFS et EFS

Comme un utilisateur disposant des privilèges administrateur peut devenir propriétaire de n'importe quel fichier sur un disque dur de sa machine, les permissions NTFS ne sont pas une protection efficace en cas de vol de disque dur, par exemple. Elles limitent uniquement l'accès aux fichiers aux utilisateurs non administrateurs. Pour protéger vos données contre le vol, utilisez plutôt le cryptage EFS fourni par NTFS. Nous traitons cet aspect au chapitre 6.

Auditer l'accès aux fichiers et répertoires

Suivant le niveau de sécurité de votre système informatique, vous renforcez la sécurité sur votre système en établissant une politique d'audit d'accès aux fichiers. En effet, en surveillant la création ou la modification d'objets sur le disque, vous contrôlez les problèmes de sécurité potentiels et vous disposez de preuves dans le cas d'une attaque sur les fichiers audités.

1 Ouvrez le menu *Démarrer*.

2 Saisissez `secpol.msc` dans la barre de recherche.

3 Dépliez l'arborescence *Paramètres de sécurité>Stratégies locales>Stratégie d'audit*.

4 Dans la partie droite de la fenêtre, double-cliquez sur *Auditer l'accès aux objets*.

VERSION Disponibilité de la fonction

Cette fonctionnalité n'est disponible que sur les versions Professionnelle, Entreprise ou Intégrale de Windows 7.

5 Sélectionnez ensuite selon vos souhaits *Réussite* et/ou *Échec*. Si vous cochez la case *Réussite*, une entrée sera écrite dans le journal chaque fois qu'un utilisateur accédera avec succès à un objet sur lequel l'audit a été activé. Cochez la case *Échec* pour écrire également au journal les tentatives d'accès infructueuses.

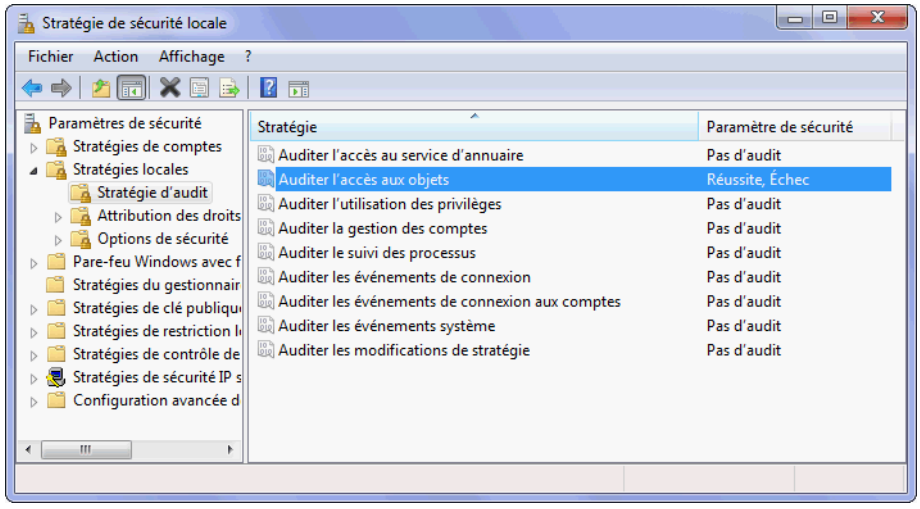


Figure 11–6
Activation de l'audit d'accès aux objets

6 Une fois cette opération effectuée, redémarrez votre machine pour que le paramètre soit pris en compte.

L'audit activé, il faut à présent choisir les dossiers ou fichiers sur lesquels l'audit va porter. Les paramètres d'audit sont stockés dans un descripteur appelé SACL (*System Access Control List*). Chaque SACL contient les paramètres suivants :

- le nom du groupe ou de l'utilisateur dont les accès au fichier ou au répertoire seront audités ;
- le type d'opération devant être audité (lecture, modification, suppression, etc.) ;
- le type d'événement à auditer (réussite ou échec de l'action).

Voici comment définir les paramètres de l'audit :

1 Cliquez avec le bouton droit sur le fichier ou dossier de votre choix et sélectionnez *Propriétés* dans le menu contextuel.

2 Dans l'onglet *Sécurité*, cliquez sur le bouton *Avancé*, puis sélectionnez l'onglet *Audit*.

3 Si le contrôle de comptes utilisateur (UAC) est activé, vous devrez confirmer votre action en cliquant sur le bouton *Continuer*.

4 La fenêtre affiche la liste des paramètres d'audit actuellement définis. Utilisez les boutons *Ajouter*, *Modifier* et *Supprimer* pour gérer cette liste.

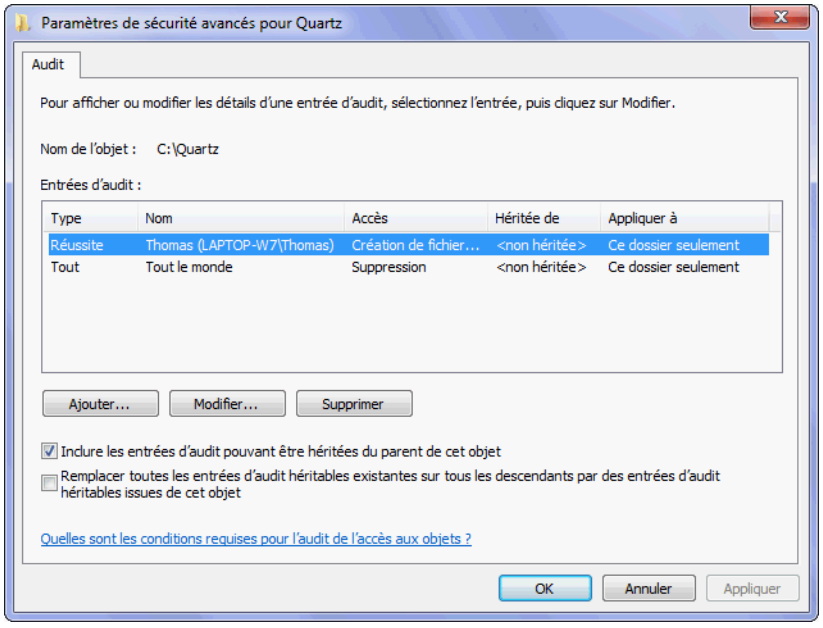


Figure 11–7
Dans notre exemple, les suppressions effectuées par tous les utilisateurs sont auditées, qu'elles aient réussi ou non (la colonne Type indique Tout). Les créations de fichiers réussies par l'utilisateur Thomas sont également auditées.

Pour ajouter une nouvelle règle d'audit,

1. Cliquez sur le bouton *Ajouter*. Choisissez tout d'abord l'utilisateur ou le groupe utilisateur auquel cette nouvelle règle s'applique.
2. Entrez le nom exact de l'utilisateur ou du groupe, ou utilisez le bouton *Avancé* pour rechercher les choix possibles. Vous pouvez également saisir `Tout le monde` pour indiquer que vous souhaitez surveiller les actions de tous les utilisateurs de l'ordinateur.
3. Validez ensuite la fenêtre de saisie avec le bouton *OK*.
4. Dans la fenêtre suivante, définissez les actions à auditer. Les différentes actions correspondent aux permissions NTFS que nous avons décrites au début de ce chapitre. Pour chaque autorisation, choisissez de surveiller la réussite et/ou l'échec de l'action.
5. Vous pouvez également choisir à quoi va s'appliquer la règle d'audit : dossier uniquement, ce dossier et les dossiers enfants, etc. Pour cela, choisissez dans la liste déroulante *Appliquer à* située au-dessus de la liste des accès.
6. Validez la fenêtre par le bouton *OK*. Si besoin, ajoutez ensuite une nouvelle règle ou accepter les règles d'audit définies en cliquant à deux reprises sur *OK*.

Une fois les règles d'audit définies, le journal de sécurité de Windows 7 enregistre chaque événement selon les règles d'audit que vous avez définies pour chaque objet.

À SAVOIR Un utilisateur après l'autre

Vous ne pouvez saisir qu'un seul nom. Si vous souhaitez cibler deux utilisateurs, vous devrez créer deux règles d'audit.

ASTUCE Tout autoriser/tout refuser

Comme pour les paramètres de sécurité, le fait d'effectuer un choix au niveau de l'accès *Contrôle total* sélectionne automatiquement toutes les cases de la colonne. Si vous désirez décocher toutes les cases de la fenêtre, utilisez le bouton *Effacer tout* présent au bas de la liste.

ASTUCE Impossible de supprimer une ligne

Si vous ne parvenez pas à supprimer une ligne dans les listes ou que certaines cases sont grisées lorsque vous voulez modifier les paramètres d'audit, c'est que les propriétés d'audit sont héritées d'un dossier parent. Si vous souhaitez tout de même modifier les règles d'audit pour l'élément, décochez la case *Inclure les entrées d'audit pouvant être héritées du parent de cet objet* dans la fenêtre affichant la liste des règles d'audit.

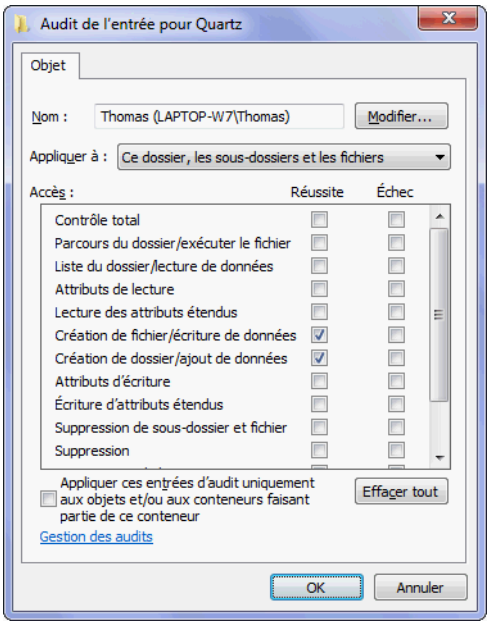


Figure 11–8
Fenêtre de sélection des types d'accès à auditer

L'accès au journal de sécurité se fait comme suit :

1. Connectez-vous en tant qu'administrateur.
2. Ouvrez le menu *Démarrer*, puis cliquez sur *Panneau de configuration*.
3. Choisissez la catégorie *Système et sécurité*.
4. Cliquez sur le lien *Afficher les journaux d'événements*.
5. Dans la colonne de gauche de l'observateur d'événements, déroulez l'arborescence *Observateur d'événements (local)>Journaux Windows>Sécurité*. Tous les événements de sécurité, y compris les audits, s'affichent de manière chronologique décroissante.

Partage de dossiers sur le réseau

Lorsque l'on possède un réseau domestique ou d'entreprise, il est essentiel de pouvoir partager certaines ressources telles que des documents ou des imprimantes. Windows 7 définit les dossiers et périphériques d'impression qui seront accessibles via les autres ordinateurs du réseau.

Dans un premier temps, assurez-vous que le service *Partage de fichiers et imprimantes réseau Microsoft* est bien installé sur votre carte réseau. Pour plus d'informations, reportez-vous au chapitre 10, « Configurer le réseau ».

RAPPEL Activer le service de partage de fichiers et d'imprimantes

1. Ouvrez le menu *Démarrer*.
2. Saisissez `centre réseau` dans la barre de recherche, puis cliquez sur *Centre Réseau et partage* dans la liste qui s'affiche.
3. Dans la colonne de gauche du centre réseau et partage, cliquez sur *Modifier les paramètres de la carte*.
4. Cliquez avec le bouton droit sur la carte correspondant à votre réseau, puis choisissez *Propriétés* dans le menu contextuel.
5. Dans la liste *Cette connexion utilise les éléments suivants*, vérifiez que la ligne *Partage de fichiers et imprimantes réseau Microsoft* est présente et cochée.
6. Si elle n'est pas présente, cliquez sur le bouton *Installer*, sélectionnez *Service*, puis cliquez sur le bouton *Ajouter...* Dans la liste, sélectionnez le service de partage de fichiers et d'imprimantes, puis cliquez sur *OK*.

EN COULISSE Ports réseau utilisés

Le service de partage de fichiers et d'imprimantes utilise 4 ports réseau pour ses échanges. Il s'agit des ports 139 et 445 en TCP, et des ports 137 et 138 en UDP.

Utiliser l'assistant partage

Windows 7 fournit une interface simplifiée pour gérer les options de partage sur les fichiers et dossiers, particulièrement adaptés aux groupes résidentiels d'ordinateurs. Cette option, appelée *Assistant partage*, est activée par défaut. Si cette option est désactivée :

1. Ouvrez l'explorateur Windows, puis le menu *Organiser*.
2. Cliquez sur *Options des dossiers et de recherche*.
3. Sélectionnez l'onglet *Affichage*, puis faites défiler la liste *Paramètres avancés* jusqu'en bas.
4. Cochez la case *Utilisez l'assistant partage (recommandé)*.
5. Validez ensuite par le bouton *OK*.
6. Si vous avez configuré un groupe résidentiel d'ordinateurs sur votre réseau, vous pouvez utiliser le menu *Partager avec* présent dans la barre de menus de l'explorateur Windows.

   À partir de ce menu, il est possible de choisir directement les paramètres de partage du dossier sélectionné. Vous pouvez ainsi en un clic donner accès en lecture seule ou bien en lecture/écriture aux membres de votre groupe résidentiel d'ordinateurs.
7. Vous pouvez également définir plus précisément les utilisateurs ayant accès à ce partage en cliquant sur *Personnes spécifiques*. La fenêtre de la figure 11–10 s'ouvre alors :

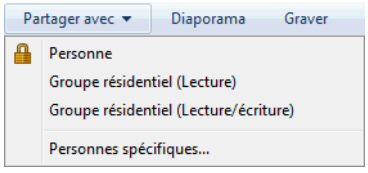


Figure 11–9
Menu Partager avec

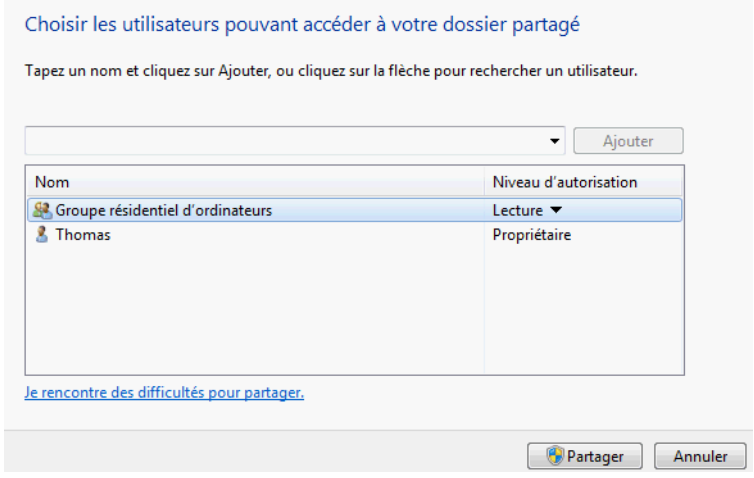


Figure 11–10
Assistant de partage de fichiers

Via cette fenêtre, vous ajoutez des utilisateurs en les choisissant dans la liste déroulante et en cliquant sur *Ajouter*.

8. Ensuite, pour chaque utilisateur représenté dans la liste au-dessous, vous choisissez le niveau d'autorisation entre *Lecture seule* et *Lecture/*

écriture. Vous avez également la possibilité de supprimer un utilisateur de la liste en cliquant sur la ligne, puis en choisissant *Supprimer* dans le menu contextuel.

9 Une fois la configuration terminée, cliquez sur le bouton *Partager* et Windows 7 se charge alors de partager le dossier selon les paramètres que vous avez sélectionnés.

Utiliser le partage avancé

Si vous ne souhaitez pas utiliser l'assistant partage pour gérer vos dossiers partagés, vous pouvez le désactiver avant de mettre en œuvre les paramètres de partage avancé.

1 Ouvrez l'explorateur Windows et déroulez le menu *Organiser*, présent en haut de la fenêtre.

2 Cliquez sur *Options des dossiers et de recherche*.

3 Dans la fenêtre *Option des dossiers* qui s'est ouverte, activez l'onglet *Affichage* et faites défiler la liste déroulante *Paramètres avancés* jusqu'en bas.

4 Décochez alors la case *Utiliser l'assistant partage (recommandé)*. Validez ensuite le paramétrage en cliquant sur le bouton *OK*.

Voyons à présent comment utiliser les options de partage avancé pour mettre à disposition des fichiers aux autres machines du réseau.

1 Le menu déroulant *Partager avec* ne contient plus qu'une seule entrée : *Partage avancé...* En cliquant sur cette ligne de menu, vous accédez alors à l'onglet *Partage* de la fenêtre de propriétés du dossier. Cliquez sur le bouton *Partage avancé*. La fenêtre de la figure 11–11 s'affiche.

ASTUCE

Fonctionnalités avancées via l'assistant

Même si l'assistant partage est activé, il est possible d'utiliser le partage avancé :

1. Cliquez avec le bouton droit sur le fichier ou le dossier de votre choix.
2. Sélectionnez *Propriétés*.
3. Rendez-vous dans l'onglet *Partage*.
4. Cliquez sur le bouton *Partage avancé*.

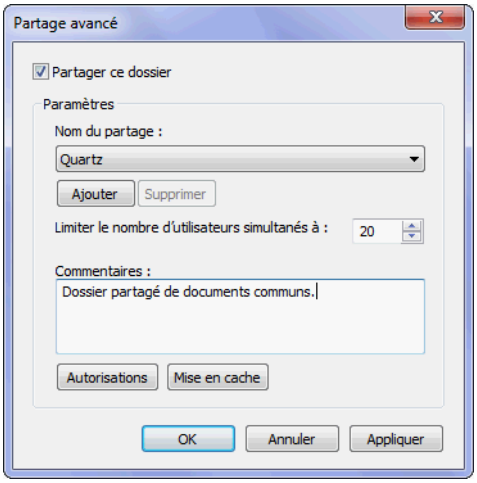


Figure 11–11
Fenêtre de paramètres du partage avancé

2 Pour activer ou désactiver le partage, cochez ou décochez la case *Partager ce dossier*. Lorsque vous décidez de partager un dossier, vous devez indiquer un nom, un nombre maximal d'utilisateurs simultanés et une éventuelle description via la zone de texte *Commentaires*.
3 Utilisez le bouton *Autorisations* pour définir les permissions pour ce partage (reportez-vous à la section suivante « Définir les permissions pour les dossiers partagés »).
4 Une fois ces informations définies, validez en cliquant sur *OK*.

Vous pouvez créer plusieurs partages pour un même dossier. Ils doivent porter des noms différents et peuvent posséder des configurations différentes (nombres d'utilisateurs, commentaires, autorisations, etc.). Pour créer un autre partage pour un dossier, ouvrez la fenêtre de paramètres du *Partage avancé* et cliquez sur le bouton *Ajouter* au-dessous de la zone *Nom du partage*. Utilisez le bouton *Supprimer* si vous voulez en éliminer un.

Astuce Cacher un dossier partagé

Lorsque vous partagez un dossier sur un réseau et que vous avez activé la découverte du réseau, il est visible pour les autres ordinateurs du réseau. Si vous souhaitez que votre dossier reste invisible, ajoutez le caractère **$** à la fin du nom réseau du dossier (par exemple, `nom-dossier$`). Le dossier n'apparaîtra plus dans la liste des ressources partagées par votre ordinateur. Pour accéder à ce dossier via le réseau, ouvrez l'explorateur Windows, dans la barre d'adresse, saisissez `\\nom-ordinateur\nom-dossier$`. N'oubliez pas le `$` à la fin.

Voir les dossiers partagés

Lorsque vous avez configuré un certain nombre de partages, il est intéressant de visualiser la liste des éléments partagés par votre ordinateur sur le réseau.

Dans un premier temps, vous pouvez ouvrir l'explorateur Windows et cliquer sur *Réseau* dans la colonne de gauche. Vous obtenez alors la liste des ordinateurs de votre réseau. En double-cliquant sur votre propre ordinateur, vous accédez alors à la liste des éléments partagés telle que la voient les autres utilisateurs. Cependant, cette liste n'affiche pas les partages cachés (nom finissant par `$`) et les partages système.

Voici la procédure à suivre afin de voir les éléments partagés par votre ordinateur plus en détail :

1 Connecté avec un compte administrateur, ouvrez le menu *Démarrer*, et cliquez avec le bouton droit sur *Ordinateur*.
2 Dans le menu contextuel, cliquez sur *Gérer*.
3 Dans la fenêtre qui s'ouvre, cliquez dans la colonne de gauche sur *Dossiers partagés*.

La partie droite de la fenêtre vous donne accès à trois sous-dossiers :

- *Partages* : cette option vous donne la liste des dossiers partagés par l'ordinateur, y compris les dossiers partagés cachés et les partages système. Le nombre de personnes en train d'accéder à chaque dossier est indiqué dans la colonne *Nb. de connexions client*. En double-cliquant sur l'un des dossiers partagés, vous avez la possibilité de modifier certains paramètres de partage tels que le nombre maximal de connexions simultanées autorisées, la description du partage et les autorisations d'accès.

Astuce Accès direct

Vous pouvez accéder directement au dossier partagé en cliquant avec le bouton droit sur celui-ci, puis en cliquant sur *Ouvrir* dans le menu contextuel.

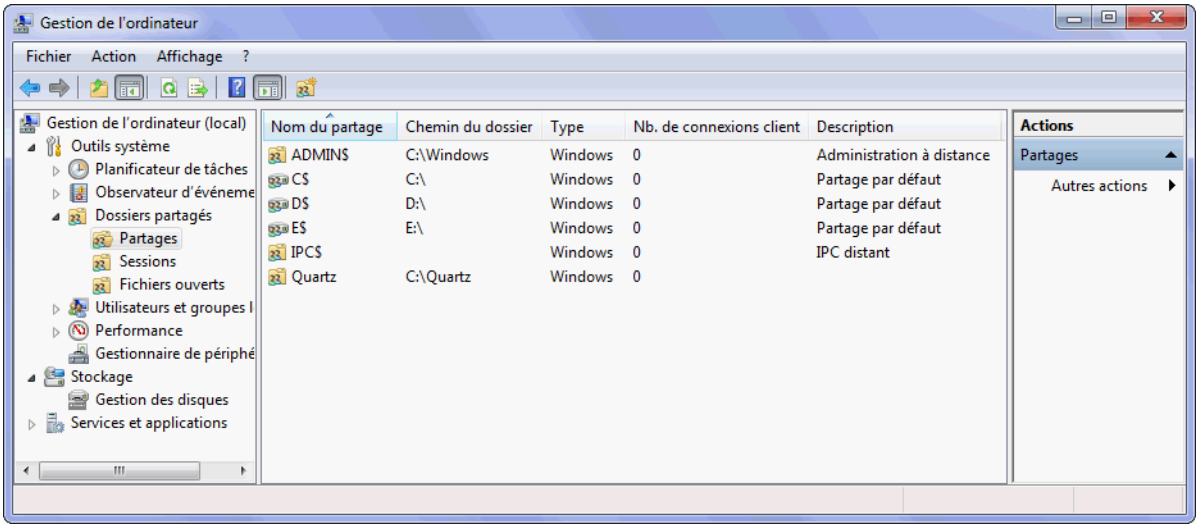


Figure 11–12 Liste des partages dans la console de gestion de l'ordinateur

ASTUCE Déconnecter un utilisateur de votre partage

Vous pouvez déconnecter l'un des utilisateurs en cliquant avec le bouton droit sur la ligne correspondante, puis en choisissant *Fermer la session*.

ASTUCE Interdire l'accès à un fichier

Si vous le souhaitez, vous pouvez fermer l'accès à un fichier actuellement ouvert en cliquant avec le bouton droit sur la ligne, puis en cliquant sur *Fermer le fichier ouvert*. Confirmez ensuite la boîte de dialogue en cliquant sur *Oui*. Attention, en effectuant cette manipulation, l'utilisateur distant peut perdre son travail s'il ne l'avait pas enregistré.

- *Sessions* : cette rubrique affiche la liste des utilisateurs actuellement connectés à votre ordinateur. Pour chaque utilisateur, les informations disponibles sont : son nom, le nom de son ordinateur, le nombre de fichiers partagés actuellement ouverts ainsi que la durée de sa connexion.
- *Fichiers ouverts* : comme son nom l'indique, cette liste affiche les fichiers partagés actuellement ouverts par les utilisateurs distants. Le nom du fichier, le nom de l'utilisateur et le mode d'accès au fichier (lecture, écriture) sont également indiqués.

Définir les permissions pour les dossiers partagés

Les permissions de partage s'appliquent aux utilisateurs qui accèdent au dossier via le réseau. En revanche, elles n'affectent pas les utilisateurs locaux pour qui les permissions NTFS continuent de s'appliquer.

Il existe deux façons d'accéder aux autorisations de partage :

- La première consiste à utiliser l'explorateur Windows. Cliquez avec le bouton droit sur le dossier, puis choisissez *Propriétés* dans le menu contextuel. Dans l'onglet *Partage*, cliquez sur le bouton *Partage avancé...*, puis sur le bouton *Autorisations*.
- La seconde utilise la console de gestion de l'ordinateur. Ouvrez le menu *Démarrer*, puis cliquez avec le bouton droit sur *Ordinateur* et choisissez *Gérer*. Déroulez l'arborescence *Gestion de l'ordinateur>Outils système>Dossiers partagés>Partages*. Double-cliquez sur la ligne représentant le dossier voulu, puis sélectionnez l'onglet *Autorisations du partage*.

Choisissez ensuite les permissions d'accès pour chaque utilisateur de la même façon que pour l'onglet *Sécurité* (voir la section précédente « Modifier les autorisations standards »).

Arrêter de partager un dossier

Il peut arriver que vous n'ayez plus besoin de partager un dossier ou que vous ne souhaitiez plus le mettre à disposition sur le réseau. Voici la procédure à suivre pour arrêter de partager un dossier :

1. Ouvrez la console de gestion de l'ordinateur : dans le menu *Démarrer*, cliquez avec le bouton droit sur *Ordinateur*, puis sélectionnez *Gérer*.
2. Déroulez l'arborescence *Gestion de l'ordinateur>Outils système>Dossiers partagés>Partages*.
3. Cliquez avec le bouton droit sur le dossier ne devant plus être partagé, puis cliquez sur *Arrêter le partage* dans le menu contextuel.
4. Confirmez la boîte de dialogue en cliquant sur *Oui* pour que le dossier ne soit plus accessible via le réseau.

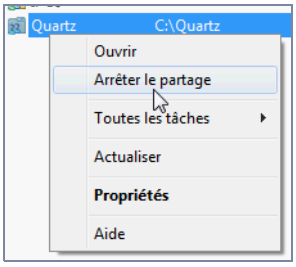


Figure 11–13
Menu contextuel pour l'arrêt du partage du dossier

Partager des fichiers via l'invite de commandes

Il est possible de partager un dossier via l'invite de commandes ou dans un fichier batch en utilisant la commande `net share`, abordée plus en détail dans le paragraphe suivant.

Pour avoir plus de détails sur cette commande, ouvrez l'invite de commandes et saisissez :

```
net help share
```

Afficher la liste des dossiers partagés

La commande sans argument suivante affiche la liste des dossiers partagés sur votre ordinateur, y compris les partages cachés et système :

```
net share
```

Vous pouvez enregistrer cette liste dans un fichier texte en utilisant la syntaxe suivante :

```
net share > nom-fichier.txt
```

Par exemple :

```
net share > "%userprofile%\Documents\liste-partages.txt"
```

Ici, `%userprofile%` représente le chemin de votre répertoire utilisateur (`C:\Utilisateurs\Thomas`).

Partager un dossier

Voici la syntaxe de la commande pour créer un nouveau partage :

```
net share nom-partage=lecteur:chemin
```

Par exemple, la commande pour partager le dossier `C:\jpg` sous le nom `photos` est la suivante :

```
net share photos=C:\jpg
```

Le partage est alors créé.

Attention, si votre chemin comporte des espaces, il faudra l'encadrer par des guillemets doubles. Par exemple :

```
net share images="C:\mes images"
```

Supprimer un partage

Pour supprimer un partage, utilisez la syntaxe suivante :

```
net share nom-partage /delete
```

Prenons un exemple :

```
net share photos /delete
```

Le dossier correspondant à ce partage ne sera plus visible sur le réseau.

Visualiser la liste des fichiers partagés ouverts

Vous avez la possibilité de consulter en ligne de commande les fichiers actuellement accédés par les utilisateurs distants.

1. Ouvrez une invite de commandes, avec les privilèges d'administrateur : ouvrez le menu *Démarrer*, puis saisissez `cmd` dans la zone de recherche. Lorsque *cmd.exe* apparaît, cliquez avec le bouton droit sur la ligne, puis choisissez *Exécuter en tant qu'administrateur* (vous pouvez également utiliser la combinaison de touches *Ctrl+Maj+Entrée*).
2. Tapez ensuite la commande `openfiles`.
3. La liste des fichiers actuellement ouverts par les utilisateurs distants s'affiche alors dans la fenêtre d'invite.

Partage d'imprimantes

Il n'est pas rare qu'il y ait plusieurs utilisateurs d'ordinateurs dans un même foyer, c'est pourquoi les postes se multiplient. Cependant, une seule imprimante suffit bien souvent. On peut en effet la partager pour la rendre accessible par tous les ordinateurs connectés au réseau domestique et c'est ce que nous allons découvrir maintenant.

Configurer le serveur d'impression

Si votre ordinateur dispose d'une imprimante et qu'il est connecté à un réseau local, vous pouvez la partager. Cette opération permet alors à tous les ordinateurs du réseau d'utiliser votre imprimante pour imprimer des documents. Ceci vous permet, par exemple, de n'acheter qu'une seule imprimante pour tous les ordinateurs de votre domicile ou d'éviter d'avoir à la déplacer de pièce en pièce pour imprimer à partir des différents ordinateurs.

1. Vérifiez tout d'abord que votre imprimante est correctement installée sur votre ordinateur.
2. Ouvrez le menu *Démarrer*, puis cliquez sur *Périphériques et imprimantes*.

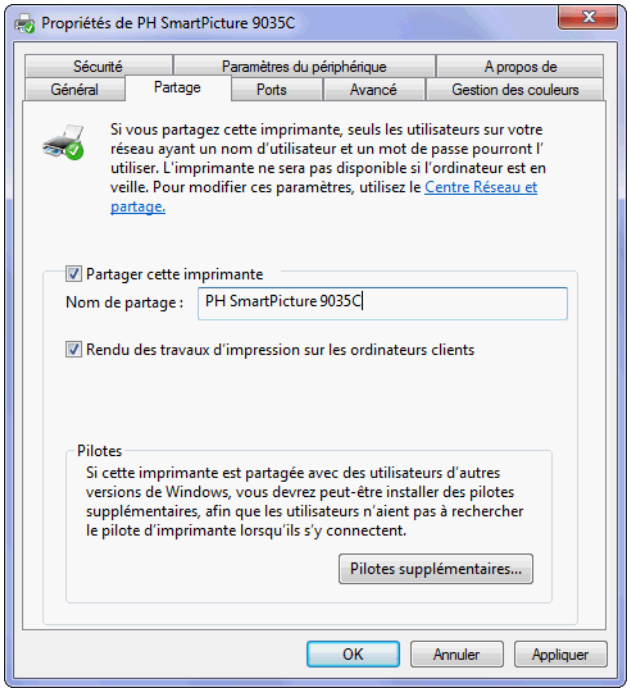


Figure 11–14
Onglet Partage des propriétés de l'imprimante

3 Cliquez avec le bouton droit sur l'icône représentant votre périphérique d'impression et sélectionnez *Propriétés de l'imprimante* dans le menu contextuel.

4 Dans la boîte de dialogue de propriétés, sélectionnez l'onglet *Partage*. Pour rendre l'imprimante accessible sur le réseau, cochez la case *Partager cette imprimante*. Votre ordinateur est désormais un serveur d'impression.

5 Dans la zone de texte *Nom du partage,* définissez le nom de l'imprimante tel qu'il apparaîtra dans les ressources partagées de votre ordinateur.

Si votre réseau comporte des ordinateurs possédant des architectures différentes (x86, x64 ou Itanium), utilisez le bouton *Pilotes supplémentaires...* pour installer les pilotes correspondant à chaque architecture. Ainsi, lorsque les utilisateurs des ordinateurs du réseau se connecteront à l'imprimante partagée sur le réseau, le pilote correspondant s'installera automatiquement sur leur ordinateur.

N'oubliez pas que l'imprimante ne sera accessible que si votre ordinateur est allumé. S'il est éteint, les autres ordinateurs du réseau ne pourront pas l'utiliser.

Se connecter à une imprimante partagée

Une fois le serveur d'impression paramétré, configurez les ordinateurs clients. Voici la procédure à suivre pour ajouter une imprimante réseau :

1 Ouvrez le menu *Démarrer*, puis cliquez sur *Périphériques et imprimantes*.

2 Cliquez ensuite sur le bouton *Ajouter une imprimante* situé en haut de la fenêtre. L'assistant d'ajout d'imprimante s'affiche alors.

3 À la première étape, cliquez sur le lien *Ajouter une imprimante réseau, sans-fil ou bluetooth*. Windows recherche alors sur le réseau les imprimantes partagées. La liste des imprimantes trouvées s'affiche dans la fenêtre représentée à la figure 11–15.

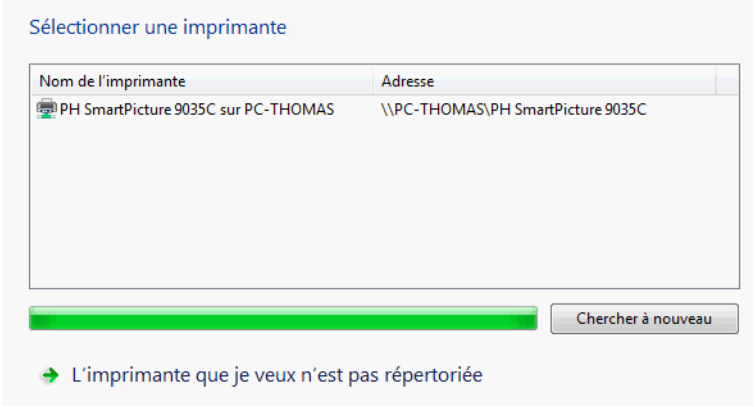


Figure 11–15
Liste des imprimantes partagées trouvées sur le réseau

PRATIQUE Afficher le rendu sur l'ordinateur de l'utilisateur

Avec la case *Rendu des travaux d'impression sur les ordinateurs clients* cochée, le calcul du rendu du document sera réalisé sur l'ordinateur ayant lancé l'impression plutôt que sur l'ordinateur sur lequel l'imprimante est branchée. Ceci permet d'économiser de la bande passante réseau et de réduire la charge du serveur d'impression.

SÉCURITÉ Identification

Suivant les paramètres de partage avancés configurés dans le Centre réseau et partage, les utilisateurs devront peut-être s'identifier pour accéder à l'imprimante. Pour plus d'informations sur les paramètres de partage avancés, consultez le chapitre « Configuration du réseau ».

Serveur d'impression

On appelle serveur d'impression l'ordinateur sur lequel est connectée l'imprimante.

Suivant le modèle de votre imprimante ou la configuration de votre réseau, l'imprimante est soit détectée automatiquement par Windows, soit vous devrez l'ajouter manuellement. Voyons maintenant la procédure à suivre pour chacun de ces cas de figure.

Ajouter une imprimante par la recherche automatique

Si la recherche automatique d'imprimante trouve des résultats, cliquez sur l'imprimante de votre choix, puis appuyez sur le bouton *Suivant*. Si aucun résultat n'a été trouvé ou que l'imprimante que vous recherchez n'apparaît pas dans la liste, cliquez sur le bouton *L'imprimante que je veux n'est pas répertoriée*.

L'assistant se connecte alors à l'imprimante et télécharge son pilote depuis l'ordinateur qui partage l'imprimante. Si l'UAC (*User Account Control*, contrôle des comptes utilisateur) est activé sur votre machine, confirmez l'installation du pilote. L'assistant installe alors le pilote sur votre machine. Une fois l'opération terminée, une fenêtre de confirmation s'affiche.

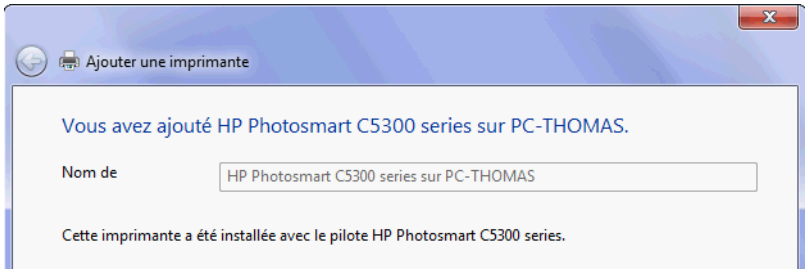


Figure 11–16
Confirmation d'installation de l'imprimante réseau

En cliquant sur le bouton *Suivant*, l'assistant vous propose d'imprimer une page de test pour vérifier le bon fonctionnement de l'imprimante et de la connexion avec celle-ci. Cliquez ensuite sur *Terminer*, vous pouvez maintenant utiliser l'imprimante sur votre ordinateur.

Ajouter une imprimante manuellement

Si la recherche automatique d'imprimantes ne détecte pas celle de votre choix, l'assistant vous propose une autre méthode d'installation :

1. Cliquez sur le bouton *L'imprimante que je veux n'est pas répertoriée*.
2. Cochez la case *Sélectionner une imprimante partagée par son nom*.
3. Saisissez l'emplacement de l'imprimante en utilisant la syntaxe suivante : `\\nom-ordinateur\nom-de-l'imprimante`. `Nom-ordinateur` correspond au nom réseau ou à l'adresse IP de l'ordinateur sur lequel l'imprimante est branchée. Si vous ne connaissez pas le nom de l'ordinateur, cliquez sur le bouton *Parcourir...* pour afficher la liste des ordinateurs du réseau.

4 Double-cliquez sur le nom de l'ordinateur servant de serveur d'impression, puis sélectionnez l'imprimante en double-cliquant sur son icône.

5 Cliquez ensuite sur le bouton *Suivant* pour installer le pilote et terminer l'installation de l'imprimante.

Ajouter une imprimante Ethernet ou Wi-Fi

De nombreuses imprimantes proposent aujourd'hui différents modes de connexion. Ainsi, on peut parfois se connecter à une imprimante par liaison Ethernet ou par une connexion Wi-Fi.

L'avantage d'une imprimante utilisant Ethernet ou le Wi-Fi est qu'elle ne vous contraint pas vous servir de votre ordinateur en tant que serveur d'impression pour imprimer depuis un ordinateur du réseau. En effet, l'imprimante est raccordée directement au réseau local par liaison Ethernet ou Wi-Fi et est donc disponible en permanence pour recevoir des informations provenant du réseau.

Que faire si votre imprimante réseau Ethernet ou Wi-Fi n'est pas détectée par la recherche automatique ?

1 Cliquez sur le bouton *L'imprimante que je veux n'est pas répertoriée*.

2 Cochez le bouton radio *Ajouter une imprimante à l'aide d'une adresse TCP/IP ou un nom d'hôte*.

3 Cliquez ensuite sur le bouton *Suivant*. L'assistant vous demande alors des informations sur l'imprimante réseau. Si vous ne savez pas comment compléter ces renseignements, consultez la documentation de votre imprimante réseau.

En résumé

Ce chapitre vous a permis de voir comment gérer les options de sécurité pour partager les fichiers de manière sécurisée entre plusieurs utilisateurs sur une même machine. Vous avez également découvert comment partager des fichiers ou des dossiers sur le réseau et enfin, vous avez mis en œuvre un partage d'imprimante au sein d'un réseau domestique.


7
TM

chapitre 12

Optimiser le système

Lorsque vous veniez de l'acheter, votre ordinateur était rapide et performant. Au fil du temps, il a perdu en réactivité et est devenu plus lent. Tel est malheureusement le constat de beaucoup d'utilisateurs. Cependant, il existe différents outils pour optimiser les performances du système.

SOMMAIRE

- Analyser les performances de l'ordinateur
- Optimisation matérielle
- Nettoyer le disque
- Défragmenter le disque
- Optimiser le paramétrage
- Améliorer les performances du système de fichiers NTFS
- Augmenter la mémoire cache avec ReadyBoost
- Mémoire virtuelle

MOTS-CLÉS

- Indice de performance
- Matériel
- Optimisation
- Performances
- Évaluation
- Désinstallation
- Programmes de démarrage
- Défragmentation
- Paramètres visuels
- Options d'alimentation
- ReadyBoost
- Mémoire virtuelle

Ce chapitre présente dans un premier temps les outils d'analyse à votre disposition pour étudier les performances de votre système et déceler les points à corriger. Il aborde également le fonctionnement des utilitaires de nettoyage de disque et de défragmentation, les différents outils et fonctionnalités du système pour la gestion des fichiers, la compression indice de performance des données et leur sécurisation via chiffrement.

Optimiser le matériel

Une des méthodes pour améliorer les performances d'un ordinateur consiste à mettre à jour ses composants. Si cette technique s'avère des plus efficaces, elle est néanmoins particulièrement coûteuse.

Par exemple, si votre ordinateur a des difficultés à faire fonctionner plusieurs programmes simultanément, il vous faut augmenter la quantité de mémoire physique (RAM). Si les images sont saccadées lorsque vous jouez à des jeux graphiquement évolués (3D, etc.), songez à changer votre carte graphique pour une version plus performante. Enfin, si vous devez travailler avec des données très volumineuses telles que des vidéos en haute résolution, vérifiez que votre disque dur possède suffisamment d'espace libre.

Analyser les performances de l'ordinateur

Afin de surveiller l'activité du système, Windows 7 met à votre disposition un ensemble d'outils pour analyser les performances de votre ordinateur.

Informations et outils de performances

Dans le panneau de configuration, Windows 7 propose un module qui analyse les performances de votre ordinateur. Voici comment y accéder :

1. Ouvrez le panneau de configuration, puis cliquez sur la catégorie *Système et sécurité*.
2. Ouvrez ensuite *Centre de maintenance*.
3. Cliquez sur *Informations et outils de performances* dans la colonne de gauche.

La fenêtre est composée de plusieurs parties :

- La colonne de gauche donne accès à des fonctions complémentaires qui améliorent les performances de l'ordinateur. Pour y accéder, cliquez sur *Outils avancés* dans la colonne de gauche. Dans la fenêtre qui

s'ouvre alors, Windows liste les outils qui vous seront utiles pour surveiller les performances de votre ordinateur. Ces différents outils sont décrits plus en détail dans les paragraphes suivants.

- Windows 7 peut détecter certains problèmes de perte de performances. Ces problèmes sont signalés en haut de la fenêtre dans le cadre intitulé *Problèmes de performances*. Par exemple, il vous avertit si des programmes de démarrage consomment trop de ressources ou si les paramètres visuels (effets visuels de Windows, comme Aero ou les effets d'ombre) sont trop élevés pour votre configuration. Dans tous les cas, en cliquant sur l'une des lignes d'erreur, vous obtenez plus d'informations sur le problème et une solution vous sera également proposée pour résoudre le problème.
- La partie centrale de la fenêtre affiche les indices de performances calculés par Windows.

Voyons à présent ce que mesurent ces indices et comment les interpréter.

Indice de performance

Windows 7 calcule un indice évaluant les performances générales de votre matériel. Son analyse porte sur les composants principaux du système en mesurant les 5 données suivantes :

- fréquence du processeur (nombre d'opérations réalisées par seconde) ;
- nombre d'opérations mémoire par seconde ;
- performances graphiques pour l'affichage du Bureau Aero ;
- performances graphiques pour les jeux ou applications 3D ;
- vitesse de transfert des données sur le disque dur.

Chacune de ces caractéristiques est évaluée et reçoit une note appelée sous-indice. Chaque sous-indice est compris entre 1,0 et 7,9. En raison de l'évolution rapide des composants matériels, il est possible que le score maximal s'élève par la suite.

Le but de l'outil *Indice de performance Windows* est tout d'abord de vous donner une idée des capacités matérielles de votre ordinateur, mais l'indice de performance vous permet également de choisir des logiciels adaptés à votre configuration. En effet, de plus en plus de logiciels et de jeux recommandent d'avoir un indice minimum, afin de garantir une utilisation optimale.

Lancer l'évaluation

Voici comment consulter votre indice de performance :

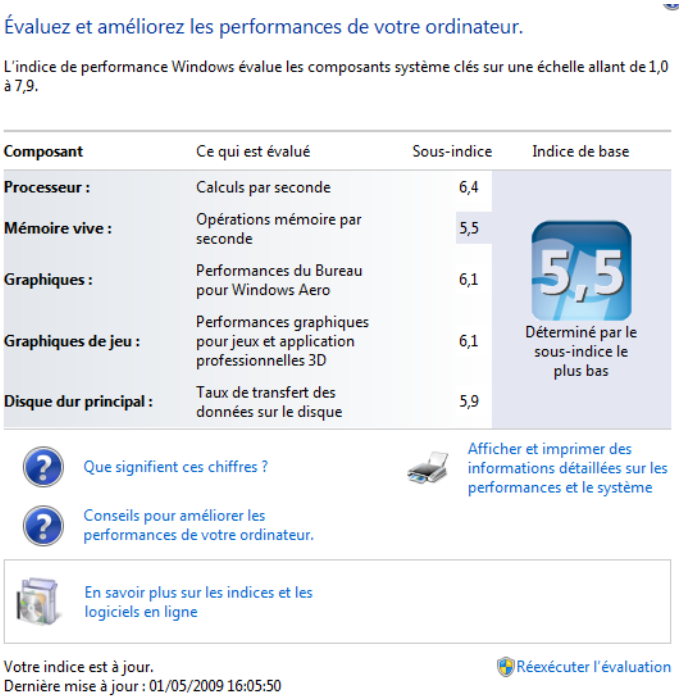
1 Ouvrez le menu *Démarrer*, effectuez un clic droit sur *Ordinateur*, puis cliquez sur *Propriétés* dans le menu contextuel.

2 Dans la fenêtre de propriétés du système, cliquez sur la ligne *Évaluation* du paragraphe *Système*.

3 La fenêtre *Informations et outils de performances* s'ouvre.

4 Si l'évaluation n'a pas été encore réalisée, cliquez sur le bouton *Évaluer cet ordinateur* pour démarrer l'analyse. Si votre ordinateur a déjà été noté et que vous avez changé un composant, vous pouvez relancer l'analyse en cliquant sur le bouton *Réexécuter l'évaluation*.

Figure 12–1
Exemple d'évaluation d'un ordinateur par Windows 7



5 Pour obtenir tous les critères de notation détaillés pour votre ordinateur, cliquez sur le lien *Afficher et imprimer des informations détaillées*.

Interpréter l'indice de base

La note globale attribuée à votre ordinateur, appelée indice de base, correspond au sous-indice le plus bas parmi les cinq caractéristiques évaluées.

Un ordinateur qui obtient un score de 2,0 peut être utilisé pour de la bureautique ou surfer sur Internet. Cependant, il sera probablement incapable d'afficher l'interface Aero de Windows 7.

Avec un score de 3,0, il affichera une version limitée de l'interface Aero. Sur un ordinateur de ce type, vous pouvez par exemple utiliser le thème Windows 7 avec une résolution élevée sur un seul moniteur. Il aura plus de difficultés à afficher le thème en haute résolution sur deux moniteurs.

EN PRATIQUE Compte administrateur

Il n'est possible de lancer l'évaluation qu'en étant connecté sous un compte administrateur.

CAS PARTICULIER Ordinateur portable

Avec un ordinateur portable, il est préférable de le raccorder au secteur avant de lancer l'évaluation. En effet, lorsque l'ordinateur est sur batterie, le système d'exploitation économise la puissance électrique, ce qui entraîne souvent une diminution des performances de votre ordinateur. Par conséquent, l'évaluation ne refléterait pas vraiment la réalité.

PRÉCAUTION
Espace disque et carte graphique

Si votre espace disque est insuffisant, l'évaluation ne peut s'effectuer. En effet, au cours de l'analyse, Windows crée un fichier de test sur le disque dur. S'il n'a pas assez de place pour le générer, il annule tout simplement l'évaluation de votre ordinateur. Vous devez donc libérer de l'espace pour pouvoir relancer l'évaluation.
Impossible d'évaluer votre ordinateur si le pilote de la carte graphique est trop ancien ou si votre machine ne dispose pas de capacités multimédias, par exemple, s'il n'est pas équipé d'une carte son.

Un ordinateur noté 4,0 ou 5,0 est en mesure d'exploiter toutes les fonctionnalités de Windows 7 sans problème et supporte l'exécution simultanée d'un grand nombre de programmes.

Avec un score de 6,0 ou supérieur, le PC possède un disque dur rapide et de puissantes capacités graphiques. Vous pouvez l'exploiter pour des jeux évolués en 3D ou pour du traitement vidéo en haute définition.

Interpréter les sous-indices

Lorsque votre ordinateur vous sert uniquement pour de la bureautique (traitement de texte, tableur, courriel, navigation Internet), un sous-indice de 2,0 est suffisant pour les catégories *Graphiques* et *Graphiques de jeu*. Veillez toutefois à avoir un score supérieur pour le processeur et la mémoire vive.

Si vous êtes intéressé par les jeux vidéo en 3D ou que vous effectuez du traitement de vidéos, vous devez avoir un score élevé dans les catégories *Processeur*, *Mémoire vive*, *Graphiques* et *Graphiques de jeu*. Un score de 3,0 est suffisant pour le sous-indice *Disque dur*.

Afin d'utiliser Windows 7 en tant que Media Center, un score de 3,0 suffira pour la mémoire vive et les graphiques de jeu, alors qu'il faudra un score supérieur pour le processeur, le disque dur et la catégorie *Graphiques*.

Analyseur de performances : perfmon.exe

Perfmon.exe évalue les performances de votre ordinateur. Cet outil donne des informations détaillées qui peuvent être difficiles à comprendre pour des utilisateurs non avertis. Il analyse l'état des ressources matérielles (disque, mémoire…) et des périphériques, les temps de réponse, ainsi que la configuration du système.

Générer un rapport

Pour lancer une analyse, vous devez utiliser un compte administrateur.

1. Ouvrez le menu *Démarrer* et saisissez `perfmon /report` dans la zone de recherche, puis appuyez sur la touche *Entrée*.
2. L'analyseur de performances démarre alors le diagnostic. Cet ensemble de tests dure environ une minute.
3. À la fin de l'analyse, le rapport de diagnostic du système s'affiche.

Les premières informations du rapport indiquent le nom de l'ordinateur, l'heure de l'analyse et la durée de celle-ci. Pour naviguer rapidement dans l'interface, cliquez dans le sommaire sur l'un des boutons en forme de fiche apparaissant sur les titres des chapitres. Le rapport se structure de la manière suivante :

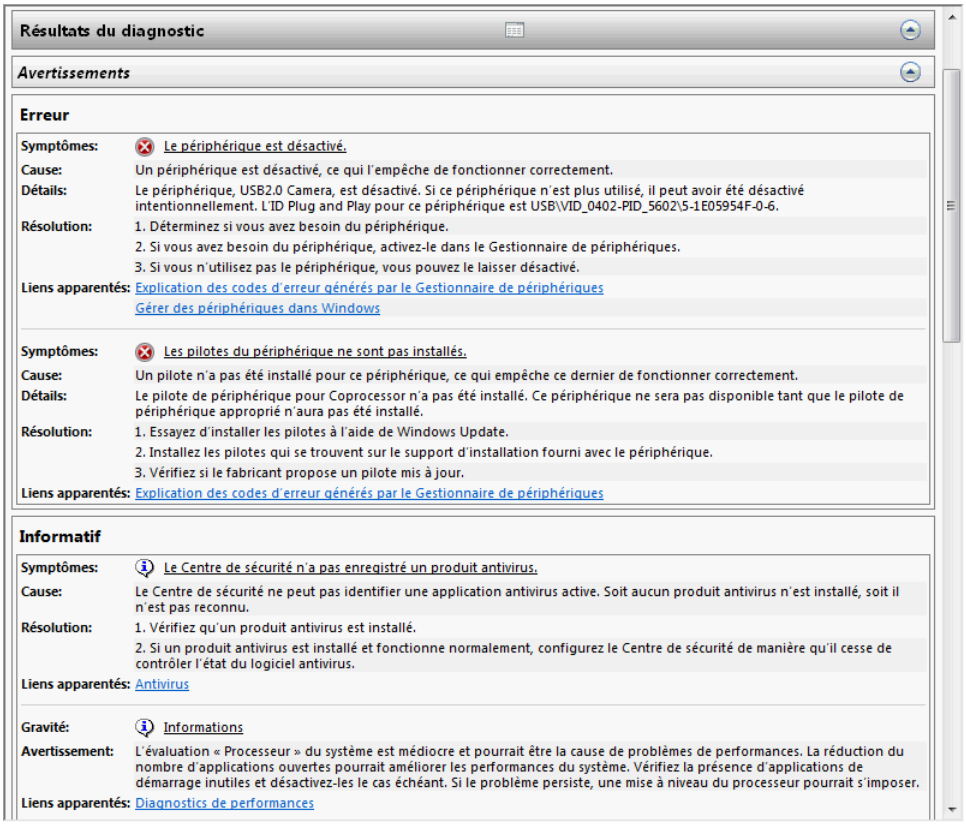


Figure 12–2
Exemple
de rapport de diagnostic

- Le premier chapitre du rapport, intitulé *Résultats du diagnostic*, affiche une synthèse des résultats obtenus. Les messages d'erreur les plus importants apparaissent en premier. Il peut, par exemple, s'agir d'un périphérique désactivé ou dont les pilotes ne sont pas installés.
- Les messages qui suivent sont informatifs : ils concernent l'antivirus si aucun antivirus n'a été détecté. Ils vous indiquent si les performances matérielles sont insuffisantes. Dans ce cas, ces informations sont une interprétation automatique des indices de performance de votre ordinateur. Ces messages donnent des suggestions pour vous aider à améliorer les performances de votre système.
- Le paragraphe suivant, intitulé *Vérifications système de base*, présente un compte-rendu de l'état du système d'exploitation, des disques durs physiques, des éléments du centre de sécurité, des services système ainsi que des périphériques. Pour chacun de ces cinq éléments, le résultat (*Réussite* ou *Échec*) est indiqué. Pour avoir plus de détail sur l'une des lignes, cliquez sur le signe + en début de ligne.
- Le dernier paragraphe du chapitre *Résultats du diagnostic* propose une vue de l'utilisation du processeur, de la mémoire vive et du réseau au moment de l'analyse.

- Les chapitres suivants du rapport contiennent différentes données techniques recueillies durant l'analyse.

Vous pouvez enregistrer le rapport généré au format HTML ou bien demander à ce qu'il vous soit envoyé par e-mail. Dans tous les cas, il sera également conservé dans l'analyseur de performances. Pour le consulter :

1. Ouvrez le menu *Démarrer*, saisissez `perfmon` dans la zone de recherche, puis appuyez sur la touche *Entrée*.
2. Déroulez l'arborescence de la partie gauche de la fenêtre comme suit : *Performance>Rapports>Système>System Diagnostics*.
3. Tous les rapports générés se trouvent listés dans la partie droite de la fenêtre accompagnés de leur date d'exécution. Vous pouvez supprimer les rapports de votre choix en cliquant avec le bouton droit sur la ligne correspondante et en choisissant *Supprimer* dans le menu contextuel.

Performances en temps réel

L'analyseur de performances vous permet également de consulter les statistiques du système en temps réel. Pour y accéder, ouvrez le menu *Démarrer*, saisissez `perfmon` dans la zone de recherche, puis tapez sur *Entrée*.

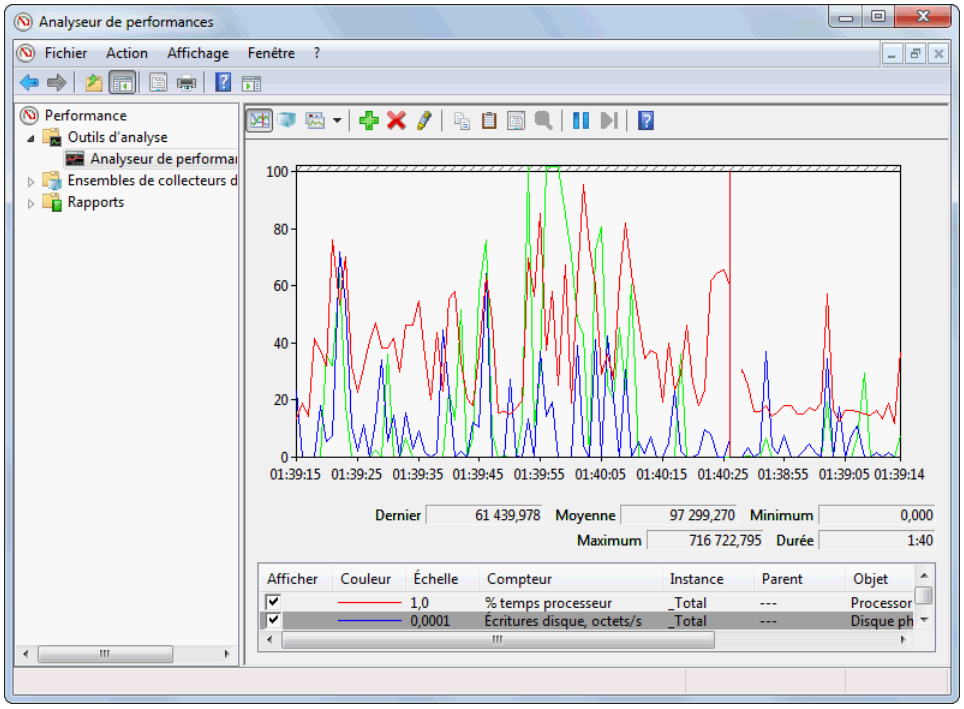


Figure 12–3
Analyseur de performances

Sur la fenêtre d'accueil de l'analyseur de performances se trouve le résumé système. Cette boîte affiche en temps réel des statistiques concernant les

disques durs, le réseau, la mémoire et le processeur. Pour visualiser plus de données, cliquez sur *Analyseur de performances* dans la colonne de gauche.

Trois modes d'affichage différents sont disponibles :

- Le mode ligne affiche les statistiques sous la forme d'un graphique linéaire en fonction du temps.
- Le mode histogramme présente les valeurs instantanées mesurées sous la forme de barres verticales dont la hauteur varie en fonction de la valeur.
- Le mode rapport affiche les valeurs numériques des données mesurées.

Pour choisir un mode d'affichage, cliquez sur la troisième icône dans la barre pour basculer entre les différents modes ou sur la petite flèche noire pointant vers le bas pour afficher la liste des modes disponibles.

Vous pouvez ajouter de nouvelles données sur le graphique en cliquant sur le signe `+` vert. Pour supprimer l'une des données du graphique, sélectionnez-la dans la liste au bas de la fenêtre, puis cliquez sur le bouton en forme de croix rouge.

Moniteur de ressources

Le moniteur de ressources sert à déterminer quels processus utilisent le processeur, la mémoire, le disque dur ou le réseau. Plusieurs méthodes s'offrent à vous pour accéder au moniteur de ressources :

- Ouvrir le gestionnaire de tâches, puis dans l'onglet *Performances*, cliquer sur le bouton *Moniteur de ressources...*
- Saisir `moniteur de ressources` dans la barre de recherche du menu *Démarrer*.
- Saisir `perfmon /res` dans la barre de recherche du menu *Démarrer* ou dans une invite de commandes.

Voyons comment s'organise la fenêtre du moniteur. L'onglet intitulé *Vue d'ensemble* permet de visualiser en un coup d'œil les processus qui utilisent trop le processeur, qui consomment trop de mémoire, les fichiers qu'ils ont ouverts ou encore les connexions qu'ils ont établies.

Si vous souhaitez visualiser les informations d'un processus en particulier, cochez la case correspondant au processus dans la première liste. Les listes afficheront alors uniquement les informations concernant le processus sélectionné.

L'onglet *Processeur* fournit une liste détaillée des services en cours d'exécution sur l'ordinateur. L'onglet *Mémoire* affiche une représentation graphique de la mémoire actuellement utilisée. L'onglet *Réseau* liste les ports ouverts sur votre machine et indique par quel logiciel ils sont utilisés. Vous pouvez également visualiser la bande passante utilisée par chaque processus ainsi que les adresses IP avec lesquelles ils communiquent.

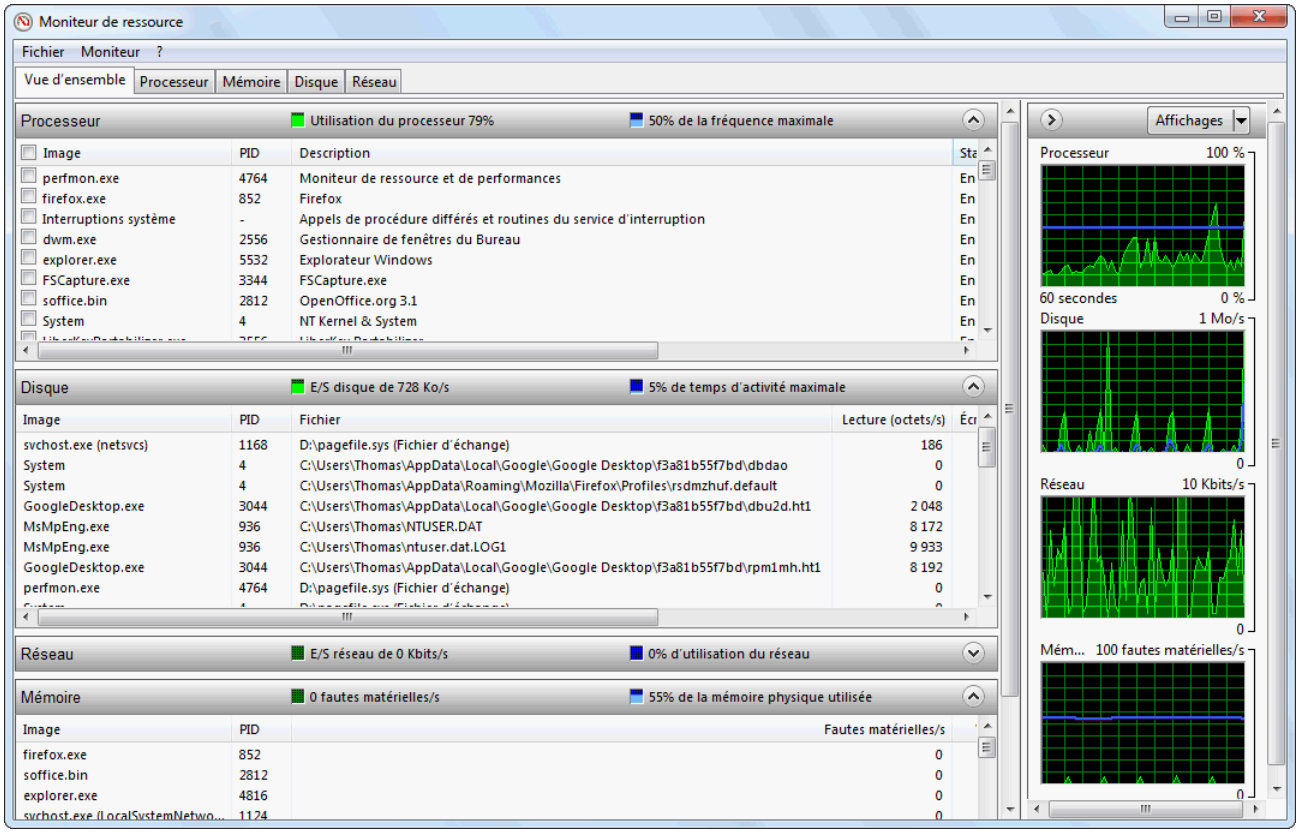


Figure 12–4 Vue d'ensemble du moniteur de ressources

Journal d'événements de performances

Windows 7 analyse en permanence les divers événements influant sur les performances. Ces différentes analyses sont ensuite enregistrées dans un journal.

Pour accéder au journal d'événements de performances, vous devez utiliser un compte administrateur de la machine.

1. Ouvrez le menu *Démarrer* et cliquez sur *Panneau de configuration*.
2. Choisissez la catégorie *Système et sécurité*.
3. Cliquez sur le lien *Afficher les journaux d'événements*.
4. Dans la colonne de gauche de l'observateur d'événements, cliquez sur *Observateur d'événements (local)*, puis sur *Journaux des applications et des services*. Dépliez le nœud *Microsoft*, puis *Windows*, ensuite *Diagnostic-Performances* et enfin cliquez sur *Opérationnel*.

Les événements enregistrés peuvent être :

- des programmes dont le démarrage a été anormalement long ;
- des pilotes qui mettent trop de temps à sortir de la mise en veille ;
- des ralentissements du système de fenêtres de Windows ;
- des statistiques sur les durées de démarrage, de mise en veille et d'arrêt de Windows.

Par défaut, les événements sont triés par ordre chronologique inversé. Cliquez sur l'un d'eux pour avoir plus d'informations.

Éliminer le superflu

Pour optimiser votre ordinateur, il faut dans un premier temps vous débarrasser de tous les logiciels et fichiers inutiles. Désinstallez les logiciels que vous n'utilisez plus, videz la corbeille, effacez les fichiers temporaires, etc.

Désinstaller les logiciels inutilisés

Le premier réflexe à avoir lorsque vous optimisez votre système d'exploitation est de désinstaller les logiciels dont vous n'avez pas ou plus besoin. En effet, en plus de prendre de la place sur le disque, ils ont peut-être créé des fichiers de configuration dans votre profil utilisateur et ont certainement ajouté quelques clés dans la base de registre.

Même si vous utilisez votre ordinateur depuis longtemps, il est possible que des utilitaires installés par le constructeur de la machine soient toujours installés. Il est souvent facile d'oublier qu'ils sont installés, car ils sont rarement utilisés. N'hésitez pas à les désinstaller si vous ne vous en servez pas. D'autant plus que le constructeur propose certainement un CD-Rom ou un site web pour vous les procurer à nouveau.

Faire le ménage dans les programmes de démarrage automatique

Certains programmes se lancent automatiquement au démarrage de votre machine. Il peut s'agir de logiciels tels qu'un client de messagerie instantanée, un utilitaire de gestion de la carte vidéo, etc. Ces différents programmes consomment de la mémoire lorsqu'ils sont lancés. Certains d'entre eux ne sont pas indispensables et ne vous ont peut-être jamais servi. C'est pourquoi il est préférable de ne conserver que les programmes dont vous avez l'utilité. Si vous avez un doute, renseignez-vous sur le logiciel pour connaître son utilité. S'il vous semble inutile de le démarrer en même temps que votre ordinateur, désactivez son démarrage automatique.

En coulisse L'exécution automatique des programmes

Les programmes qui s'exécutent automatiquement au démarrage de Windows sont définis soit dans le menu *Démarrer*, soit dans la base de registre. Dans les deux cas, l'exécution automatique peut être définie pour tous les utilisateurs ou pour un utilisateur unique.
Les programmes exécutés au démarrage pour tous les utilisateurs sont définis à l'un des emplacements suivants :

- `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`
- `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`

Les programmes exécutés au démarrage pour l'utilisateur courant sont définis à l'un des emplacements suivants :

- `C:\Users\{nom-de-l'utilisateur}\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup`
- `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`

Voyons à présent comment effectuer cette manipulation.

L'utilitaire de configuration système MSConfig

Pour consulter la liste des programmes lancés automatiquement au démarrage, vous pouvez utiliser l'utilitaire de configuration du système intégré à Windows. Pour le démarrer,

1. Ouvrez le menu *Démarrer*, saisissez `msconfig` dans la barre de recherche, puis tapez sur la touche *Entrée*.
2. Sélectionnez l'onglet *Démarrage* pour consulter la liste des programmes lancés au démarrage de l'ordinateur.
3. Désactivez le démarrage automatique des programmes inutiles en décochant la case en début de ligne.

Autoruns, utilitaire de gestion des programmes de démarrage

Logiciel gratuit distribué par Microsoft, Autoruns se présente sous la forme d'un simple exécutable. Il suffit donc de le placer sur son disque dur, puis de double-cliquer sur son icône pour obtenir des informations très détaillées sur les programmes lancés au démarrage. Pour vous le procurer, rendez-vous sur le site www.sysinternals.com.

Dans Autoruns, ouvrez le menu *File* et cliquez sur *Run as administrator* pour afficher la totalité des informations. Utilisez l'onglet *Logon* pour afficher la liste des programmes qui sont lancés au démarrage.

Avant de supprimer complètement un programme du démarrage automatique, désactivez-le dans un premier temps en décochant la case en début de ligne. Ainsi, si le fait d'avoir désactivé le programme au démar-

rage entraîne un dysfonctionnement de l'ordinateur, il vous sera facile de le réactiver en cochant la case de nouveau.

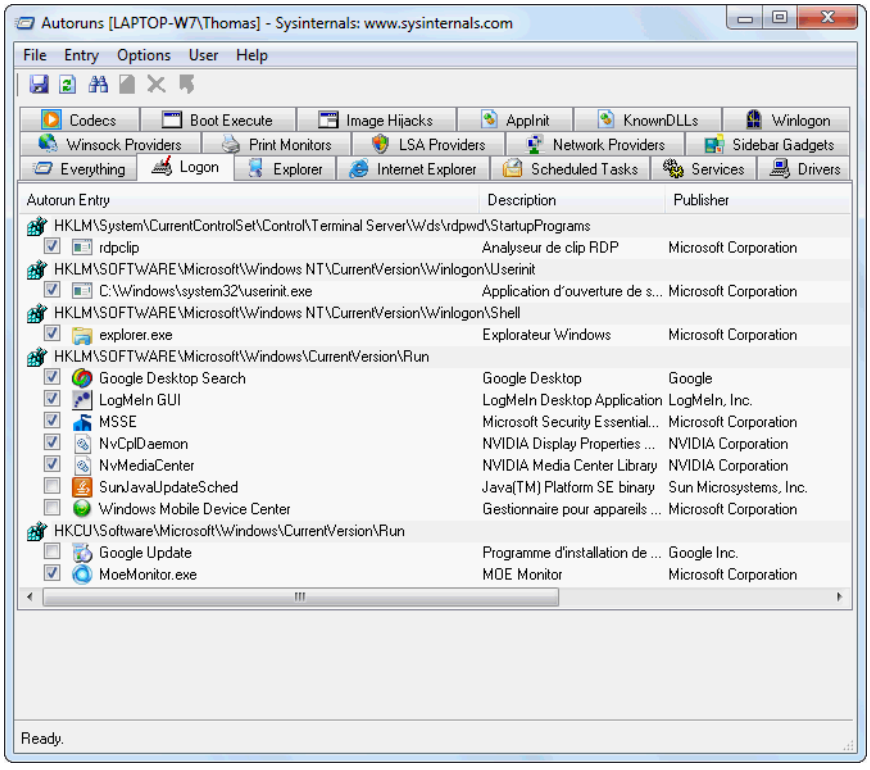


Figure 12–5
Onglet Logon de Autoruns

Nettoyer le disque dur

Au fur et à mesure de l'utilisation de Windows, les différents logiciels installés ainsi que le système lui-même créent des fichiers temporaires, qui ne sont pas indispensables au fonctionnement et qui occupent inutilement de l'espace sur le disque. Ainsi, les fichiers temporaires sont créés notamment lors de l'installation de nouveaux logiciels, lors des crashs de Windows ou lorsque des programmes cessent de fonctionner normalement.

Comme ses prédécesseurs, Windows 7 propose un utilitaire de nettoyage de disque qui se charge de supprimer tous les fichiers superflus. Voici comment le lancer :

1. Saisissez `nettoyage de disque` dans la barre de recherche du menu *Démarrer*.
2. Cliquez ensuite sur le lien *Nettoyage de disque* qui apparaît dans la liste.
3. Le nettoyeur de disque vous demande tout d'abord de sélectionner le disque dur que vous souhaitez nettoyer.

EN PRATIQUE Ne pas oublier la corbeille

La corbeille est également un emplacement qui peut vite occuper un volume considérable si vous avez tendance à oublier de la vider régulièrement.

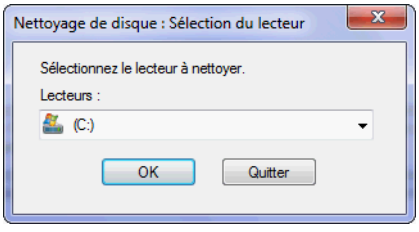


Figure 12–6
Choix du disque à nettoyer

4 Lorsque vous avez sélectionné le lecteur de votre choix et cliqué sur le bouton *OK*, Windows analyse tous les emplacements susceptibles de contenir des fichiers à nettoyer.

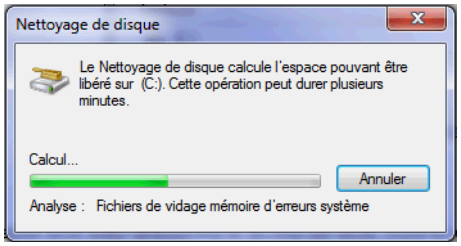


Figure 12–7
Analyse du disque

5 Lorsque l'analyse est terminée, Windows affiche le résultat sous la forme d'une liste d'éléments précédés par des cases à cocher. Chaque ligne représente un ensemble de fichiers pouvant être nettoyés.

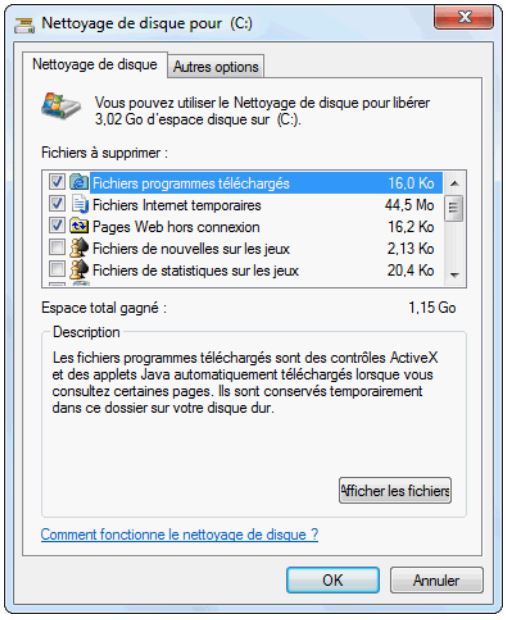


Figure 12–8
Liste des éléments à nettoyer

6 Pour obtenir plus de détails sur l'un des éléments, cliquez sur la ligne de votre choix, puis consultez le panneau *Description*.

Si vous n'avez pas démarré le nettoyeur de disque avec les privilèges administrateur, le bouton *Nettoyer les fichiers système* apparaît dans la partie *Description*. Si vous cliquez sur ce bouton, l'UAC affichera l'habituelle fenêtre d'élévation de privilèges.

7 Une fois identifié en tant qu'administrateur, un nouvel onglet apparaît dans le nettoyeur de disque. Il vous donne accès à des options de net-

EN PRATIQUE Actions supplémentaires

Pour certains éléments, des actions supplémentaires sont disponibles, par exemple, afficher les fichiers qui seront supprimés.

toyage supplémentaires. Le bouton *Nettoyer*, situé dans le cadre *Programmes et fonctionnalités*, est un simple raccourci vers le panneau *Programmes et fonctionnalités* qui permet de désinstaller les logiciels installés sur le système. Le nettoyeur de disque vous fera également gagner de l'espace disque en supprimant les données stockées dans les points de restauration. En général, si le système fonctionne de manière stable depuis quelque temps, il est tout à fait possible de supprimer tous les points de restauration que le système a créés antérieurement (en conservant bien sûr le dernier). Pour cela, cliquez sur le bouton *Nettoyer* dans le cadre *Restauration du système et clichés instantanés*.

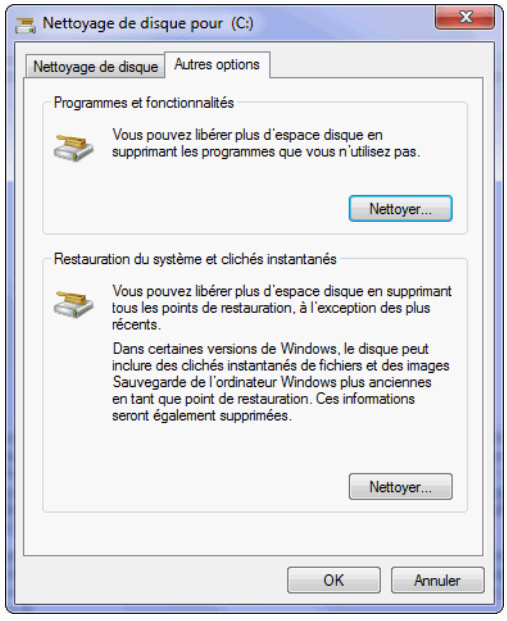


Figure 12–9
Onglet Autres options du nettoyeur de disque

Défragmenter le disque

Votre disque dur vous paraît lent. Plusieurs raisons peuvent expliquer ce ralentissement : soit votre disque est plein, soit, s'il reste de l'espace libre, il est temps de le défragmenter.

Comprendre la fragmentation

Pour saisir l'importance de la défragmentation de disque, il faut tout d'abord comprendre comment Windows stocke physiquement les fichiers sur le disque dur.

Sous Windows 7, le système de fichiers est NTFS (*New Technology File System*). Ce système de fichiers a été créé en 1993 et succède à la technologie FAT utilisée à l'origine par MS-DOS. FAT possédait de nombreuses lacunes comme des limitations de taille de fichier, une absence de gestion de la sécurité et du multi-utilisateur. Les fonctionnalités principales de NTFS sont :

- la gestion des droits utilisateur sur les fichiers et répertoires ;
- la compression des fichiers ;
- le chiffrement des fichiers (technologie EFS) ;
- l'attribution de quotas par volume.

Tout comme FAT, le système de fichiers NTFS est basé sur une table de fichiers appelée *Master File Table* ou MFT. Elle contient toutes les données concernant les fichiers comme leurs attributs et leur emplacement physique sur le disque. Elle se présente sous la forme d'une base de données relationnelle constituée d'enregistrements correspondant aux fichiers et dans lesquels les colonnes contiennent les attributs. La MFT contient d'ailleurs un enregistrement pour se décrire elle-même. Elle est dupliquée sur le disque pour éviter tout risque de perte de données en cas de défaillance d'un secteur.

Lorsque vous écrivez un fichier sur un disque dur vide, ses données sont stockées les unes à la suite des autres sur le disque. Lorsque vous créez un deuxième fichier, son contenu s'écrit à la suite du premier fichier sur le disque et ainsi de suite avec les fichiers suivants. Jusqu'ici, pas de problème.

Figure 12–10 Contenu initial du disque dur

Imaginons maintenant que vous supprimez des fichiers. Des « trous » se forment alors sur le disque.

Figure 12–11 Les fichiers de couleur mauve et bleu ont été supprimés : il y a des trous.

Si vous enregistrez maintenant un fichier un peu plus grand, il vient combler les trous. Le fichier va donc être stocké physiquement en plusieurs endroits distincts sur le disque. La tête de lecture du disque dur devra parcourir une plus grande distance pour lire la totalité du fichier. Un fichier stocké en plusieurs endroits du disque est appelé fichier fragmenté.

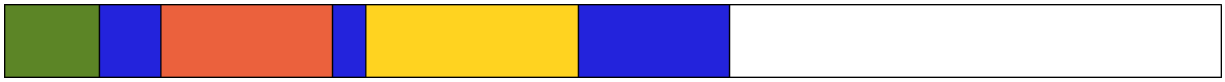


Figure 12–12 On écrit maintenant le fichier bleu foncé : il est fragmenté en 3 parties.

La défragmentation rassemble tous les fragments de fichiers éparpillés sur le disque dur en replaçant les fragments d'un même fichier dans une zone contiguë.

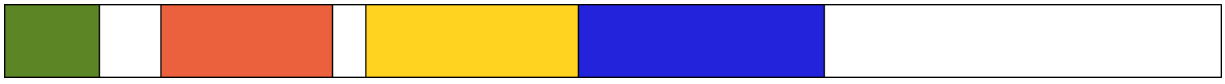


Figure 12–13 Après défragmentation, le fichier bleu foncé est regroupé dans un espace disque contigu. Il n'est plus fragmenté.

ASTUCE Optimiser la défragmentation

Afin d'optimiser au maximum le travail du défragmenteur de disque, il est recommandé de nettoyer le disque dur, en particulier les fichiers temporaires et la corbeille. En effet, il n'est pas nécessaire de défragmenter des fichiers qui ne seront plus utilisés et qui prennent de la place inutilement sur le disque. Pour cela, vous pouvez utiliser l'utilitaire de nettoyage de disque décrit précédemment.

Défragmenter le disque

Le défragmenteur de disque intégré à Windows se lance de la manière suivante :

1. Saisissez `defragmenteur` dans la zone de recherche du menu *Démarrer*.
2. Cliquez ensuite sur *Défragmenteur de disque*.
3. Pour déterminer si vos différents disques durs doivent être défragmentés, il faut les analyser. Pour analyser un lecteur, cliquez sur celui-ci dans la liste, puis appuyez sur le bouton *Analyser le disque*. Windows 7 parcourt alors le contenu du disque à la recherche de fichiers fragmentés. À la fin de l'analyse, le défragmenteur vous indique la proportion du disque qui contient des fichiers fragmentés.
4. Pour démarrer la défragmentation, cliquez sur le bouton *Défragmenter le disque*.

EN PRATIQUE Pendant la défragmentation

La défragmentation peut être longue, mais vous pouvez continuer à utiliser votre ordinateur pendant ce temps. Cependant, il est préférable de ne pas le faire.

Vous pouvez configurer l'utilitaire de dégragmentation de disque pour qu'il défragmente automatiquement le disque dur à la fréquence que vous souhaitez. Cette fréquence dépend de l'utilisation que vous en faites. Si vous créez beaucoup de fichiers et en supprimez souvent, vous devrez défragmenter plus souvent que si vous utilisez peu votre disque dur.

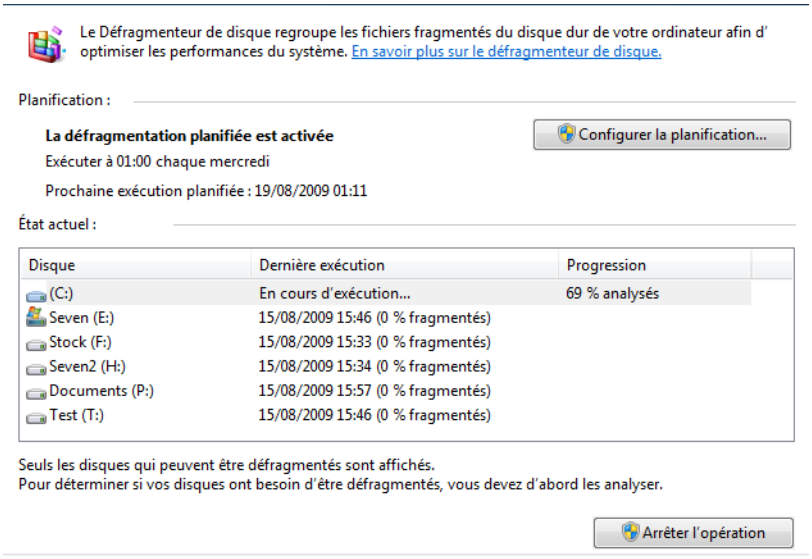


Figure 12–14
Analyse du lecteur C:

Windows 7 propose de planifier le défragmenteur de disque, c'est-à-dire que la défragmentation s'effectuera automatiquement, sans intervention de votre part à des jours et heures que vous choisissez en cliquant sur le bouton *Configurer la planification*... La planification évite d'oublier de défragmenter régulièrement votre disque dur.

En ligne de commande

Il est possible d'appeler l'utilitaire de défragmentation en ligne de commande (ou dans un fichier batch). Il faut pour cela faire appel à l'utilitaire `defrag.exe`.

La syntaxe de la commande est :

```
defrag.exe <volume> <options>
```

Le volume représente la lettre du lecteur suivie du caractère deux-points. Les différentes options pouvant être utilisées sont récapitulées dans le tableau 12-1 :

Tableau 12–1 Options de la commande defrag.exe

Option	Description
/A	Effectue une analyse sur le volume spécifié.
/C	Effectue l'opération sur tous les volumes.
/E	Effectue l'opération sur tous les volumes sauf ceux spécifiés.
/H	Exécute l'opération à une priorité normale (par défaut, la priorité du processus est basse).

Tableau 12–1 Options de la commande defrag.exe (suite)

Option	Description
/M	Exécute l'opération sur chaque volume en parallèle et en arrière-plan.
/T	Permet de suivre une opération déjà en cours sur le volume spécifié.
/U	Affiche l'état d'avancement de l'opération à l'écran.
/V	Affiche une sortie détaillée comprenant notamment les statistiques de fragmentation.
/X	Effectue une consolidation de l'espace libre sur les volumes spécifiés.

Par exemple, pour analyser l'état de la fragmentation du lecteur C:, lancez la commande suivante :

```
defrag.exe C: /a /u /v
```

Optimiser le paramétrage

Différents paramètres de Windows améliorent les performances de votre ordinateur. Par exemple, vous pouvez modifier les paramètres visuels de Windows ou modifier le mode d'alimentation. Nous allons explorer ces deux options dans les sections suivantes.

Modifier les paramètres visuels de Windows

Les paramètres visuels servent à ajuster les options d'un certain nombre d'effets présents dans l'interface de Windows 7. Voici la procédure à suivre pour accéder à ces options :

1. Ouvrez le menu *Démarrer*, puis cliquez avec le bouton droit sur *Ordinateur* et choisissez *Propriétés* dans le menu contextuel.
2. Dans la colonne de gauche de la fenêtre *Système*, cliquez sur *Paramètres avancés*.
3. Dans le cadre *Performances*, cliquez sur le bouton *Paramètres*. La fenêtre de paramétrage des effets visuels s'affiche.

Cette fenêtre est également accessible depuis le module *Informations et outils de performance* du panneau de configuration en cliquant sur *Effets visuels* dans la colonne de gauche.

Par défaut, Windows détecte automatiquement la meilleure stratégie à adopter en fonction de votre configuration matérielle. Avant de commencer votre paramétrage dans cette fenêtre, décidez si vous préférez optimiser l'apparence de Windows ou bien les performances du système.

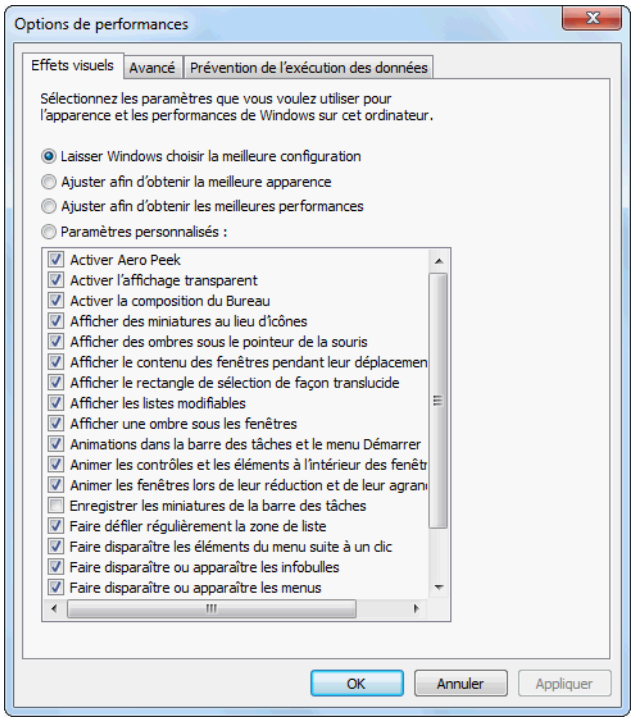


Figure 12–15
Fenêtre de paramétrage des effets visuels de Windows

- Si vous souhaitez profiter de tous les effets graphiques proposés par Windows, cochez le bouton radio *Ajuster afin d'obtenir la meilleure apparence*. Tous les effets visuels sont alors activés dans la liste. Ce choix nécessite un ordinateur performant pour profiter pleinement de tous les effets.
- Dans le cas où vous n'êtes pas intéressé par l'aspect esthétique du système, mais que votre seule préoccupation est d'utiliser une machine performante, sélectionnez le bouton radio *Ajuster afin d'obtenir les meilleurs performances*. L'interface graphique sera alors dépouillée de tout effet visuel inutile dans le but de préserver les ressources du système. Cette option désactive l'interface Windows Aero et votre thème sera semblable à celui de Windows 98.
- Le dernier bouton radio vous permet de personnaliser chaque effet. Vous pouvez activer ou désactiver des effets de transparence et d'ombre ainsi que divers autres effets en cochant les cases de votre choix dans la liste.

Après avoir configuré les effets visuels, cliquez sur le bouton *OK* pour appliquer les changements et fermer la fenêtre de paramètres.

Modifier les options d'alimentation

Les options d'alimentation influent sur les performances de votre système. En effet, suivant le mode d'alimentation que vous choisissez, Windows ajuste les performances du système. Cette fonctionnalité est particulièrement utile sur les ordinateurs portables.

Pour modifier les options d'alimentation sur un ordinateur portable, il suffit de cliquer sur l'icône batterie dans la barre de notification système (à côté de l'horloge).

Dans le cas d'un ordinateur de bureau, ouvrez le panneau de configuration, cliquez sur la catégorie *Système et sécurité*, puis sur *Options d'alimentation*.

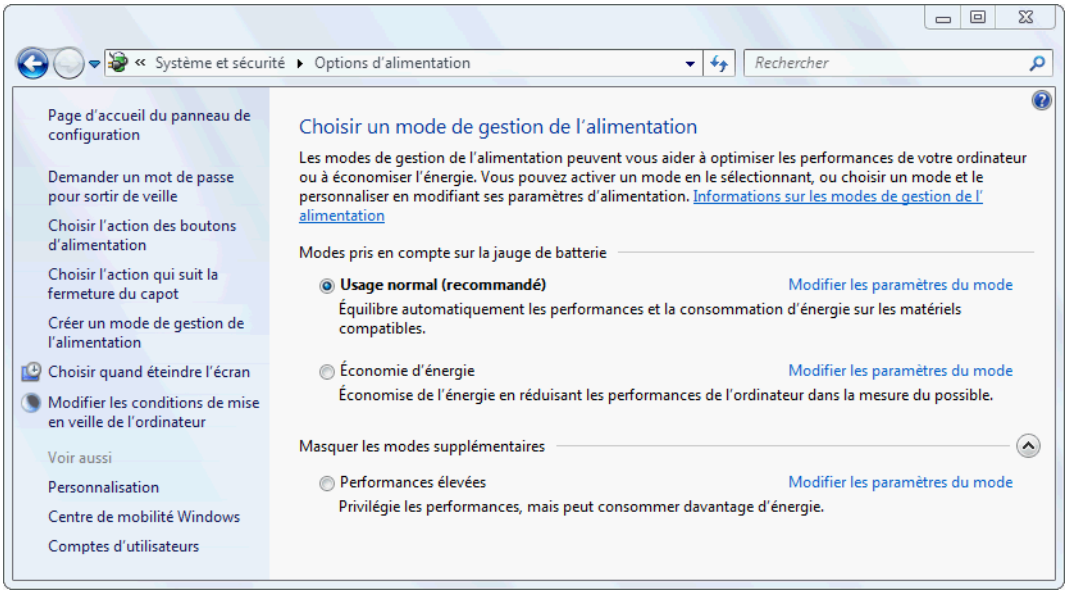


Figure 12–16 Panneau de configuration des options d'alimentation

CAS PARTICULIER **Ordinateur portable**

Attention, ceci se fera au détriment de la consommation électrique et donc de l'autonomie.

Lorsque vous choisissez le mode *Économie d'énergie*, les performances du processeur sont volontairement diminuées pour conserver le maximum d'énergie électrique. Si vous souhaitez améliorer les performances de votre système, choisissez le mode *Performances élevées*.

Configuration intermédiaire entre *Économie d'énergie* et *Performances élevées*, le mode *Usage normal* convient dans la plupart des cas. Si vous rencontrez des problèmes de performances avec un jeu vidéo ou une application 3D, essayez le mode *Performances élevées*.

Améliorer les performances du système de fichiers

Il est possible d'augmenter légèrement les performances du système de fichiers NTFS. En effet, lors de chaque accès à un fichier, le système de fichiers met à jour la date de dernier accès dans les propriétés du fichier. Vous pouvez donc choisir de ne pas mettre à jour cette date afin de gagner en performances.

Pour désactiver la mise à jour systématique de la date du dernier accès, il faut modifier une valeur dans le registre Windows :

1. Ouvrez le menu *Démarrer*, saisissez `regedit` dans la barre de recherche, puis appuyez sur *Entrée* quand la ligne `regedit.exe` apparaît dans le menu.
2. Déroulez l'arborescence du registre comme suit : *HKEY_LOCAL_MACHINE>SYSTEM>CurrentControlSet>Control>FileSystem*.
3. Dans la partie de droite, repérez la valeur `NtfsDisableLastAccessUpdate`. Double-cliquez sur son nom et mettez `1` dans la zone *Données de la valeur*.

COMPRENDRE
Organisation du registre Windows

Le registre Windows est composé d'un ensemble de clés, de valeurs et de données. Les clés et les sous-clés contiennent des valeurs. Chaque valeur contient une donnée (texte, valeur booléenne, numérique ou hexadécimale). Dans l'éditeur de registre Regedit, les clés et sous-clés sont représentées dans la partie gauche de la fenêtre sous la forme d'une arborescence de petits dossiers. Lorsqu'une clé est sélectionnée, la partie droite de la fenêtre affiche la liste des valeurs contenues dans cette clé, ainsi que la donnée contenue dans chacune des valeurs. Pour modifier une valeur, il suffit de double-cliquer dessus.
Attention, la modification du registre est une opération délicate et sensible. Une mauvaise manipulation peut rendre le système inutilisable et nécessiter une réinstallation de Windows.

Augmenter la mémoire cache avec ReadyBoost

Sur un PC, les vitesses du processeur et de la mémoire sont largement supérieures à celles des disques durs. Le disque dur est donc le périphérique qui fait perdre le plus de temps à l'ordinateur. Afin de réduire le temps d'attente, Windows utilise un système de cache : il stocke en mémoire les données souvent lues ou susceptibles d'être lues. Ainsi, l'accès à ces données se fera beaucoup plus rapidement.

L'idéal est donc de disposer d'une grande mémoire cache pour accélérer encore les lectures. Le problème est que la mémoire vive, utilisée comme mémoire cache, s'avère relativement chère. La solution à ce problème a été trouvée grâce à la technologie ReadyBoost. Elle utilise des périphériques USB externes, tels que des clés USB comme mémoire cache additionnelle. En réalité, ReadyBoost sert d'intermédiaire entre la mémoire vive et le disque dur.

Voici la procédure à suivre pour activer ReadyBoost sur un périphérique USB :

1. Connectez le périphérique à votre ordinateur.

VÉRIFIER **Caractéristiques requises pour un périphérique ReadyBoost**

Pour savoir si votre clé USB ou périphérique externe est compatible avec ReadyBoost, vérifiez qu'elle respecte les caractéristiques suivantes :

- la capacité doit être comprise entre 256 Mo et 32 Go ;
- l'espace libre sur le périphérique doit être d'au moins 235 Mo ;
- le périphérique doit être compatible USB 2 ;
- le taux de transfert en lecture doit être au moins égal à 2,5 Mo/s ;
- le taux de transfert en écriture doit être au moins égal à 1,75 Mo/s.

2 Ouvrez le menu *Démarrer* et cliquez sur *Ordinateur*.

3 Cliquez avec le bouton droit sur le périphérique à utiliser en ReadyBoost et choisissez *Propriétés* dans le menu contextuel.

4 Sélectionnez ensuite l'onglet *ReadyBoost*. Si votre périphérique est compatible, les options de ReadyBoost sont disponibles dans cet onglet.

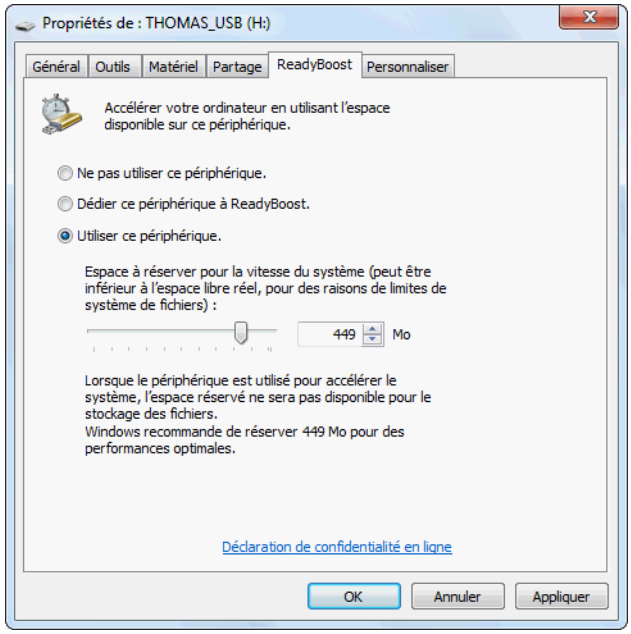


Figure 12–17
Propriétés ReadyBoost pour un périphérique USB

5 Lorsque votre périphérique est compatible avec la technologie ReadyBoost, vous avez la possibilité de choisir parmi trois options :
- *Ne pas utiliser ce périphérique pour ReadyBoost*.
- *Dédier ce périphérique à ReadyBoost* : la totalité de l'espace libre sur le périphérique sera utilisée pour ReadyBoost.
- *Utiliser ce périphérique* : vous pouvez choisir manuellement la quantité d'espace à allouer sur le périphérique USB. Windows 7 affiche une préconisation en fonction des caractéristiques de votre périphérique.

6 Une fois ReadyBoost activé, Windows crée un fichier nommé `ReadyBoost.sfcache` de la taille spécifiée dans les paramètres ReadyBoost à la racine du lecteur.

Vous pouvez éjecter un périphérique sur lequel ReadyBoost est activé. La fonctionnalité ReadyBoost recommencera à fonctionner sur le périphérique dès que vous le connecterez de nouveau au système.

Optimiser la mémoire virtuelle

Nous le savons tous, la mémoire vive (ou RAM) est un composant essentiel de l'ordinateur. En effet, plus le PC en contient, mieux il fonctionne. De manière générale, plus il y a de mémoire vive (RAM) installée dans un ordinateur, plus les programmes s'exécutent rapidement et plus vous pouvez lancer de programmes simultanément. L'idéal est donc d'avoir le plus de mémoire vive possible. Malheureusement, l'inconvénient majeur de la RAM est son prix.

Afin de permettre au système de disposer de plus de mémoire que de mémoire physique réellement installée, le mécanisme de la mémoire virtuelle a été implanté dans les systèmes d'exploitation. Il exploite les disques durs afin de stocker une partie des données présentes en mémoire. En effet, les disques durs possèdent une plus grande capacité et sont moins coûteux que la mémoire vive. Cependant, ils traitent les données à une vitesse bien inférieure à celle de la mémoire vive.

Windows utilise la mémoire virtuelle si la quantité de mémoire vive disponible est insuffisante. Les zones mémoire les moins utilisées sont déplacées de la mémoire vive vers la mémoire virtuelle. La place ainsi libérée dans la RAM va pouvoir être utilisée par un autre logiciel.

Si le manque de mémoire vive ralentit votre ordinateur, la première chose à faire est évidemment d'ajouter des barrettes de mémoire. Si vous n'avez plus d'emplacement sur votre carte mère ou si cette opération est trop coûteuse, augmentez la mémoire virtuelle. Attention, dans ce cas, le gain de performance ne sera pas aussi important que si vous aviez ajouté de la mémoire physique, mais cela constitue une solution si vous rencontrez des messages d'erreur de type « Mémoire insuffisante ».

Pour accéder aux options de mémoire virtuelle, la procédure est la suivante :

1. Ouvrez le menu *Démarrer*, puis cliquez avec le bouton droit de la souris sur *Ordinateur*. Sélectionnez *Propriétés* dans le menu contextuel.
2. Dans la colonne de gauche de la fenêtre *Système*, cliquez sur le lien *Paramètres système avancés*.
3. Cliquez sur le bouton *Paramètres...* dans le cadre intitulé *Performances*.
4. Sélectionnez l'onglet *Avancé*, puis cliquez sur le bouton *Modifier...* dans le cadre *Mémoire virtuelle*. La fenêtre de paramétrage de la mémoire virtuelle s'affiche alors.
5. Par défaut, la case *Gestion automatique du fichier d'échange pour les lecteurs* est cochée et Windows se charge de définir les disques durs contenant de la mémoire virtuelle et la quantité d'espace disque allouée sur chacun d'eux. Laisser cette case cochée est en général la

FICHIER

Matérialisation de la mémoire virtuelle

La mémoire virtuelle est matérialisée sur le disque par un fichier système caché appelé fichier d'échange, fichier de pagination ou swap. Il porte le nom `pagefile.sys` et est présent sur chaque lecteur sur lequel la mémoire virtuelle est activée.

configuration la plus adaptée. Si vous souhaitez personnaliser les paramètres de mémoire virtuelle, décochez la case.

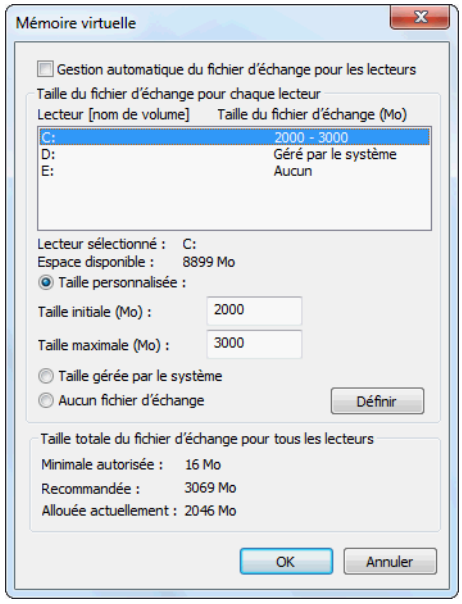


Figure 12–18
Fenêtre de configuration de la mémoire virtuelle

6 Une fois la case décochée, les autres zones de la fenêtre sont modifiables. La mémoire virtuelle est configurée de manière indépendante pour chacun des lecteurs de disque dur de l'ordinateur. Un récapitulatif de la configuration s'affiche sous forme de liste. La partie inférieure de la fenêtre propose un résumé de la configuration actuelle de la mémoire virtuelle, tous lecteurs confondus. Windows recommande également une taille de mémoire virtuelle en fonction des caractéristiques de votre système.

Voici comment modifier la configuration de l'un des lecteurs :

1 Dans la liste, sélectionnez le lecteur.

2 Définissez les options de mémoire virtuelle. Trois choix sont possibles :

- *Taille personnalisée* : si vous cochez ce bouton radio, vous définissez manuellement une taille minimale et une taille maximale pour le fichier de mémoire virtuelle. Pour vous aider dans la saisie, l'espace actuellement disponible sur le lecteur sélectionné est affiché au-dessus des zones de saisie.
- *Taillé gérée par le système* : la taille du fichier de mémoire virtuelle est définie par le système qui l'ajuste en fonction de la demande mémoire.
- *Aucun fichier d'échange* : si vous choisissez cette option, Windows n'utilisera pas le lecteur sélectionné pour stocker de la mémoire virtuelle.

3 Validez ensuite votre choix en cliquant sur le bouton *Définir*. Vous pouvez ensuite recommencer l'opération avec les autres lecteurs.

4 Une fois la configuration achevée pour tous les lecteurs, validez en cliquant sur le bouton *OK*.

5 Si vous avez augmenté la taille de la mémoire virtuelle, le redémarrage de la machine ne sera pas nécessaire. En revanche, si vous avez diminué la taille, vous devrez redémarrer votre ordinateur pour que la modification soit prise en compte.

ATTENTION **Recommandations de Windows**

Microsoft recommande de ne pas désactiver complètement la mémoire virtuelle et de ne pas supprimer le fichier d'échange.

En résumé

Dans ce chapitre, nous avons appris à optimiser notre ordinateur afin d'en améliorer les performances. Dans un premier temps, nous avons évalué les performances matérielles de l'ordinateur, puis nous avons détaillé les différents nettoyages à faire sur le disque permettant de gagner de l'espace.

Nous avons expliqué ce qu'est la fragmentation et comment défragmenter un disque dur. Nous avons également vu comment le paramétrage de Windows 7 permet d'optimiser les performances.

chapitre 13

Sécuriser son système

La sécurité est la pierre angulaire d'un système équilibré et fiable. Lorsque votre système est mal configuré, vous vous exposez aux virus ou à l'exécution d'opérations qui auraient dû être interdites. Votre système devient alors instable et vos données sont en péril. Il est donc indispensable d'être proactif et prévoyant pour se prémunir contre tout désagrément.

SOMMAIRE

- Se protéger des virus et autres logiciels indésirables
- Configurer son pare-feu
- Surveiller son système
- Installer le pare-feu Windows

MOTS-CLÉS

- Checklist
- Adware
- Spyware
- Virus
- Cheval de Troie
- Attaque
- Infection
- Windows Defender
- Pare-feu
- Journalisation

Ce chapitre présente les différents types d'éléments contre lesquels il est nécessaire de se protéger. Nous expliquons ensuite comment Windows 7 permet de se protéger contre les menaces, et nous décrivons les moyens qui sont à votre disposition pour renforcer au mieux votre système.

Surveiller et contrôler son système d'exploitation

Chaque nouvelle version d'un système d'exploitation apporte son lot de nouveautés et rend bien souvent l'administration du système plus complexe. Windows 7 n'échappe pas à cette règle et il a donc fallu l'équiper d'un centre de contrôle intuitif permettant d'avoir un compte-rendu général (concernant les attaques extérieures, les virus, l'état du système au niveau de ses mises à jour, etc.) du système. C'est pour répondre à ce besoin que le centre de maintenance a été ajouté au système. Le centre de maintenance a deux objectifs :

- Proposer un aperçu rapide de l'état du système du point de vue de la sécurité et de la configuration des sauvegardes.
- Proposer un accès rapide aux outils et aux informations pour améliorer la maintenance du système.

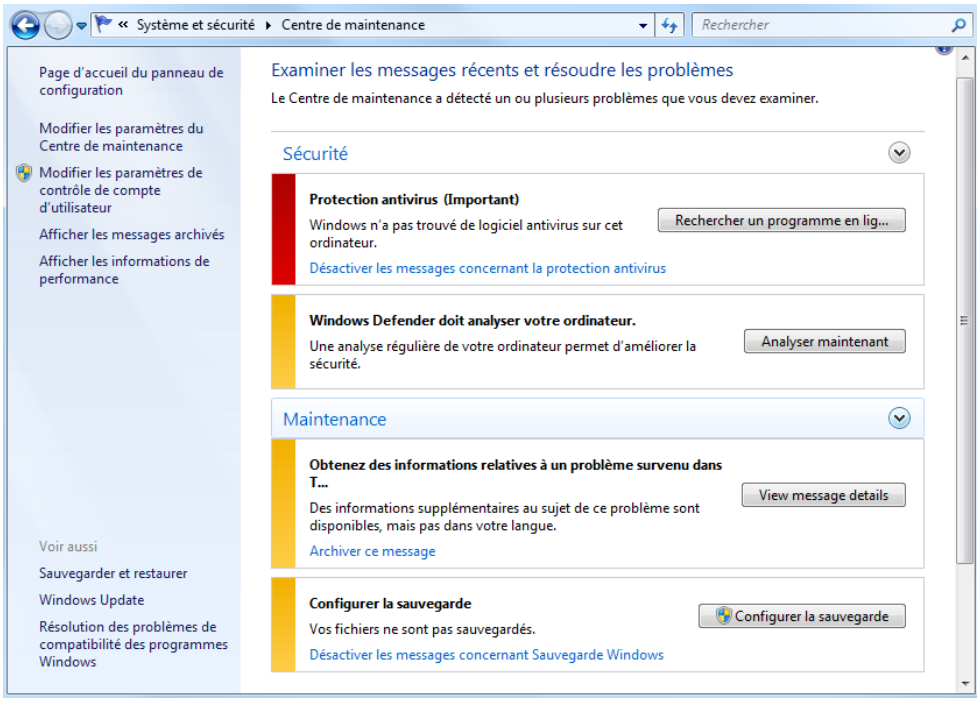


Figure 13–1
Le centre de maintenance

Il s'agit d'un emplacement de contrôle centralisé depuis lequel vous pourrez entreprendre une grande partie des actions nécessaires au bon fonctionnement de votre système. Voici comment y accéder :

1. Ouvrez le menu *Démarrer*.
2. Cliquez sur *Panneau de configuration*.
3. Cliquez alors sur le libellé *Centre de maintenance*.

L'interface du centre de maintenance comporte deux parties principales :

- la barre latérale contient des raccourcis vers les outils du centre de maintenance (comme le paramétrage ou encore le journal de suivi des messages du système) ;
- tandis que la partie de droite propose un compte-rendu de l'état du système.

Le centre de maintenance fonctionne par bloc afin de représenter l'état actuel d'éléments bien précis du système relevant soit de la sécurité du système (antivirus, Windows Defender, etc.), soit de la maintenance (sauvegarde, mise à jour système, recherche de solutions aux problèmes, etc.), et utilise des couleurs pour indiquer le niveau de risque et l'état du système. Les blocs sont alors marqués soit par un bandeau jaune en cas d'avertissement de niveau moyen, soit par un bandeau rouge lorsqu'un problème sérieux est détecté.

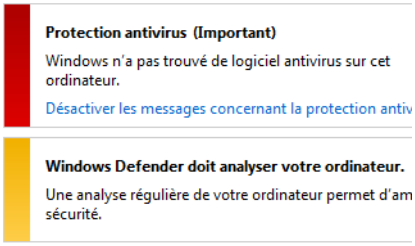


Figure 13–4
Le bandeau de couleur permet de repérer rapidement la criticité de l'état du système.

Chacun des blocs est dépliable et propose alors différentes actions contextuelles pour corriger les problèmes signalés. Par exemple, si l'antivirus n'est pas à jour, un lien pour lancer la mise à jour des définitions virus s'affichera, et si jamais le système ne détecte aucun antivirus, un lien vers une page de téléchargement des principaux antivirus vous sera proposé.

La checklist de sécurité

Le centre de maintenance permet de vérifier un certain nombre de paramètres de sécurité que tout bon administrateur système doit mettre en place. En voici la liste détaillée :

Astuce Le centre de maintenance depuis la barre des tâches

Le centre de maintenance est associé à une icône se trouvant dans la zone de notification (à côté de l'horloge). Cette icône change d'apparence en fonction de l'état du système.

Figure 13–2 Icône du centre de maintenance avec (à droite) et sans (à gauche) problème

Si vous cliquez sur l'icône, les messages du système s'affichent, vous informant si le système lui semble insuffisamment protégé ou tout simplement si un incident est arrivé et qu'une action de votre part est requise pour résoudre le problème.

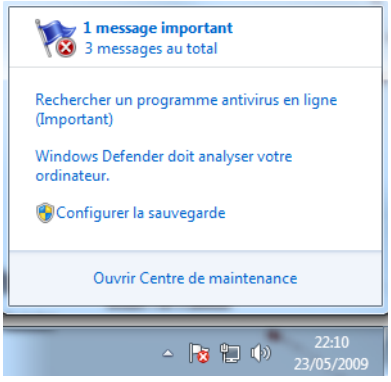


Figure 13–3 Affichage des informations du centre de maintenance

- Windows Defender : Windows Defender doit être activé et un scan récent de la machine doit avoir été effectué afin de s'assurer qu'aucun logiciel indésirable n'est présent.
- Contrôle utilisateur : le contrôle utilisateur doit être activé, y compris pour les administrateurs.
- Sauvegarde et restauration : une sauvegarde doit être mise en place afin de sauvegarder régulièrement les données essentielles. Ce point est abordé en détail au chapitre 8.
- Windows Update : il faut que toutes les mises à jour critiques du système soient installées.
- Pare-feu Windows : le pare-feu doit être activé afin de protéger l'ordinateur contre les *hackers* et les logiciels indésirables tentant d'y accéder à travers le réseau.

C'est seulement lorsque tous ces points ont été vérifiés que le centre de maintenance estime que le système est convenablement sécurisé.

La checklist de maintenance

Le centre de maintenance utilise également une checklist de bonnes pratiques de maintenance. Celle-ci s'intéresse particulièrement à la fiabilité du système et à la pérennité des données qu'il contient. Si cette liste concerne également la mise à jour du système et la mise en place de procédures de sauvegarde, elle met surtout en avant l'outil de résolution des problèmes.

Dès qu'un problème survient sur une application ou sur le système, il est consigné dans le journal de log et l'application Résolution des problèmes remonte alors à Microsoft les détails du problème. Par la même occasion, l'application interroge la base de connaissances de Microsoft afin de vérifier si une manipulation est possible ou si un patch est disponible pour corriger le problème. Nous traiterons en détail les menus *Dépannage* et *Récupération*, ainsi que la résolution des problèmes dans le chapitre 15.

Les enjeux de la sécurité

De nos jours, la recrudescence de petits programmes indésirables que l'on nomme « pourriciels » ou *malwares* s'avère être une véritable plaie informatique. Ces logiciels, qui se répandent dans le monde entier grâce à Internet, sont une manne financière pour leurs créateurs et une vraie épine dans le pied pour les utilisateurs. On distingue plusieurs types de logiciels indésirables :

- Les virus, qui ont pour objectif d'empêcher le fonctionnement normal de l'ordinateur.
- Les *adwares*, qui affichent des publicités pour inciter l'utilisateur à acheter des produits.
- Les *spywares*, qui tentent de voler des informations personnelles (numéro de Carte Bleue, mot de passe, type de produit que l'utilisateur achète sur Internet, etc.);
- Les *bots (*robots*)*, petits programmes qui restent actifs sur votre ordinateur et attendent les ordres d'un attaquant distant. Par exemple, celui-ci pourra demander à votre ordinateur de porter une attaque DDoS contre un site web particulier.
- Les chevaux de Troie, qui sont des petits programmes permettant à un utilisateur distant de prendre le contrôle de votre ordinateur sans votre accord.

Ces logiciels sont plus nombreux que l'on ne le croit et ont surtout la fâcheuse tendance de s'installer à notre insu, bien souvent en même temps qu'un autre logiciel licite ou alors au sein de pièces jointes d'e-mail, que l'on pense inoffensives. Désormais, guérir et nettoyer son système est une manipulation courante pour beaucoup d'utilisateurs. Cependant, il vaut mieux tout faire pour se protéger et ne plus avoir à effectuer ces tâches de nettoyage des plus rébarbatives.

Se protéger signifie tout d'abord prendre de bonnes habitudes comme ne faire confiance à rien ni personne et analyser tout nouvel élément arrivant sur le système, mais c'est aussi utiliser les outils adéquats. Pour être efficace face à chaque menace (virus, *adwares* ou autres) il convient de faire appel à un outil dédié. Il est donc normal et recommandé de posséder différents outils ciblant chacun un type de malwares bien précis.

Attaques DDoS (Distributed Denial of Service)

Très complexes, les attaques par déni de service ont pour objectif de gêner, voire bloquer, le fonctionnement d'un serveur informatique en le submergeant de connexions utilisateur. Dans le cas d'une attaque distribuée, il s'agit bien souvent d'un certain type de virus, dit *bot*, qui contrôle des centaines de milliers (ou plus) de machines (appelées zombies), et leur donne l'ordre à la même seconde de se connecter à un même serveur. Ne pouvant rarement tenir la charge face à ces trop nombreuses connexions, les serveurs deviennent inaccessibles. Le seul moyen efficace de s'en protéger consiste à acheter et à mettre en place plusieurs serveurs parallèles pour redistribuer la charge des connexions, mais ceci a un coût élevé pour le propriétaire du site web.

Malwares

Le terme *malware* est la contraction des termes anglais *malicious* (malveillant) et *software* (logiciel) ; il se traduit donc littéralement par logiciel malveillant. Il s'agit d'un logiciel développé pour causer des dégâts à un système informatique. Dans la catégorie des malwares, on trouve donc très logiquement les virus, les chevaux de Troie, etc.

Se protéger des adwares et spywares

- Depuis les versions XP et Vista, Windows propose son propre logiciel de sécurité, Windows Defender, contre les indésirables logiciels espions. Windows Defender est un antispyware complet proposant des fonctionnalités de désinfection et de protection en temps réel. Il analyse non seulement les fichiers téléchargés sur Internet, les pièces jointes des e-mails, mais également les programmes qui s'exécutent sur votre ordinateur et essayent de modifier des paramètres de votre système, comme les fichiers Windows ou la liste des programmes à lancer au démarrage.

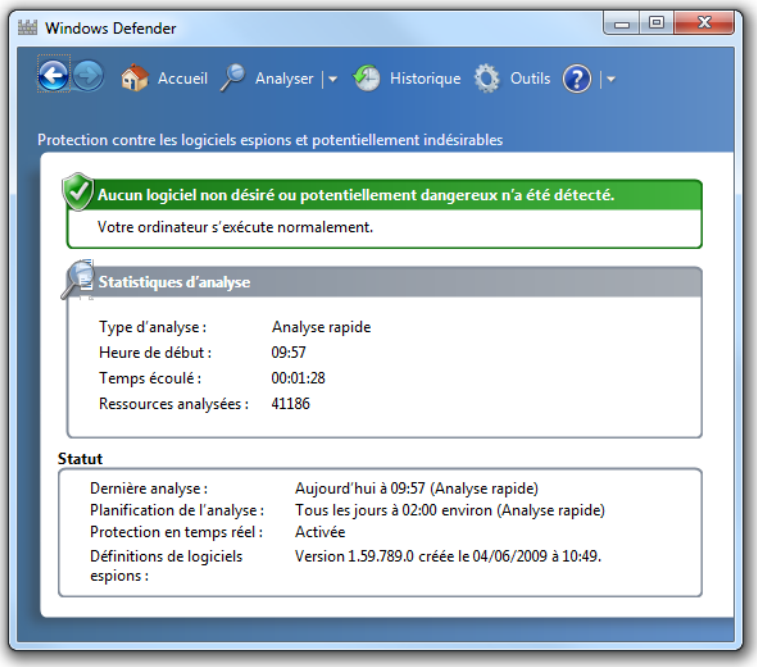


Figure 13–5
Écran principal de Windows Defender

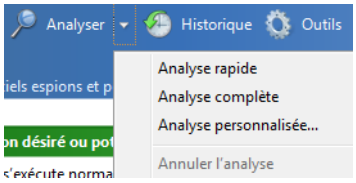


Figure 13–6
Analyse du système

Identifier les fichiers infectés avec l'analyse de Windows Defender

La première fonctionnalité de Windows Defender, disponible depuis son écran principal, est une analyse complète du système. Cette analyse est personnalisable en cliquant sur la flèche qui se trouve à droite du bouton *Analyser*. Il est alors possible de lancer une analyse rapide du système (seuls les fichiers système seront analysés) ou de lancer une analyse personnalisée, pour laquelle vous définissez les répertoires à vérifier.

Lors de l'analyse, différentes méthodes de recherche sont mises en œuvre pour traiter rapidement l'ensemble des fichiers de votre ordinateur. Pour chaque fichier, Windows Defender vérifie si sa signature (soit son nom, soit l'emplacement, soit la taille, soit ses métadonnées) correspond à un *malware* connu.

À la fin de l'analyse, Windows Defender affiche les résultats trouvés. Si des éléments dangereux ont été repérés, ils sont listés dans un tableau récapitulatif avec le nom du malware identifié, ses informations ainsi que l'emplacement des fichiers infectés. À vous de décider, ensuite, si vous préférez ignorer ou supprimer le malware.

Bien que Windows Defender constitue une protection en temps réel, une analyse régulière du système est fortement recommandée.

Paramétrer finement Windows Defender

Alors que les précédentes versions de Windows Defender étaient fort peu personnalisables, la version incluse au sein de Windows 7 propose un grand nombre de paramétrages. Il est ainsi possible de configurer l'horaire précis où les analyses seront déclenchées, mais surtout de configurer leur exécution en précisant les répertoires et les périphériques à analyser.

DOMMAGE **Éléments exclus des analyses**

Par défaut, les périphériques USB et les pièces jointes des e-mails ne sont pas analysés.

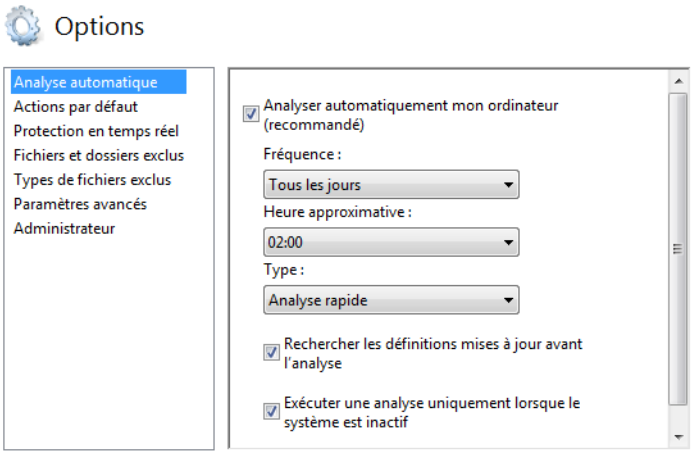


Figure 13–7
Panneau de configuration de Windows Defender

Pour contrôler le paramétrage de Windows Defender pour l'ensemble des utilisateurs, il est possible d'utiliser des stratégies de groupe locales.

1. Ouvrez la console de gestion des stratégies de groupe en saisissant `gpedit.msc` dans le menu *Démarrer*.
2. Dépliez l'arbre latéral.
3. Sélectionnez *Configuration de l'ordinateur*, puis *Modèles d'administration*. Sélectionnez *Composants Windows* et enfin *Windows Defender*.

Différentes possibilités vous sont proposées, vous pouvez notamment :

- Désactiver totalement Windows Defender dans le cas où vous souhaitez utiliser un utilitaire tiers.
- Configurer les rapports d'erreur envoyés au réseau Microsoft SpyNet.
- Forcer le téléchargement des dernières signatures logicielles avant chaque analyse du système.

Les paramétrages des stratégies sont prioritaires par rapport aux paramétrages utilisateur. Vous pouvez ainsi mieux contrôler la sécurité des différents profils.

Réseau Microsoft SpyNet

Cette base de connaissances de Microsoft répertorie les différents malwares existant afin d'en améliorer la détection future.

Se protéger des virus

Quid de la protection antivirale ? Comme toutes les versions précédentes, Windows 7 ne possède pas nativement d'antivirus. Disposer d'un antivirus dès l'installation du système aurait permis d'être directement protégé. Bien qu'éditant son propre antivirus, à savoir OneCare, Microsoft a décidé de ne pas intégrer directement d'antivirus, afin de se prémunir contre un éventuel procès antitrust.

Culture Microsoft et les procès antitrust

Les règles et lois sur la concurrence sont très strictes. Comme toute société en position dominante sur son marché, Microsoft a connu plusieurs procès pour abus de position dominante et concurrence déloyale pour avoir imposé son lecteur multimédia Windows Media Player dans son système d'exploitation. Au terme de plusieurs mois de procès, la firme de Redmond a été condamnée par la Commission européenne à vendre un système d'exploitation sur lequel le lecteur multimédia ne serait pas installé par défaut. C'est ainsi que sortirent les « versions N » de XP et de Vista, vendues au même prix, mais dépourvues de fonctionnalités multimédias. Sur les centaines de millions de Windows (toutes versions confondues) vendues depuis 2001 (sortie de Windows XP), on estime le nombre de ventes de Windows Édition N à quelques centaines, pour un coût incluant préparation, procès et distribution dépassant plusieurs dizaines de millions d'euros. Cette malheureuse expérience a motivé Microsoft à ne pas inclure d'antivirus.

Il vous faut donc installer un antivirus sur votre système. En effet, seul un antivirus est capable de repérer efficacement les virus présents sur votre ordinateur, car ceux-ci sont aujourd'hui des logiciels parfois très évolués, capables de changer de forme, de nom, d'emplacement et pour certains, de manière de se reproduire de système en système.

Un antivirus utilise trois méthodes différentes pour repérer les virus :

- La signature : chaque virus a une empreinte propre, constituée, en général, par une partie de leur code. Les empreintes sont répertoriées dans les bases de données des antivirus. C'est la méthode la plus répandue.
- L'analyse heuristique : cette méthode permet surtout de découvrir des virus qui ne sont pas encore connus et répertoriés. L'antivirus analyse le code et essaie de le reproduire pour y repérer d'éventuelles actions malveillantes. Très complexe à mettre en place, cette méthode a aussi le défaut de produire des faux-positifs et de générer des alertes pour des fichiers inoffensifs.
- Le comportement : l'antivirus utilise une protection en temps réel qui surveille certains éléments du système. Ainsi, il observe les programmes qui tentent d'accéder à ces points stratégiques, comme la liste des programmes à lancer au démarrage. Généralement, il prévient l'utilisateur qui autorise ou non le logiciel repéré à agir.

Conseil Choisir un antivirus

Malheureusement, il n'existe pas de solution miracle pour choisir un antivirus. Contrairement aux idées reçues, les antivirus du commerce ne sont pas forcément plus efficaces que les antivirus gratuits et vice-versa. Choisissez le produit avec lequel vous avez eu le plus de bonnes expériences. Si, jusqu'à présent, vous n'avez pas connu de déconvenues avec votre antivirus actuel, c'est qu'il est probablement suffisamment efficace.
Soyez conscient que même équipé du meilleur antivirus au monde, un ordinateur est toujours susceptible d'être infecté car la première source d'infection reste… l'utilisateur lui-même !

Cependant, il est nécessaire de toujours posséder à porter de main, soit sur le disque, soit sur une clé USB, un petit scanner antivirus afin de réaliser rapidement une réparation du système. L'utilitaire gratuit Malicious Software Removal Tool (MSRT), fourni par Microsoft, est tout à fait adéquat.

Cet exécutable autonome (c'est-à-dire ne nécessitant pas d'installation) de quelques mégaoctets seulement contient une liste très limitée de virus. Il s'agit néanmoins des virus les plus courants et l'outil est parfaitement capable de désinfecter le système contre ces virus.

Pour connaître la liste de virus gérés par le système, cliquez sur le bouton *Afficher la liste des logiciels malveillants*. Une liste exhaustive apparaît alors. Cliquer sur le nom d'un des virus affiche la fiche descriptive contenant les symptômes, la méthode de réparation, les moyens de prévention et d'autres informations techniques permettant de mieux comprendre le fonctionnement de ce virus.

RESSOURCE MSRT

MSRT contient systématiquement une liste de virus récente. L'adresse de téléchargement est la suivante :

- http://www.microsoft.com/security/malwareremove/

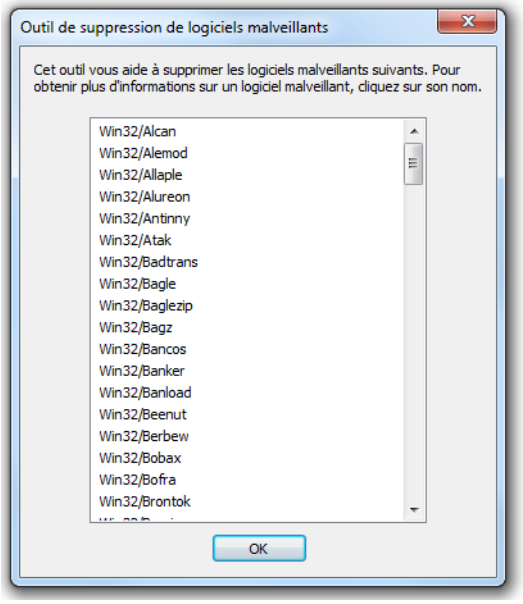


Figure 13–8
Liste des logiciels malveillants supportés par l'utilitaire

L'intérêt de cet outil réside dans sa simplicité d'utilisation. Même s'il ne propose que trois options, son efficacité est redoutable :

- *Analyse rapide* : analyse uniquement les zones susceptibles de contenir des logiciels malveillants tels que les répertoires système.
- *Analyse complète* : analyse complètement le système. La durée de cette analyse augmente en même temps que la taille du disque dur à scanner et le nombre fichiers à analyser.
- *Analyse personnalisée* : analyse vous permettant de choisir les répertoires à vérifier.

ATTENTION MSRT et la protection continue

Bien qu'étant utile, léger et efficace, cet utilitaire ne remplace pas un antivirus. Il ne propose en effet qu'un outil de désinfection là où d'autres antivirus proposent une protection et empêchent l'installation de virus. Rappelons qu'il vaut mieux prévenir que guérir.

- L'analyse et la désinfection se font alors automatiquement et ne nécessitent aucune intervention de votre part. Quand ces opérations sont terminées, un écran de résultat s'affiche, indiquant les conclusions de l'analyse.

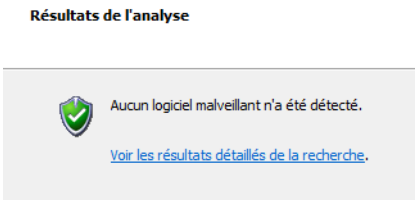


Figure 13–9
Fenêtre de résultat de l'analyse

Mettre en place et configurer le pare-feu Windows

En s'ouvrant au monde extérieur, par un réseau local ou par Internet, un système d'exploitation s'expose à de nouvelles attaques pouvant provenir soit d'attaquants humains cherchant à voler des informations, soit de simples programmes (tels des virus ou bots) cherchant à s'installer sur l'ordinateur. Dans les deux cas, le principe est le même : fouiller la partie publique de l'ordinateur jusqu'à trouver une faille et s'y introduire. Puisqu'il s'agit d'une faille, c'est-à-dire un point faible encore inconnu, il n'existe pas forcément de protection simple pour la combler. Il n'existe donc qu'une seule et unique alternative : mettre en œuvre un pare-feu.

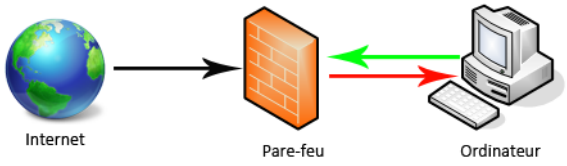


Figure 13–10
On peut comparer un pare-feu à un mur que l'on bâtirait autour de l'ordinateur et dans lequel on n'aurait laissé qu'une petite porte hautement surveillée qui serait l'unique point d'entrée de la totalité du trafic réseau.

VERSION Intégration d'un pare-feu dans Windows

Ce n'est qu'avec le Service Pack 2 de XP que Microsoft a intégré nativement un pare-feu au sein de son système. La première version était limitée et bien souvent décriée, car moins efficace que des outils tiers. Depuis Vista, le pare-feu est capable de surveiller le trafic entrant, mais également le trafic sortant, tout en apportant un paramétrage plus fin au niveau des exceptions de trafic autorisé ou bloqué.

Croire qu'un pare-feu n'est nécessaire que lorsque l'ordinateur est connecté à Internet est une idée fausse qui a la peau dure. Pour sécuriser son réseau, il est primordial d'envisager chaque ordinateur comme un point d'attaque potentiel. Imaginons qu'un simple ordinateur portable nomade infecté par un virus soit connecté à votre réseau. Même s'il n'est connecté que quelques secondes, il est parfaitement en mesure d'infecter toutes les autres machines de votre réseau, si elles n'ont pas été convenablement protégées : chaque ordinateur doit se trouver derrière un pare-feu activé et configuré.

Activer ou désactiver le pare-feu Windows

Comme la majorité des composants de Windows, le pare-feu possède sa propre interface d'administration accessible par le panneau de configuration. Elle se présente sous la forme d'un rapport sur l'état du pare-feu, en fonction du profil réseau utilisé.

Pour accéder à l'interface d'administration du pare-feu, ouvrez le menu *Démarrer*, saisissez `pare-feu windows` dans la zone de saisie, puis cliquez sur l'élément affiché.

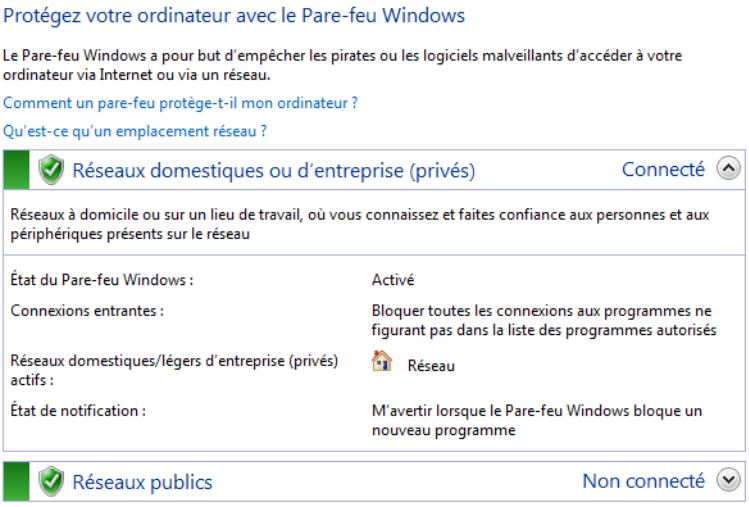


Figure 13–11
Panneau de configuration du pare-feu Windows

Ce compte-rendu offre une vision globale du paramétrage du pare-feu selon le profil utilisé. Vous remarquez qu'au moins deux configurations différentes du pare-feu sont disponibles : profils public et privé. Ainsi, selon que vous vous trouvez chez vous ou au travail, vous activerez l'une ou l'autre configuration. Cette configuration est choisie au moment de la première connexion au réseau, puis est mémorisée pour les prochaines fois où vous vous connecterez.

Dans tous les cas, désactiver le pare-feu est une mauvaise idée. Il vaut mieux le paramétrer de façon à l'ouvrir davantage que de supprimer totalement la protection qu'il apporte. Néanmoins, si vous souhaitez le désactiver temporairement, il vous suffit de cliquer sur le bouton *Activer ou désactiver le pare-feu Windows* qui se trouve dans la partie gauche du panneau de configuration.

Pour chaque profil, vous pouvez activer ou désactiver complètement le pare-feu. Dans le cas d'une activation, vous pouvez bloquer toutes les connexions entrantes. Ceci rend l'ordinateur très sécurisé, ne permettant que la navigation Internet, l'envoi et la réception d'e-mails et la messagerie instantanée.

BON À SAVOIR Bloquer les nouveaux logiciels

Si vous cochez la case *Me prévenir lorsque le pare-feu Windows bloque un nouveau programme*, une notification vous permettra de bloquer ou non tout nouveau logiciel.

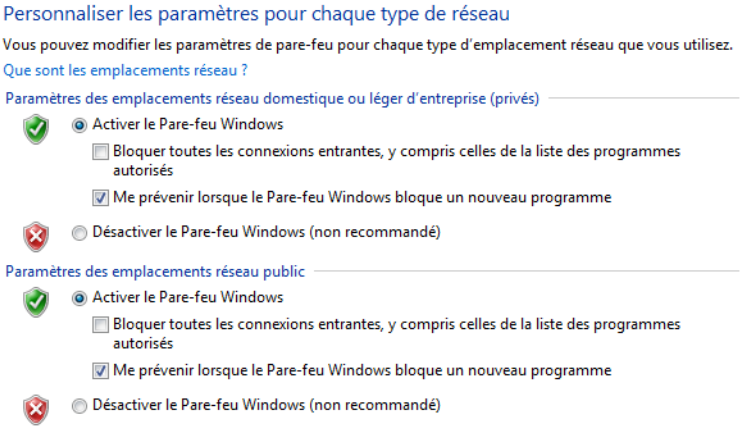


Figure 13–12
Activation ou désactivation du pare-feu Windows

Configurer le pare-feu

La configuration du pare-feu va bien évidemment plus loin que l'activation et la désactivation. En effet, il est possible de modifier à tout moment les logiciels et les communications autorisés à traverser le pare-feu. En fonction de vos besoins, il existe deux manières de configurer votre pare-feu.

Configuration simple

La méthode de configuration du pare-feu la plus simple consiste à définir les programmes autorisés. Le système se charge alors d'ouvrir les ports correspondants et les applications seront autorisées dans tous les cas d'utilisation.

1 Dans la partie gauche du panneau de configuration, cliquez sur *Autoriser un programme ou une fonctionnalité Windows via le Pare-feu Windows*.

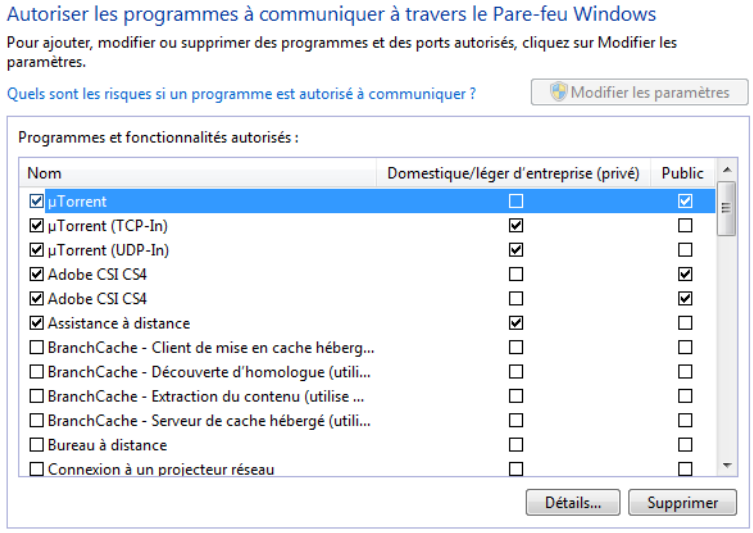


Figure 13–13
Interface de gestion des programmes et fonctionnalités autorisées via le pare-feu Windows

Communications TCP et UDP

Transmission Control Protocol (TCP) est un protocole réseau qui contrôle la fiabilité des connexions en se chargeant de la connexion entre les deux hôtes communicants, du transfert de données et de l'arrêt de la connexion.
User Datagram Protocol (UDP) est un protocole réseau capable de transmettre des données. Il est plus rapide, mais moins fiable, car il ne vérifie pas la validité des données à l'arrivée. UDP est généralement utilisé pour des données non importantes comme les fichiers de streaming, pour lesquels la vitesse est plus importante que la fiabilité des données.

2 Pour chaque application enregistrée, autorisez ou non son utilisation à travers le pare-feu en cochant (ou décochant) la case située devant son nom.

3 Définissez si cette autorisation d'accès concerne le profil privé ou public, voire les deux.

BON À SAVOIR Application absente de la liste

Si votre application n'apparaît pas dans la liste, cliquez sur le bouton *Autoriser un autre programme* et utilisez l'assistant pour aller chercher l'exécutable de votre application.

Configuration avancée

Bien que facile d'utilisation, le panneau de configuration allégé du pare-feu est vite limité et ne montre qu'une infime partie des possibilités de paramétrage. Pour effectuer un paramétrage poussé, il est nécessaire d'utiliser la console MMC qui va au cœur du pare-feu et permet de définir des règles de filtrage très fines.

Pour lancer la console MMC de gestion du pare-feu, ouvrez le menu *Démarrer*, saisissez `wf.msc` dans la zone de saisie, puis appuyez sur *Entrée*.

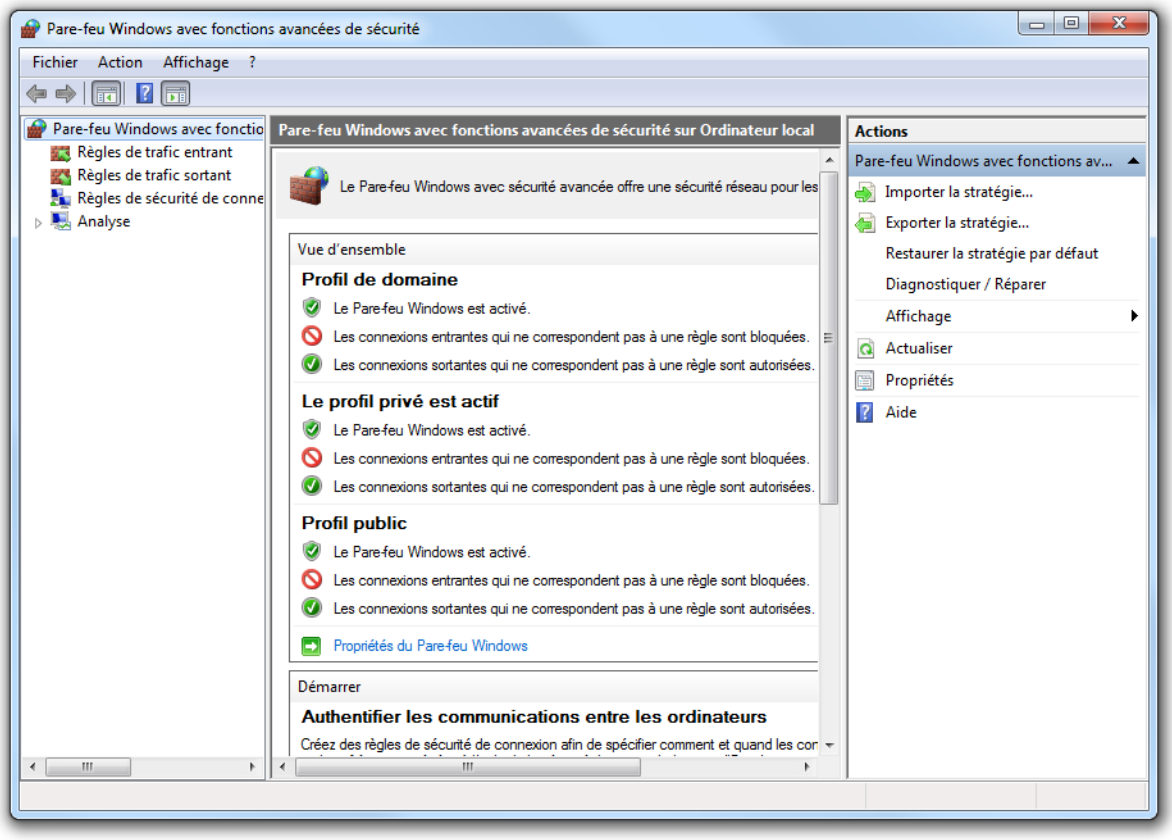


Figure 13–14 Console MMC de gestion avancée du pare-feu Windows

Entreprise Profil domaine

En plus des profils public et privé, il en existe un troisième, intitulé profil domaine. Il n'est mis en œuvre que dans certains réseaux d'entreprise lorsque ces derniers utilisent un domaine réseau, relié à un annuaire Active Directory.

Comme le panneau de configuration, la console MMC donne une vue d'ensemble de la configuration du pare-feu selon les profils réseau utilisés. La fenêtre de la console se divise en trois parties :

- La partie latérale gauche qui sert à naviguer entre les différentes fonctionnalités. On distingue, entre autres, la configuration de règles pour le trafic entrant et sortant, la configuration de la sécurité des connexions et enfin des outils pour surveiller les communications réseau.
- La partie centrale qui permet de contrôler chaque fonctionnalité, soit en affichant les règles à modifier, soit en affichant les rapports.
- La partie de droite qui affiche des actions contextuelles et permet d'agir rapidement en fonction de la catégorie sélectionnée.

Le pare-feu est dédié à une tâche principale, à savoir vous protéger contre tout type d'attaque réseau externe ou interne, mais il a pour second objectif de sécuriser les communications entre les différents ordinateurs de votre réseau. Pour cela, il est configuré par défaut avec un comportement moyennement restrictif, suffisamment sécurisé, mais qui ne répond pas forcément aux besoins de chaque utilisateur. Il est alors nécessaire de le paramétrer convenablement.

Contrôler le trafic entrant

Le trafic entrant concerne toutes les tentatives d'intrusion extérieures, mais également l'ouverture de port par des applications installées qui cherchent à « écouter » les appels venant de l'extérieur. Le comportement par défaut du pare-feu Windows est de bloquer toutes ces communications émanant de l'extérieur. Ceci peut s'avérer gênant dans plusieurs cas d'utilisation comme la prise de contrôle à distance du système ou encore l'utilisation de logiciel d'échange de fichiers (*peer-to-peer*). Dans ce genre de situations, il est alors de la responsabilité de l'administrateur du système de paramétrer le traitement des données transitant au travers du pare-feu. Ce paramétrage se fait à l'aide de règles. Chacune d'entre elles répond à un besoin précis, pour une application ou un port donné tout en présidant l'action à accomplir. Voyons comment les configurer.

Personnaliser Colonnes de la vue d'ensemble

Pour personnaliser les colonnes de la partie présentant la vue d'ensemble, sélectionnez *Affichage>Ajouter/Supprimer des colonnes*.

1. Cliquez dans la partie gauche sur *Règles de trafic entrant*. S'affichent alors toutes les règles configurées sur l'ordinateur, qu'elles soient activées (icône colorée) ou désactivées (icône grisée). La vue d'ensemble présente les informations principales de chaque règle comme son nom, le ou les profils réseau sur lesquels elle s'applique, l'action à effectuer (autoriser ou bloquer le transfert d'informations), le programme concerné, les ports et bien d'autres colonnes.
2. La création d'une règle se fait via un assistant dynamique qui, en fonction des choix que vous ferez, proposera plus ou moins d'étapes avec différents paramètres à renseigner. Il ne nous sera pas possible de

tous les voir en détail dans ce livre, mais en cas de difficulté, reportez-vous à l'aide contextuelle, fort complète. Dans la partie de droite, cliquez sur *Nouvelle Règle*.

3 L'assistant vous permet de choisir parmi les quatre types de règles possibles :
   – *Programme* : la règle est propre à un exécutable du disque dur.
   – *Port* : la règle s'applique à un port ou un protocole particulier, quelle que soit l'application qui l'utilise.
   – *Prédéfinie* : la règle est basée sur une règle système. Vous surchargez de paramétrages différents ceux prévus pour une règle par défaut.
   – *Personnalisée* : la règle est totalement paramétrable. Vous la configurez entièrement pour une application, un port et/ou un protocole donné.

Contrôler le trafic sortant

Le contrôle du trafic sortant présente l'avantage de vérifier ce que réalise le système en l'empêchant de communiquer sur Internet si l'on ne l'y a pas autorisé (par exemple, infection par un virus qui tenterait de communiquer des informations à un serveur distant).

Cette configuration sert également à bloquer certains logiciels en éditant des règles pour leur bloquer l'accès à Internet, ou au contraire, à leur autoriser un accès complet afin d'activer entièrement leurs fonctionnalités, comme les communications audio et vidéo des logiciels de messagerie instantanée.

Le paramétrage est identique à celui du trafic entrant.

Mettre en place des sécurités de connexion

Sécuriser les connexions vous permet de communiquer et d'échanger entre les différents ordinateurs de votre réseau (filaire ou Wi-Fi) en garantissant la protection des données transmises.

Les connexions sécurisées impliquent l'authentification réciproque de deux ordinateurs souhaitant communiquer entre eux, ainsi que la sécurisation des données qui transitent entre les deux. Pour établir ces connexions sécurisées, le pare-feu Windows utilise le protocole de communication IPSec qui se charge de la sécurité de la connexion grâce à l'échange de clés, une authentification et éventuellement un chiffrement des données.

En coulisse Le fonctionnement d'IPSec

IPSec est une extension sur protocole IP. IPSec, qui est inclus dans IPv6 et optionnel dans Ipv4, sécurise de façon transparente les données utilisant le protocole IP.
Le protocole IP transmet les données sur le réseau par paquets. Pour que ces données soient envoyées au bon destinataire, elles sont découpées en blocs, puis regroupées dans des datagrammes contenant plusieurs informations complémentaires. Celles-ci sont donc accolées aux données, puis envoyées à travers le réseau, laissant aux routeurs, passerelles et autres périphériques réseau le soin d'acheminer le message à destination. Un datagramme IP contient généralement :

- La version du protocole utilisée.
- La longueur de l'en-tête, ce qui permet de savoir combien d'informations il faut lire avant d'arriver aux données.
- Le type de service, qui indique la façon dont le datagramme doit être traité.
- La longueur totale du message pour s'assurer que l'intégralité du message est arrivée.
- L'identification, les drapeaux et les déplacements de fragment, qui régissent le découpage du datagramme.
- La durée de vie (TTL, *Time To Live*), qui indique le nombre de saut que le message peut faire à travers des routeurs. Cela permet de détruire les messages qui transitent sur le réseau sans jamais trouver de destinataire.
- Le protocole, ICMP, IGMP, TCP ou UDP, représenté par une notation décimale.
- La somme de contrôle de l'en-tête (*checksum*) pour vérifier que les données n'ont pas été corrompues.
- L'adresse IP source, qui correspond à l'envoyeur.
- L'adresse IP de destination.
- Les données.

Toute ces informations du datagramme sont donc lisibles de façon claire par tous les éléments de type routeur du réseau, ainsi que par les analyseurs de trafic (en anglais *sniffers*). IPSec a donc pour objectif de masquer ces informations afin de garantir la protection des données contre la lecture extérieure et contre la modification en cours de transport.

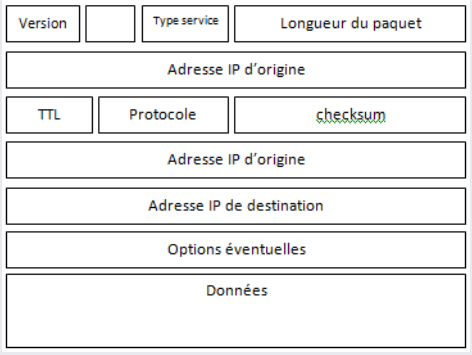


Figure 13–15 Datagramme d'un paquet IP

Il utilise pour cela deux modes possibles : le mode transport pour la communication PC à PC (*Host-to-Host*), en sécurisant uniquement les données ; le mode tunnel pour les communications réseau à réseau (*LAN-to-LAN*), en sécurisant totalement les données du réseau y compris les adresses source et destination. Quel que soit le mode choisi, IPSec met en œuvre deux sous-protocoles complémentaires nommés AH (*Authentication Header*) et ESP (*Encapsulating Security Payload*) qui sont chargés de contrôler que les données n'ont pas été modifiées, et qu'elles ont bien été émises par l'hôte à l'autre bout de la communication sécurisée.
Le propre d'IPSec est surtout d'échanger des clefs d'authentification dès le contact entre deux ordinateurs, afin d'authentifier de façon très claire les deux éléments communicants. Avant même que la moindre donnée ne soit échangée, IPSec utilise le protocole IKE (*Internet Key Exchange*) afin d'échanger des clefs ou des signatures (RSA).
Si IPSec est une évolution sérieuse dans la sécurité et même s'il est très flexible (algorithmes de chiffrage indépendants du protocole lui-même), sa grande complexité le rend délicat à mettre en place dans des réseaux complexes. La documentation de référence d'IPSec, représenté par la RFC 2401, est accessible à l'adresse suivante :

▸ http://tools.ietf.org/html/rfc2401

Voici comment mettre en place des règles de connexion sécurisées :

1. Cliquez dans la partie gauche sur *Règles de sécurité de connexion*.
2. Dans la partie droite, cliquez sur *Nouvelle Règle*. Un assistant s'ouvre alors, permettant de définir l'une des très nombreuses combinaisons de sécurité possibles.

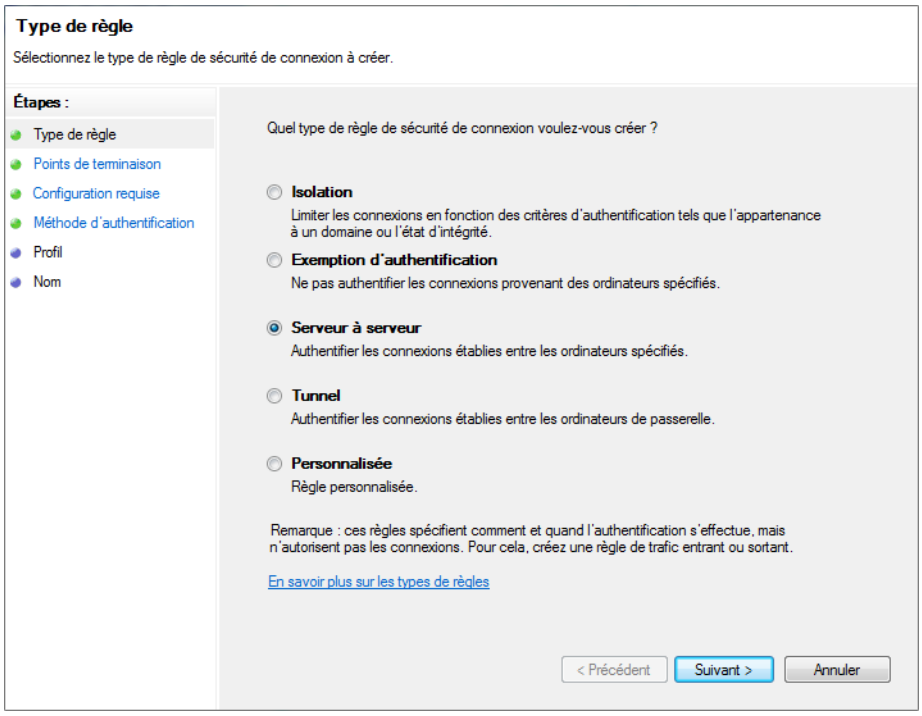


Figure 13–16
Assistant de création de règle de sécurité de connexion – Type de règle

3 Le premier écran sert à définir le type de règle de sécurité. Vous pouvez y définir soit des règles d'exception (*Isolation* et *Exemption d'authentification*), soit des règles de configuration de sécurité de connexion. Ainsi, les règles *Serveur à Serveur* et *Tunnel* correspondent respectivement aux modes IPSec Transport et Tunnel.
   - Une règle *Isolation* restreint les connexions en se basant sur vos critères. Vous pouvez, par exemple, utiliser cette règle pour isoler les ordinateurs de votre domaine des ordinateurs extérieurs afin de limiter les communications entre eux.
   - Une règle *Exemption d'authentification* définit les ordinateurs pour lesquels les règles de sécurité ne s'appliqueront pas.
   - *Serveur à Serveur* et *Tunnel* forcent l'utilisation de connexion IPSec entre différents ordinateurs. Il faut alors préciser si cela concerne toutes les connexions IP ou seulement les communications avec certaines IP particulières.
4 Vous définissez ensuite le niveau de flexibilité quant à l'authentification lors de l'établissement de connexions sécurisées. Cette authentification peut être rendue optionnelle pour un contexte particulier (optionnelle pour les communications sortantes, pour les communications entrantes ou les deux) ou obligatoire quel que soit le contexte.

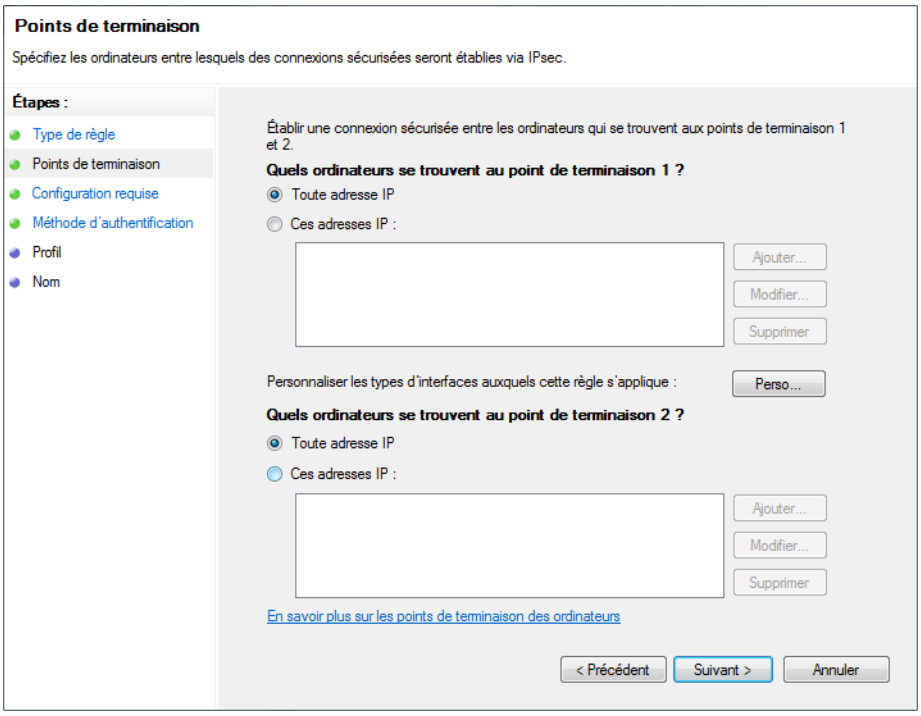


Figure 13–17
Assistant de création de règle de sécurité de connexion – Points de terminaison

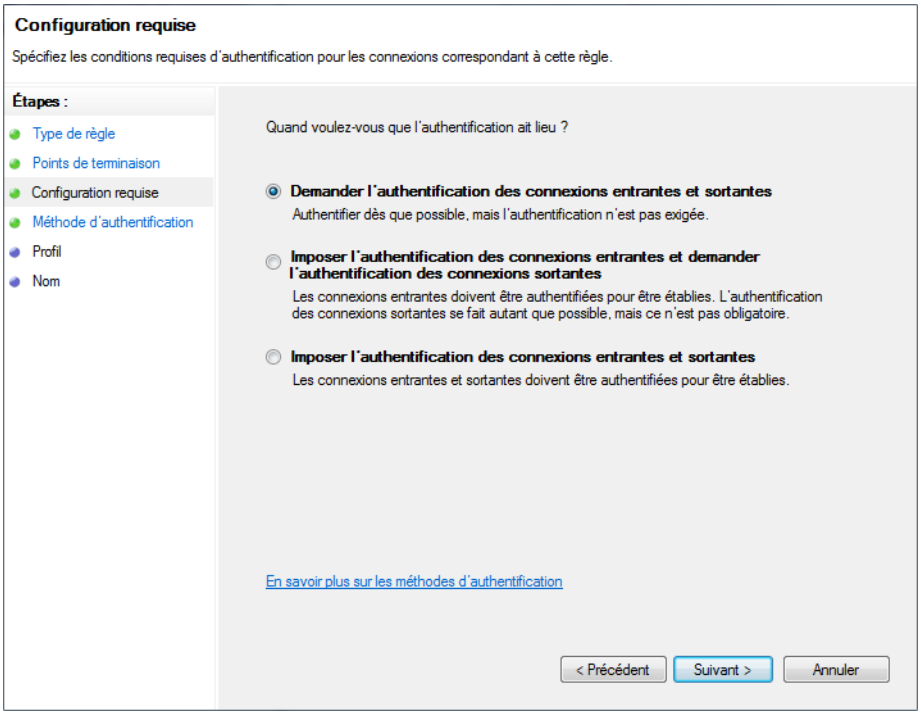


Figure 13–18
Assistant de création de règle de sécurité de connexion – Configuration requise

5 Paramétrez le mode d'authentification utilisé et le type de signature (certificat) qui sera utilisé lors de la connexion, ainsi que l'origine d'émission des certificats. Pour une utilisation avancée, mais hors contexte d'entreprise, il est conseillé de laisser la configuration par défaut, suffisamment restrictive.

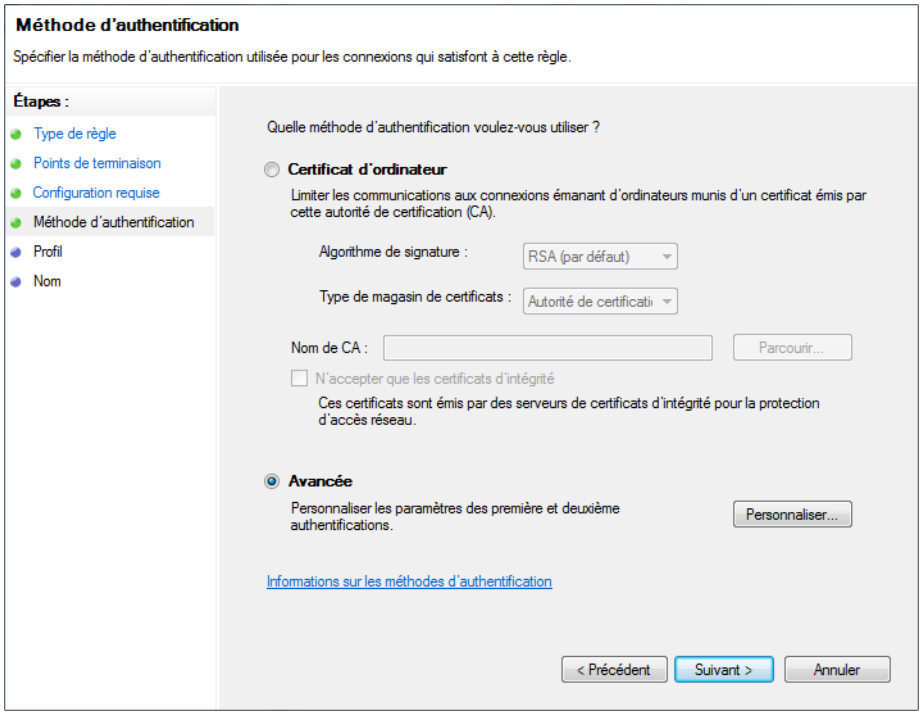


Figure 13–19
Assistant de création de règle de sécurité de connexion – Méthode d'authentification

6 Définissez enfin les profils réseau, comme pour les règles de pare-feu (domaine, privé et/ou public) pour lesquels la règle s'appliquera.

ATTENTION **Sécurité bilatérale**

Contrairement aux règles de pare-feu qui ne dépendent que de l'ordinateur local, les règles de connexion sécurisée requièrent de configurer la connexion sécurisée sur les deux ordinateurs qui doivent communiquer de façon protégée.

Analyser le trafic réseau

La partie *Analyse* de la console de paramétrage avancé du pare-feu ne permet pas réellement d'effectuer une analyse du réseau ou des données qui y transitent. Néanmoins, cet écran vous procure une vue d'ensemble de la configuration réseau. Vous pouvez ainsi filtrer les informations que vous souhaitez voir et vérifier rapidement quelles sont les règles de pare-feu actuellement actives sur votre ordinateur.

BONNE PRATIQUE **Convention de nommage des règles de sécurité**

Donnez à chacune de vos règles des noms courts mais suffisamment clairs et descriptifs. Chaque nom doit être unique et ne comportera aucun caractère spécial ni accent. Ainsi, par la suite, vous administrerez facilement vos règles via la commande en ligne `netsh`, lorsque vous souhaiterez paramétrer votre configuration réseau à l'aide de scripts batch ou PowerShell.

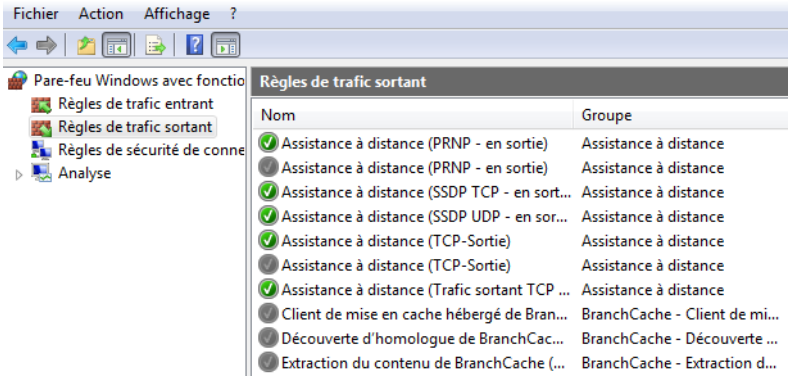


Figure 13–20
Interface de gestion
des règles de filtrage du pare-feu

Mettre en place une journalisation du pare-feu

La mise en place d'un journal de log pour le pare-feu est hautement instructive, car vous pouvez :

- Affiner le paramétrage et détecter des programmes licites qui sont actuellement bloqués.
- Détecter une éventuelle infection de l'ordinateur qui tenterait de se connecter à Internet pour y transmettre des informations.
- Surveiller les paquets entrant bloqués et donc vérifier si quelqu'un ou quelque chose ne tenterait pas de pénétrer dans votre ordinateur.

Mais tout ceci nécessite d'analyser régulièrement les fichiers de log. Voici la procédure à suivre pour activer la journalisation :

1. Ouvrez la console MMC de gestion du pare-feu, et dans la partie latérale, cliquez avec le bouton droit sur *Pare-feu Windows avec fonctions avancées de sécurité sur Ordinateur local*. Sélectionnez ensuite le menu *Propriétés*.
2. La fenêtre qui s'ouvre contient quatre onglets. Les trois premiers correspondent à chaque type de réseau qu'il est possible d'avoir, le type de réseau étant défini par l'utilisateur la première fois qu'il se connecte à un réseau. Possédant trois profils différents, il est possible de configurer son pare-feu différemment selon que l'on se connecte chez soi ou à un réseau public (cybercafé, conférence, hot spot Wi-Fi, etc.).

Si vous souhaitez bénéficier de la même configuration quel que soit l'endroit où vous vous connectez, voici la manipulation à suivre :

1. Dans l'onglet du profil réseau que vous souhaitez paramétrer, cliquez sur le bouton *Personnaliser* se trouvant dans la partie *Enregistrement*.

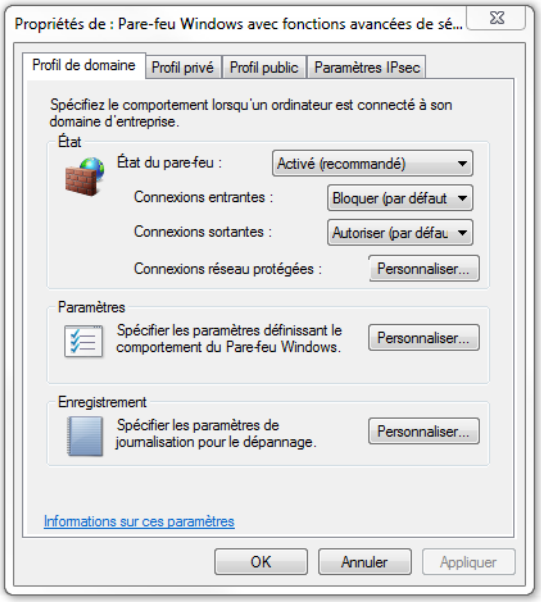


Figure 13–21
Propriétés avancées du pare-feu

2 Dans la fenêtre de personnalisation de la journalisation, spécifiez l'emplacement et le nom des fichiers de log. Définissez la taille maximale des fichiers ainsi que le type d'information que vous souhaitez enregistrer (la liste des paquets ignorés ou des connexions réussies, par exemple).

3 *Enregistrer les paquets ignorés* détecte tout ce qui est bloqué. Ceci permet de découvrir si une application ou une personne tente d'accéder à l'ordinateur ou à Internet sans y avoir été autorisée.

4 *Enregistrer les connexions réussies* vérifie que les applications autorisées réussissent à passer à travers le pare-feu. Cette option peut également servir à détecter une application qui aurait été autorisée par erreur et qu'il faudrait dorénavant bloquer.

5 Une fois la configuration achevée, cliquez sur le bouton *OK*.

Vous pouvez alors vous rendre dans le répertoire de stockage du journal de log, qui est un simple fichier texte lisible avec Notepad. Celui-ci contient les informations suivantes :

- statut du paquet (bloqué ou autorisé) ;
- type de communication (TCP/UDP) ;
- IP d'origine ;
- IP de destination ;
- ports ;
- direction du paquet (entrant/sortant).

ATTENTION Journalisation et droits d'accès

Si vous modifiez l'emplacement du répertoire de stockage des journaux du pare-feu, assurez-vous que le pare-feu a les droits d'accès pour écrire dans le répertoire spécifié. Le pare-feu étant un logiciel, il ne pourra écrire dans un répertoire dont vous avez restreint les droits d'accès. Dans ce cas, le répertoire restera vide et la journalisation n'aura tout simplement pas lieu.

Voici un extrait de journal :

```
07 10:42:49 ALLOW TCP 192.168.0.30 210.191.189.38 52107 49521 0 - 0 0 0 - - - SEND
2009-06-07 10:42:49 ALLOW TCP 94.137.6.243 192.168.0.30 2879 14816 0 - 0 0 0 - - - RECEIVE
2009-06-07 10:42:49 ALLOW TCP 192.168.0.30 69.214.12.185 521061 14813 0 - 0 0 0 - - - SEND
2009-06-07 10:42:53 ALLOW UDP 192.168.0.30 224.0.0.253 57204 3544 0 - - - - - - - SEND
2009-06-07 10:42:55 ALLOW TCP 192.168.0.30 124.105.233.7 52111 26445 0 - 0 0 0 - - - SEND
```

En résumé

Grâce à ce chapitre, vous avez vu les principales briques qui entrent en jeu dans la sécurité d'un système d'exploitation. Gardez cependant toujours à l'esprit que la plus grosse faille d'un système reste l'utilisateur lui-même. Si celui-ci n'a pas de bonnes habitudes et de bons réflexes, il y a fort à parier qu'il passera tôt ou tard outre les protections et introduira des logiciels malicieux au sein du système.


7
TM

chapitre 14

Des données accessibles de partout : mettre en place un serveur web et un FTP

N'avez-vous jamais pensé à installer un serveur web ou un serveur FTP sur votre ordinateur ? Avoir son propre site web ou serveur FTP, c'est pouvoir accéder à son ordinateur depuis le monde entier et pourquoi pas, interagir avec des personnes connectées.

SOMMAIRE

- Installer un serveur web
- Configurer un serveur FTP

MOTS-CLÉS

- Site web
- Serveur FTP
- Partage
- IIS
- Internet
- Service web
- Serveur web

Ce chapitre explique comment approfondir l'utilisation de votre ordinateur en termes de partage et de communication avec le monde extérieur. Nous commencerons par expliquer comment installer un serveur web afin de créer vos sites web. Dans la seconde partie du chapitre, nous traiterons de la mise en place d'un serveur FTP qui transformera votre ordinateur en serveur de fichiers.

Mettre en place un serveur web

Un serveur web transforme votre ordinateur en source de partage, que ce soit pour héberger votre propre site web, afficher une galerie de photos ou rendre accessibles certains fichiers. La majorité des versions de Windows, à l'exception des versions familiales, possèdent un serveur web intégré. Par défaut, il est désactivé pour éviter d'éventuelles failles de sécurité. Il se nomme IIS (*Internet Information Services*) et propose de nombreuses fonctionnalités pour héberger du contenu web. Voici les principales fonctionnalités qu'il propose :

- Modularité – IIS héberge un grand nombre de sites web mettant en œuvre différentes technologies (PHP, J2EE, etc.).
- Sécurité – Il accepte plusieurs types d'authentification et gère les certificats de sécurité. Les communications entre vous et le client accédant à votre ordinateur (chiffrage des échanges, etc.) peuvent être sécurisées.
- Gestion complète – À l'aide d'interfaces d'administration, vous configurez finement chaque paramètre du serveur web ou de ses modules.
- Fiabilité – Il est possible de séparer les processus entre les différents sites web. De cette manière, la défaillance d'un site Internet n'affecte pas les autres.
- Développement amélioré – IIS est compatible avec la plupart des langages web et respecte les standards internationaux définis par la commission du W3C.

Pour profiter de tout cela, il faut tout d'abord installer le module de serveur web.

W3C, le World Wide Web Consortium

Le W3C est un organisme à but non lucratif dont l'objectif est de définir des standards web afin de garantir une compatibilité entre les technologies et les différents périphériques de lecture, qu'il s'agisse de navigateurs web, de périphériques mobiles ou autres. Ces standards ne constituent en rien des obligations, mais sont autant de recommandations d'utilisation. Ils sont considérés comme une référence et la quasi totalité des acteurs d'Internet essaie de se conformer à leurs recommandations. Elles concernent des technologies web d'affichage comme le HTML, XHTML ou le CSS, mais également des formats d'image (PGN et SVG), des formats de communication réseau (SOAP) ou encore des méthodologies d'accessibilité pour améliorer l'accès aux ressources web à des personnes subissant un handicap.

▸ http://www.w3.org/

Installer IIS

Le serveur IIS fait partie des modules du système : il n'est pas nécessaire de télécharger quoi que ce soit. L'installation consiste à activer un module déjà présent sur le système.

1. Ouvrez le *Panneau de configuration* et cliquez sur le lien *Programmes*.
2. Cliquez ensuite sur *Ajouter ou désactiver des fonctionnalités Windows*. Une fenêtre s'ouvre alors listant tous les modules du système. Vous

pouvez depuis ce panneau activer ou désactiver n'importe lequel de ces modules. Celui qui nous intéresse se nomme *Services Internet (IIS)* ainsi que le module enfant *Service World Wild Web* qui va nous permettre la publication de sites web directement sur notre ordinateur.

3 Cochez la case *Services Internet (IIS)*, le sous-service web est alors lui aussi automatiquement coché.

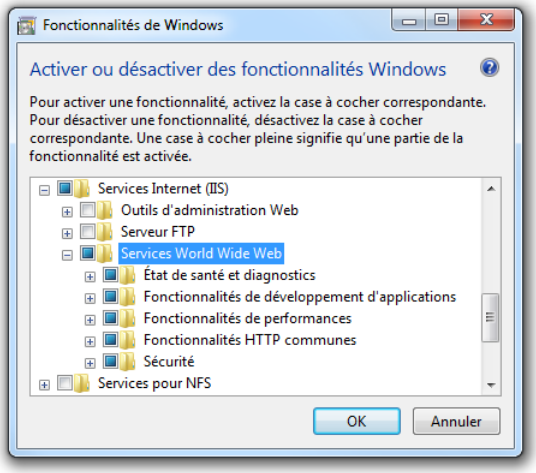


Figure 14–1
Ajout de la fonctionnalité IIS au système

4 Cliquez ensuite sur le bouton *OK* et laissez le système installer le module et l'intégrer au système en y intégrant un service Windows complémentaire, ainsi que des consoles d'administration. Dorénavant, vous les trouverez dans *Panneau de configuration>Outils d'administration*. N'hésitez pas à lancer une recherche filtrée du *Panneau de configuration* pour trouver rapidement la console de votre choix.

5 Vérifiez ensuite que le composant s'est parfaitement activé : lancez le navigateur Internet de votre choix et saisissez http://localhost dans la barre d'adresse. Si le logo suivant apparaît, c'est que le service IIS est bien lancé et que vous avez devant vous le site web par défaut de votre ordinateur.

Figure 14–2
Page par défaut de IIS

ASTUCE Le paquet WAMP

Si vous souhaitez ne pas à avoir à activer IIS et installer tous les éléments pour créer un site dynamique (PHP, MySQL), tournez-vous vers le packaging gratuit nommé WAMP (qui signifie *Windows Apache MySQL PHP*). Il s'agit d'installer automatiquement sur un système Windows, un serveur web Apache (qui est un équivalent Open Source de IIS), MySQL et les modules permettant d'écrire du code PHP. Apache gère la plupart des langages disponibles sur IIS, y compris ASP.NET.

Pour faire cohabiter les deux serveurs web sur le même ordinateur, il faut les configurer pour utiliser des ports différents.

▸ http://www.wampserver.com/

C'est ce site web que vous allez remplacer par le contenu de votre choix.

Créer une page web

Si la création d'un site Internet est facile à appréhender, elle peut rapidement devenir compliquée dans le cas d'utilisations avancées telles que des portails complexes, reposant sur différentes technologies web ou mettant en œuvre des modules sécurisés (paiement en ligne, etc.). Pour aborder la mise en place et la configuration d'un serveur web, nous allons commencer par créer un site web contenant une seule page.

Nous allons maintenant créer une page web et configurer IIS pour pouvoir l'utiliser. Nous allons recourir à un éditeur HTML afin de procéder très rapidement. Nous vous conseillons le logiciel Kompozer, parce qu'il est suffisamment complet et surtout entièrement gratuit. De plus, il ne nécessite pas d'installation, mais juste le téléchargement de quelques fichiers.

1. Téléchargez Kompozer et exécutez-le. Par défaut, un nouveau document est ouvert dans la partie centrale. C'est à cet endroit que vous allez définir le contenu de votre première page web.
2. Saisissez alors un texte de votre choix (qui servira de texte d'accueil), puis sauvegardez cette page quelque-part sur votre disque dur. Nommez-le `accueil`. Kompozer enregistre alors un fichier comportant l'extension `.html` afin d'indiquer qu'il s'agit d'un fichier web. Nous avons donc maintenant un serveur web et une page web à afficher, mais encore faut-il que le serveur sache qu'il doit utiliser ce fichier en particulier.
3. Reprenez votre fichier et déplacez-le dans le répertoire `C:\Inetpub\wwwroot\`, le répertoire par défaut de IIS. Remarquez qu'il s'y trouve déjà un fichier image et une page `iistart.htm` qui correspond à la page affichée lorsque vous allez à l'adresse http://localhost. Une fois votre fichier copié, ouvrez votre navigateur et saisissez l'adresse http://localhost/accueil.html afin d'afficher votre page web.

TÉLÉCHARGEMENT Éditeur HTML Kompozer

L'éditeur Kompozer est un logiciel entièrement gratuit, multi-plates-formes.

- http://kompozer.net

À SAVOIR L'adresse localhost

L'adresse http://localhost, qui correspond également à http://127.0.0.1, est ce que l'on appelle l'adresse de *loopback* (boucle). Elle sert à simuler l'accès à votre ordinateur depuis l'extérieur. En pratique, lorsque vous tentez d'accéder à une adresse, celle-ci est envoyée à la carte réseau qui l'envoie vers Internet ou le réseau. Lorsque la carte réseau détecte que l'adresse IP du serveur web visé est 127.0.0.1, elle redirige la communication vers elle-même, donnant l'impression que la requête d'origine provient de l'extérieur. Ainsi, ce que vous voyez en tapant http://localhost est exactement ce que verront les utilisateurs qui utilisent l'adresse de votre ordinateur (http://adresse-ip).

RAPPEL Fonctionnement de l'affichage d'un site web

Un site web est composé de pages web qui sont transmises à un navigateur Internet par un serveur web. Lorsque vous cherchez à accéder à un site web, vous accédez en réalité à son serveur web, en lui demandant une page précise identifiée par son URL (*Uniform Ressource Locator*). Ce dernier cherche alors la page correspondante, transforme au besoin son contenu, puis le renvoie au navigateur web qui l'affiche avec la mise en forme. Nous parlons de transformation, car la majorité des sites Internet possèdent des pages dynamiques, ce qui signifie que la page renvoyée au client (le navigateur) change avec le temps.

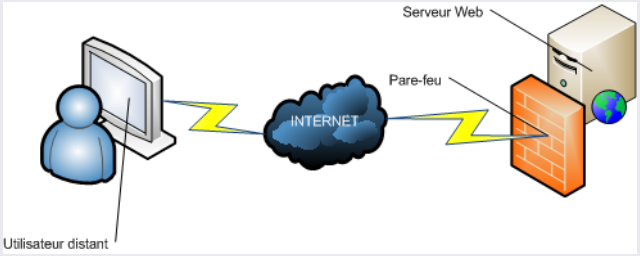


Figure 14–3 Schéma de la communication entre un utilisateur et un serveur web

Bien qu'il vous apparaisse coloré, avec des images, du texte et des formes, un site web n'est en réalité qu'un simple texte écrit dans un langage de description spécifique, nommé HTML. Le HTML (*HyperText Markup Langage*) est un langage de balises universel, qui sert à décrire l'affichage final des données. Par exemple, pour mettre un texte en valeur chez le visiteur, il faut l'encadrer des balises `<strong>` et `</strong>` pour qu'il apparaisse avec une graisse plus importante que le reste du contenu textuel.

Ouvrez de nouveau la page http://localhost/. Vous constatez qu'une image est affichée sur un fond gris. Ce principe d'image+fond gris nécessite, malgré sa simplicité, un certain nombre de lignes de code. Cliquez n'importe où sur le fond gris avec le bouton droit de la souris, et choisissez le menu *Afficher la source*. Le code suivant apparaît :

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0
   Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html;
charset=iso-8859-1" />
<title>IIS7</title>
<style type="text/css">
<!--
body {
        color:#000000;
        background-color:#B3B3B3;
        margin:0;
}

#container {
        margin-left:auto;
        margin-right:auto;
        text-align:center;
        }

a img {
        border:none;
}

-->
</head>
</style>
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/
?linkid=66138&amp;clcid=0x409">
<img src="welcome.png" alt="IIS7" width="571"
height="411" /></a>
</div>
</body>
</html>
```

Si vous n'êtes pas adepte du HTML, ce code vous semble peut-être abscons et barbare. Il est pourtant extrêmement bien organisé et universel, dans le sens où il sera interprété et affiché de la même façon par tous les navigateurs web, qu'il s'agisse d'Internet Explorer, de Mozilla Firefox, de Safari ou autres. Mais, en réalité, le rendu n'est pas identique sur tous les navigateurs. Il existe différents standards établis par le consortium W3C. Internet Explorer, pour ne pas le citer, fait partie de ces navigateurs qui ne respectent pas ces standards. À cause de ce type de différences entre les navigateurs, bon nombre d'intégrateurs web s'arrachent les cheveux pour obtenir un rendu identique…

Analysons rapidement ce code source. Il se découpe en trois parties.

- L'en-tête – Elle sert à préciser la version HTML utilisée, le titre de la page ainsi que les informations complémentaires comme l'encodage du texte (servant à préciser les caractères employés afin de gérer les accents ou les caractères asiatiques, par exemple).
- La partie style – À l'aide d'un système de feuilles de styles en cascade (CSS signifie *Cascading Style Sheets*), sont définies les règles d'affichage, de coloration et de mise en forme de la page. Il y est ainsi indiqué que le fond est gris, que le texte devra s'afficher en noir, que le contenu sera centré au milieu de la page et que les images imbriquées dans un lien hypertexte (permettant de rejoindre une nouvelle URL) n'auront pas de bordure.
- La partie de contenu ou `<body>` – Elle accueille les informations à afficher sur la page. Dans notre exemple, elle contient des balises HTML servant à l'affichage d'un fichier image (nommé `welcome.png`).

Certains développeurs écrivent ce code dans un éditeur de texte comme Notepad. Il existe également des logiciels de création de sites qui ne nécessitent pas de connaissances en HTML. Ces éditeurs, dits WYSIWYG (prononcez « oui-zi-oui-gue ») pour *What You See Is What You Get* (c'est-à-dire ce que vous voyez est ce que vous obtenez), sont des applications qui placent les éléments HTML (texte, images, boutons, etc.) à l'aide de la souris et modifient leurs propriétés à l'aide d'assistants faciles d'utilisation. Si beaucoup de développeurs préfèrent utiliser un logiciel textuel, c'est simplement pour avoir la main sur le code HTML et CSS produit. En effet, la plupart des éditeurs WYSIWYG ne se soucient pas vraiment de générer un code propre et valide selon les recommandations du W3C.

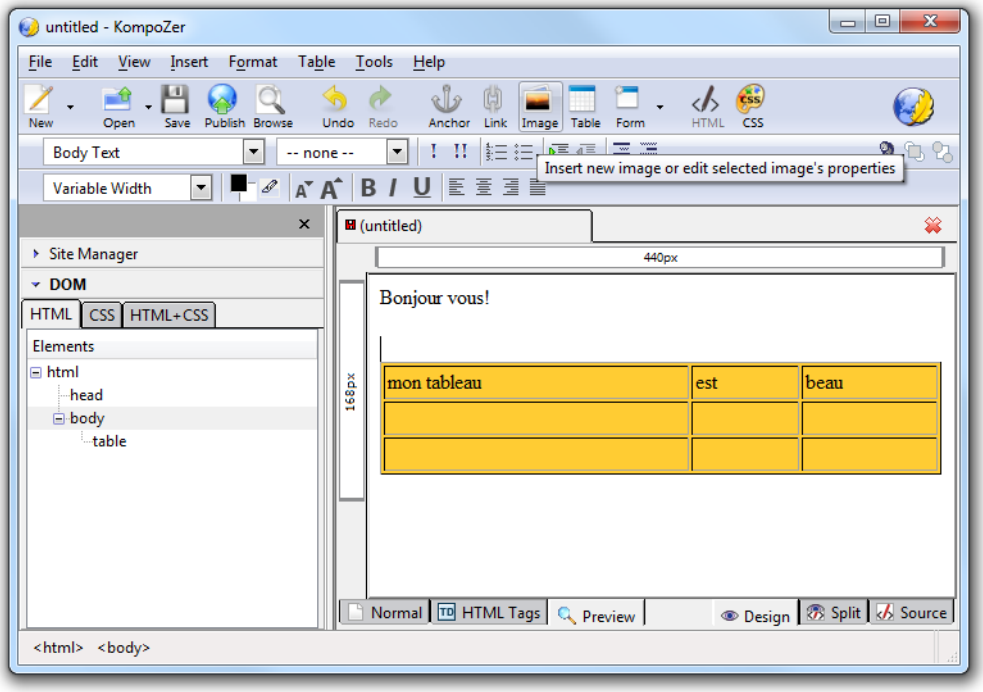


Figure 14–4
Interface du logiciel Kompozer

ASTUCE Console d'administration manquante

Si la console d'administration IIS n'est pas présente, c'est que l'option correspondante n'a pas été cochée lors de l'installation du serveur web.

1. Rendez-vous dans le *Panneau de configuration*, retrouvez la console via le menu *Programmes>Ajouter et désactiver des fonctionnalités Windows*.
2. Cochez la case *Services Internet (IIS)>Outils d'administration web>Console de gestion IIS*.
3. Cliquez enfin sur *OK*. La console d'administration s'installe.

Petite touche finale : il nous reste à configurer IIS pour n'avoir que http://localhost à saisir (et non l'adresse complète) pour afficher la page que nous venons de créer.

1. Ouvrez le menu *Démarrer* et saisissez `IIS` pour choisir l'élément *Gestionnaire des services Internet (IIS)*.
2. Dans le panneau latéral des connexions, dépliez l'arborescence et cliquez sur *Sites>Default web Site*. La partie centrale d'IIS affiche alors les différents modules et options disponibles pour paramétrer notre site web.
3. Cliquez sur le module *Document par défaut*.

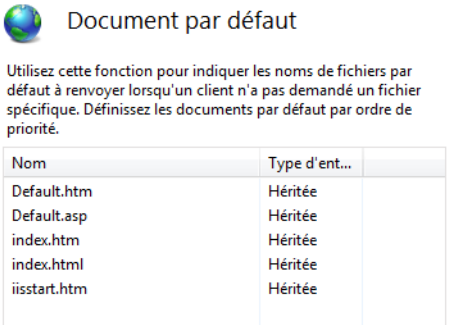


Figure 14–5
Paramétrage du document par défaut d'un site web

4 Les fichiers indiqués ici sont ceux que IIS chargera par défaut pour afficher la page d'accueil. Ainsi, il cherche tout d'abord le fichier `Default.htm`, puis, s'il ne le trouve pas, `Default.asp`, puis `index.htm` et ainsi de suite. Comme nous souhaitons que ce soit notre page `accueil.html` qui soit affichée, cliquez sur le bouton *Ajouter* situé dans la partie droite de la console, puis dans la zone de saisie, tapez `accueil.html` et cliquez enfin sur le bouton *OK*.

Pour vérifier que votre manipulation a été parfaitement exécutée, ouvrez de nouveau votre navigateur et saisissez l'adresse http://localhost. C'est maintenant notre page web qui remplace la page par défaut.

Bien que très simple, votre premier site est prêt pour être publié sur le Web. Il faudra encore communiquer l'adresse IP de votre réseau familial aux personnes qui voudront accéder à votre ordinateur, et si vous voulez que l'on accède à votre site via un nom propre, il vous faudra acheter un nom de domaine, qui vous coûtera une dizaine d'euros par an, suivant le prestataire que vous choisirez.

POUR ALLER PLUS LOIN

Développer un site web complet

Pour développer un beau site web, commencez par apprendre les langages XHTML et CSS. Il existe de très bons livres simples d'accès. Nous vous recommandons notamment l'ouvrage suivant :

📖 *Réussir son site web avec XHTML et CSS*, Mathieu Nebra aux éditions Eyrolles.

ou la lecture, certes moins plaisante, mais très complète, des standards web du W3C.

▸ http://www.w3.org/TR/xhtml1/

Partager des fichiers

S'il est facile de partager des fichiers au sein d'un réseau local, il est plus contraignant de le faire à travers Internet. Pour différentes raisons techniques dont la principale est que votre ordinateur n'est pas toujours directement visible et accessible depuis l'extérieur, les partages réseau habituels sont inefficaces lorsqu'il s'agit de donner accès à une partie de son disque dur à distance. Bien que délicate dans le cas de redirection de ports au niveau d'un routeur, la solution du serveur web reste la plus rapide et la plus facile à mettre en place pour partager des fichiers.

La première manipulation consiste à copier dans le répertoire du site web par défaut (avec lequel nous avons travaillé dans la partie précédente) les fichiers que vous souhaitez partager.

1 Ouvrez le dossier `C:\Inetpub\wwwroot\`.

2 Créez-y un dossier nommé `fichier`.

3 Copiez-y les fichiers à partager.

Lorsqu'un utilisateur tente d'accéder à votre ordinateur, le navigateur dresse la liste des fichiers du répertoire. L'utilisateur peut alors les télécharger à sa guise comme le montre la capture suivante.

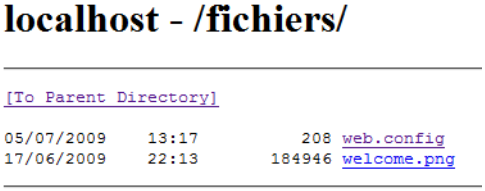


Figure 14–6
Liste des fichiers d'un répertoire web

Afin de protéger les fichiers sensibles du site web, la liste des fichiers des répertoires est désactivé par défaut par IIS. Si vous tentez d'accéder à l'adresse http://localhost/fichiers, un message d'erreur s'affiche.

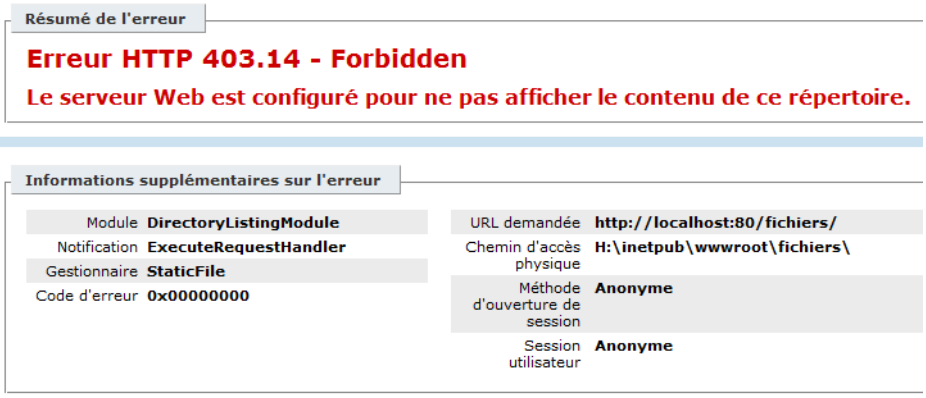


Figure 14–7
Message d'erreur en cas d'accès non autorisé à un répertoire

Pour autoriser l'accès et la visibilité des fichiers du répertoire :

1. Ouvrez la console d'administration de IIS.
2. Cliquez sur *Default web Site* dans la partie gauche, puis sur le dossier *Fichiers*.
3. Cliquez alors dans la partie centrale sur le module *Exploration de répertoire*.
4. Dans la partie *Actions*, cliquez sur le bouton *Activer*.

Ceci a pour effet de n'activer le listing des fichiers que pour ce répertoire bien précis.

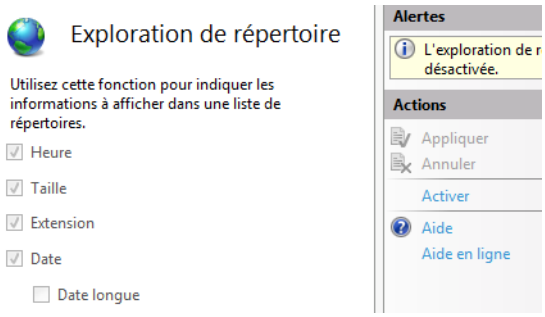


Figure 14–8
Activation de l'exploration de répertoire

Cette solution comporte malheureusement des défauts. En effet, elle requiert de copier des fichiers sur la partition `C:\`, ce qui signifie qu'en cas de corruption du système, ces données seront perdues lorsqu'il faudra réinstaller. De la même manière, si vous souhaitez partager un répertoire de photos, par exemple, il est nécessaire de déplacer ou de copier ces

données depuis leur lieu de stockage d'origine, vers le répertoire du site web (`wwwroot`), ce qui entraîne une duplication inutile des données. La solution consiste alors à créer un site web depuis l'endroit où se trouvent déjà les données.

1. Ouvrez la console d'administration de IIS.
2. Dans la partie *Site web* sur la gauche, cliquez à l'aide du bouton droit et choisissez *Ajouter un site web*.
3. Saisissez un nom de site web et le chemin menant aux fichiers que vous souhaitez partager.

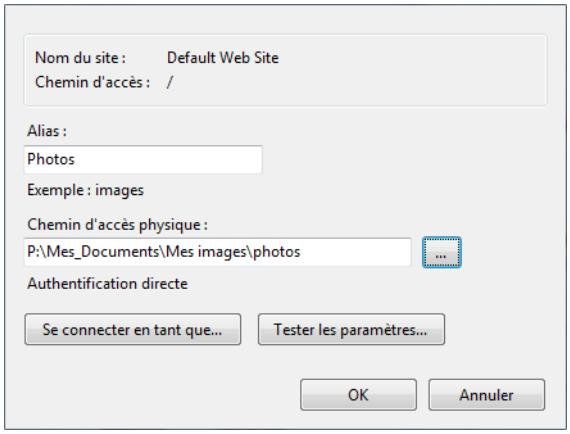


Figure 14–9
Ajout d'un nouveau site web : vous accédez à l'ensemble des fichiers à partager depuis l'adresse http://localhost/Photos.

4. Après cela, il est également nécessaire d'autoriser les droits de lecture et de parcours du répertoire comme vu juste avant.

Malheureusement, dans le cas de l'utilisation d'un répertoire physique ou virtuel, l'échange de fichiers n'est possible que dans un seul sens, l'utilisateur ne pouvant pas vous envoyer ses propres fichiers. Dans ce cas, il faut alors passer par un serveur FTP, destiné à l'échange de fichiers de façon bidirectionnelle. Nous abordons ce point un peu plus loin dans ce chapitre.

Cas d'utilisation avancée d'un site web

Un serveur web est un outil complexe qui répond à différents types de situations, en fonction des sites que vous souhaitez héberger ou des fonctionnalités que vous voulez implémenter. Intéressons-nous donc à l'ensemble des possibilités qu'offre IIS. Vous pourrez ainsi faire le bon choix technique le jour venu.

Lorsque vous cliquez sur un site web, différents paramétrages sont disponibles. Passons-les en revue.

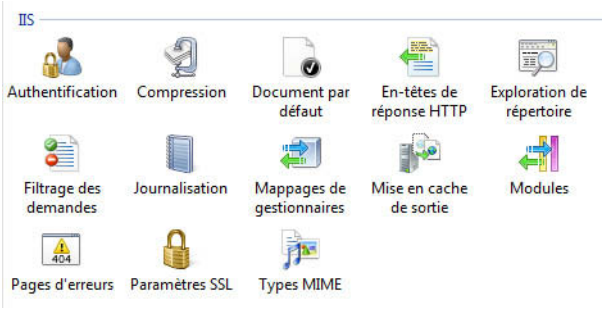


Figure 14–10
Modules de configuration d'un site web

Authentification

Ce premier panneau permet de définir les méthodes d'authentification exploitables pour le site web. En tout et pour tout, on distingue sept méthodes différentes, qui dépendent de l'utilisation que vous allez faire de votre site web et dans quel environnement vous le déployez.

Tableau 14–1 Liste des filtres de demandes

Filtre	Description
Authentification anonyme	Authentification utilisée pour la majorité des sites web. Accessible par tous, aucun identifiant ou mot de passe n'est demandé à l'utilisateur.
Impersonation ASP.NET	Permet aux applications ASP.NET d'utiliser un compte spécifique, différent du compte ASP.NET par défaut qui n'a que peu de droits et qui est limité à l'accès aux dossiers des applications web.
Authentification simple	Il s'agit d'une authentification basique où l'utilisateur renseigne un identifiant et un mot de passe. Néanmoins, cette authentification est gérée par l'application elle-même et non par IIS.
Authentification par certificat de client Active Directory	Dans un domaine d'entreprise, il est possible de relier les utilisateurs à des certificats particuliers qui leur serviront de badge pour accéder à certains sites web. Ceci sert principalement pour les intranets et évite aux utilisateurs d'avoir à saisir leurs identifiants de connexion.
Authentification Windows	Le compte Windows courant de l'utilisateur est utilisé et il n'est pas nécessaire de renseigner des identifiants de connexion.
Authentification Forms	Mode d'authentification particulier des applications ASP.NET. L'utilisateur saisit ses identifiants de connexion, qui sont validés par l'application. IIS aide ensuite à gérer l'accès aux différentes pages du site web.
Authentification Digest	Version améliorée d'authentification simple. Dans le cas d'un domaine, sert à renforcer la sécurité des connexions. Pour fonctionner, l'authentification anonyme doit être désactivée.

Compression

La compression permet de préciser si le serveur IIS doit compresser les données HTML renvoyées au navigateur web. Ceci réduit la consommation de la bande passante réseau et permet aux clients de télécharger plus rapidement les pages web. Néanmoins, la compression entraîne un surcoût en charge processeur pour le serveur.

En-têtes de réponse HTTP

Lorsqu'un client demande une page web à un serveur, celui-ci retourne également différentes informations dans le paquet HTTP envoyé au navigateur web. Ces informations sont stockées dans l'en-tête HTTP et concernent la date de mise à jour, la date de péremption, le type de contenu (texte, image, son, vidéo, fichier PDF, etc.), etc.

Le panneau *En-têtes de réponse HTTP* sert à créer des données personnalisées sous forme de clés-valeurs. Elles seront retournées aux clients web, qui les utiliseront ou non.

Exploration de répertoire

L'exploration de répertoire permet d'autoriser ou non le serveur web à afficher son contenu. Si vous rassemblez vos photos dans un dossier, en activant l'exploration du répertoire, il est alors possible de toutes les télécharger sans avoir à connaître par cœur le nom des fichiers image.

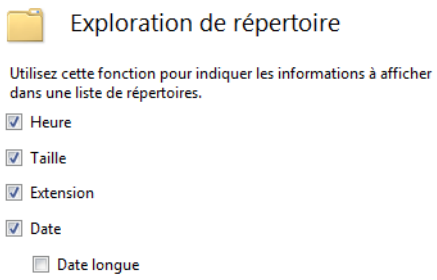


Figure 14–11
Paramétrage de l'exploration de répertoire

Filtrage des demandes

Ce paramètre est sûrement le plus complexe de toutes les fonctionnalités proposées dans cette fenêtre. Il remplace l'add-on Url-Scan disponible sur IIS 6.0, et permet de définir des règles quant aux demandes faites au serveur web. Le filtrage peut se faire à différents niveaux, comme le montre le tableau 14-2 de la page suivante.

COMPRENDRE Attaque et SQL Injection

S'il existe plusieurs attaques possibles sur un site web, toutes ont pour objectif le vol de données, si ce n'est leur destruction pure et simple. L'une d'entre elles, l'injection par script SQL consiste à insérer du code malveillant dans les champs de saisie des formulaires. Ainsi, lorsque l'information est envoyée en base, le code malveillant est exécuté. Le *SQL Injection* n'est la conséquence que d'un mauvais développement, et il est aujourd'hui facile de s'en protéger. Néanmoins, comme une erreur est vite arrivée, une protection supplémentaire n'est jamais superflue.

Tableau 14–2 Liste des filtrages web disponibles

Niveau	Description
Extension de fichiers	Il est possible de bloquer l'accès à certaines extensions de fichiers. Ce filtrage est utile lorsque vous stockez vos données dans une base de données autonome de type SQLite ou MsAccess, et empêche ainsi le téléchargement de votre fichier si jamais une personne malveillante venait à connaître son chemin d'accès.
Verbes HTTP	Les verbes HTTP sont des commandes qui sont envoyées via le protocole HTTP. Les plus courants sont les paramètres GET et POST qui permettent d'envoyer des informations à une page, mais il en existe d'autres comme COPY ou MOVE, capables dans certains cas d'entraîner des opérations sur le serveur. Il est donc utile de limiter les verbes dont l'application web aura besoin.
Segments cachés	Les segments cachés servent à faire croire qu'un fichier ou un répertoire n'existe pas. Ainsi, plutôt que refuser l'accès à un répertoire sensible, il vaut mieux créer un segment caché pointant sur ce répertoire afin de le rendre invisible.
URL filtrées	Les URL filtrées bloquent certaines URL ou, au contraire, en autorisent en outrepassant les autres paramétrages. Ceci peut servir pour bloquer l'accès à certains répertoires de l'application.
Chaînes de requêtes	Il s'agit ici de bloquer certaines séquences d'URL, notamment lors d'utilisation de paramètres GET afin de se protéger contre des attaques extérieures. Il est ainsi possible de bloquer des séquences connues pour être utilisées par les hackers pour tenter de réaliser du SQL Injection sur votre application, comme l'utilisation de caractères d'échappement ou l'appel à des méthodes SQL.

Journalisation

Ce module sert à activer l'enregistrement des opérations et des requêtes effectuées sur le serveur. Grâce à ce journal, l'utilisateur averti détecte les tentatives d'attaques sur son serveur. Il s'en sert également pour comprendre le comportement des utilisateurs et en déduire les modifications à effectuer pour améliorer son site.

Mappage de gestionnaires

Par défaut, IIS ne gère que le rendu de pages statiques HTML. Dans le cas d'applications à code compilé ou interprété, il requiert des modules complémentaires tel que le framework .NET ou encore les composants PHP.

Ce module indique au serveur web de faire appel à tel ou tel composant tiers lorsqu'une extension bien précise est demandée. Il est ainsi possible de dire que les fichiers `.php` seront utilisés par le module PHP, tout comme il est possible de renommer les fichiers `.php` en `.htm` et de les mapper sur le même module afin de donner l'impression que le site est statique.

CULTURE Tromper l'utilisateur à l'aide de la réécriture d'URL

Il existe également la solution qui consiste à réécrire les URL à la volée (*URL Rewriting*) pour cacher la structure d'un site web ou des pages réellement appelées. Ainsi, il est possible de transformer (via une configuration serveur), une adresse du type http://monsite.com/dossiers/critiques/afficher.php?id=1 en une adresse http://monsite.com/Afficher/1, ne permettant pas de deviner la technologie utilisée ou tout simplement la structure du site web. Ce leurre a aussi l'avantage de créer des URL plus simples et plus claires pour le visiteur.

Aucun langage n'étant infaillible, il existe des portes au travers desquelles un utilisateur malveillant peut effectuer diverses actions malhonnêtes telles que le vol ou la destruction de données. Bien que rapidement repérées et corrigées dans la plupart des cas, ces failles subsistent parfois sur certains serveurs qui n'auraient pas été mis à jour récemment. En modifiant l'URL d'une page (en remplaçant un `.php` en `.html`), le pirate ne saura pas quelle technologie a été utilisée et ne saura donc pas de quel côté chercher les éventuelles failles de sécurité.

Mise en cache de sortie

Comme son nom l'indique, la mise en cache consiste à stocker à un endroit précis des pages déjà générées, qui seront directement renvoyées au navigateur. En effet, certaines pages, bien que dynamiques, n'ont pas besoin d'être régénérées à chaque appel par un poste client. Afin de diminuer l'utilisation processeur du serveur, les accès à une base de données ou tout simplement le temps de traitement des informations, il est utile de mettre en cache certaines pages web pour une durée correspondant à la fréquence de modification des données.

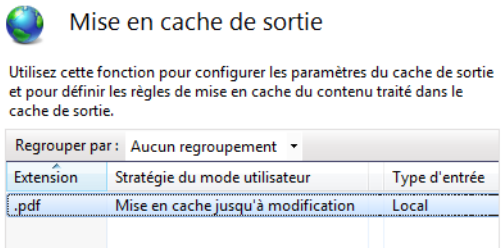


Figure 14–12
Configuration de la mise en cache des éléments du site web

Modules

Il s'agit ici de définir et d'ajouter des modules extérieurs qui seront ensuite utilisés par le serveur web, grâce aux mappages de gestionnaires.

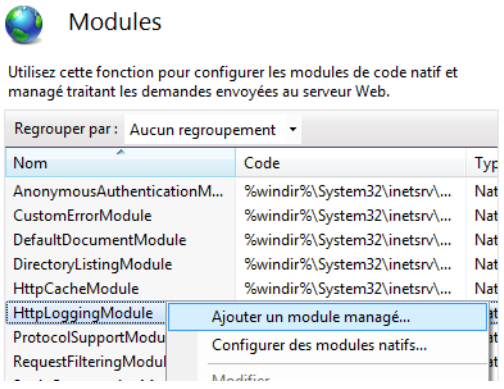


Figure 14–13
Configuration des modules du site web

Les fonctionnalités apportées par ces modules sont diverses : par exemple, certains listent un répertoire ou permettent l'utilisation de langages de programmation pour créer des sites dynamiques comme PHP, ASP.NET, ASP, etc.

Pages d'erreur

Des codes d'erreur universels définissent les erreurs qui se produisent sur un site web. Ainsi, lorsqu'un utilisateur tente d'accéder à un fichier inexistant, le serveur lui renvoie toujours le code 404, ainsi qu'une vilaine page d'erreur selon le navigateur web qu'il utilise.

Il est néanmoins possible de forcer l'affichage d'une page spécifique en fonction du code retourné. De cette façon, vous affichez une belle page contenant les informations de votre choix à tout utilisateur, quel que soit son navigateur, et en fonction de l'erreur qu'il déclenche.

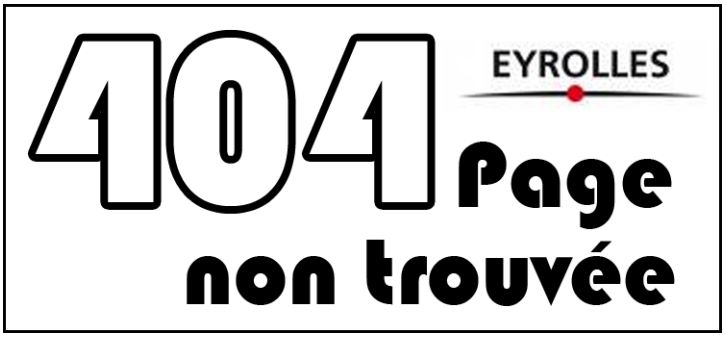


Figure 14–14
Exemple de page d'erreur 404 personnalisée

Paramètres SSL

Lorsque vous devez sécuriser votre site, la configuration SSL permet de forcer ou non l'utilisation du protocole HTTPS.

Au préalable, il faut obtenir un certificat SSL, l'enregistrer sur le serveur web et créer une liaison au niveau du site web pour relier l'utilisation du protocole HTTPS au certificat. Sans ce prérequis, le paramétrage SSL est indisponible.

Secure Socket Layer

Anciennement nommé TLS (*Transport Layer Security*), SSL est un protocole de sécurisation des données. Il crée une connexion sécurisée entre un navigateur et un site web. Couplé au protocole HTTPS, on le rencontre généralement pour les sites d'achat en ligne, car il garantit la transmission d'informations sensibles (numéro de Carte Bleue, par exemple) de façon sécurisée et inviolable.

Types MIME

Les types MIME sont des codes définissant le type de fichiers en fonction d'une extension. Si pour vous, un fichier d'extension `.pdf` est forcément un PDF, il n'en va pas forcément de même pour tous les types d'extensions. Par exemple, le logiciel ArcView enregistre la configuration utilisateur dans un fichier `.pdf` (*Preferences Definition File*) : c'est donc le type MIME du fichier qui permettra au système de décider de quel type de fichier il s'agit réellement.

Créer des types MIME sert à indiquer la correspondance entre une extension et un type de fichier. Si vous configurez l'extension `.pdf` avec le type image/JPEG, le navigateur web, qui télécharge un fichier PDF depuis votre site, tentera d'afficher le contenu sous forme d'image. Les types MIME prennent toute leur importance lorsque vous gérez des extensions personnalisées, ne correspondant pas aux types de fichiers courants.

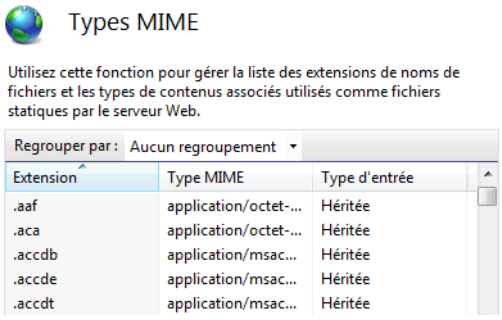


Figure 14–15
Configuration des types MIME

Ainsi, que vous soyez développeur ou utilisateur averti, et bien que vous n'ayez pas pour le moment besoin de tous ces paramétrages, vous connaissez maintenant les capacités du serveur web IIS, et savez utiliser les différents modules de configuration afin d'administrer votre site web plus efficacement.

Mettre en place un serveur FTP

Protocole réseau, le FTP (*File Transfert Protocol*) permet de faire transiter des fichiers depuis un ordinateur vers un autre, à travers un réseau ou Internet. Le transfert des données est alors sécurisé, et un système d'autorisation permet de définir qui peut lire les fichiers et qui peut en déposer de nouveaux.

Avant toute chose, précisons ce qu'est un serveur FTP. Un serveur FTP n'est rien de plus qu'un petit programme, c'est-à-dire un service, tournant en tâche de fond sur votre ordinateur. À l'aide d'un logiciel spécifique (appelé client FTP), il sert à envoyer des commandes à votre ordinateur soit pour y récupérer des fichiers, soit pour en déposer.

Un serveur FTP donne accès à une partie spécifique de votre disque dur et permet de paramétrer le type d'accès autorisé aux fichiers (lecture, écriture, modification), en fonction de comptes utilisateur que vous aurez définis. Lorsque vous mettez en place un serveur FTP sur votre ordinateur, vous avez le choix entre :

- Configurer un seul et unique serveur avec des paramétrages complexes, pour un grand nombre d'utilisateurs ayant chacun des paramètres différents.
- Séparer vos besoins et créer plusieurs serveurs FTP.

Bien entendu, il n'est pas question de posséder un serveur FTP par utilisateur, mais plutôt de séparer les besoins entre différents serveurs. Si vous souhaitez faire profiter d'une partie de vos fichiers à vos amis et d'autres fichiers au monde entier, nous vous conseillons de créer un serveur dédié pour chacun de ces deux cas. Même si cela nécessite une double configuration au départ, vous pourrez faire évoluer les configurations de chacun des différents serveurs. Néanmoins, nous ne nous intéressons ici qu'à la mise en place d'un serveur FTP unique et nécessitant une authentification.

Installer le service FTP

L'installation du service FTP est aussi simple que celle du serveur web.

Il suffit de se rendre dans la console *Activer ou désactiver des composants Windows* (dans le *Panneau de configuration*) et d'y cocher la case *Serveur FTP*.

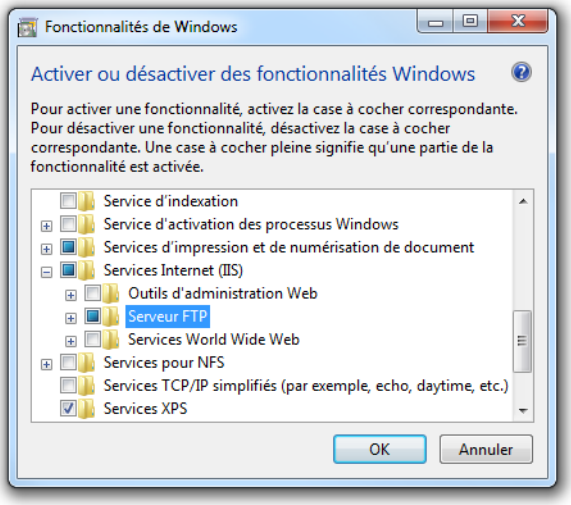


Figure 14–16
Ajout de la fonctionnalité de serveur FTP au système

Créer le serveur FTP

Comme pour les sites web, les serveurs FTP sont gérés par IIS et sont par conséquent administrables par la console *Gestion des services Internet (IIS)* située dans le *Panneau de configuration*.

1. Dans la console, cliquez dans la partie gauche sur *Sites*.
2. À l'aide du bouton droit, choisissez *Ajouter un site FTP*.
3. Dans l'assistant, donnez un nom à votre FTP et indiquez le répertoire racine de votre serveur FTP.
4. Sur l'écran suivant, activez si besoin la connexion sécurisée SSL et cliquez sur *Suivant*.
5. Définissez alors le type d'authentification. Avec *De base*, des identifiants de connexion seront requis, tandis qu'avec *Authentification anonyme*, vous autorisez l'accès à toute personne se connectant au serveur.
6. Précisez dans le paramètre *Autorisation* si tous les comptes de l'ordinateur ont le droit de se connecter au serveur FTP. En effet, comme nous le verrons juste après, les comptes utilisés pour la connexion sont des comptes Windows et non des comptes propres au serveur FTP.
7. Cliquez sur *Terminer*.

Votre serveur FTP est fonctionnel, mais il faut encore définir les accès utilisateur.

Définir les accès des utilisateurs

La gestion des utilisateurs se fait grâce à des comptes Windows. Ceci présente l'avantage de ne pas nécessiter la création de comptes supplémentaires, lorsque les utilisateurs habituels de l'ordinateur souhaitent se connecter au serveur FTP depuis un ordinateur distant. Cependant, cette méthode mélange comptes utilisateur machine et comptes FTP, ce qui a pour conséquence, lorsque les utilisateurs sont nombreux, de multiplier le nombre de comptes visibles dans la console de gestion des utilisateurs.

Vous avez la possibilité de créer un compte par utilisateur ou bien de créer un compte partagé par plusieurs utilisateurs. À vous de décider quelle méthode utiliser, l'une apportant plus de flexibilité, l'autre une maintenance aisée.

Pour créer un utilisateur, passez par la console d'administration :

1. Ouvrez le menu *Démarrer*.
2. Cliquez avec le bouton droit sur le lien *Ordinateur*, puis sélectionnez le menu *Gérer*.
3. Dépliez l'arborescence pour sélectionner le menu *Utilisateurs et groupes locaux*.
4. Cliquez alors sur le menu *Action*>*Nouvel utilisateur* et renseignez les propriétés principales.

Il est également possible d'utiliser des groupes utilisateur comme nous l'avons vu en détail dans le chapitre 7.

ATTENTION Accès illimité

Les utilisateurs ont par défaut accès à ce dossier et à tous ses fichiers et dossiers enfants.

BONNE PRATIQUE
Choix du dossier racine du serveur FTP

Beaucoup d'utilisateurs choisissent à tort le dossier racine d'une partition (`C:` ou autre) en tant que répertoire principal, afin de partager rapidement l'ensemble de leurs données. Il s'agit là d'une très mauvaise habitude.
Il est très fortement conseillé de créer un nouveau dossier dédié au serveur FTP et d'y inclure des répertoires virtuels, afin de partager les données se trouvant dans d'autres emplacements, voire d'autres partitions. D'une part, ceci facilite l'administration des droits, car vous n'avez pas besoin d'ajouter des règles de filtrage sur ce que vous ne désirez pas partager. D'autre part, vous n'avez pas à déplacer tous les fichiers sur une même partition de façon hiérarchique. Cela vous évite également d'éventuels problèmes de sécurité, car vous auriez donné accès à des fichiers sensibles, comme les fichiers système.

BONNE PRATIQUE Comptes FTP limités

Il est recommandé de mettre en place des comptes dédiés au serveur FTP, en en limitant les droits. En effet, comme un pirate peut tout à fait récupérer les identifiants de connexion FTP en écoutant les paquets réseau, il pourra alors contrôler votre ordinateur à l'aide de ces comptes piratés. Il vaut donc mieux que ces comptes aient le moins de droits possibles afin de limiter les risques.

Paramétrage avancé du serveur FTP

Comme pour le serveur web, un très grand nombre de paramétrages sont disponibles afin de configurer le serveur FTP pour qu'il réponde parfaitement à vos besoins ou à ceux de vos utilisateurs. Rapidement, vous devriez rencontrer des cas d'utilisation particuliers qui nécessiteront de configurer très précisément votre serveur.

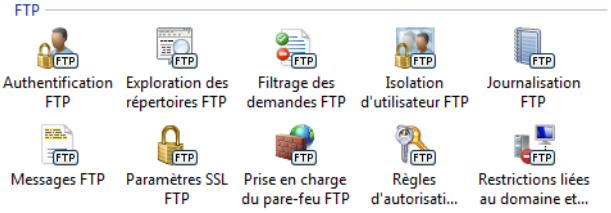


Figure 14–17
Console d'administration avancée du serveur FTP

La majorité des paramétrages se configure au niveau de la racine du serveur FTP (une fois sélectionnée dans la liste des sites FTP disponibles), ou au niveau de chaque serveur FTP en cliquant sur son nom dans l'arborescence des sites située sur la gauche de le fenêtre.

Authentification FTP

Le premier module de configuration permet de modifier la manière dont les utilisateurs se connectent au serveur FTP pour accéder aux fichiers. Par défaut, seules deux méthodes d'authentification sont disponibles :

- La méthode anonyme, qui donne potentiellement accès à toute personne du réseau ou d'Internet.
- La méthode d'authentification basique, qui nécessite de posséder un compte bien défini sur le serveur.

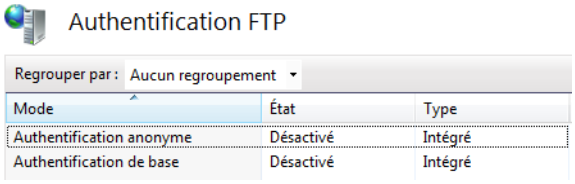


Figure 14–18
Module de configuration de l'authentification

C'est l'authentification basique qu'il faudra utiliser dans la majorité des cas. Il faut savoir qu'elle est nécessaire pour pouvoir utiliser certaines fonctionnalités du serveur et/ou pour donner des droits d'accès particuliers à certains des répertoires partagés via le serveur FTP.

Exploration des répertoires FTP

Le paramétrage de l'exploration des répertoires n'a qu'un intérêt limité pour un serveur FTP basique. En effet, il est ici question de configurer la manière dont sont affichées les informations des fichiers lorsqu'ils sont listés par un client FTP.

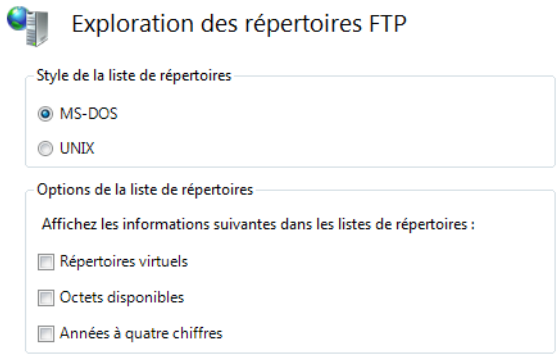


Figure 14–19
Paramétrage de l'exploration des répertoires

Cependant, certains clients FTP (qu'il s'agisse d'un vrai client FTP comme FileZilla ou d'un navigateur web), outrepassent les paramètres d'affichage d'IIS et mettent en œuvre leurs propres formats de date et choisissent eux-mêmes les informations à afficher.

Filtrages des demandes FTP

Le filtrage des demandes limite les actions possibles sur le serveur, que cela concerne les commandes FTP ou l'accès à certains fichiers. Le tableau 14-3 détaille les filtres disponibles.

Tableau 14–3 Liste des filtres de demandes

Intitulé du filtre	Action
Extensions de noms de fichiers	Refuse l'upload et le téléchargement de certaines extensions de fichiers.
Segments masqués	Rend des répertoires ou des fichiers totalement invisibles, bien qu'ils se trouvent dans des répertoires accessibles par les utilisateurs du serveur FTP.
Séquence d'URL refusées	Alternative aux segments masqués, les séquences d'URL servent à définir des noms de dossiers qui seront visibles dans le client FTP mais pour lesquels tout accès sera refusé sans définir des droits d'accès particuliers. Le dossier sera refusé y compris pour les administrateurs qui se connectent au serveur FTP.
Commandes	Bloque certaines commandes. Le protocole FTP contient plusieurs dizaines de commandes dont certaines agissent sur les fichiers. Par exemple, il est possible de bloquer la commande `MKDIR` et de s'assurer qu'aucun utilisateur ayant des droits d'écriture ne pourra créer un dossier : il pourra seulement uploader des fichiers.

Isolation d'utilisateur FTP

Grâce à l'isolation des utilisateurs, vous créez des dossiers séparés pour chaque utilisateur se connectant au serveur.

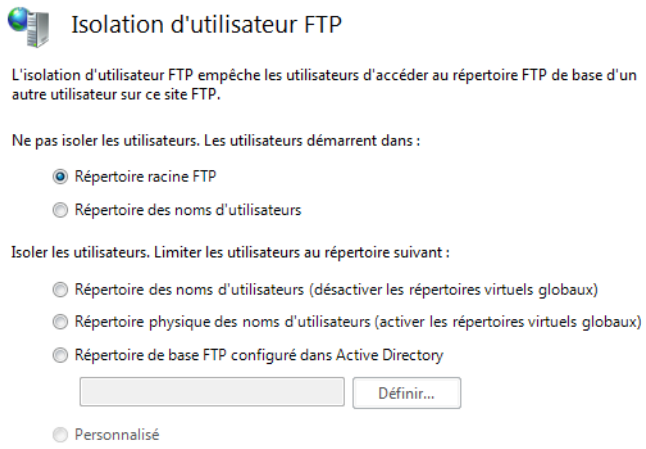


Figure 14–20
Module de paramétrage d'isolation d'utilisateur

Deux grands principes peuvent être mis en œuvre. Le premier consiste à faire démarrer tous les utilisateurs dans un répertoire commun. Cette solution est généralement utilisée lorsque les fichiers sont accessibles de manière identique par tout le monde (bien qu'il soit ensuite possible de créer des règles spécifiques pour les sous-dossiers).

La seconde solution consiste à créer un répertoire physique ou virtuel pour chaque utilisateur afin de faire démarrer l'utilisateur dans le répertoire qui lui est propre. Les dossiers utilisateur doivent être nommés de la même façon que le nom du compte auquel ils sont liés. Ainsi, pour l'utilisateur Jean, il faut créer un dossier `Jean`. Si le dossier n'existe pas, l'utilisateur est alors renvoyé vers le dossier racine du serveur FTP.

ATTENTION

Isolation des utilisateurs et sécurité

Isoler des utilisateurs en choisissant l'option *Répertoire des noms d'utilisateurs* dans la partie haute du module sert uniquement à définir le point de départ de l'utilisateur lorsqu'il se connecte au serveur. Cela ne l'empêche pas de remonter l'arborescence et d'aller voir dans les dossiers des autres utilisateurs. Vous devez également vous assurer, au niveau de chaque répertoire, d'avoir appliquer des règles d'autorisation limitant l'accès au seul utilisateur à qui est censé appartenir le dossier.

Journalisation FTP

La journalisation FTP permet d'enregistrer dans un fichier toutes les opérations se déroulant sur votre serveur. Que ce soit pour surveiller les connexions, les transferts de données ou encore les commandes reçues par votre serveur, un journal d'événements FTP ne peut que vous aider dans l'administration du serveur.

Vous pouvez définir certains paramètres, notamment leur place et leur affichage.

Personnalisez les informations que vous décidez de stocker via le bouton *Sélectionner des champs W3C*. Elles vous serviront à détecter deux types d'informations complémentaires. D'une part, vous y repérerez les con-

nexions qui ont échouées et vous serez ainsi informé de toute tentative d'accès par une personne non habilitée. D'autre part, vous y trouverez les erreurs d'accès à certains fichiers/répertoires. Vous pourrez donc améliorer le support auprès des utilisateurs lorsqu'ils vous indiqueront n'avoir pas accès à tel ou tel fichier alors qu'ils le devraient.

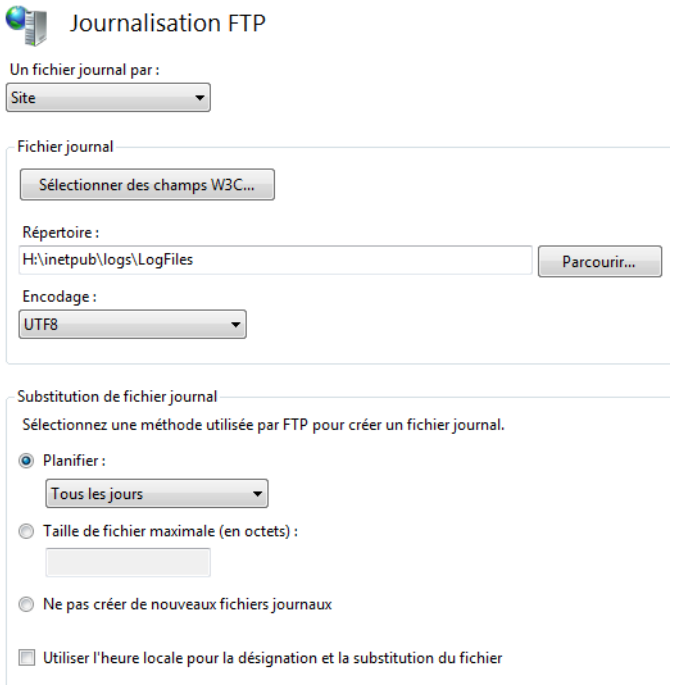


Figure 14–21
Module de paramétrage de la journalisation

Messages FTP

Il est possible d'afficher des messages spécifiques aux utilisateurs au moment de leur connexion. Ces messages servent notamment à transmettre des informations contextuelles ou des instructions. On distingue quatre messages :

- la *bannière*, qui est affichée dès que l'utilisateur tente de se connecter au serveur ;
- le message de *bienvenue* qui est affiché lorsque les identifiants de connexion sont corrects ;
- le message *Quitter*, affiché lorsque l'utilisateur se déconnecte ;
- le message *Maximum de connexion*, affiché lorsque le nombre de connexions simultanées autorisé sur le serveur est atteint.

Il est également possible de rendre les messages dynamiques à l'aide de variables utilisateur. Ces variables contiennent des informations contex-

tuelles, comme le nom de l'utilisateur ou des informations sur les données transférées. Les variables supportées sont au nombre de cinq.

Tableau 14–4 Liste des variables utilisateur du serveur FTP

Variable	Description
%BytesReceived%	Le nombre d'octets téléchargés depuis le serveur pour la session en cours.
%BytesSent%	Le nombre d'octets envoyés au serveur pour la session en cours.
%SessionID%	L'identifiant unique pour la session en cours.
%SiteName%	Le nom du site FTP qui héberge la connexion courante.
%UserName%	Le nom de l'utilisateur actuellement connecté.

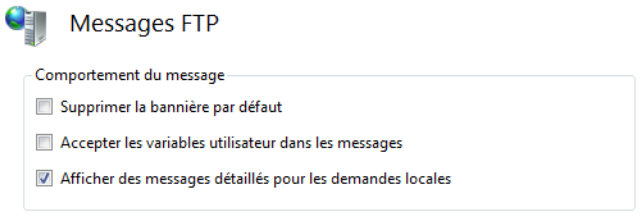


Figure 14–22
Personnalisation des messages FTP

Paramètres SSL FTP

Forcer les connexions sécurisées pour accéder au serveur FTP n'est pas obligatoire, mais fortement recommandé. En effet, il est relativement aisé pour un attaquant d'écouter les messages réseau afin de récupérer les paquets FTP. Dans ces paquets de données, il trouvera notamment les fichiers, mais surtout vos identifiants de connexion, à savoir le nom de votre compte Windows et le mot de passe associé. Une fois ces identifiants récupérés, il lui sera alors facile de contrôler entièrement votre ordinateur. FTPS (*FTP over SSL*) s'avère une protection efficace.

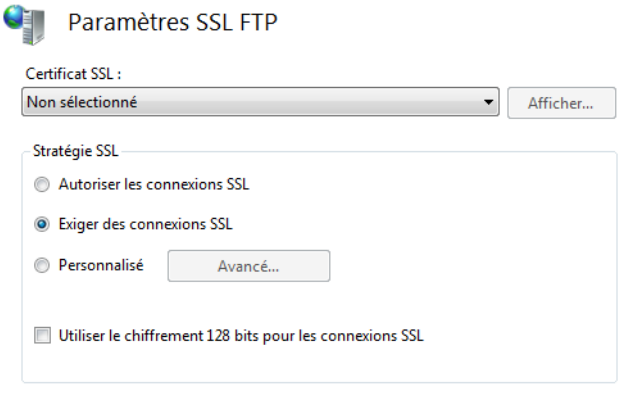


Figure 14–23
Module de paramétrage SSL

Trois types de paramétrages SSL sont disponibles :

- *Autoriser les connexions SSL*, qui rend optionnelle la connexion sécurisée.
- *Exiger des connexions SSL*, qui rend obligatoire l'utilisation de SSL.
- *Personnalisée*, qui permet de séparer le canal de contrôle (les commandes envoyées aux serveurs) du canal des données (les données transférées dans un sens ou dans l'autre).

La majorité des clients FTP actuels gère SSL. Il n'y a donc aucun inconvénient à forcer ces connexions sécurisées et elles ne devraient être désactivées qu'en cas de force majeure, comme une utilisation limitée au réseau interne ou pour du transfert de données non sensibles, ou encore dans le cas où le client FTP des utilisateurs ne gère pas les connexions sécurisées.

Prise en charge du pare-feu FTP

L'utilisation de ce module est relativement rare. Il faut le mettre en œuvre pour une infrastructure réseau bien particulière : votre serveur FTP est séparé du réseau extérieur par un serveur de pare-feu et les connexions à votre FTP se font de manière passive.

Le premier paramètre définit la plage de ports utilisés pour les connexions passives. Il n'est généralement pas nécessaire de modifier sa valeur par défaut, `0-0`, qui utilise les ports Windows TCP/IP (1 025 à 5 000). Le second paramètre précise l'adresse du serveur faisant office de pare-feu. L'IP sera insérée au sein des paquets pour pouvoir utiliser le serveur de pare-feu comme passerelle.

Connexion passive

Le mode de connexion passive est un mode sécurisé où les flux de données transférées sont pilotés par le client FTP et non par le serveur.

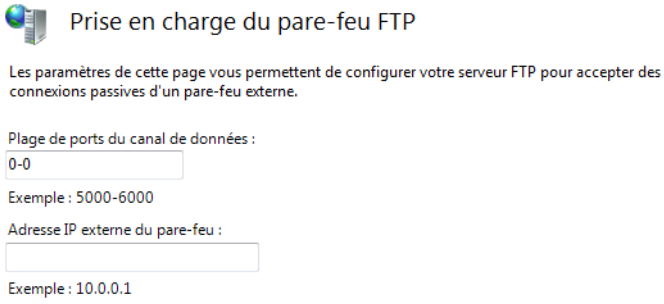


Figure 14–24
Paramétrage par rapport au pare-feu Windows

Attention, ce module n'ouvre pas les ports du pare-feu de la machine pour autoriser les connexions FTP. Vous devez les configurer spécifiquement dans l'interface d'administration du pare-feu, comme nous l'avons vu précédemment.

Règles d'autorisation FTP

Ce panneau est sûrement le plus important, car il concerne la sécurité que vous allez mettre en place pour chacun des répertoires. À titre de comparaison, il est l'équivalent de la fenêtre *Sécurité des dossiers et des fichiers* que nous avons traitée au chapitre 11.

La gestion des autorisations est fort simple.

1. Dans l'arborescence de votre site FTP, cliquez sur le répertoire de votre choix, puis, dans la partie centrale, cliquez sur *Règles d'autorisation FTP*. Une grille affiche les règles actuellement en place.
2. Cliquez sur la grille avec le bouton droit et choisissez *Ajouter une règle d'autorisation*.
3. Un écran s'affiche alors vous permettant de désigner en premier les personnes pour qui cette règle s'applique, puis les droits que cette règle accorde. Vous avez le choix entre lecture (téléchargement des fichiers) et écriture (dépôt de fichier et modification des fichiers existants).

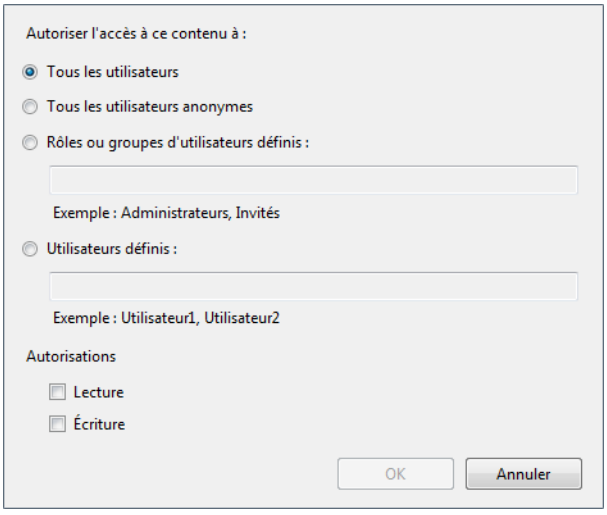


Figure 14–25
Assistant d'ajout d'autorisation sur un répertoire FTP

Si un répertoire n'a pas d'autorisation, qu'il s'agisse de règles d'autorisation ou de règles d'accès, le serveur FTP considère alors que toute tentative d'accès à ce dossier doit être refusée. Il faut donc donner explicitement des accès d'autorisation, quitte à accorder une autorisation en choisissant l'option *Tout le monde*.

Restrictions liées au domaine et à l'adresse Ipv4

Imaginons que les connexions à votre serveur FTP émanent d'une IP particulière. Par exemple, vous souhaitez vous connecter via FTP à votre ordinateur personnel depuis votre entreprise. Dans ce cas précis, il est

PRÉCISION Différence avec les ACL

La principale différence entre les autorisations FTP et les fichiers ACL (*Access Control List*) est qu'il est ici impossible de donner des autorisations au niveau des répertoires et non des fichiers. Ce comportement des serveurs FTP existants implique de classer les fichiers afin que l'utilisateur accède bien aux fichiers selon ses droits.

EN PRATIQUE Refuser l'accès

Pour refuser l'accès spécifique à certaines personnes, effectuez la même manipulation qu'à l'étape 2, en choisissant *Ajouter une règle de refus*.

EN PRATIQUE Héritage des droits

Par défaut, le serveur FTP applique l'héritage d'autorisation. Si un dossier est ajouté à un répertoire parent, il a alors les mêmes règles d'autorisation et les mêmes règles de refus.

judicieux de mettre en place des restrictions afin de limiter les connexions pour qu'aucun autre ordinateur ne puisse se connecter au serveur. Ceci évitera les tentatives d'accès extérieures. En effet, il arrive régulièrement que de jeunes hackers (que l'on nomme *scripts kiddies*) lancent des outils de scanner qui tombent par hasard sur votre adresse IP et cherchent à forcer l'authentification à votre serveur FTP en essayant une multitude de couples identifiant/mot de passe. Bien que détectable en analysant les journaux d'événements du serveur, il est impossible de se protéger contre ce genre d'attaque, que l'on nomme attaque par force brute.

Si le texte de la fenêtre de propriétés et l'aide de Windows indiquent que des restrictions sont disponibles pour les adresses IP et pour les domaines, il est impossible au niveau du paramétrage de saisir un nom de domaine. Où est donc le formulaire de restriction de domaine ?

Il est tout simplement désactivé par défaut. En effet, comme vous l'explique un message d'avertissement au moment de l'activation, le blocage par domaine nécessite une opération DNS à chaque connexion, ce qui s'avère coûteux en performances pour le serveur entier. Néanmoins, voici comment activer cette fonctionnalité.

1. Cliquez sur la grille à l'aide du bouton droit et choisissez le menu *Modifier les paramètres de fonction*.
2. Dans l'écran qui s'ouvre, cochez la case *Activer les restrictions de domaine*.
3. Cliquez sur le bouton *OK*.
4. Recommencez la manipulation pour *Ajouter une entrée d'autorisation* pour que s'ajoute au formulaire la partie dédiée aux noms de domaine.

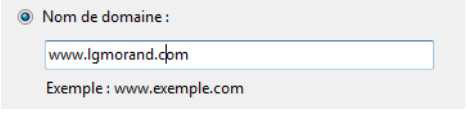


Figure 14–26
Restriction d'un domaine

En résumé

Dans ce chapitre, nous avons transformé un simple ordinateur en un système ouvert vers Internet, qu'il s'agisse d'héberger des sites web ou d'installer un serveur FTP pour échanger des fichiers rapidement en toute sécurité.

Si tout le monde ne souhaite pas forcément héberger un site web chez soi, ce serveur nous fait entrevoir de nombreuses possibilités. Citons, par exemple, l'installation de sites web préconfigurés destinés au partage de photos ou la mise en place d'un forum pour discuter avec un groupe d'amis.

chapitre 15

Résoudre les problèmes de Windows 7

Chaque problème informatique a une solution logique. Pour la trouver, il est souvent plus simple de chercher méthodiquement la source du problème, plutôt que de lancer des procédures à l'aveuglette.

SOMMAIRE

- Débloquer Windows quand il ne démarre pas
- Restaurer le système
- Exploiter l'utilitaire de résolution de problèmes
- Utiliser les outils de détection de problèmes
- Créer sa boîte à outils

MOTS-CLÉS

- Résolution
- Problème
- Restauration
- Analyse
- Réparation
- Solution
- Assistance
- Événements
- Journal
- Outil
- Mode sans échec

Ce chapitre explique comment mettre en place une stratégie de détection de problèmes et présente les différents outils à votre disposition, afin de rendre stabilité et performance à votre système. Nous y décrirons également les bons réflexes et les bonnes pratiques à suivre lorsque votre ordinateur se trouve dans un état critique et ne démarre plus convenablement.

Restaurer le système

La restauration d'un système consiste à remettre le système dans un état pleinement fonctionnel. Cette réparation peut se faire de différentes manières ; la plus simple et la plus intuitive est d'utiliser la fonction *Restauration système*.

La restauration système est un dispositif intégré à Windows 7 qui permet, lorsque l'ordinateur fonctionne mal, de revenir à une configuration antérieure.

IMPORTANT Nature des données des points de sauvegarde

Les informations sauvegardées dans les points de restauration sont les fichiers système Windows, les programmes et le registre. Aucun document de l'utilisateur n'est enregistré. Veillez donc à sauvegarder régulièrement vos documents importants.

En effet, Windows 7 enregistre des informations sur les fichiers et les paramètres du système. Cette sauvegarde est appelée point de restauration. Ces points de restauration sont créés lors de divers événements tels que l'installation de nouveaux programmes, de pilotes de périphériques ou lors de mises à jour de Windows. Si aucun de ces événements ne survient pendant sept jours, Windows crée automatiquement un point de restauration. Vous pouvez également en forcer la création manuellement.

Voyons à présent comment configurer et utiliser la restauration système de Windows 7.

Configurer la protection du système

Voici comment accéder aux options de la protection système :

1. Ouvrez le menu *Démarrer*.
2. Cliquez avec le bouton droit de la souris sur *Ordinateur* et sélectionnez *Propriétés* dans le menu contextuel.
3. Dans la partie gauche de la fenêtre *Système*, cliquez alors sur *Paramètres système avancés*.
4. Sélectionnez l'onglet *Protection du système*.

Le bouton *Restauration du système* vous permet d'accéder directement à l'assistant de restauration. Celui-ci est décrit un peu plus loin dans ce chapitre.

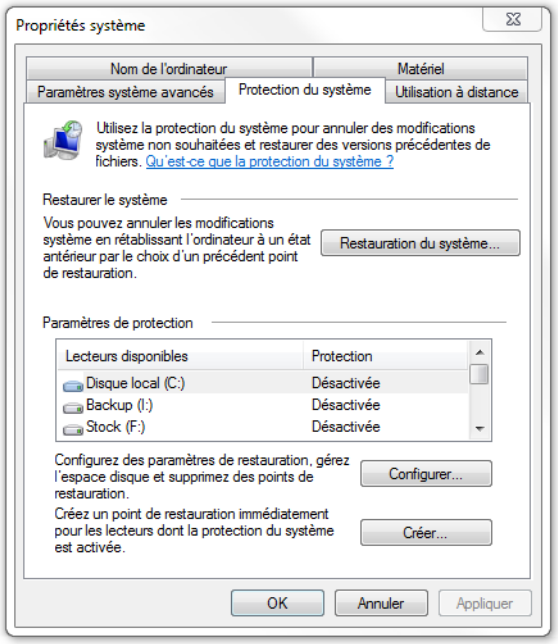


Figure 15–1
Fenêtre de configuration de la protection du système

La partie inférieure de la fenêtre affiche toutes les partitions de votre système, et, pour chacune d'elles, l'état d'activation de la protection. Vous pouvez ainsi personnaliser la configuration de la protection du système pour chaque partition. Pour cela, cliquez sur la partition de votre choix, puis sur le bouton *Configurer...* situé au bas de la liste.

Dans la configuration, vous pouvez préciser l'espace disque maximal que peuvent occuper les points de restauration. Une fois cette taille limite atteinte, les points de restauration les plus anciens seront effacés pour permettre la création de nouveaux points de restauration.

Nous l'avons vu, Windows crée automatiquement des points de restauration lorsque certains événements surviennent. Vous pouvez, si vous le souhaitez, forcer la création d'un point de restauration en cliquant sur le bouton *Créer...* Vous devrez alors donner une description du point de restauration (par exemple, la raison pour laquelle vous créez ce point). Cette description vous permettra de retrouver plus facilement le point de restauration par la suite. Un message de confirmation vous indique en fin de procédure le succès de l'opération.

ATTENTION Partition Windows

Par défaut, la protection est activée sur la partition sur laquelle est installé Windows.

FORMAT NTFS uniquement

Il n'est possible d'activer la protection que sur des partitions formatées en NTFS.

IMPORTANT La restauration et les données personnelles

La restauration système prend en charge les logiciels, les pilotes, les fichiers système et certaines entrées registre ainsi que quelques scripts. Elle ne prend pas en compte les fichiers personnels et ne pourra donc jamais vous aider à récupérer un fichier que vous auriez malencontreusement supprimé. Pour les données, pensez à mettre en place des sauvegardes, comme indiqué au chapitre 8.

Restaurer un point de sauvegarde

Puis, vient le jour où votre ordinateur est dans un état insatisfaisant et où la solution la plus rapide pour tenter de récupérer un état stable et correct reste la restauration système. Deux méthodes s'offrent à vous.

Pour lancer la restauration système, ouvrez le menu *Démarrer* et tapez `restauration` dans la zone de saisie. Cliquez alors sur l'élément *Restauration du système*.

La seconde méthode consiste à utiliser le bouton *Restauration du système* qui se trouve dans l'onglet *Protection du système* de la fenêtre *Propriétés système* (figure 15–1). Un assistant s'ouvre et vous donne le choix entre :

- Une restauration recommandée – Il s'agit tout simplement du dernier point de restauration, celui qui fera perdre le moins de données et de programmes.
- Une restauration sélective – Vous pouvez choisir parmi tous les points de restauration existants.

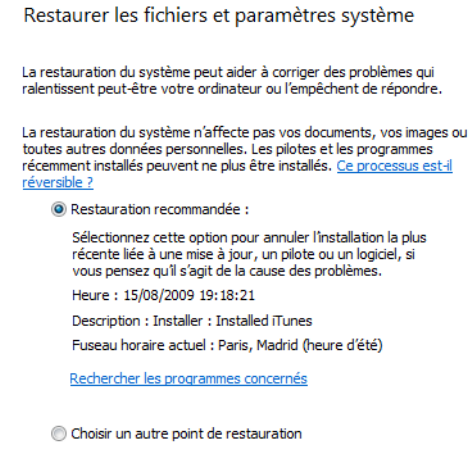


Figure 15–3 L'assistant de restauration du système vous donne le choix entre une restauration automatique et une restauration personnalisée.

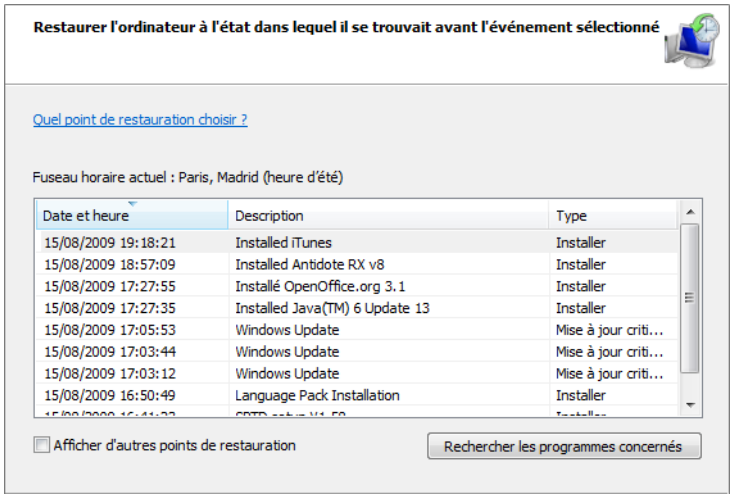


Figure 15–2 Choix d'un point de restauration particulier

Avant de cliquer sur le bouton *Suivant* (et d'afficher une confirmation pour lancer la sauvegarde), cliquez sur le bouton *Rechercher les programmes concernés*. Vous visualisez alors les éléments qui vont être modifiés. Vous pouvez ainsi vérifier si cette restauration et les modifications qu'elle va entraîner ont une chance de corriger le problème de votre système.

Cette fenêtre est composée de deux parties. La première liste les programmes et pilotes installés après le dernier point de sauvegarde qui seront supprimés (fichiers et registre) lors de la restauration. La seconde

partie de la fenêtre affiche les programmes qui étaient installés auparavant et que vous avez supprimés depuis. La restauration tente de les restaurer, sans pour autant garantir leur fonctionnement futur.

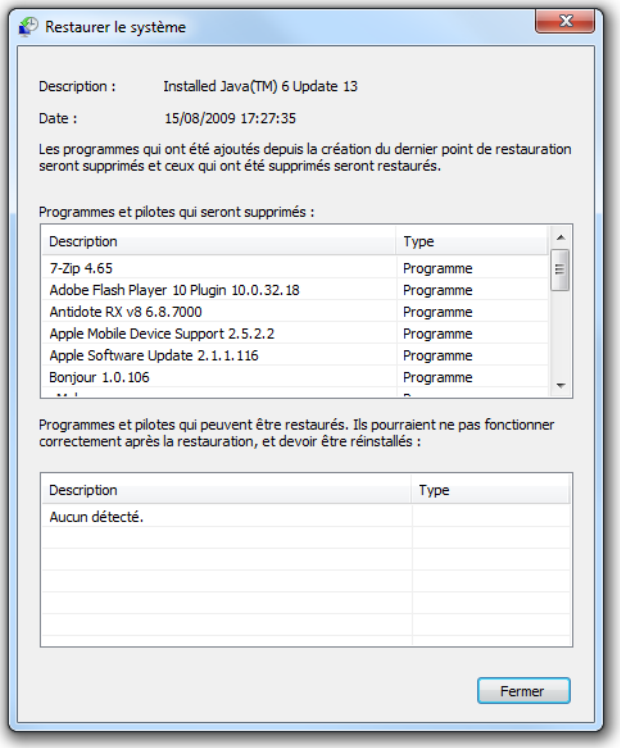


Figure 15–4
Descriptif des modifications
entre un point de restauration et l'état actuel du système

Profitez de cette fenêtre pour noter la liste des programmes que vous savez non problématiques mais que vous allez devoir réinstaller par la suite.

Lorsque vous êtes prêt, cliquez sur le bouton *Fermer*. Dans la fenêtre de l'assistant, cliquez sur le bouton *Suivant*. Un écran de confirmation apparaît pour vous permettre de valider votre choix. Fermez toutes les applications ouvertes de votre session et cliquez sur *Terminer* afin de laisser l'ordinateur redémarrer et restaurer.

Que faire si la restauration n'a pas résolu le problème ?

Dans un monde parfait, la restauration résout tous vos problèmes. Cependant, la réalité est bien souvent différente, soit parce que le problème ne vient pas d'un mauvais programme installé, soit parce que le problème est apparu avant le plus ancien de vos points de sauvegarde.

Plusieurs solutions s'offrent alors à vous :

- La première consiste à prendre un point de restauration plus ancien, et ainsi de suite, mais si le problème ne vient pas de là, vous risquez de perdre beaucoup de programmes pour rien.
- La deuxième consiste à utiliser une ancienne image disque que vous savez sans aucun problème. Vous pouvez également recourir à un utilitaire de restauration d'état d'usine (dans le cas d'un ordinateur acheté tout préparé). Vous perdez alors tout ce que vous avez fait depuis, donc pensez à sauvegarder vos données avant de réaliser toute opération.
- La dernière solution est la plus fastidieuse mais bien souvent la plus efficace : la recherche manuelle du problème. Ici, c'est votre logique et votre perspicacité qui vont vous aider à répondre à la situation. Vous pouvez utiliser des forums d'entraide, des chats de support mais également les outils que Windows met à votre disposition pour repérer et résoudre les problèmes.

L'outil de résolution de problèmes

Il existe plusieurs manières de vérifier qu'un système s'exécute correctement ou, au contraire, qu'il rencontre d'éventuels problèmes. Le moyen le plus rapide pour corriger les problèmes est de recourir au centre de maintenance, et plus précisément, à son module *Moniteur de fiabilité*. Il s'agit d'un graphique affichant l'historique des problèmes survenus sur le système, ainsi qu'une courbe de stabilité globale du système.

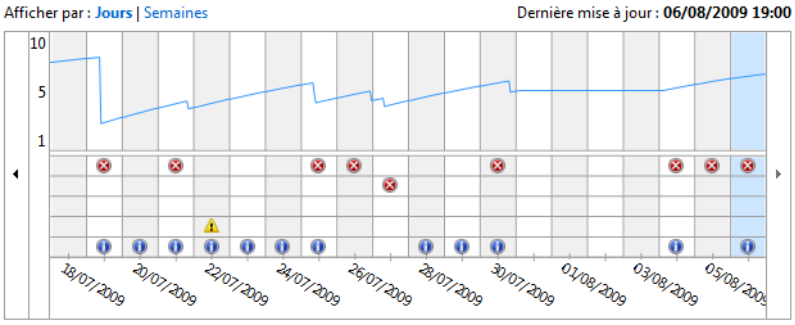


Figure 15–5
Graphique de la stabilité globale du système

La courbe représente l'index de stabilité, sur une échelle de 1 à 10, où 10 représente le niveau de stabilité maximal. Son interprétation est facile : elle croît doucement et décroît brusquement à chaque problème applicatif ou système. Ainsi, si votre système passe une quinzaine de jours sans problèmes, l'index de stabilité se rapprochera fortement du nombre 10.

Le graphe liste jour par jour les informations, avertissements et échecs apparus sur le système. Vous y trouvez une proposition de solution.

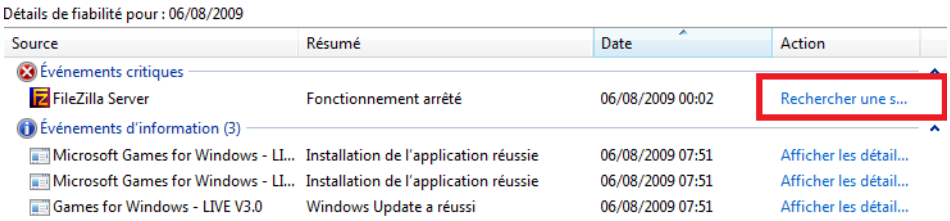


Figure 15–6
Détails des problèmes et recherche de solutions

Cliquez sur le bouton *Rechercher une solution* et votre système enverra un rapport d'erreur (sans informations confidentielles) à un serveur Microsoft qui contient une base de connaissances d'erreurs. Il enregistre automatiquement votre erreur et, s'il le peut, vous renvoie des informations pour résoudre le problème, soit en proposant un lien pour télécharger un patch, soit par un conseil, soit par une manipulation système expliquée pas à pas.

S'il constitue une solution rapide dans la plupart des cas, ce module de résolution de problèmes n'est pas pour autant d'une efficacité redoutable, puisqu'il lui est impossible de connaître tous les problèmes existants. Dans le cas où la base ne vous propose aucune solution, passez à la recherche approfondie, en utilisant le journal d'événements.

Journal d'événements

Le journal d'événements est le meilleur ami de l'administrateur système, qu'il s'agisse de procéder à des vérifications d'usage, d'identifier des problèmes qui se seraient produits de façon invisible, ou encore pour avoir une vue d'ensemble du fonctionnement de l'ordinateur sur les jours/semaines/mois précédents. Il permet également de remonter à la source d'un dysfonctionnement et donc d'obtenir une ébauche de solution.

Comparable à la boîte noire d'un avion, cet outil vous permet de retracer la majorité des événements qui se sont produits juste avant le dysfonctionnement de l'ordinateur.

Comprendre le journal d'événements

Le journal d'événements est un *snap-in* (voir chapitre 9) de la console de gestion MMC (*Microsoft Management Console*). Elle permet de visualiser et de gérer en un unique endroit, les événements système ou applicatifs de votre ordinateur. Il ne s'agit pas d'un simple visualiseur de fichiers de log, habituellement lisibles à l'aide d'un éditeur de texte, mais bel et bien

d'un outil complet avec lequel vous réglerez les problèmes présents sur votre système. Parmi ses nombreuses fonctionnalités, soulignons :

- la visualisation des fichiers de log ;
- la personnalisation de vues et de filtres afin d'étudier efficacement les journaux ;
- le déclenchement de tâches en réponses à des événements particuliers ;
- l'abonnement à des événements extérieurs et l'agrégation des journaux d'autres ordinateurs.

Ces fonctionnalités permettent d'affiner la configuration du système et d'en corriger les problèmes, mais surtout, au fil du temps, d'en améliorer la stabilité.

Exploiter le journal d'événements comme outil de diagnostic

Les journaux d'événements contenant énormément d'informations, il est facile de s'y perdre et de ne pas y trouver l'information pertinente. Il est donc important de savoir exploiter les journaux, tant pour trouver très rapidement ce que l'on cherche, que pour mettre en place des rapports qui permettront d'avoir une vue rapide des différents soucis du système.

Analyser les journaux d'événements

L'objectif premier d'un journal d'événements est d'enregistrer tout ce qui s'est passé d'important sur l'ordinateur. Au nombre des choses que vous apprend l'étude des journaux, soulignons :

- le détail ou l'origine d'un problème que vous avez remarqué ;
- les problèmes qui se sont déclenchés de façon invisible ;
- les avertissements que vous envoie le système.

Il n'est pas nécessaire de se rendre dans l'observateur d'événements quotidiennement pour s'assurer que tout fonctionne. Son étude dépend principalement de votre système, de son état de stabilité, de votre besoin d'informations pour résoudre un problème particulier, et surtout de la façon dont vous avez configuré votre observateur. En effet, il est possible d'être alerté par e-mail lorsqu'une erreur se produit. Inutile alors d'aller consulter les journaux régulièrement.

Pour ouvrir l'observateur d'événements :

1. Ouvrez le *Panneau de configuration*.
2. Dans la zone de recherche, tapez le mot-clé `admin`.
3. Cliquez sur *Outils d'administration*.

VERSION 7 Nouveautés

Par rapport à Windows Vista, l'observateur d'événements contient deux nouveautés. Il propose d'une part une vue d'ensemble qui affiche des statistiques sur les différents journaux du système, et d'autre part des vues personnalisées, qui servent à filtrer les événements affichés.

4 Cliquez sur le raccourci *Observateur d'événements*.

L'interface se découpe en trois parties.

- Dans la partie gauche se trouve la liste de tous les journaux système et applicatifs.
- La partie centrale contient soit la vue d'ensemble, soit la vue détaillée du journal sélectionné.
- La partie droite propose des actions contextuelles. Elles permettent non seulement d'agir sur les différents journaux ou événements, mais aussi de mettre en place des tâches planifiées d'alerte.

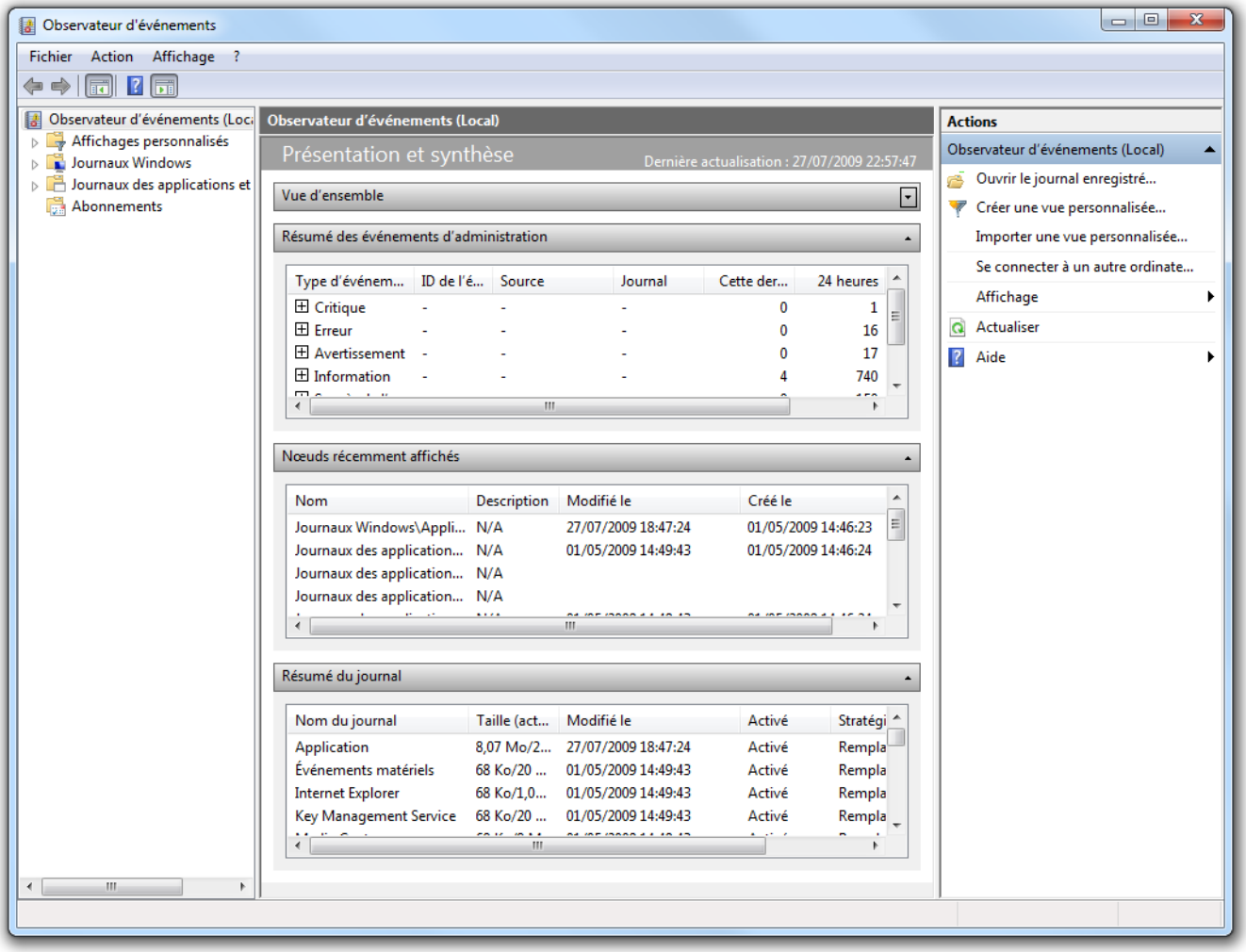


Figure 15–7 Vue globale de l'observateur d'événements

Les événements sont classés dans différents journaux, qui sont soit des journaux système, soit des journaux applicatifs (c'est-à-dire des journaux qui correspondent à une application bien précise). Il est important de bien différencier les journaux d'événements. Vous retrouverez ainsi rapidement l'information que vous recherchez. Par défaut, il existe trois journaux. Ils contiennent chacun des événements qui ne seront pas présents dans les autres, et qui dépendent soit de leur type, soit de leur source (programme à l'origine de l'événement).

- Le journal *Sécurité* rassemble tous les audits de sécurité relatifs à l'ouverture de session, les stratégies d'audit ou encore certaines traces d'élévation de privilèges.
- Le journal *Système* présente tous les événements ayant été déclenchés par des programmes ou des services faisant partie du cœur de Windows.
- Le journal *Applications* contient tout le reste : les applications que vous avez vous-même installées (si elles possèdent une fonctionnalité d'enregistrement d'événements), certaines applications de Windows comme Windows Error Reporting, MsiInstaller, ou encore les éléments installant automatiquement des pilotes pour les périphériques.

En fonction du problème que vous vous efforcez de résoudre, la réponse se trouvera donc soit dans l'un de ses trois journaux, soit dans un journal spécifique créé par l'application (telle que Internet Explorer, SQL Serveur et bien d'autres).

Trouver l'information pertinente

Chaque événement contient un certain nombre d'informations, dont la plupart ne vous sera pas nécessairement utile. Il existe avant tout, plusieurs niveaux d'événement :

- commentaires ;
- information ;
- avertissement ;
- erreur ;
- critique.

Les trois derniers possèdent leur icône propre permettant de les repérer rapidement dans le journal. Pour étudier un événement particulier, il suffit de double-cliquer sur son nom pour ouvrir sa fenêtre de détails.

Ensuite, regardez dans l'ordre :

1. La source de l'événement pour détecter le logiciel incriminé.
2. Le message d'erreur, qui est bien souvent suffisamment clair pour comprendre l'origine du problème.

3 L'ID de l'événement. Ce code d'erreur correspond à une erreur bien précise du logiciel ou du système. Si le message d'erreur vous résiste, lancez alors une recherche via votre moteur préféré sur l'ID. Il y a fort à parier que vous trouverez alors une solution pas à pas, sur la base de connaissances de l'éditeur, ou sur des forums.

Dans la majorité des cas, fort de ces trois informations, vous ciblerez précisément la cause du problème et saurez ce qui se passe en arrière-plan sur votre ordinateur. Ainsi, tout utilisateur qui sait trouver ces informations est potentiellement capable de résoudre n'importe quel problème technique.

Il est possible d'optimiser le processus de résolution de problème en réduisant le temps de détection des problèmes et de récupération des informations critiques. Ceci peut notamment se réaliser à l'aide de vues filtrées.

Personnaliser les vues

On dit bien souvent que les bons développeurs sont feignants. En effet, ils cherchent systématiquement à réaliser toute tâche en déployant le moins d'effort possible. Ceci vaut aussi probablement pour les administrateurs système, puisqu'ils ont compris comment gagner du temps en exploitant les outils mis à leur disposition pour réaliser les tâches qui leur incombent.

L'une des tâches les plus longues et fastidieuses pour un administrateur ou un utilisateur avancé est d'analyser tous les journaux d'événements afin de localiser les problèmes ou de rechercher des solutions. Comment éviter de parcourir tous les événements pour trouver rapidement ce que l'on cherche ? Tout simplement en créant une vue personnalisée.

Une vue personnalisée est une vue filtrée d'un ou plusieurs journaux d'événements. Dans celle-ci, vous pouvez préciser les types d'événements à afficher (critique, avertissement, commentaires, erreur ou information), la source de l'événement (un programme ou un service en particulier), mais également les codes ou les mots-clés apparaissant dans les messages d'erreur.

CITATION Des programmeurs feignants ?

« C'est bien par la nécessité d'automatiser de plus en plus son périmètre d'action que l'informaticien multiplie les méta modèles. La généralisation d'un modèle permet en effet d'automatiser bien d'autres champs applicatifs et de résoudre avec un effort moindre toujours plus de problèmes.
C'est donc bien un but de productivité que recherche l'informaticien, c'est-à-dire comment produire plus (de données résultat, d'organisation) en développant moins. L'erreur communément effectuée par la suite est d'affirmer que les informaticiens sont feignants. Produire plus en faisant moins, c'est avant tout pouvoir réinvestir ce que l'on vient de gagner pour produire encore plus. »
Valéry-Guilhem Frémaux In *Principes d'architecture des programmes Java* (éditions Ellipses)

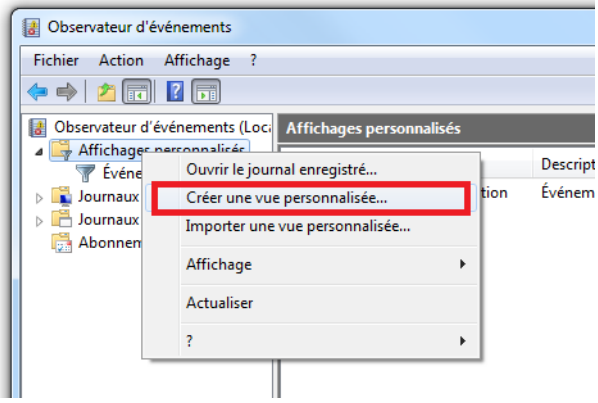


Figure 15–8
Création d'une nouvelle vue personnalisée

La fenêtre d'assistant de création de vue personnalisée propose alors un certain nombre de filtres. Le premier critère de filtre est la date maximale des événements retournés. Grâce à lui, vous paramétrez l'affichage des événements s'étant déclenchés les douze dernières heures.

Vient ensuite le niveau des événements. C'est sûrement le critère le plus important, puisque c'est lui qui sert à créer une vue retournant toutes les remontées d'événements de niveau critique ou erreur, et permet ainsi de voir rapidement ce qu'il faut réparer sur le système.

Pour être exhaustif, d'autres critères sont à votre disposition pour filtrer les événements retournés :

- par rapport à la source de l'événement, soit le journal, soit une application ou un service particulier ;
- par rapport à l'ID de l'événement ;
- par rapport à certains mots-clés ;
- par rapport à un utilisateur précis ;
- par rapport à un ordinateur précis (dans le cas d'agrégation de journaux distants).

Avec chacun de ces filtres, vous personnalisez une ou plusieurs vues afin d'isoler les informations dont vous avez besoin.

L'onglet *XML* affiche les filtres que vous avez sélectionnés sous forme d'une requête XPath. Il permet de copier rapidement votre requête sur un autre ordinateur ou dans une seconde vue personnalisée, puis de la modifier.

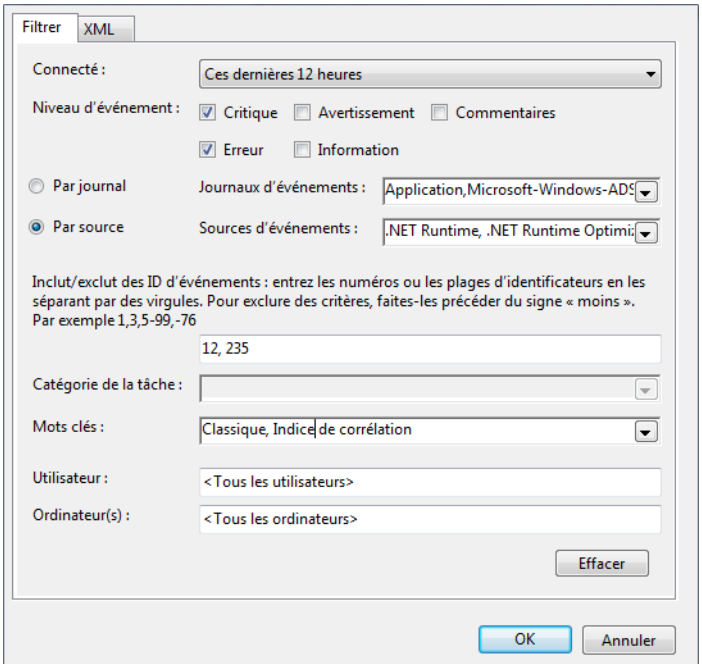


Figure 15–9
Assistant de création d'une vue personnalisée

BON À SAVOIR Vues personnalisées et performances

Les vues personnalisées n'ont strictement aucune incidence sur les performances de votre système. Vous pouvez en créer des centaines sans que cela ne ralentisse votre ordinateur. Elles n'utilisent le processeur qu'au moment de l'affichage d'une fiche précise.

POUR ALLER PLUS LOIN XPath et XML

Les journaux d'événements sont enregistrées dans des fichiers XML. Il existe plusieurs méthodes pour les lire, un peu à la façon d'une base de données. Les deux méthodes les plus connues sont SAX (*Simple API for XML*, un moyen simple de parcourir un fichier XML nœud par nœud) et XPATH. XPATH est une syntaxe de requête qui, à l'aide d'un moteur intégré à Windows, retourne uniquement certaines informations d'un fichier XML.
La requête XPATH suivante (non représentative du format XML Windows) :

```
//event[@type='critical']
```

permet de ne retourner que les événements donc le niveau est critique.
Cet outil est parfait pour la création de vue personnalisée et permet d'obtenir très rapidement les résultats à afficher. Pour en savoir plus sur la norme XPATH, consultez la recommandation W3C de description de cette syntaxe :

- http://www.w3.org/TR/xpath

Si le résultat obtenu n'est pas satisfaisant, cliquez sur le nom de la vue personnalisée à l'aide du bouton droit de la souris, et sélectionnez *Filtrer la vue personnalisée actuelle* afin d'ouvrir ses propriétés et de modifier les critères de filtrage.

Exploiter le journal d'événements comme outil d'alerte

Beaucoup d'administrateurs système pensent que le journal d'événements n'est utile que lorsque l'on prend le temps de s'y plonger pour en analyser le contenu. Ils sont loin d'imaginer que le journal d'événements est capable d'agir seul pour résoudre un problème, ou bien de prévenir les bonnes personnes en cas de levée d'événement.

En effet, le journal d'événements est capable de déclencher une tâche particulière à chaque fois qu'il enregistre un événement bien précis. Cette tâche peut se lancer :

- Au niveau d'un journal : la tâche se déclenche à chaque événement enregistré.
- Au niveau d'un événement : la tâche ne se déclenche que pour cet événement et les événements identiques.

Voyons comment créer une tâche planifiée, non pas à partir de critères horaires ou journaliers, mais à partir de critères événementiels.

1. Ouvrez le journal d'événements de votre choix.
2. Cliquez sur l'événement que vous souhaitez surveiller. Le menu *Actions*, situé sur la droite, se met alors à jour.
3. Choisissez le menu *Joindre une tâche à cet événement*. Un assistant de création de tâche s'ouvre alors.

Figure 15–10
Création d'une tâche planifiée événementielle

4. Donnez un nom et une description à votre événement.

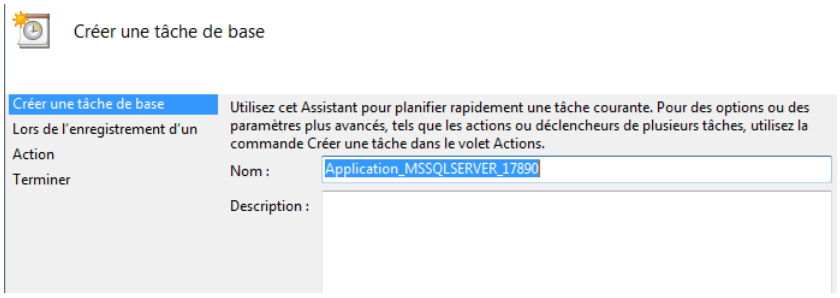


Figure 15–11
Assistant d'ajout d'une tâche planifiée

BONNE PRATIQUE De l'intérêt d'être précis

Comme il est possible de créer un nombre infini de tâches pour un événement donné, soyez aussi précis que possible dans le choix du nom. Vous vous y retrouverez plus vite par la suite.

5 À la seconde étape de l'assistant, vérifiez les critères déclencheurs de la tâche : le journal où est enregistré l'événement, sa source (c'est-à-dire le programme qui a généré l'enregistrement) et son ID (un code d'erreur pour l'application concernée).

Figure 15–12
Critères de l'événement

6 Définissez si votre tâche planifiée exécute un programme défini. Le cas échéant, passez les arguments nécessaires. Ce programme peut être un programme de reporting, d'utilisation des logs ou encore un script. Dans notre cas, l'événement déclencheur est une erreur fatale du serveur. Nous souhaitons lancer un script qui se chargera de redémarrer le service, nous permettant ainsi d'assurer une disponibilité maximale de notre serveur SQL.

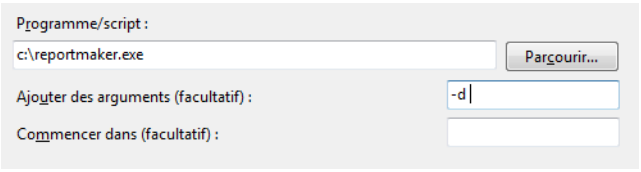


Figure 15–13
L'assistant permet de préciser un programme à exécuter en cas d'événement

7 Précisez si vous souhaitez que le journal déclenche l'envoi d'un e-mail paramétré. Avec cette solution, plus besoin de surveiller constamment le serveur et les services SQL. Il nous suffit d'attendre un e-mail pour être instantanément averti en cas d'erreur critique sur le serveur. Vous pouvez même demander à ce que le rapport soit attaché en pièce jointe, ce qui vous évitera de devoir vous rendre sur le serveur incriminé pour analyser la source du problème.

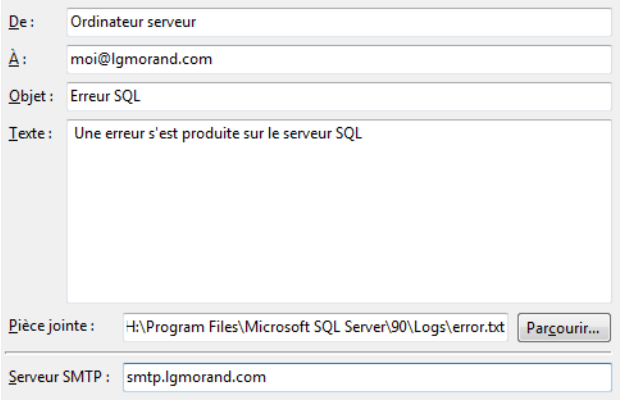


Figure 15–14
E-mail à envoyer en cas d'événement

8 Configurez également l'affichage d'un message. Cette option est utile pour les ordinateurs utilisés comme station de travail.

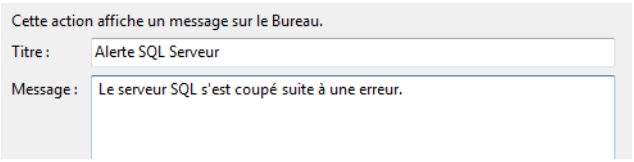


Figure 15–15
Message à afficher en cas d'événement

9 Cliquez sur le bouton *Terminer*. Votre tâche est maintenant prête à être exécutée.

10 Une fois vos tâches planifiées configurées, ouvrez le *Planificateur de tâches*, situé dans les *Outils d'administration* du *Panneau de configuration*, pour vérifier que toutes les tâches répondant à votre besoin s'y trouvent.

ASTUCE Plusieurs actions pour un événement unique

Si vous souhaitez paramétrer plusieurs actions en même temps (par exemple, afficher un message et envoyer un e-mail), il suffit de créer plusieurs tâches planifiées pour un même événement.

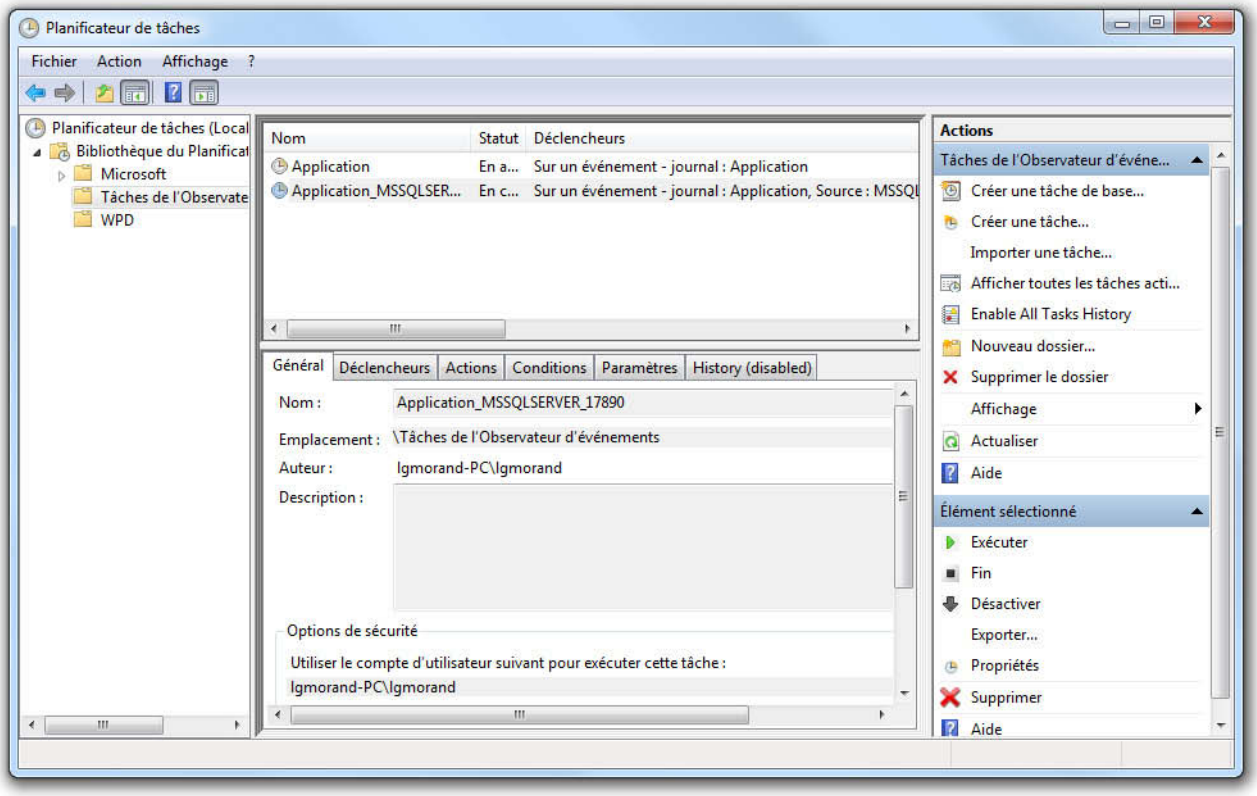


Figure 15–16 Fenêtre du planificateur de tâches

À SAVOIR

Limitations des tâches sur événements

Soulignons une limitation dans l'utilisation des tâches liées aux événements : il est impossible de lier une tâche à un événementsi celui-ci est archivé ou s'il fait partie des journaux d'analyse ou de débogage. Il est cependant possible d'attacher une tâche au niveau du journal même.

Voici comment procéder pour réaliser la même opération de création mais au niveau d'un journal sans vous limiter à un seul événement.

1. Cliquez sur le journal de votre choix.
2. Dans la zone des actions sur la droite, choisissez le menu *Joindre une tâche à ce journal*.
3. La suite des étapes est parfaitement identique à la procédure que nous venons de voir.

Exploiter le journal d'événements comme outil d'agrégation

Que vous soyez administrateur système au sein d'un domaine ou utilisateur avancé possédant plusieurs ordinateurs dans un réseau local, vous désirez certainement gérer depuis un seul ordinateur les événements de tous les ordinateurs de votre parc.

La console de gestion des journaux d'événements propose une méthode très simple : récupérer les journaux d'événements des ordinateurs distants et les afficher localement. Si elle est facile à comprendre et à utiliser, cette solution est malheureusement délicate à mettre en place et nécessite un certain nombre d'étapes et de paramétrages spécifiques.

Configurer les ordinateurs source

La première chose à faire est de configurer les ordinateurs source, c'est-à-dire ceux dont les journaux seront rapatriés. Il est nécessaire que ces machines soient configurées pour partager leurs journaux. Cela ne peut se faire que via un outil spécifique nommé WinRM (*Windows Remote Management*).

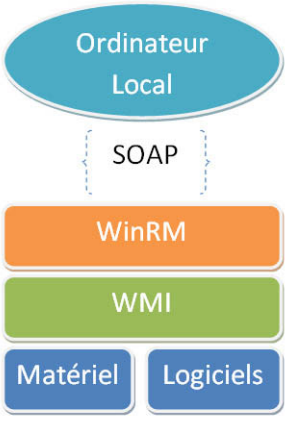


Figure 15–17
Fonctionnement de l'interrogation distante via WinRM

WinRM est un outil qui permet, à travers des pare-feu, d'échanger des informations matérielles et logicielles entre deux ordinateurs. Lorsqu'un ordinateur est interrogé, il est contacté via un écouteur (*listener*), correspondant au service Windows WinRM local. Via la couche WMI (*Windows Management Instrumentation*), l'écouteur permet de collecter des données qui sont ensuite renvoyées par le réseau, selon un protocole propriétaire de Microsoft (*WS-Management Protocol*) basé sur SOAP (*Simple Object Access Protocol*).

Pour configurer tout ceci convenablement, il faut procéder avec méthode et ordre.

Le matériel et les logiciels ne requièrent pas de paramétrages particuliers, car ce qui nous intéresse est le journal d'événements. Normalement, la couche WMI est, elle aussi, active.

Cependant, WMI ne nous intéresse pas outre mesure, car WinRM (*Windows Remote Management*) se charge d'interroger lui-même WMI en fonction des demandes que lui fera l'ordinateur demandeur (hôte). Penchons-nous donc sur WinRM.

Si WinRM est actif par défaut sur les versions serveur de Windows, comme Windows Serveur 2008, il n'en est pas de même sur les stations de travail équipées de Vista ou de Windows 7. Il faut donc l'activer et le configurer pour qu'il puisse communiquer avec des ordinateurs distants. Vous pouvez procéder manuellement ou bien lancer une ligne de commande.

1. Ouvrez une invite de commandes (avec les droits administrateur) sur l'ordinateur hôte, puis saisissez la commande `WINRM quickconfig`.
2. Un message vous demande alors si vous souhaitez lancer la configuration rapide, acceptez. Cette commande effectue les trois paramétrages requis pour l'utilisation de WinRM, à savoir :
   - le démarrage du service WinRM et sa configuration en automatique (pour un démarrage lors de prochaines sessions si l'ordinateur est éteint entre-temps) ;
   - la création d'un écouteur pour entendre les requêtes distantes ;
   - l'ouverture des ports nécessaires dans le pare-feu Windows.
3. Vient ensuite la configuration des autorisations. Ouvrez la console MMC de gestion des utilisateurs et groupes utilisateur. Ajoutez l'ordinateur collecteur au groupe des administrateurs locaux. Il vous faudra peut-être cocher le type d'objet *Ordinateurs* pour pouvoir ajouter le nom de votre ordinateur.

Il reste encore à configurer l'ordinateur hôte pour qu'il aille précisément interroger tel ou tel ordinateur que vous venez de préparer.

WMI

Présente depuis les premières versions de Windows, WMI est une surcouche système qui interroge les ressources logicielles et matérielles, sans requérir d'accès bas niveau complexes à mettre en œuvre. Elle peut être interrogée à l'aide de WQL (*WMI Query Language*), langage de requête de type SQL dérivé. Il suffit, par exemple, d'exécuter la requête suivante pour obtenir la liste de tous les processus en cours d'exécution :

```
Select * from Win32_Process
```

Configurer l'ordinateur hôte

L'ordinateur hôte a lui aussi besoin d'un service Windows particulier. Il s'agit de Windows Event Collector.

1. Activez le service via la commande `wecutil qc`.
2. Acceptez de configurer le service en démarrage différé. À partir de ce moment, les deux ordinateurs sont prêts à travailler ensemble : l'un est prêt à écouter et l'autre à collecter. Il faut ensuite indiquer ce que vous souhaitez collecter et comment.
3. Dans la console de gestion des journaux d'événements, cliquez dans la partie gauche sur *Abonnements*.
4. Cliquez ensuite sur le menu *Action>Créer un abonnement*, afin d'ouvrir un assistant de création.

ATTENTION

La collecte d'événements dans un environnement de groupe de travail

Si vous travaillez dans un petit réseau sans domaine, il est impossible d'ajouter un ordinateur comme élément d'un groupe. Cette limitation provient du fait qu'un ordinateur ne peut être fortement authentifié si l'on utilise pas Active Directory.
Dans ce cas de figure, une alternative existe. Sur l'ordinateur source, créez un compte avec des privilèges administrateur et ajoutez-le au groupe local *Lecteur des journaux d'événements*. Lorsque par la suite, vous configurerez la partie abonnement sur l'ordinateur collecteur, il vous faudra préciser, dans les paramètres avancés, l'utilisation de ce compte spécifique. Répétez cette opération pour chaque ordinateur pour lequel vous souhaitez collecter des données.

5 Nommez l'abonnement et cliquez sur *Sélectionner des ordinateurs* pour définir la liste des ordinateurs depuis lesquels vous souhaitez collecter les événements.

Dorénavant, vous pouvez visualiser les journaux distants sans quitter votre ordinateur.

À l'instar du mécanisme des vues filtrées, il est possible de configurer précisément les événements qui sont collectés. Pour modifier le filtrage, il vous suffit d'ouvrir les propriétés d'un abonnement déjà créé, ou tout simplement, au moment de sa création.

Résoudre les problèmes du journal d'événements

Nous avons comparé le journal d'événements à la boîte noire d'un avion. Que se passe-t-il lorsque les boîtes noires sont irrécupérables ? Il devient tout simplement très difficile de déterminer les origines d'un problème. Il en va de même pour le journal d'événements : s'il n'est pas pleinement fonctionnel, il vous sera difficile de résoudre les problèmes.

Si le principal avantage du journal d'événements est de s'être amélioré au fil des versions de Windows, sa complexité ascendante implique de nouveaux problèmes, qui découlent bien souvent d'une mauvaise configuration de la part de l'administrateur du système.

Au fil des années, nous avons constaté que quatre problèmes reviennent régulièrement, laissant cois des administrateurs chevronnés devant un journal, qui ne les aide plus beaucoup.

Pourquoi la tâche planifiée ne s'est-elle pas lancée lorsque l'événement s'est déclenché ?

Répondre à cette question n'est pas chose facile. Cependant, l'origine du problème se trouve généralement dans une mauvaise configuration de votre part : ouvrez le gestionnaire de tâches planifiées et vérifiez que la tâche existe bien et qu'elle est bien configurée pour le bon événement.

Pourquoi le journal d'événements est-il vide ?

À cette question, plusieurs réponses sont possibles :

- L'application n'a peut-être pas envoyé d'informations à stocker.
- Le journal vient d'être vidé, soit par vous, soit par un autre utilisateur. Il suffit en effet de cliquer sur *Effacer le journal* pour remettre à zéro les données qu'il contient.
- Le problème vient peut-être des filtres : si vous consultez une vue filtrée et que le filtre est trop restrictif ou qu'il a été mal configuré, la

Solution Réactiver l'enregistrement des événements

1. Cliquez avec le bouton droit sur votre journal.
2. Dans le menu contextuel, sélectionnez *Propriétés*.
3. Cochez la case *Activer la journalisation*.
4. Cliquez sur *OK*.

vue ne retourne aucun résultat, bien que des événements aient bel et bien été enregistrés. Ceci arrive plus souvent qu'on ne le croit !

- L'enregistrement des événements pour ce journal est désactivé.

Pourquoi les événements arrivés il y a quelques jours sont-ils absents ?

Une fois n'est pas coutume, la réponse à ce problème est toute simple : la taille maximale du fichier de journal est trop petite. Un fichier de journal est dit roulant, ce qui signifie que lorsque la taille maximale est atteinte, les enregistrements les plus anciens sont effacés, afin de laisser de la place aux nouveaux.

Normalement la taille des journaux est suffisante pour stocker plusieurs jours voire semaines d'enregistrements. Néanmoins, si votre ordinateur est instable ou très sollicité, il enregistre plusieurs centaines d'entrées par jour, ce qui entraîne la disparition rapide des événements qui auraient pu vous intéresser.

Si cela vous arrive, augmentez la taille du journal en vous rendant dans ses propriétés, puis en augmentant la valeur contenue dans la case *Journal max. (Ko)*. Vous pouvez également choisir l'une des deux autres méthodes de gestion des journaux, à savoir l'archivage des journaux pleins (option *Archiver le journal lorsqu'il est plein, ne pas effacer d'événements*) ou bien outrepasser la limite de taille à l'aide de l'option *Ne pas remplacer les événements (nettoyage manuel du journal)*.

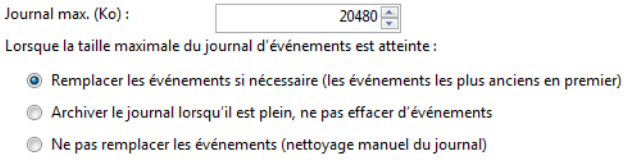


Figure 15–18
Propriétés d'un journal d'événements

Pourquoi est-il impossible de se connecter à un ordinateur distant pour y récupérer les journaux d'événements ?

Lors de la mise en place d'un abonnement pour récupérer les journaux d'un ordinateur distant, il arrive que l'abonnement reste en mode inactif. En général, cela signifie que le client WinRM n'a pas réussi à se connecter à l'ordinateur distant, bien souvent parce qu'il est bloqué par le pare-feu de l'ordinateur auquel il tente d'accéder.

Vérifiez alors :

- que les règles de trafic nommées *Gestion à distance des journaux d'événements* sont bien activées sur l'ordinateur distant ;

- que votre compte utilisateur, s'il n'est pas administrateur d'un domaine, a des droits administrateur sur l'ordinateur distant ;
- vérifiez tout simplement que l'ordinateur distant est allumé et configuré pour partager ses journaux d'événements.

EN PRATIQUE

Configuration automatique de WinRM

Sur l'ordinateur distant, ouvrez une invite de commandes et lancez la configuration automatique de WinRM en exécutant la commande suivante :

```
winrm quickconfig
```

Réparer un ordinateur qui ne démarre plus

Que l'ordinateur ne démarre plus du tout (problème matériel) ou que le système d'exploitation se bloque lors du processus de chargement, le résultat est le même : l'utilisateur se retrouve privé de son outil de travail. Il est courant de se trouver démuni face à un écran noir sans savoir par quoi commencer pour le faire fonctionner de nouveau.

Nous n'aborderons pas dans cette section les cas d'échecs matériels tant les possibilités sont nombreuses. Si votre ordinateur ne démarre plus, la réparation nécessite un minimum de connaissances hardware. Nous préférons nous focaliser sur le cas où l'ordinateur démarre mais qu'il vous est impossible d'accéder à votre session.

Afficher le menu de démarrage alternatif

Le démarrage d'un système Windows suit trois étapes principales :

- Le *bootloader* choisit le système d'exploitation à charger, lorsque plusieurs systèmes sont installés sur le même ordinateur.
- Le *bootscreen* s'affiche pendant que le noyau de Windows se charge.
- Le *logonscreen* permet de choisir le compte à utiliser.

B.A.-BA **Sélectionner sans souris**

Naviguez entre les différents items du menu à l'aide des flèches du clavier. Validez votre choix en appuyant sur la touche *Entrée*.

Cependant, il existe une étape alternative, qui se situe juste après le choix du système d'exploitation (bootloader). Pour la faire apparaître, dès que votre ordinateur démarre, appuyez plusieurs fois de suite sur la touche *F8* jusqu'à ce qu'un menu blanc sur fond noir apparaisse. Ce menu propose différentes solutions et outils qui vont vous aider à corriger votre système. Le tableau 15-1 présente les solutions qu'il propose.

Tableau 15–1 Solutions et outils pour corriger le système

Intitulé	Description
Réparer l'ordinateur	Lance l'assistant de récupération qui vous permettra de faire certaines opérations système avancées. Nous l'abordons dans la section « Restauration du système ».
Mode sans échec	Le système démarre mais ne charge que les éléments système (services, pilotes, etc.) afin d'avoir un minimum de composants s'exécutant. Ce mode est conseillé pour nettoyer un système de potentiels virus ou pour détecter plus facilement la source d'un problème logiciel.

Tableau 15–1 Solutions et outils pour corriger le système (suite)

Intitulé	Description
Mode sans échec avec prise en charge réseau	Identique au mode sans échec normal mais cette fois-ci, les services réseau démarrent et l'accès à Internet est possible.
Invite de commandes en mode sans échec	Invite de commandes Windows.
Inscrire les événements de démarrage dans le journal	Permet de créer un fichier de log enregistré dans le répertoire et nommé `ntbtlog.txt`. Il contient la liste des éléments chargés par le système au démarrage ainsi que l'état de leur chargement (réussite/échec).
Activer la vidéo à basse résolution	Lance le système avec une résolution de 640 x 480.
Dernière configuration valide connue	Recharge la dernière configuration stable du système.
Mode restauration des services d'annuaire	Utile lorsque vous utilisez un contrôleur de domaine.
Mode débogage	Mode verbeux, contenant plusieurs journaux de logs supplémentaires et presque exclusivement utilisés par les développeurs de pilotes pour périphériques afin de détecter d'éventuels problèmes.
Désactive le redémarrage automatique en cas d'échec du système	Empêche le rédémarrage automatique en cas d'erreur fatale et active l'affichage des « écrans bleus de la mort » (*Blue Screen Of Death*).
Désactiver le contrôle obligatoire des signatures de pilotes	Mode permettant l'installation de pilotes non signés.
Démarrer Windows normalement	Mode de démarrage utilisé par défaut.

Dernière bonne configuration connue

En cas de problème, un réflexe très répandu est de se tourner immédiatement vers le mode sans échec. C'est là une grossière erreur. En effet, il est possible que le système d'exploitation ne démarre plus, suite à l'installation d'un logiciel ou d'un pilote matériel. Bien évidemment, c'est au redémarrage que vous identifiez que Windows ne démarre plus ou affiche un écran bleu (ou BSOD).

Lorsque vous faites une modification, elle n'est pas définitivement enregistrée sur votre système. Certains paramétrages personnels sont enregistrés à l'extinction de l'ordinateur, tandis que d'autres sont enregistrés au démarrage de votre session. C'est notamment le cas des pilotes Windows. Le système a pour principe de considérer une configuration système comme stable si vous redémarrez votre ordinateur et arrivez jusqu'à votre Bureau. À ce moment précis, il enregistre cette configuration comme « dernière bonne configuration système ». Un peu à la manière d'un point de restauration, elle servira à revenir à un état stable du système si jamais votre système est défaillant et que vous n'avez pas réussi à trouver l'origine du problème ou à le corriger (suite à un virus, par exemple).

BSOD

Le BSOD (*Blue Screen of Death*) ou « écran bleu de la mort » est un écran d'erreur originaire de Windows. Il s'affiche lorsqu'une erreur irréversible s'est produite sur le système et que celui-ci a été coupé par sûreté. Synonyme de gros problème sur le système, les causes du BSOD peuvent là encore être logicielles (souvent pilotes) ou matérielles. L'écran contient néanmoins des informations sur le module défaillant et les informations qu'il affiche sont parfois primordiales pour résoudre le problème.

Astuce **Afficher les écrans bleus**

Depuis Windows XP, il n'est plus aussi simple d'obtenir un écran bleu, non pas parce que le système est plus stable, mais parce que par défaut, dans les versions Windows XP, Vista et 7, le système préfère redémarrer l'ordinateur et tenter de retrouver un état de lancement, plutôt que de rester bloqué sur un écran bleu. Ceci améliore la disponibilité de l'ordinateur, y compris en cas de problème grave, mais peut malheureusement entraîner des redémarrages en boucle, ou provoquer un redémarrage en cours d'utilisation. Désactivez alors le redémarrage automatique pour obtenir l'affichage de l'écran bleu. Pour cela :

1. Ouvrez le menu *Démarrer*.
2. Affichez les propriétés de *l'Ordinateur* (via un clic droit).
3. Dans la barre latérale, cliquez sur le bouton *Paramètres système avancés*.
4. Dans la fenêtre qui s'ouvre, cliquez sur le bouton *Paramètres* situé sous *Démarrage et récupération* et décochez la case *Redémarrer automatiquement*.
5. Cliquez sur le bouton *OK* pour sauvegarder votre choix.

Vous pouvez également désactiver le redémarrage automatique avant le démarrage de l'ordinateur via le menu de démarrage alternatif.
Les éventuels écrans bleus s'afficheront dorénavant et votre ordinateur ne redémarrera pas à l'improviste, sans que vous en connaissiez la raison.

Imaginons que vous souhaitez installer un nouveau périphérique pour votre imprimante. Le pilote s'installe sans encombre, mais vous demande de redémarrer pour être pleinement fonctionnel. Malheureusement, le redémarrage se passe mal et le système n'arrive pas à se charger complètement. C'est là que la dernière bonne configuration entre en jeu. Comme vous n'êtes pas encore arrivé jusqu'à votre Bureau, la dernière configuration est celle qui existait avant l'installation du pilote.

1. Redémarrez votre ordinateur complètement (touche *Reset*).
2. Affichez le menu de démarrage alternatif.
3. Choisissez alors l'option *Dernière configuration valide connue*.

Le système démarre alors normalement, mais vous devez retenter l'installation de votre imprimante. Pensez éventuellement à vous procurer une version plus récente du pilote.

Il arrive que, suite à l'installation d'un pilote, votre ordinateur parvienne à démarrer jusqu'à l'affichage du Bureau, mais n'aille pas plus loin. Dans ce cas, il est possible que la dernière bonne configuration soit finalement instable. C'est dans ce genre de situation qu'il faut alors tenter le mode sans échec.

Le mode sans échec

Le mode sans échec est un mode restrictif du système d'exploitation dans lequel aucun service ou pilote (à l'exception des services système) n'est chargé. Pour les pilotes du clavier, de la souris et de la carte gra-

phique, des pilotes génériques et limités sont chargés. Les programmes censés se lancer au démarrage sont désactivés.

Cette configuration favorise temporairement la stabilité du système, afin que vous puissiez effectuer vos opérations de maintenance, qu'il s'agisse de changer un pilote matériel, de sauvegarder des données, d'appliquer des antivirus ou encore d'accéder aux outils d'administration, tels que les journaux d'événements, afin de diagnostiquer l'état du système.

Lorsque vous redémarrerez l'ordinateur, le système quittera automatiquement le mode sans échec pour revenir en mode par défaut.

Outils de récupération système

Lorsqu'aucun mode de démarrage ne convient, il vous reste la possibilité d'utiliser les options de récupération système.

Pour les utiliser, choisissez l'option *Réparer l'ordinateur* du menu de démarrage. Un assistant multilingue vous demande alors d'utiliser un compte utilisateur, puis vous propose les cinq outils présentés dans le tableau 15-2.

Tableau 15–2 Outils de réparation du système

Outil	Action
Réparation du démarrage	Répare le *bootloader* ou les fichiers permettant de charger le noyau du système. Cet outil est notamment capable de vous fournir un journal de log si des problèmes ont été détectés.
Restaurer le système	Charge un ancien point de restauration.
Récupération de l'image système	Charge une image disque et écrase votre système avec cette dernière.
Diagnostic de mémoire Windows	Vérifie l'état des barrettes mémoire de votre ordinateur afin d'éviter la corruption des données lors de l'utilisation normale de l'ordinateur.
Invite de commandes	Lance la console Windows.

Vérifier l'état des fichiers système

Windows intègre un utilitaire très peu connu même s'il était déjà présent dans les versions antérieures du système. Cet utilitaire est un vérificateur de fichiers système (en anglais, SFC pour *System File Checker*). Il fonctionne en ligne de commande et vérifie l'intégrité des fichiers système, c'est-à-dire qu'il s'assure qu'aucun fichier système n'a été modifié et qu'ils sont donc tous bien identiques à leur version originale.

Pour vérifier les fichiers système sur votre ordinateur, ouvrez tout d'abord une invite de commandes. Pour cela, allez dans le menu *Démarrer*, saisissez `invite de commandes` dans la zone de recherche, puis tapez sur la touche *Entrée*. Dans la fenêtre qui s'ouvre alors, saisissez la commande suivante :

```
sfc /scannow
```

Si jamais l'ordinateur ne démarre pas du tout, vous pouvez, avec un CD d'installation, lancer la console de récupération et y saisir la ligne de commande précédente.

L'analyse dure quelques minutes. Lorsqu'elle est terminée, le résultat s'affiche et vous indique si les fichiers sont intègres ou si des erreurs ont été détectées. Dans ce cas, l'utilitaire remplace les fichiers erronés par leur version originale.

De l'aide à distance

Windows 7 intègre un utilitaire appelé *Assistance à distance Windows*. Il vous permet de demander de l'aide à un ami via Internet. Il pourra ainsi visualiser votre écran en temps réel et prendre les commandes pour vous montrer les manipulations au clavier ou à la souris.

Se faire aider

ALTERNATIVE **Lancer Assistance à distance Windows**

Vous pouvez également saisir `assistance` dans la barre de recherche du menu *Démarrer* ou faire appel à l'exécutable `msra.exe` présent dans le dossier `\Windows\System32`.

L'outil d'aide à distance se trouve dans le menu *Démarrer* dans *Programmes>Maintenance>Assistance à distance Windows*.

Lorsque vous démarrez l'outil, un assistant se lance et vous demande si vous voulez être aidé ou si vous souhaitez aider quelqu'un.

Lorsque vous avez besoin d'aide, sélectionnez l'option *Inviter une personne de confiance à vous aider*. L'assistant vous demande si vous souhaitez générer un fichier d'invitation ou utiliser la fonction Easy Connect.

Avec la méthode du fichier d'invitation, l'assistant fournit un fichier qu'il vous faut faire parvenir à la personne qui vous aide. En ouvrant le fichier, elle se connectera à votre ordinateur. Si vous utilisez Windows Mail, l'assistant vous propose d'envoyer directement l'invitation par courrier électronique.

La dernière méthode, baptisée Easy Connect est une nouveauté de Windows 7. Elle permet une connexion plus rapide entre la personne assistée et son assistant. Pour utiliser cette fonctionnalité, cliquez sur *Utiliser Easy Connect*. Un mot de passe de 12 caractères s'affiche alors sur votre écran. De son coté, la personne qui vous porte assistance doit démarrer l'utilitaire d'assistance à distance et choisir *Aider quelqu'un qui vous invité*, puis *Utiliser Easy Connect*.

POUR ALLER PLUS LOIN Paramètres

Le bouton *Paramètres* vous donne accès aux options de l'utilitaire d'assistance à distance. Ces options sont les suivantes :

- *Pour cesser le partage du contrôle, appuyer sur Echap* : cette option vous permet, si vous vous faites aider, de retirer immédiatement le contrôle de votre machine à l'utilisateur connecté en appuyant sur la touche *Echap*. Il faut la désactiver si la personne qui vous aide doit utiliser la touche *Echap* dans sa démonstration.
- *Enregistrer le journal de cette session* : cette fonctionnalité vous permet de conserver une trace de tout ce qui s'est passé durant la session d'assistance à distance. Vous pouvez, par exemple, voir quels sont les fichiers échangés avec la personne qui vous a aidé. Ces journaux sont sauvegardés dans `Documents\Remote Assistance Logs`.

Activer l'assistance à distance

Lorsque vous êtes administrateur sur votre machine, vous pouvez activer l'utilisation de la fonctionnalité d'assistance à distance pour prendre le contrôle depuis un autre ordinateur et effectuer différentes tâches.

1. Rendez-vous dans la fenêtre de propriétés système (accessible via un clic droit sur *Ordinateur* ou par la combinaison de touches *Windows+Pause*).
2. Dans la colonne de gauche, cliquez sur *Paramètres d'utilisation à distance*. La partie supérieure de la boîte de dialogue qui s'affiche vous donne accès aux paramètres avancés de l'assistance à distance.

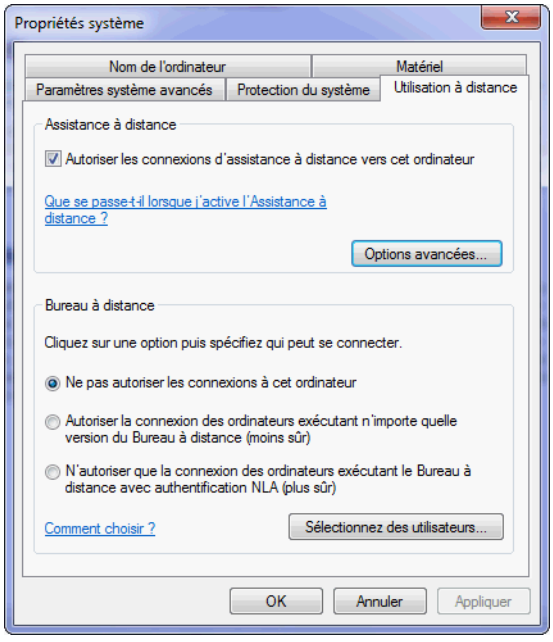


Figure 15–19
Boîte de dialogue de paramètres avancés de l'assistance à distance

3 Via la case à cocher, activez ou désactivez la fonctionnalité d'assistance à distance.

Le principe de l'assistance à distance consiste à envoyer une invitation à un ordinateur distant pour se connecter à l'ordinateur local. L'utilisateur distant voit alors s'afficher sur son écran ce qui est affiché sur l'ordinateur en détresse. L'utilisateur distant peut également bouger la souris ou taper au clavier et administrer le système comme s'il était en local et obtient automatiquement les mêmes droits que l'utilisateur actuellement connecté.

De cette manière, il est possible à un néophyte de demander à une personne expérimentée d'effectuer les opérations à sa place. Néanmoins, il n'est pas toujours souhaitable de laisser quelqu'un avoir complètement la main sur le système. Ceci se paramètre dans les options avancées. Le bouton *Options avancées* vous permet d'accéder à la boîte de dialogue représentée sur la figure 15–20 :

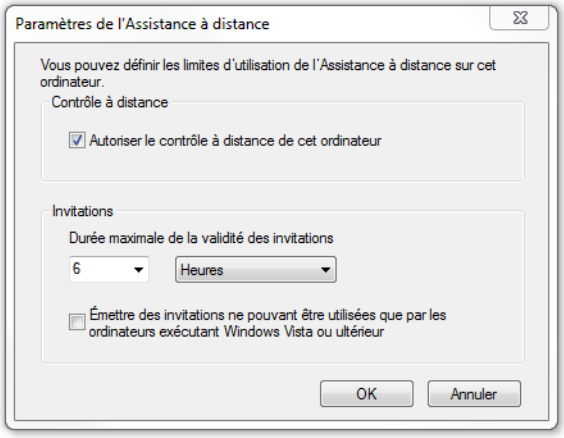


Figure 15–20
Paramètres avancés de l'assistance à distance

La première option est la plus importante puisqu'elle concerne le contrôle à distance. En décochant cette case, vous permettez à quelqu'un de se connecter à votre ordinateur et de voir temporairement votre écran, mais il ne pourra en aucun cas faire de manipulation ni bouger la souris.

La seconde partie des options avancées concernent les invitations. Il est possible de les limiter dans le temps ou alors à un type d'ordinateur distant possédant une version de Windows particulière. Cette dernière option améliore la sécurité.

La boîte à outils indispensable

Un bon administrateur est avant tout un administrateur prévoyant. Que ce soit par une corruption du système, une coupure Internet ou une

infection virale, il doit être préparé et avoir à portée de main les outils qui lui permettront de se sortir de situations complexes. Voici une sélection d'outils que nous jugeons vraiment pratiques.

Un grand nombre de ces outils existe en version autonome (*standalone*) et peut donc être placé sur une clé USB sans requérir la moindre installation de votre part. Le but de cette section est de vous aider à élaborer votre couteau suisse, afin de vous sortir de toute sorte de problèmes.

UltraVNC

Gratuit, UltraVNC (http://www.ultravnc.fr/) permet de prendre le contrôle d'un PC à distance. Il est capable d'afficher l'écran de l'ordinateur distant et de contrôler souris et clavier comme si l'on se trouvait physiquement sur l'ordinateur. Le fonctionnement nécessite néanmoins l'installation préalable d'un client de connexion sur les ordinateurs à contrôler.

Parmi ses fonctionnalités, soulignons le transfert de fichier, le chiffrage des communications (via des plug-ins), l'authentification Windows, la messagerie instantanée intégrée, la gestion du multi-écrans, la reconnexion automatique, la gestion des proxies, etc. UltraVNC fonctionne sur toutes les versions Windows depuis Windows 95.

Les outils SysInternals

Racheté par Microsoft en 2006, SysInternals est une petite société qui a produit près de 66 outils. Beaucoup sont des incontournables. Le tableau 15-3 présente notre sélection.

http://technet.microsoft.com/en-us/sysinternals/

Tableau 15–3 Principaux utilitaires SysInternals

Intitulé	Description
AccessChk	Outil en ligne de commande permettant de vérifier les autorisations aussi bien sur des fichiers que des clés de registre, ou encore de vérifier les droits sur des éléments bien précis, tels que des services Windows par rapport à un groupe utilisateur donné.
AccessEnum	Complément d'AccessChk, AccessEnum permet de façon très rapide et visuelle d'énumérer les autorisations d'accès à une arborescence de répertoires. Très utile pour découvrir d'éventuelles failles dans la configuration des autorisations !
Autoruns	Sert à visualiser rapidement tous les logiciels s'exécutant au démarrage, quel que soit leur emplacement.
ListDLLs	Affiche toutes les bibliothèques chargées en temps réel. Utile pour détecter la présence de malwares ou de virus au sein du système.
PageDefrag	Défragmente le fichier de pagination ainsi que la ruche du registre.

Tableau 15–3 Principaux utilitaires SysInternals (suite)

Intitulé	Description
Process Explorer	Surveille les processus lancés et les modules qu'ils utilisent. Un outil fort utile pour détecter des outils malveillants et les éradiquer.
Process Monitor	Surveille l'activité du registre, des processus et du système de fichiers en temps réel.
PsKill	Tue les processus sur sa machine ou sur une des machines du réseau.
RootkitRevealer	Petit outil pour détecter les malwares de type rootkit, logiciel permettant d'accéder de manière frauduleuse aux données d'une machine.
ShareEnum	Scanne les partages du réseau et indiquer leur configuration de sécurité, afin de découvrir d'éventuelles failles de sécurité.

Ultimate Boot CD

Ultimate Boot CD est un live-CD (directement bootable) qui contient énormément d'utilitaires, tous gratuits, permettant de réparer un ordinateur dont le système d'exploitation serait endommagé et ne démarrerait plus. Qu'il s'agisse de problème de partition, de carte mère ou même de fichiers système, Ultimate Boot CD est capable de vous sortir de bien des situations.

http://www.ultimatebootcd.com/

Spybot Search & Destroy

Spybot n'est pas un antivirus mais est considéré comme l'un des meilleurs anti-malwares existants. Il est capable de détecter et de supprimer un peu plus de 30 000 malwares différents. Il est également capable de « vacciner » le système pour empêcher l'installation de certains malwares.

www.safer-networking.org

CCleaner

CCleaner est sûrement le nettoyeur de système le plus réputé sous Windows. Il est capable de supprimer les fichiers inutiles, les fichiers temporaires et de nettoyer le registre. Il ravira les maniaques d'un système propre.

http://www.ccleaner.com

ClamWin

Il s'agit d'un des rares antivirus gratuits portables : il ne nécessite pas d'installation et peut être placé sur une clé USB pour effectuer un scan

antivirus en cas d'infection grave. Il est néanmoins important de télécharger régulièrement une nouvelle version pour avoir une base de signatures antivirus à jour.

http://www.clamwin.com/

Cette liste n'est bien sûr pas exhaustive et vous êtes libre – et nous vous le conseillons vivement – d'étoffer votre boîte à outils en gardant à l'esprit l'objectif principal : être capable de réagir rapidement à tout type de situation ou problème, mais également anticiper les problèmes potentiels.

En résumé

Au cours de ce chapitre, nous avons abordé les différentes manières de détecter, réparer et anticiper les problèmes. Au travers des outils dédiés, mais également à l'aide de simples journaux d'événements, nous avons vu comment répondre efficacement aux différentes situations critiques auxquelles votre ordinateur peut avoir à faire face. Vous disposez maintenant des connaissances pour résoudre les problèmes passés, présents et futurs de votre système.

chapitre 16

Personnaliser le panneau de configuration et les menus contextuels

La personnalisation du système ne se limite pas à des paramétrages esthétiques comme le fond d'écran ou le thème général. Elle concerne également à la modification des éléments du système afin de le rendre non seulement plus agréable à utiliser, mais surtout pour faire en sorte qu'il réponde au mieux à certains de vos besoins tout en en optimisant le fonctionnement.

SOMMAIRE

- Créer un applet et l'ajouter au panneau de configuration
- Ajouter des options au menu contextuel de l'explorateur
- Ajouter des fonctionnalités Windows au menu contextuel

MOTS-CLÉS

- Applet
- Personnalisation
- Panneau de configuration
- Registre
- Clé
- XML
- Fonctionnalité Windows
- Menu contextuel
- Tâche
- Icône
- UAC

Ce chapitre détaille la personnalisation même du système, de la création de menus personnalisés au sein du menu contextuel de l'explorateur, jusqu'à l'intégration des composants de votre choix dans le panneau de configuration.

Ajouter des éléments au panneau de configuration

Dans le chapitre précédent, nous avons vu comment étoffer sa boîte à outils et comment améliorer l'administration du système grâce à elle. À présent, nous allons les intégrer au système afin de gagner en efficacité et en organisation pour les principales tâches d'administration du système. Peu compliquée et rapide à mettre en place, cette modification du système sera appréciée par les utilisateurs les plus perfectionnistes. Nous allons voir comment personnaliser le panneau de configuration pour y faire apparaître nos propres éléments.

Jusqu'à Windows Vista, ceux qui développaient leur propre composant et souhaitaient l'ajouter au panneau de configuration devaient suivre scrupuleusement les étapes décrites sur la MSDN (*Microsoft Developer Network*). Il leur fallait suivre une longue et complexe procédure pour créer un composant `.cpl`, un exécutable possédant plusieurs fonctionnalités pour interagir avec le système. Une chance pour nous, tout ceci a été revu sous Windows Vista et Windows 7 et personnaliser le panneau de configuration est maintenant chose facile.

MSDN

MSDN est une section de Microsoft qui s'occupe de la communauté de développeurs utilisant les technologies telles que les langages de programmation (.NET, par exemple), les pilotes, les nouvelles technologies, Windows Mobile, etc. Son équivalent orienté système (serveur, exchange, etc.) est TechNet.

Créer un applet

Le panneau de configuration est composé de groupement de liens vers des composants système ou des applications. Ces regroupements sont appelés des applets et c'est cela que nous allons maintenant créer. Si par le passé, vous deviez créer une DLL (renommée en `.cpl`) en CplApplet, il est maintenant possible, avec quelques clés registre et un fichier XML, d'ajouter plusieurs actions aux différents applets qui composent le panneau de configuration.

La première étape consiste à générer un GUID.

Créer un GUID

Un GUID est un *Global Unique IDentifier*, c'est-à-dire, une chaîne de caractères servant d'identifiant unique et permettant de désigner un élément, un programme ou autre, de façon unique, un peu comme le

numéro sur votre carte d'identité. Pratiquement tous les éléments de votre système, que ce soit un dossier système particulier, un gestionnaire d'extension et bien d'autres choses, ont leur GUID.

Un GUID est de la forme `{CEC124F7-656C-458b-9E7C-43462DE09D01}`. Le créer à la main en s'assurant qu'il soit unique n'est pas évident. En effet, il faut pour cela vérifier dans votre registre qu'il n'est pas utilisé. Il n'y a donc pas de solution manuelle magique : il vous faut utiliser un petit utilitaire fourni par Microsoft qui se nomme GUIDGEN.exe.

1. Une fois l'utilitaire téléchargé, cliquez sur *Registry format*.
2. Cliquez sur *New GUID.*
3. Cliquez ensuite *Copy.*

Ainsi, vous créez, puis copiez un nouveau GUID dans votre Presse-papiers.

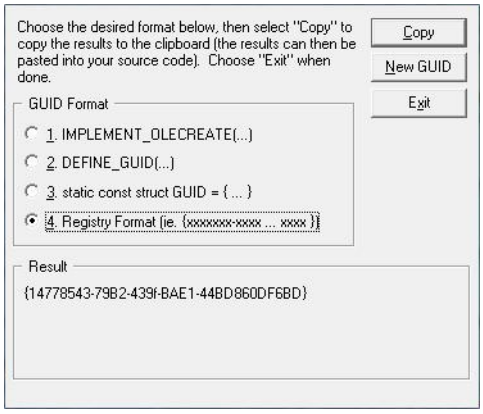


Figure 16–1
Interface de l'utilitaire GUIDGEN

Notez-le dans un fichier texte car vous devrez l'utiliser plusieurs fois. Profitez-en pour créer trois autres GUID que vous copierez aussi dans le fichier texte afin de ne pas les oublier.

Enregistrer le GUID dans le registre

Chaque GUID doit être enregistré dans le registre, c'est la seule manière de s'assurer de son unicité en vérifiant qu'aucune clé du même nom n'existe.

1. Ouvrez Regedit.exe.
2. Rendez-vous à la clé `HKEY_CLASSES_ROOT\CLSID\`.
3. Créez une nouvelle clé en lui donnant le nom de votre premier GUID.
4. Dans sa valeur *default*, indiquez `Mon Premier Applet`.

TÉLÉCHARGEMENT Utilitaire GUIDGEN

GUIDGEN.exe est en téléchargement (gratuit) à l'adresse suivante :

- http://www.microsoft.com/downloads/details.aspx?familyid=94551f58-484f-4a8c-bb39-adb270833afc

PRÉCISION

Par souci de clarté, nous utilisons ici des GUID factices, mais facilement reconnaissables. Nous aurons ainsi :

- {00000000-0000-0000-0000-000000000000}
- {00000000-0000-0000-0000-000000000001}
- {00000000-0000-0000-0000-000000000002}
- {00000000-0000-0000-0000-000000000003}

Enregistrer l'applet

Créez ensuite quatre autres valeurs de type chaîne (*string value*) en vous aidant dubleau 16-1.

Tableau 16–1 Clés registre à créer

Nom de clé	Exemple	Description
`Default`	`Mon premier applet`	Le texte de l'applet.
`InfoTip`	`mon tooltip à moi!`	Le texte affiché par l'infobulle quand la souris survolera l'applet.
`System.ApplicationName`	`Eyrolles.MonApplet`	Le nom de votre applet. Essayez d'utiliser la forme des espaces de noms, à savoir VotreNomOuEntreprise.NomApplet.
`System.ControlPanel.Category`	`1,8`	Catégories où apparaîtra votre applet.
`System.Software.TasksFileUrl`	`C:\infos.xml`	Chemin vers un fichier XML de configuration de l'applet. Créez un fichier XML vide sur votre disque et pointez dessus.

Pour les catégories, les valeurs possibles sont décrites dans le tableau 16-2.

Tableau 16–2 Liste des catégories du panneau de configuration et de leur identifiant associé

Valeur	Catégorie
1	Apparence et personnalisation
2	Matériel et audio
3	Réseau et Internet
4	Non utilisé
5	Système et maintenance
6	Horloge, langue et région
7	Options d'ergonomie
8	Programmes
9	Comptes utilisateur et protection des utilisateurs
10	Sécurité
11	Ordinateur mobile (uniquement visible sur les ordinateurs portables)

Dans le registre, vous obtenez un affichage proche de celui présenté à la figure 16-2.

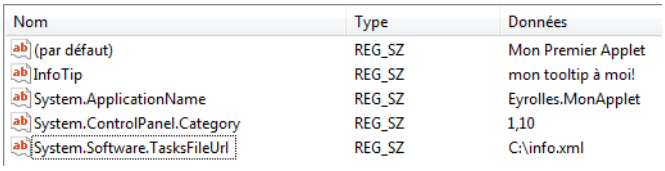


Figure 16–2
Aperçu de la clé registre de notre applet

Afficher l'applet dans le panneau de configuration

Il reste une étape importante pour utiliser l'applet créé. Jusqu'à présent, nous avons déclaré un GUID et ajouté quelques informations dans le registre : rien ne permet à Windows de savoir que ce GUID identifie un applet.

1. Rendez-vous dans le registre à la clé `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace\`
2. Ajoutez une clé portant le nom de votre premier GUID.
3. Dans sa clé par défaut, saisissez le nom de votre applet, c'est-à-dire `MonPremierApplet`. Avec cette simple ligne, vous indiquez au système de charger les informations de l'applet du panneau de configuration identifié par ce GUID.

À présent, l'applet est visible dans le panneau de configuration dans les deux catégories sélectionnées, à savoir *Sécurité* et *Apparence et personnalisation.*

OUPS ID erroné

Si vous indiquez un mauvais ID, votre applet n'apparaît pas, mais n'empêche pas pour autant le chargement des autres applets.

Ajouter des tâches

Maintenant que votre applet est visible dans le panneau de configuration, nous allons le personnaliser. Souvenez-vous, nous avons créé un fichier XML vide nommé `infos.xml`.

1. Ouvrez le fichier de configuration `infos.xml` précédemment créé.
2. Collez-y le code suivant :

OUPS L'applet n'apparaît pas

Si votre nouvel applet n'apparaît pas dans le panneau de configuration, recommencez la procédure de création depuis le début en vérifiant bien le GUID.

```
<?xml version="1.0" ?>
<applications xmlns="http://schemas.microsoft.com/windows/cpltasks/v1"
              xmlns:sh="http://schemas.microsoft.com/windows/tasks/v1">

  <application id="{00000000-0000-0000-0000-000000000000}">   <!-- id de votre applet

  </application>
</applications>
```

3. À l'intérieur du bloc de code, entre les balises `<application>` et `</application>`, décrivez trois tâches. Chacune d'elles ressemble à ceci :

BONNE PRATIQUE Nombre de tâches

Évitez de décrire plus de quatre ou cinq tâches pour un même applet pour des raisons d'esthétisme au moment de l'affichage dans le panneau de configuration.

```
<sh:task id="{00000000-0000-0000-0000-000000000001}" >
   <sh:name>Lancer PowerShell</sh:name>

<sh:command>H:\Windows\system32\WindowsPowerShell\powershell_ise.exe</sh:command>
</sh:task>
```

4 Créez deux tâches supplémentaires, l'une lançant une page web et l'autre un fichier de votre disque dur.

```
<sh:task id="{00000000-0000-0000-0000-000000000002}">
   <sh:name>Visiter Eyrolles</sh:name>
   <sh:keywords>eyrolles</sh:keywords>
</sh:task>
<sh:task id="{00000000-0000-0000-0000-000000000003}">
   <sh:name>Ouvrir un fichier</sh:name>

<sh:keywords>fichier;aide</sh:keywords>
   <sh:command>C:\test.txt</sh:command>
</sh:task>
```

5 Dans le registre, nous avons précisé que l'applet apparaîtra dans les catégories 1 et 8. Créez ces catégories dans le XML grâce au code suivant :

```
<category id="1">
    <sh:task idref="{00000000-0000-0000-0000-000000000001}"/>
    <sh:task idref="{00000000-0000-0000-0000-000000000002}"/>
    <sh:task idref="{00000000-0000-0000-0000-000000000003}"/>
  </category>
  <category id="10">
    <sh:task idref="{00000000-0000-0000-0000-000000000003}"/>
    <sh:task idref="{00000000-0000-0000-0000-000000000002}"/>
  </category>
```

Vous avez certainement remarqué que l'une des deux catégories n'a que deux tâches, et surtout que l'ordre de ces tâches diffère. Ceci a pour but de créer un applet unique, qui s'affichera sous différentes formes et proposeront des tâches différentes selon la catégorie dans laquelle elle est chargée. Voici le résultat final :

Figure 16–3
Affichage final de notre applet

Personnaliser l'icône de l'applet

Il est possible de configurer l'icône de l'applet qui s'affichera.

1 Dans le registre, rendez-vous dans `CLSID` (*CLasS IDentifier*).
2 Sous la clé de votre applet, ajoutez la clé `DefaultIcon`.
3 Dans sa sous-clé par défaut, saisissez le chemin d'une image PNG.

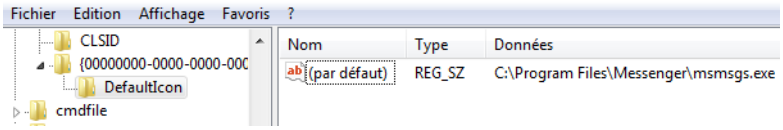


Figure 16–4
Modification de l'icône de l'applet

Afficher le bouclier de l'UAC à côté des tâches critiques

Dans le développement sur Windows 7, Microsoft recommande de signaler les applications qui lancent une tâche impliquant une élévation de privilèges. Ce signe distinctif est un petit bouclier.

Pour se conformer à cette recommandation, il suffit d'ajouter l'attribut `needsElevation` à la tâche de votre choix. Dans notre exemple, cela donne ceci :

```
<sh:task id="{00000000-0000-0000-0000-000000000002}" needsElevation="true">
```

Figure 16–5
Aperçu de l'applet personnalisé

Lancer une application à partir du titre de l'applet

Il est possible de lancer une application en cliquant sur le titre de l'applet. Voici comment paramétrer ce comportement :

1. Rendez-vous dans le registre dans `CLSID/votre_guid`.
2. Ajoutez une sous-clé nommée `Shell` contenant elle-même une sous-clé `Open` et enfin une sous-clé `Command`. La valeur par défaut de `Command` contiendra le chemin vers l'application que vous souhaitez lancer.

EN PRATIQUE **Chemin vers l'application**

Le chemin doit être complet. Si l'application à lancer se trouve dans un chemin que vous avez préalablement déclaré dans la variable d'environnement `Path`, indiquez comme chemin le nom de l'application.

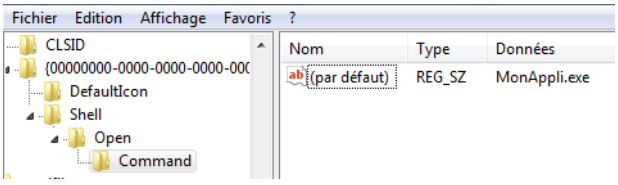


Figure 16–6
Ajout d'une commande par défaut à l'applet

En quelques clés registre, il est donc possible d'intégrer vos applets et surtout vos outils au panneau de configuration. Grâce à cette personnalisation, vous regroupez vos outils d'administration ou vos liens utiles à l'endroit où ils devraient se trouver s'il s'agissait de fonctionnalités de base du système.

Personnaliser les menus contextuels du système

La personnalisation du système et surtout l'intégration de vos fonctionnalités personnelles peut également se faire au sein des menus contextuels. Outre le gain d'efficacité, cette intégration rend l'utilisation de vos programmes et fonctions plus intuitive.

Ajouter des options au menu contextuel de l'explorateur

Comme son nom l'indique, le menu contextuel s'adapte en fonction de l'élément auquel il est attaché. Qu'il s'agisse d'un fichier ou d'un dossier, les menus qu'il contient se conforment au type de l'élément, ou à son extension, lorsqu'il s'agit d'un fichier.

Un jour ou l'autre, vous serez amené soit à développer un script PowerShell acceptant des paramètres de ligne de commande, soit à faire appel à un utilitaire tiers fonctionnant en ligne de commande. Dans les deux cas, votre travail sera facilité si vous avez la possibilité d'appeler automatiquement ces éléments depuis le menu contextuel de l'explorateur. Prenons comme exemple le cas d'un script PowerShell qui zippe un fichier pour l'envoyer par e-mail. Voyons la procédure pour créer ce menu personnalisé.

EN PRATIQUE Menu spécifique aux dossiers

Si vous souhaitez afficher un menu disponible uniquement pour les dossiers, ajoutez la clé de votre menu à la clé `HKEY_CLASS_ROOT\folder\shell`.

1. Ouvrez le menu *Démarrer*, et saisissez `regedit` dans la zone de saisie afin d'ouvrir le registre.
2. Naviguez jusqu'à la clé `HKEY_CLASS_ROOT\*\shell`.
3. Créez une clé et donnez le nom que vous souhaitez.
4. Dans la valeur `default`, indiquez le nom du menu tel que vous voulez qu'il apparaisse.
5. Sous cette clé, créez une seconde clé `command`. Pour sa valeur `default`, indiquez le chemin d'exécution de votre application ou de votre script, comme le montre la figure 16–7 :

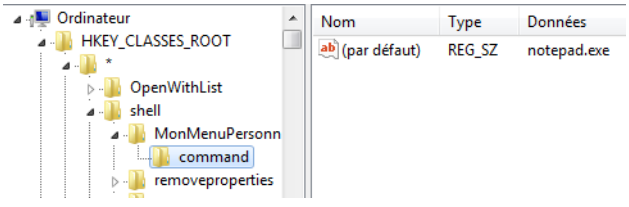


Figure 16–7
Clé registre de notre menu personnalisé

Ajouter des fonctionnalités Windows au menu contextuel

La personnalisation des menus devient particulièrement intéressante lorsqu'il s'agit d'activer des fonctionnalités Windows déjà présentes sur le système, mais inactives. Pour l'exemple, nous allons ajouter des menus de déplacement et de copie de fichiers afin de gérer les fichiers avec uniquement deux clics de souris.

1. Ouvrez le registre (Regedit.exe), puis rendez-vous à la clé `HKEY_CLASSES_ROOT\AllFilesystemObjects\shellex\ContextMenuHandlers`.
2. Créez-y deux clés nommées *Copier vers* et *Déplacer vers*.
3. Saisissez respectivement dans leurs valeurs par défaut, les GUID `{C2FBB630-2971-11D1-A18C-00C04FD75D13}` et `{C2FBB631-2971-11D1-A18C-00C04FD75D13}`.

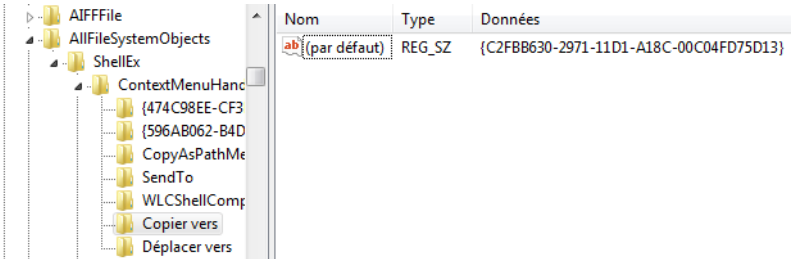


Figure 16–8
Modification du registre pour le menu Copier vers

La modification est instantanée et deux nouveaux menus contextuels *Copier dans un dossier* et *Déplacer vers un dossier* font leur apparition. Si vous cliquez sur ces menus, une fenêtre de choix de dossier cible s'ouvre. Plus besoin d'ouvrir deux fenêtres de l'explorateur.

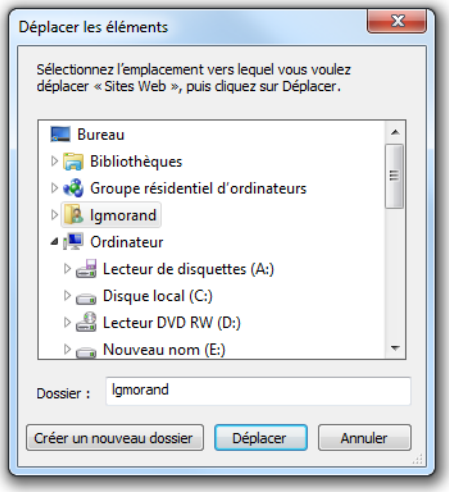


Figure 16–9
Choix du dossier cible

ASTUCE **Rendre visible les menus contextuels cachés**

Au sein du système, il existe plusieurs types de fichiers ou dossiers pour lesquels le menu contextuel contient des menus visibles et invisibles. Ces menus ont été dissimulés, car il est rare de les utiliser. Cependant, il est possible de les faire réapparaître à la demande. Il suffit d'appuyer sur la touche *Maj* lorsque vous affichez le menu contextuel. Pour les dossiers, les deux menus suivants s'affichent en plus des autres :

- *Ouvrir dans un nouveau processus*
- *Ouvrir une fenêtre de commandes ici*

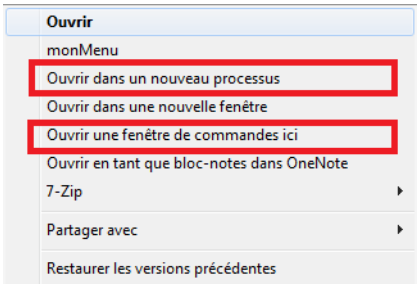


Figure 16–10 Menus cachés des dossiers

Pour les fichiers, c'est un menu *Copier en tant que chemin d'accès* qui apparaît. Ce menu place dans le Presse-papiers le chemin complet d'accès au fichier.

ASTUCE

Faire apparaître le menu Chiffrer ou Déchiffrer dans le menu contextuel

Nous avons abordé dans le chapitre sur la sécurité, le chiffrement des fichiers et des dossiers à l'aide du chiffrement EFS. Par défaut, il est nécessaire d'aller dans les propriétés de chaque fichiers ou dossier, de cliquer sur le bouton *Avancé*, de cocher la case de chiffrement, puis de cliquer deux fois sur le bouton *OK*. Cependant, il est possible à l'aide d'une simple clé registre de faire apparaître un menu permettant de chiffrer ou déchiffrer d'un simple clic.

1. Ouvrez le registre et naviguez jusqu'à la clé `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced`
2. Créez la valeur de type `DWORD` nommée `EncryptionContextMenu`.
3. Donnez-lui la valeur `1`.

Un nouveau menu *Chiffrer* (ou *Déchiffrer* selon le cas) apparaît alors dans le menu contextuel de l'explorateur Windows.

Figure 16–11 Menu contextuel permettant le chiffrement rapide d'un fichier ou d'un dossier

En résumé

La personnalisation du système va beaucoup plus loin qu'une simple amélioration graphique : il est possible d'intégrer différents utilitaires ou d'ajouter différentes fonctionnalités au sein des différents menus contextuels du système.

chapitre 17

PowerShell

Également connu sous le nom de Microsoft Command Shell (MSH), Windows PowerShell est le dernier langage de script créé par Microsoft pour remplacer au sein des systèmes, le langage Batch vieillissant et fort limité. Basé sur le framework .NET 2.0, PowerShell est ce qui ce qui se fait de mieux pour administrer un système d'exploitation de type Windows.

AU SOMMAIRE

- Définition et enjeux
- Prise en main
- L'environnement de PowerShell : le framework .NET
- Les éléments du langage
- Interagir avec WMI
- Interagir avec le registre

MOTS-CLÉS

- Framework
- PowerShell
- Script
- Commande
- WMI

PowerShell, langage de script de Windows

Surcouche de WMI (*Windows Management Instrumentation*), le langage de script PowerShell permet de contrôler tout un système et ses ressources, que ce soit localement ou à distance. Puissant et évolué, ce langage s'efforce toutefois de rester aussi simple que possible comme nous allons le voir.

PowerShell est basé sur la version 2.0 du framework .NET. Il permet par conséquent d'utiliser des scripts développés en orienté objet (OOP, *Object Oriented Programing*). Il possède son propre langage pour coupler les avantages d'un langage orienté commande, comme le font les shells UNIX/Linux, et la gestion d'objets. Il a néanmoins le mérite d'être très simple à comprendre, d'être bien documenté et de permettre d'atteindre rapidement des résultats qu'il aurait été difficile d'obtenir avec un autre langage script tel que VBScript, largement utilisé sous Windows.

Windows PowerShell comprend un environnement de ligne de commande, dit shell, et un environnement de scripts, permettant l'exécution de scripts. Les scripts peuvent alors utiliser l'un ou l'autre (ou les deux) afin d'avoir la main sur le système et le contrôler sans nécessiter l'ouverture d'une quelconque fenêtre d'administration.

Windows 7 est la première version de Windows à inclure nativement PowerShell. Si les anciennes versions de Windows sont capables d'utiliser la version 1.0 de PowerShell en installant un module complémentaire, Windows 7 intègre PowerShell 2.0 par défaut. Plus complète, la version 2.0 contient notamment de nouvelles commandes, des performances accrues, mais également un éditeur de script (ISE, *Integrated Scripting Environment*)

Il nous est impossible d'aborder de façon approfondie PowerShell dans le cadre de ce livre, tant le sujet est large et complexe. Néanmoins, nous tâcherons ici de vous aider à le prendre en main, d'en exposer les bases et de vous accompagner dans la rédaction de vos premiers scripts.

PRÉ-REQUIS .NET 2.0

Le framework .NET 2.0 est nécessaire pour utiliser PowerShell sur d'anciennes versions Windows telles que Windows XP ou antérieures.

À SAVOIR Incidence de la version .NET au sein de PowerShell

Présenté plus en détail en annexe, le framework .NET est, au moment où nous écrivons ce livre, en version 3.5. Il utilise le noyau de la version 2.0 (utilisée par PowerShell) auquel se sont adjointes des technologies de communication (WCF), de présentation (WPF), de workflow (WF) et d'accès aux bases de données (LINQ). Ces technologies ne sont malheureusement pas exploitables par les autres langages de script existants. Le fait que PowerShell soit basé sur le framework .NET signifie qu'il est capable de s'ouvrir vers tout l'environnement Microsoft, qu'il s'agisse d'environnement serveur (Active Directory), d'environnement professionnel (SharePoint) ou de bureautique (suite Microsoft Office). PowerShell n'a que peu de limites et aucun langage de script n'est à l'heure actuelle aussi complet, sans nécessiter de module tiers.

TÉLÉCHARGEMENT Installer PowerShell

PowerShell peut être téléchargé et installé à partir de l'adresse suivante :

- http://www.microsoft.com/windowsserver2003/technologies/management/powershell/download.mspx

Premier script

Mais ne tardons plus, voyons comme écrire notre premier script : le traditionnel « Hello World ». Les scripts PowerShell s'écrivent grâce à n'importe quel éditeur de texte de type Notepad afin de générer des fichiers texte portant l'extension `.ps1`. Il est néanmoins conseillé d'utiliser l'éditeur de code fourni avec PowerShell v2. Nommé *Windows PowerShell Intergrated Scripting Environment* ou tout simplement *ISE*, il possède de nombreux avantages par rapport à un éditeur de texte basique :

- coloration syntaxique du code pour une meilleure lisibilité ;
- système d'onglets pour ouvrir plusieurs scripts en parallèle ;
- activation du débogage des scripts ;
- découpage en panneaux avec une partie pour saisir le code, une partie console pour l'exécution du script et un panneau commande utilisé lors du débogage.

1 Ouvrez le menu *Démarrer* et tapez `ISE` dans la zone de saisie.

2 Cliquez sur *Windows PowerShell ISE*.

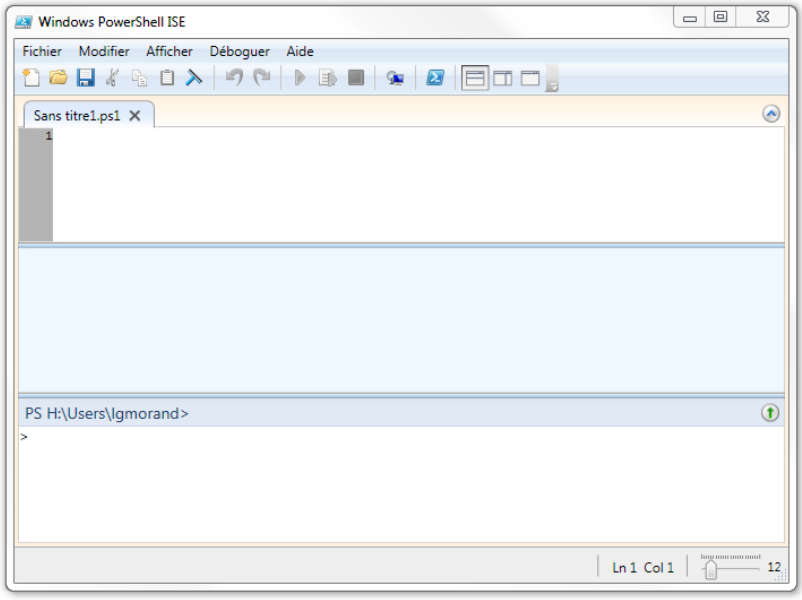


Figure 17–1
Éditeur de script PowerShell

3 Dans la partie supérieure de l'éditeur d'ISE, saisissez le code suivant :

```
$var = "Bonjour"
$var
```

4 Appuyez ensuite sur la touche *F5* pour l'exécuter. Le texte « Bonjour » s'affiche.

Regardons ce code de plus près. La première ligne déclare une variable `$var`, dont le nom doit toujours commencer par le symbole `$` et à laquelle est assignée la chaîne de caractères `Bonjour`. À la seconde ligne, seul le nom de la variable apparaît. Elle affiche son contenu (ici `Bonjour`). Ce script est rudimentaire, nous allons voir qu'il est possible d'en écrire de bien plus utiles et surtout bien plus avancés.

EN PRATIQUE Utilisation en ligne de commande ou par bloc de script

Les scripts PowerShell s'écrivent soit ligne par ligne dans la console, soit par bloc dans un fichier script. Bien que l'éditeur utilise l'exécution par bloc de code, le résultat est identique à l'utilisation de la console PowerShell.

PowerShell et le framework .NET

La puissance de PowerShell vient principalement du fait qu'il est basé sur la version 2.0 du framework .NET, version encore couramment utilisée aujourd'hui pour le développement de bon nombre d'applications. Avec ce socle technique, on comprend qu'avec PowerShell, tout est objet et que ces objets sont fortement typés. Ceci présente aussi l'avantage d'augmenter la robustesse des scripts.

Pour le vérifier, reprenons le code précédent et saisissons le script suivant :

```
$var = "Bonjour"
$var.GetType()
```

À l'exécution, le texte suivant s'affiche :

```
IsPublic IsSerial Name                                     BaseType
-------- -------- ----                                     --------
True     True     String                                   System.Object
```

L'affichage de la console nous indique donc qu'il s'agit d'un objet de type `String` (chaîne de caractères), héritant logiquement de `System.Object` en étant public et sérialisable. S'ils semblent inutiles, ces détails prouvent qu'il est possible de faire avec PowerShell quasiment tout ce qu'il est possible de faire avec un langage dépendant du framework .NET, tel que C# ou VB.NET.

Ceci implique également qu'il est possible d'accéder à d'autres types du framework et de les utiliser directement. Par exemple, pour utiliser une date dans un script PowerShell, il suffit d'appeler le nom de sa classe (entre crochets), puis d'appeler la méthode ou la propriété qui nous intéresse :

```
$var =[DateTime]::Now
$var
```

Le code précédent récupère la date actuelle ainsi que l'heure et affiche le tout :

```
samedi 4 juillet 2009 13:49:21
```

Remarquez que le nom de la classe est entre crochets, mais surtout qu'au lieu d'utiliser un point pour accéder aux membres de l'objet comme on l'a fait précédemment pour la méthode `GetType()`, nous utilisons un signe `:`. Cette façon d'écrire est réservée aux méthodes statiques des objets (méthodes ne nécessitant pas d'instanciation), afin de les différencier facilement des méthodes publiques basiques. Soulignons également que la variable `$var` contient non pas une chaîne de caractères, mais une instance d'un objet de type date, initialisé à la date et l'heure actuelles.

Ceci a son importance : les commandes (`cmdlets`) retournent à chaque fois une instance d'un objet permettant par la suite d'accéder directement à ses informations internes. Ainsi, si vous instanciez une date, vous pouvez directement la traiter avant de l'afficher.

Le script suivant modifie la façon dont la date sera affichée :

```
[DateTime]::Now.ToShortDateString()
[DateTime]::Now.ToString("yyyy/MM/dd")
```

Les dates formatées apparaissent alors ainsi à l'écran :

```
04/07/2009
2009/07/04
```

Là encore, rien d'extraordinaire à première vue. Néanmoins, cette possibilité de traiter des objets à la volée, couplée aux commandes PowerShell que nous allons voir juste après, permet d'obtenir des scripts complexes.

Le langage PowerShell

Langage complet, PowerShell met en œuvre différents concepts tels que des méthodes (commandes), des alias, des expressions mais également des mécanismes de gestion avancée des données utilisées, tels que la notion de pipeline.

Les commandes

PowerShell étant un langage de script orienté commande, tout objectif (modifier un paramètre, retourner une information, créer un fichier, etc.) doit être réalisé à l'aide de commandes, qu'elles soient simples ou composées. Contrairement à d'autres shells, les commandes de PowerShell (`cmdlets`) sont des instances de classe .NET et non des exécutables basiques.

Ces applets de commandes sont, pour chacune, une fonctionnalité unique réalisant une (seule) tâche simple, un peu à la façon des commandes UNIX/Linux qui reposent sur le paradigme suivant : chaque commande (ou utilitaire) réalise un travail unique mais elle le fait bien.

Par défaut, PowerShell contient une centaine d'applets de commande dont la liste est disponible en annexe. Les `cmdlets` sont facilement reconnaissables à leur format. Elles sont toujours composées de deux mots anglais : un verbe et un nom, le tout séparé par un trait d'union, par exemple `Get-Help` ou `Copy-Item`.

ÉQUIVALENCE

Cette commande équivaut au paramètre `/?` de l'invite de commandes Windows.

ÉQUIVALENCE Get-Help et man

La commande `Get-Help` correspond à la commande `man` des shells Linux : toutes deux permettent d'obtenir l'explication d'une commande.

EN SAVOIR PLUS Liste complète des commandes PowerShell

Dans l'annexe B, nous présentons une liste exhaustive des commandes. Vous pouvez également l'obtenir en ouvrant une console PowerShell et y saisissant la commande `Get-Command`.

La majorité des commandes PowerShell ont une fonction très simple et beaucoup d'entre elles sont combinables avec d'autres commandes. Par exemple, il faut coupler la commande `Get-Help` avec une autre pour en obtenir la description :

```
Get-Help <nom-applet> -detailed
```

Ainsi, pour obtenir la notice d'utilisation de la commande `Get-Help`, saisissez :

```
Get-Help Get-Help -detailed
```

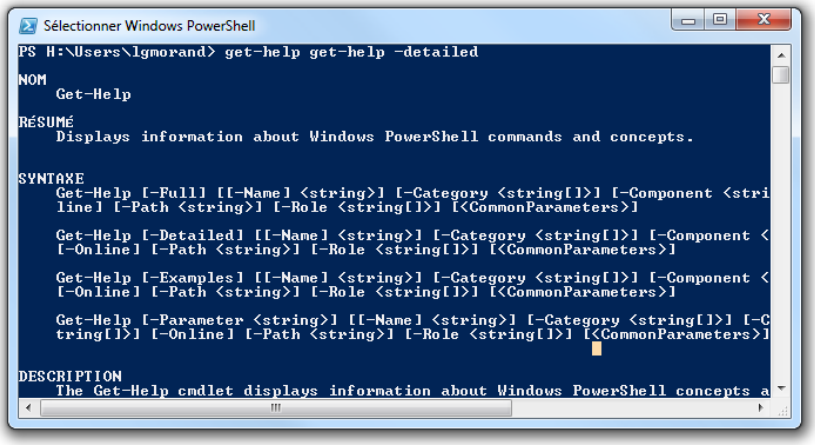


Figure 17–2
Résultat de la commande Get-Help

EN SAVOIR PLUS
Liste complète des alias PowerShell

Pour obtenir la liste complète et exhaustive des alias, vous pouvez, soit consulter l'annexe B, soit ouvrir une console PowerShell et y saisir la commande `Get-Alias`.

Les alias

Bien qu'il soit possible de profiter de l'autocomplétion du nom de commande à l'aide de la touche *Tabulation*, il est peu productif de ressaisir la commande en entier alors qu'il serait agréable d'appeler la commande par un diminutif ou alias, et pourquoi pas par un alias que nous aurions déjà l'habitude d'utiliser. Ainsi, l'alias de `Get-Help` est tout simplement `man` (pour *manual*). La commande devient donc :

```
man Get-Help -detailed
```

Il existe ainsi un grand nombre d'alias. Le tableau 17-1 en donne quelques exemples.

Tableau 17–1 Exemples d'alias de commandes PowerShell

Alias	Commande associée
%	ForEach-Object
?	Where-Object
ac	Add-Content
asnp	Add-PSSnapIn
cat	Get-Content

PowerShell est d'autant plus intéressant qu'il est possible de créer des alias personnalisés. Si `man` vous semble trop long, créez l'alias `g` grâce à la commande `Set-Alias` :

```
Set-Alias g Get-Help
```

Si l'envie vous prend de supprimer cet alias, appelez la commande `Remove-Item` :

```
Remove-Item alias:g
```

Pensez donc à utiliser les alias, que ce soit au sein de vos commandes ou de vos scripts, ils vous feront gagner un temps précieux. Intéressons-nous maintenant au principe de pipeline au sein de PowerShell.

Les pipelines

Au sens géographique du terme, un *pipeline* est une large canalisation servant au transport de certains fluides (essence, eau, gaz). Les pipelines existent également en informatique et tout particulièrement dans les langages de script. En effet, ils servent au transfert d'informations entre deux éléments.

PowerShell profite également du mécanisme de pipeline pour partager des résultats de commandes avec d'autres commandes : le premier traitement ou commande émet un résultat qui sera utilisé en tant que paramètre d'entrée pour un second traitement. On appelle *piping* l'utilisation des pipelines. Tôt ou tard, vous aurez recours au piping pour réaliser certains de vos scripts. Il est donc important de bien comprendre ce mécanisme.

EN SAVOIR PLUS

L'aide contextuelle des pipelines

Pour obtenir la documentation officielle des pipelines au sein même de PowerShell, saisissez la commande suivante :
`Get-Help About_pipeline`

Prenons l'exemple simple d'une commande telle que `Get-Process`. Elle retourne la liste de tous les processus actuellement actifs sur l'ordinateur. Si la liste est utile, elle contient par défaut trop d'informations comme le handle du processus, mais aussi son PID (ProcessID) et la mémoire utilisée. Grâce à un pipeline, nous allons filtrer le résultat comme nous le souhaitons.

Pour commencer, nous sélectionnons tous les processus, mais en n'affichant que les propriétés qui nous intéressent, à savoir l'ID du processus et son nom (`ProcessName`).

```
Get-Process | select ProcessName, PID
```

Cette commande affiche :

```
ProcessName
Id
-----------
--
Ati2evxx
1000
Ati2evxx
1400
audiodg
1180
```

```
conime
992
csrss
476
csrss
532
daemon
2936
```

Nous avons effectué la commande `Get-Process`. Son résultat est transmis via le symbole pipe `|` à une seconde commande qui ne sélectionne que deux propriétés.

Il n'y a pas de limites aux pipelines. Vous pouvez, par exemple, en utiliser un pour formater l'affichage, comme le montre la commande suivante :

```
get-Process | format-list -property ProcessName,Id
```

pour obtenir l'affichage :

```
ProcessName : Ati2evxx
Id          : 1000

ProcessName : Ati2evxx
Id          : 1400

ProcessName : audiodg
Id          : 1180

ProcessName : conime
Id          : 992
```

De façon plus pratique, vous pouvez vous en servir pour contrôler des processus et les couper dans certaines conditions. Le script suivant tue le processus `jusched` (qui met à jour Java) :

```
get-Process -name jusched | stop-Process
```

Les pipelines sont capables d'accueillir un nombre illimité de commandes conjointement :

```
get-Process | select ProcessName, Id | sort Id
```

Partie intégrante de PowerShell, les pipelines lui confèrent flexibilité et robustesse afin de créer des traitements complexes et efficaces.

RACCOURCI CLAVIER Symbole pipe

Pour insérer rapidement ce symbole dans votre éditeur, le raccourci clavier est *Alt Gr+6*.

POUR ALLER PLUS LOIN
Explication détaillée des pipelines

Si vous recherchez une documentation plus approfondie sur les pipelines au sein de PowerShell, reportez-vous à l'article de Laurent Dardenne, disponible à l'adresse suivante :

- http://laurent-dardenne.developpez.com/articles/Windows/PowerShell/Pipelining/

Les expressions

Les expressions servent à filtrer à la volée ou à effectuer des modifications sur certains éléments au moment de leur traitement.

Le script précédent affichait les tailles en octets, nombres peu lisibles pour l'humain. Il serait intéressant d'afficher les résultats sous forme réduite, soit en mégaoctets, soit en gigaoctets. Une première solution serait d'afficher le résultat divisé par 1 073 741 824 (1 024 × 1 024 × 1 024) pour avoir les tailles en Go. Avec une expression, cela donne :

```
$var | select Size, @{expression{$_.Size/(1024*1024*1024)}}
```

Bien que facile à utiliser, cela requiert toutefois de calculer à chaque fois la division, ce qui dans certains cas peut vite devenir répétitif. Une autre solution consiste à utiliser une expression couplée à des constantes. Ainsi, il est possible de représenter un gigaoctet en écrivant 1 Gb. Ce qui donne la nouvelle expression :

```
$var | select Size, @{expression{$_.Size/1Gb}}
```

La commande est plus courte, plus propre et surtout elle est rapidement modifiable en remplaçant par exemple, 1 Gb par 1 Mb ou encore 1 Kb.

Interagir avec WMI

WMI (*Windows Management Instrumentation*) est une surcouche intégrée à Windows depuis ses toutes premières versions. Elle permet d'interroger les ressources système, à l'aide d'un langage de requête propre, le *WMI Query Langage*. WMI est utilisable depuis de nombreux langages, allant du VBScript au .NET, et est par conséquent également utilisable au sein des scripts PowerShell.

WMI est peu connu des utilisateurs alors que la richesse de ses fonctionnalités en fait l'outil par excellence pour collecter des informations sur son système. En effet, WMI est capable de renvoyer les informations détaillées sur les périphériques, les connexions réseau, le matériel ou encore l'utilisation de la mémoire, mais peut encore et surtout contrôler les processus et les services Windows, tant en local qu'à distance.

L'exploitation de WMI au sein de PowerShell passe par la commande `Get-WMIObject`. Elle se charge d'effectuer une connexion entre PowerShell et la couche WMI. Il est ainsi possible d'accéder à toutes les informations de WMI comme la liste des processus en cours d'exécution :

```
Get-WMIObject win32_Process
```

EN COULISSE Windows Management Instrumentation

WMI a été créé pour répondre à un objectif basique mais compliqué à mettre en œuvre : la gestion et l'interrogation de tous les systèmes et de toutes les ressources à travers une seule interface normalisée. Quelle que que soit la version Windows, la marque de votre disque dur ou de votre carte réseau, WMI apporte une solution simple pour vous permettre d'obtenir l'information que vous désirez.
WMI permet à un développeur ou un administrateur système capable d'écrire des scripts, de configurer, gérer ou interroger la majorité des ressources de son ordinateur (applications, système, réseau, base de données, etc.) sans connaître l'API propre à chacune de ces ressources. Soulignons également que tout ceci peut se faire sur la machine locale mais également à distance. WMI est donc l'outil idéal pour l'administrateur système, car il lui évite de se déplacer d'ordinateur en ordinateur pour récupérer ses informations.

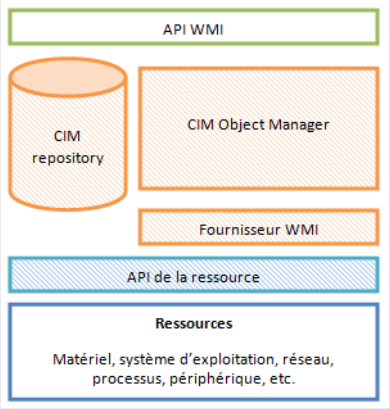


Figure 17–3 Architecture de la plate-forme WMI

Via un script ou une application, l'utilisateur interroge le service WMI à travers l'API WMI. Ce service enregistre les différents fournisseurs de ressources, tout en gérant les aspects de sécurité par rapport aux autorisations de l'utilisateur. Il se charge de la communication entre l'utilisateur et les fournisseurs ; les fournisseurs s'occupant alors d'accéder à la ressource pour en demander les informations ou appliquer les modifications demandées par l'utilisateur.

Il est également possible de récupérer une représentation objet du système d'exploitation pour en afficher les informations :

```
Get-WMIObject win32_operatingsystem
```

Mais PowerShell se démarque par sa façon de communiquer avec le système d'exploitation. L'OS est considéré comme un objet (au sens pro-

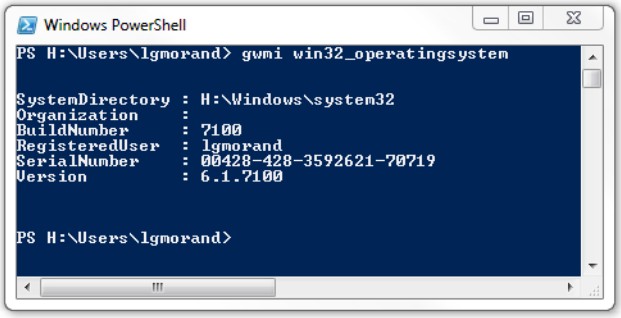


Figure 17–4
Affichage des informations du système d'exploitation

grammation), vous agissez directement sur lui par des méthodes. Vous pouvez ainsi l'éteindre ou le redémarrer :

```
$server = gwmi win32_operatingsystem
$server.reboot()
```

Il peut également être interrogé à la façon d'une base de données via des requêtes spécifiques. Prêtons-nous à un petit exercice : nous voulons lister dans un fichier, tous les services Windows démarrés de la machine. Ainsi, nous pourrons comparer le fichier avec les services d'un second ordinateur.

```
gwmi -query <notre requête>
```

Nous souhaitons obtenir les services démarrés uniquement :

```
select * from win32_service where state='Running'
```

Nous souhaitons formater l'affichage de façon claire en ne récupérant que les propriétés nom et description des services :

```
format-table -property name, description
```

Nous plaçons le tout dans un fichier texte :

```
> services.txt
```

Au final, notre commande donne :

```
gwmi -query " Select * from win32_service where
state='Running' " | format-table -property name, description |
> services.txt
```

PRÉCISION Alias

Ici, `gwmi` est l'alias de `Get-WMIObject`.

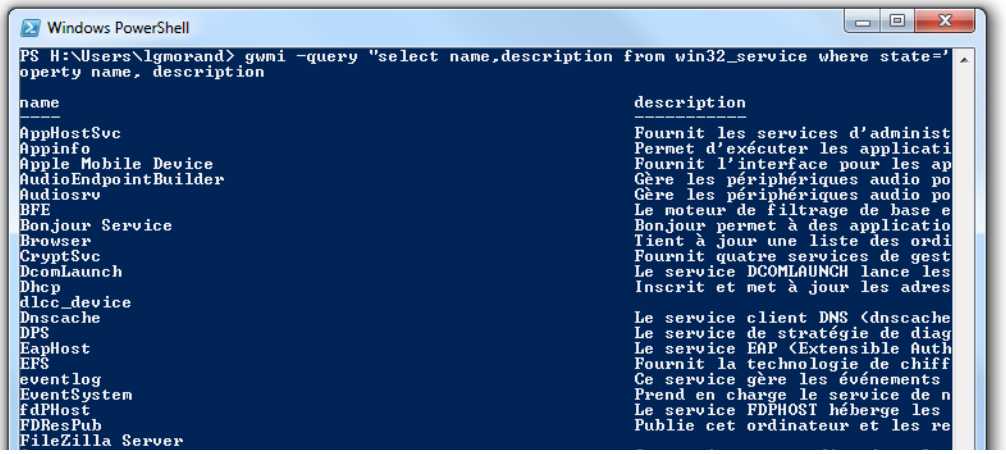


Figure 17–5
Affichage de la commande de récupération des services démarrés

Ces exemples démontrent l'intérêt et l'interaction entre PowerShell et WMI pour interroger, puis agir sur un système sans avoir à connaître à l'avance les éléments qui vont être concernés

PowerShell et le registre

Avez-vous déjà essayé d'accéder au registre via un script ou l'invite de commandes ? C'est soit impossible, soit extrêmement compliqué. Avec PowerShell, c'est devenu aussi simple que d'accéder au système de fichiers : un simple `cd hklm:Software` et vous vous retrouvez au niveau de la clé `HKEY_LOCAL_MACHINE/SOFTWARE`.

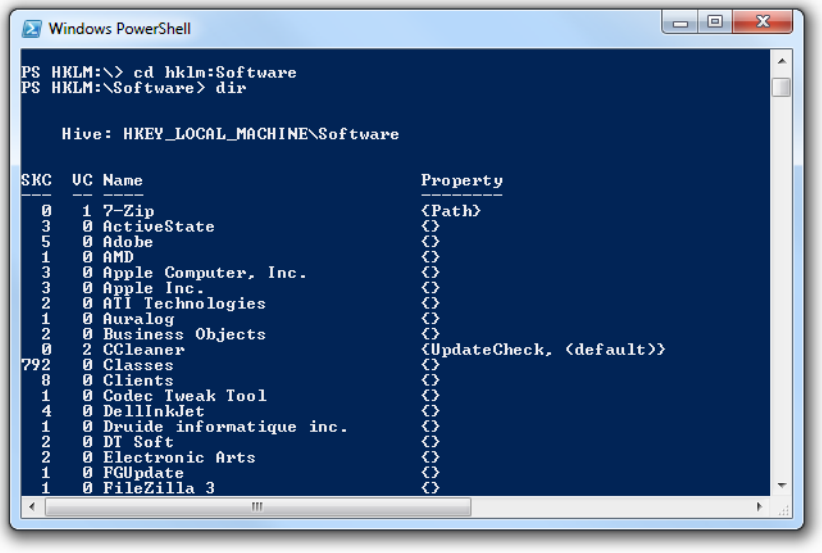


Figure 17–6
Navigation au sein du registre à travers la console PowerShell

À partir de là, avec les commandes `dir` ou `ls` (alias de `Get-Children`), `cd` (alias de `Set-Location`) ou `gp` (alias de `Get-ItemProperty`), vous naviguez dans les clés et les valeurs.

Il est ensuite facile de modifier les valeurs des clés à l'aide de la commande `sp` (ou `Set-ItemProperty`).

POUR ALLER PLUS LOIN **Sites francophones**

Si vous souhaitez aller un peu plus loin dans l'utilisation de PowerShell, nous vous recommandons les deux adresses suivantes :
Tenu par deux experts français de PowerShell, PowerShell-Scripting, bien que peu esthétique à première vue, peut revendiquer d'être le regroupement de ressources PowerShell le plus complet dans la langue de Molière. Il contient plusieurs dizaines d'articles de qualité, des aide-mémoire ainsi que de nombreux scripts permettant à tout un chacun de trouver rapidement réponse à ses besoins. Il contient également un forum d'entraide où poser vos questions. Un site à posséder dans ses favoris.

- http://www.powershell-scripting.com/

La seconde adresse est un regroupement de ressources réalisé par Laurent Dardenne, membre de Developpez.com. En plus d'avoir rassemblé les meilleures ressources sur le sujet, il a également rédigé de nombreux tutoriels allant de la prise en main de PowerShell jusqu'à l'utilisation avancée de scripts système.

- http://laurent-dardenne.developpez.com/#L2-4

POUR ALLER PLUS LOIN **Blog officiel francophone**

Pour vous tenir au courant de tout ce qui tourne autour de PowerShell, sur son utilisation, les nouveautés ou encore les ressources pour se former, rien de tel que le blog officiel :

- http://blogs.technet.com/powershell/

En résumé

PowerShell est un langage de script nouvelle génération, complet et puissant. Il vous permettra, à vous utilisateur averti, d'automatiser certaines tâches, de collecter des informations sur votre système ou tout simplement de le configurer.

N'hésitez pas à fouiller sur Internet à la recherche de scripts PowerShell prêts à l'emploi, vous pourriez y découvrir des cas d'utilisation intéressants qui vous amèneront peut-être à utiliser PowerShell là où vous ne pensiez pas qu'il vous serait utile.

Raccourcis clavier

A

Raccourcis clavier généraux

Raccourci	Effet
Alt+double-clic	Affiche les propriétés de l'élément sélectionné.
Alt+Entrée	Affiche les propriétés de l'élément sélectionné .
Alt+Echap	Parcourt les éléments dans l'ordre dans lequel ils ont été ouverts.
Alt+F4	Ferme l'élément ouvert ou le programme.
Alt+espace	Ouvre le menu contextuel de la fenêtre active (réduire, agrandir, fermer, etc.).
Alt+tabulation	Change d'élément ouvert.
Alt+lettre soulignée	Exécute la commande du menu.
Alt+flèche haut	Affiche le dossier parent dans Windows Explorer.
Ctrl+A	Sélectionne tous les éléments dans un document ou une fenêtre.
Ctrl+Alt+Suppr	Affiche des options pour : verrouiller l'ordinateur, changer d'utilisateur, éteindre, changer de mot de passe et démarrer le gestionnaire de tâches.
Ctrl+Alt+tabulation	Sert à naviguer parmi les éléments.
Ctrl+flèche gauche	Déplace le curseur au début du mot précédent.
Ctrl+flèche droite	Déplace le curseur au début du mot suivant.
Ctrl+flèche haut	Déplace le curseur au début du paragraphe précédent.
Ctrl+flèche bas	Déplace le curseur au début du paragraphe suivant.
Ctrl+Echap	Ouvre le menu *Démarrer*.
Ctrl+F4	Ferme le document courant.

Raccourci	Effet
Ctrl+Maj+flèche directionnelle	Sélectionne un bloc de texte.
Ctrl+Maj+Echap	Ouvre le gestionnaire de tâches.
Ctrl+C	Copie l'élément sélectionné.
Ctrl+X	Coupe l'élément sélectionné.
Ctrl+V ou *Maj+Inser*	Colle l'élément sélectionné.
Ctrl+Z	Annule une action.
Ctrl+Y	Recommence une action.
Suppr	Efface l'élément sélectionné et le déplace à la corbeille.
Maj+Suppr	Supprime l'élément sélectionné sans le placer dans la corbeille (suppression définitive).
Echap	Annule la tâche courante.
F1	Affiche l'aide.
F2	Renomme l'élément sélectionné.
F3	Recherche un fichier ou un dossier.
F4	Affiche la barre d'adresse dans Internet Explorer.
F5 ou *Ctrl+R*	Rafraîchit la fenêtre courante.
F6	Navigue parmi les éléments d'une fenêtre.
F10	Active la barre de menus dans le programme courant.
Flèche gauche	Ouvre le menu suivant sur la gauche, ou ferme un sous-menu.
Flèche droite	Ouvre le menu suivant sur la droite, ou ferme un sous-menu.
Impr écran	Effectue une capture de l'écran entier dans le Presse-papiers.
Alt+Impr écran	Effectue une capture d'écran de la fenêtre courante dans le Presse-papiers.
Maj pendant l'insertion d'un CD	Empêche le lancement automatique.
Maj+flèche directionnelle	Sélectionne plus d'un élément dans une fenêtre ou sur le Bureau, ou sélection du texte dans un document.
Maj+F10	Affiche le menu de raccourci pour l'élément sélectionné.
*Maj+*bouton droit de la souris	Affiche des commandes alternatives pour l'objet sélectionné.

Raccourcis d'accessibilité

Raccourci	Effet
Maj droite pendant 8 secondes	Active/désactive les touches filtres.
Alt+Maj+Verr num	Active/désactive les touches souris.
Alt+Maj+Impr écran	Active/désactive le contraste élevé.
Maj cinq fois	Active/désactive les touches rémanentes.
Verr num pendant 5 secondes	Active les touches de bascule.
Windows+U	Ouvre les options d'ergonomie.

Claviers possédant une touche Windows

Raccourci	Effet
Windows	Ouvre ou ferme le menu *Démarrer*.
Windows+Pause	Affiche la fenêtre de propriétés du système.
Windows+Ctrl+F	Cherche des ordinateurs (si vous êtes en réseau).
Windows+Ctrl +tabulation	Permet de parcourir les éléments de la barre des tâches en utilisant Windows Flip 3-D.
Windows+Pause	Affiche la fenêtre des *Propriétés système*.
Windows+D	Affiche le Bureau.
Windows+E	Ouvre le poste de travail.
Windows+F	Ouvre la recherche Windows.
Windows+G	Navigue parmi les gadgets de la barre d'espace.
Windows+L	Verrouille votre ordinateur ou change d'utilisateur.
Windows+M	Réduit toutes les fenêtres.
Windows+Maj+M	Restaure les fenêtres réduites.
Windows+R	Ouvre la boîte de dialogue *Exécuter*.
Windows+barre d'espace	Affiche les gadgets de la barre d'espace au premier plan.
Windows+T	Navigue parmi les programmes de la barre des tâches.
Windows+tabulation	Navigue parmi les programmes de la barre des tâches Flip 3-D.
Windows+Ctrl+ tabulation	Navigue parmi les programmes de la barre des tâches Flip 3-D avec les flèches du clavier.
Windows+U	Ouvre le centre d'aide à accessibilité.
Windows+X	Ouvre le centre de mobilité Windows.

Raccourci	Effet
Windows+numéro	Démarre le programme épinglé à la barre des tâches correspondant au numéro. Si le programme est déjà démarré, bascule vers celui-ci.
Windows+Maj+numéro	Démarre une nouvelle instance du programme épinglé à la barre des tâches à la position indiquée par le numéro.
Windows+espace	Affiche un aperçu du Bureau.
Windows+flèche haut	Maximise la fenêtre courante.
Windows+flèche bas	Minimise la fenêtre courante.
Windows+flèche gauche	Maximise la fenêtre dans la partie gauche de l'écran.
Windows+flèche droite	Maximise la fenêtre dans la partie droite de l'écran.
Windows+home	Minimise toutes les fenêtres sauf la fenêtre courante.
Windows+Maj+flèche haut	Étire la fenêtre sur toute la hauteur de l'écran.
Windows+Maj+flèches gauche ou droite	Déplace la fenêtre d'un moniteur à un autre.

Raccourcis des boîtes de dialogue

Raccourci	Effet
Ctrl+tabulation	Passe à l'onglet suivant.
Ctrl+Maj+tabulation	Retourne à l'onglet précédent.
Tabulation	Avance parmi les options ou passe au champ suivant.
Maj+tabulation	Recule parmi les options ou passe au champ précédent.
Alt+lettre soulignée	Appelle la commande associée à cette lettre.
Entrée	Équivalent du clic gauche pour la commande sélectionnée.
Espace	Coche ou décoche la case active.
Flèche directionnelle	Sélectionne un bouton si l'option active est un groupe de boutons options.
Retour arrière (backspace)	Ouvre un dossier parent si l'élément est dans une fenêtre *Enregistrer Sous...* ou *Ouvrir...*
F1	Affiche l'aide.
F4	Affiche les éléments dans la liste active.

Raccourcis de l'explorateur Windows

Raccourci	Effet
Ctrl+N	Ouvre une nouvelle fenêtre.
Ctrl+W	Ferme la fenêtre courante.
Ctrl+Maj+N	Crée un nouveau dossier.
Fin	Affiche le bas de la fenêtre active.
Début (home)	Affiche le haut de la fenêtre active.
F11	Maximise ou restaure la fenête courante.
Ctrl+point-virgule	Fait pivoter une image dans le sens des aiguilles d'une montre.
Ctrl+virgule	Fait pivoter une image dans le sens inverse des aiguilles d'une montre.
*Verr num+** sur le clavier numérique	Affiche tous les sous-dossiers sous le dossier sélectionné.
Verr num+- sur le clavier numérique	Réduit le dossier courant.
Verr num++ sur le clavier numérique	Explore le dossier.
Alt+flèche gauche ou *retour arrière*	Remonte au dossier précédent.
Alt+flèche droite	Remonte au dossier suivant.
Alt+flèche haut	Remonte au dossier parent.
Alt+Entrée	Affiche la boîte de dialogue de propriétés de l'élément sélectionné.
Alt+P	Affiche le panneau de visualisation.
Flèche gauche	Réduit la sélection courante (si elle est dépliée), ou sélectionne le dossier parent.
Flèche droite	Affiche la sélection courante (si l'élément est réduit), ou sélectionne le premier sous-dossier.
Alt+D	Sélectionne la barre d'adresse.
Ctrl+E ou *Ctrl+F*	Sélectionne la zone de recherche.
Ctrl+molette de la souris	Change la taille et l'apparence des icônes des fichiers et dossiers.

Raccourcis de la barre des tâches

Raccourci	Effet
Maj+clic sur un bouton	Démarre une nouvelle instance du programme sélectionné.
Ctrl+Maj+clic sur un bouton	Démarre le programme sélectionné en tant qu'administrateur.
Maj+clic droit sur un bouton	Affiche le menu *Système* pour le programme.
Maj+clic droit sur un bouton groupé	Affiche le menu *Système* pour le groupe.
Ctrl+clic sur un bouton groupé	Fait défiler les différentes fenêtres du groupe.

Raccourcis de la loupe Windows

Raccourci	Effet
Touche Windows++ (signe plus)	Effectue un zoom avant.
Touche Windows+– (signe moins)	Effectue un zoom arrière.
Ctrl+Alt+espace	Quand l'affichage est en zoom, affiche un aperçu de l'écran entier.
Ctrl+Alt+F	Bascule en mode zoom Plein écran.
Ctrl+Alt+L	Bascule en mode Loupe.
Ctrl+Alt+D	Bascule en mode Dock.
Ctrl+Alt+I	Inverse les couleurs.
Ctrl+Alt+flèche directionnelle	Fait défiler dans la direction de la flèche.
Ctrl+Alt+R	En mode Loupe, redimensionne la loupe.
Windows+Echap	Quitte la loupe Windows.

Raccourcis du Bureau à distance

Raccourci	Effet
Alt+page précédente	Bascule entre les programmes de gauche à droite.
Alt+page suivante	Bascule entre les programmes de droite à gauche.
Alt+Inser	Bascule tous les programmes ouverts dans l'ordre d'ouverture.
Alt+home	Affiche le menu *Démarrer*.
Ctrl+Alt+Pause	Bascule entre le mode Fenêtre et le mode Plein écran.
Ctrl+Alt+Fin	Affiche la boîte de dialogue *Sécurité* de Windows.
Alt+Suppr	Affiche le menu *Système*.
Ctrl+Alt+- du pavé numérique	Place une capture d'écran de la fenêtre courante dans le Presse-papiers (identique à *Alt+Impr. écran* l'un ordinateur local).
Ctrl+Alt++ du pavé numérique	Place une capture d'écran de la fenêtre entière dans le Presse-papiers (identique à *Impr. écran* sur l'ordinateur local).
Ctrl+Alt+flèche droite	Effectue une tabulation en dehors du Bureau à distance vers un contrôle de l'ordinateur hôte.

Raccourcis de Microsoft Paint

Raccourci	Effet
Ctrl+N	Crée un nouveau dessin.
Ctrl+O	Ouvre un dessin existant.
Ctrl+S	Enregistre les changements apportés au dessin.
F12	Enregistre le dessin sous...
Ctrl+P	Imprime un dessin.
Alt+F4	Ferme un dessin et la fenêtre Paint.
Ctrl+Z	Annule une action.
Ctrl+Y	Répète une action.
Ctrl+A	Sélectionne le dessin entier.
Ctrl+X	Coupe une sélection vers le Presse-papiers.
Ctrl+C	Copie une sélection vers le Presse-papiers.
Ctrl+V	Colle une sélection à partir du Presse-papiers.
Flèche directionnelle	Déplace la sélection ou la forme active d'un pixel dans la direction de la flèche.
Echap	Annule une sélection.

Raccourci	Effet
Suppr	Supprime une sélection.
Ctrl+B	Met en gras le texte sélectionné.
Ctrl++	Augmente d'un pixel l'épaisseur de la brosse, de la ligne ou du contour de la forme.
Ctrl+-	Diminue d'un pixel l'épaisseur de la brosse, de la ligne ou du contour de la forme.
Ctrl+I	Met en italique le texte sélectionné.
Ctrl+U	Souligne le texte sélectionné.
Ctrl+E	Ouvre la boîte de dialogue *Propriétés*.
Ctrl+W	Ouvre la boîte de dialogue *Redimensionner et incliner*.
Ctrl+page précédente	Effectue un zoom avant.
Ctrl+page suivante	Effectue un zoom arrière.
F11	Affiche le dessin en mode Plein écran.
Ctrl+R	Affiche ou masque la règle.
Ctrl+G	Affiche ou masque la grille.
F10 ou *Alt*	Affiche les raccourcis clavier.
F1	Ouvre l'aide de Paint.

Raccourcis de Microsoft WordPad

Raccourci	Effet
Ctrl+N	Crée un nouveau document.
Ctrl+O	Ouvre un document existant.
Ctrl+S	Enregistre les changements.
F12	Enregistre sous...
Ctrl+P	Imprime le document.
Alt+F4	Ferme WordPad.
Ctrl+Z	Annule une action.
Ctrl+Y	Répète une action.
Ctrl+A	Sélectionne le document entier.
Ctrl+X	Coupe la sélection.
Ctrl+C	Copie la sélection vers le Presse-papiers.
Ctrl+V	Colle la sélection à partir du Presse-papiers.
Ctrl+B	Met en gras le texte sélectionné.
Ctrl+I	Met en italique le texte sélectionné.

Raccourci	Effet
Ctrl+U	Souligne le texte sélectionné.
Ctrl+=	Met le texte sélectionné en indice.
Ctrl+Maj+=	Met le texte sélectionné en exposant.
Ctrl+L	Aligne le texte à gauche.
Ctrl+E	Centre le texte.
Ctrl+R	Aligne le texte à droite.
Ctrl+J	Justifie le texte.
Ctrl+1	Insère un interligne simple.
Ctrl+2	Insère un interligne double.
Ctrl+5	Insère un interligne de 1,5.
Ctrl+Maj+>	Augmente la taille de la police.
Ctrl+Maj+<	Diminue la taille de la police.
Ctrl+Maj+A	Met le texte sélectionné en majuscule.
Ctrl+Maj+L	Change le style de puce.
Ctrl+D	Insère un dessin Microsoft Paint.
Ctrl+F	Recherche un texte dans le document.
F3	Recherche l'instance de texte suivante.
Ctrl+H	Remplace le texte dans le document.
Ctrl+flèche gauche	Déplace le curseur d'un mot vers la gauche.
Ctrl+flèche droite	Déplace le curseur d'un mot vers la droite.
Ctrl+flèche haut	Déplace le curseur à la ligne précédente.
Ctrl+flèche bas	Déplace le curseur à la ligne suivante.
Ctrl+home	Déplace le curseur au début du document.
Ctrl+Fin	Déplace le curseur à la fin du document.
Ctrl+Suppr	Supprime le mot suivant.
F10	Affiche les raccourcis clavier.
F1	Ouvre l'aide de WordPad.

Raccourcis de la calculatrice Windows

Raccourcis généraux

Raccourci	Effet
Alt+1	Bascule vers le mode Standard.
Alt+2	Bascule vers le mode Scientifique.

Raccourci	Effet
Alt+3	Bascule vers le mode Programmeur.
Alt+4	Bascule vers le mode Statistiques.
Ctrl+E	Ouvre l'outil de calcul de dates.
Ctrl+H	Active ou désactive l'historique des calculs.
Ctrl+U	Ouvre le convertisseur d'unités.
Alt+C	Calcule ou résout les calculs de dates et feuilles de calcul.
F1	Ouvre l'aide de la calculatrice.
Ctrl+Q	Appuie sur le bouton M-.
Ctrl+P	Appuie sur le bouton M+.
Ctrl+M	Appuie sur le bouton MS.
Ctrl+R	Appuie sur le bouton MR.
Ctrl+L	Appuie sur le bouton MC.
%	Appuie sur le bouton %.
F9	Appuie sur le bouton +/-.
R	Appuie sur le bouton 1/x.
@	Appuie sur le bouton racine carrée.
=	Appuie sur le bouton =.
.	Appuie sur le bouton point (.).
Retour arrière (backspace)	Efface le dernier chiffre saisi.
Echap	Appuie sur le bouton C.
Suppr	Appuie sur le bouton CE.
Ctrl+Maj+D	Efface l'historique de la calculatrice.
F2	Modifie l'historique de la calculatrice.
Flèche haut	Navigue vers le haut dans l'historique des calculs.
Flèche bas	Navigue vers le bas dans l'historique des calculs.
Echap	Annule l'édition de l'historique des calculs.
Entrée	Recalcule l'historisque des calculs après modification.

Mode Scientifique

Raccourci	Effet
F3	Sélectionne les degrés.
F4	Sélectionne les radians.
F5	Sélectionne les grades.
I	Appuie sur le bouton Inv.

Raccourci	Effet
D	Appuie sur le bouton Mod.
Ctrl+S	Appuie sur le bouton sinh.
Ctrl+O	Appuie sur le bouton cosh.
Ctrl+T	Appuie sur le bouton tanh.
(	Appuie sur le bouton (.
)	Appuie sur le bouton).
N	Appuie sur le bouton ln.
;	Appuie sur le bouton Int.
S	Appuie sur le bouton sin.
O	Appuie sur le bouton cos.
T	Appuie sur le bouton Tabulation.
M	Appuie sur le bouton dms.
P	Appuie sur le bouton pi.
V	Appuie sur le bouton F-E.
X	Appuie sur le bouton Exp.
Q	Appuie sur le bouton x^2.
Y	Appuie sur le bouton x^y.
#	Appuie sur le bouton x^3.
L	Appuie sur le bouton log.
!	Appuie sur le bouton n!.
Ctrl+Y	Appuie sur le bouton $y\sqrt{x}$.
Ctrl+B	Appuie sur le bouton $3\sqrt{x}$.
Ctrl+G	Appuie sur le bouton 10x.

Mode Programmeur

Raccourci	Effet
F5	Sélectionne Hex.
F6	Sélectionne Dec.
F7	Sélectionne Oct.
F8	Sélectionne Bin.
F12	Sélectionne Qword.
F2	Sélectionne Dword.
F3	Sélectionne Word.
F4	Sélectionne Byte.
K	Appuie sur le bouton RoR.

Raccourci	Effet
J	Appuie sur le bouton RoL.
<	Appuie sur le bouton Lsh.
>	Appuie sur le bouton Rsh.
%	Appuie sur le bouton Mod.
(	Appuie sur le bouton (.
)	Appuie sur le bouton).
|	Appuie sur le bouton Or.
^	Appuie sur le bouton Xor.
~	Appuie sur le bouton Not.
&	Appuie sur le bouton And.
A-F	Appuie sur les bouton A-F.
Espace	Bascule la valeur du bit.

Mode Statistiques

Raccourci	Effet
A	Appuie sur le bouton Average (moyenne).
Ctrl+A	Appuie sur le bouton Average Sq.
S	Appuie sur le bouton Sum.
Ctrl+S	Appuie sur le bouton Sum Sq.
T	Appuie sur le bouton S.D.
Ctrl+T	Appuie sur le bouton Inv S.D.
D	Appuie sur le bouton CAD.

Raccourcis de l'aide Windows

Raccourci	Effet
Alt+C	Affiche la table des matières.
F10	Ouvre le menu *Options*.
Alt+flèche gauche	Va au sujet consulté précédemment.
Alt+flèche droite	Va au sujet suivant.
Alt+home	Affiche la page d'accueil.
Home	Va au début de la page.
Fin	Va à la fin de la page.
Ctrl+F	Effectue une recherche dans la page courante.

Raccourci	Effet
Ctrl+P	Imprime une page d'aide.
F3	Place le curseur dans la barre de recherche.

Raccourcis clavier Windows Media Center

Raccourci	Effet
Windows +Alt+Entrée	Ouvre Windows Media Center ou retourne à l'écran de démarrage de Windows Media Center.
Alt+Entrée	Affiche ou quitte le mode Plein écran.
Alt+F4	Ferme Windows Media Center.
Flèche directionnelle	Bouge vers la gauche, vers la droite, vers le haut ou vers le bas.
Retour arrière (backspace)	Revient à l'écran précédent.
Fin	Va au dernier élément d'une liste.
Entrée	Accepte la sélection.
Home	Va au premier élément d'une liste.
Page précédente	Va à la page suivante.
Page suivante	Va à la page précédente.

Raccourcis audio du Windows Media Center

Raccourci	Effet
Ctrl+B	Rejoue un fichier audio.
Ctrl+D	Affiche le menu contextuel.
Ctrl+F	Passe à la chanson suivante.
Ctrl+M	Va dans la catégorie Musique.
Ctrl+P	Met en pause ou reprend la lecture d'un fichier audio.
Ctrl+R	Grave un CD.
Ctrl+Maj+C	Active/désactive la capture.
Ctrl+Maj+F	Avance rapidement dans un fichier audio.
Ctrl+Maj+P	Joue un fichier audio.
F10	Monte le volume.
F8	Coupe le son.
F9	Baisse le volume.

Raccourcis clavier pour contrôler la TV du Windows Media Center

Raccourci	Effet
Ctrl+B	Recule.
Ctrl+D	Affiche le menu contextuel.
Ctrl+F	Avance.
Ctrl+G	Va dans *Guide*.
Ctrl+O	Va dans *Recorded TV*.
Ctrl+P	Met en pause la lecture.
Ctrl+R	Enregistre un show TV.
Ctrl+Maj+B	Rembobine un enregistrement TV.
Ctrl+Maj+F	Avance rapidement dans un enregistrement TV.
Ctrl+Maj+P	Reprend la lecture d'un show TV.
Ctrl+Maj+S	Stoppe l'enregistrement ou la lecture d'un show TV.
Ctrl+T	Va dans live TV.
Page suivante	Va à la chaîne précédente.
Page précédente	Va à la chaîne suivante.

Raccourcis clavier pour la lecture de radios du Windows Media Center

Raccourci	Effet
Ctrl+A	Va dans *Radios*.
Ctrl+B	Recule.
Ctrl+D	Affiche le menu contextuel.
Ctrl+F	Avance.
Ctrl+P	Met en pause ou reprend la lecture de la radio.
Ctrl+Maj+P	Reprend la lecture de la radio.
Ctrl+Maj+S	Arrête la radio.

Raccourcis clavier pour la visualisation d'images du Windows Media Center

Raccourci	Effet
Ctrl+D	Affiche le menu contextuel.
Ctrl+I	Va dans *Images*.

Raccourci	Effet
Ctrl+P	Met en pause un diaporama.
Ctrl+Maj+P	Lance un diaporama.
Ctrl+Maj+S	Arrête le diaporama.
Flèche bas ou *flèche droite*	Passe à l'image suivante.
Entrée	Zoome.
Flèche haut ou *flèche gauche*	Revient à l'image précédente.

Raccourcis clavier pour la lecture de vidéos du Windows Media Center

Raccourci	Effet
Ctrl+B	Va à l'élément précédent.
Ctrl+E	Va dans *Vidéos*.
Ctrl+F	Va à l'élément suivant.
Ctrl+P	Met en pause.
Ctrl+Maj+B	Rembobine.
Ctrl+Maj+F	Avance rapidement.
Ctrl+Maj+S	Stoppe.

Raccourcis clavier pour la lecture de DVD du Windows Media Center

Raccourci	Effet
Flèche directionnelle	Change l'angle du DVD.
Ctrl+B	Va au chapitre précédent.
Ctrl+F	Va au chapitre suivant.
Ctrl+P	Met en pause.
Ctrl+Maj+A	Change la sélection audio du DVD.
Ctrl+Maj+B	Rembobine.
Ctrl+Maj+F	Avance rapidement.
Ctrl+Maj+M	Va au menu DVD.
Ctrl+Maj+P	Lance le DVD.
Ctrl+Maj+S	Stoppe.
Ctrl+U	Change la sélection de sous-titres du DVD.

Commandes et alias de PowerShell

B

Liste des commandes

A	
Add-Computer	Ajoute l'ordinateur local à un domaine ou à un groupe de travail.
Add-Content	Ajoute le contenu aux éléments spécifiés (ajout de mots à un fichier, par exemple).
Add-History	Ajoute des entrées à l'historique de la session.
Add-Member	Ajoute un membre personnalisé défini par l'utilisateur à une instance d'un objet Windows PowerShell.
Add-PSSnapin	Ajoute un ou plusieurs composants logiciels enfichables Windows PowerShell à la session active.
Add-Type	Ajoute un type (une classe) Microsoft .NET Framework à une session Windows PowerShell.
C	
cd..	Équivaut à Set-Location.
Checkpoint-Computer	Crée un point de restauration système sur l'ordinateur local.
Clear-Content	Supprime le contenu d'un élément, par exemple le texte d'un fichier, mais ne supprime pas l'élément.
Clear-EventLog	Supprime toutes les entrées des journaux d'événements spécifiés sur les ordinateurs locaux ou distants.
Clear-History	Supprime des entrées de l'historique des commandes.
Clear-Host	
Clear-Item	Supprime le contenu d'un élément mais pas l'élément.
Clear-ItemProperty	Supprime la valeur d'une propriété mais pas la propriété.
Clear-Variable	Supprime la valeur d'une variable.
Compare-Object	Compare deux jeux d'objets.
Complete-Transaction	Valide la transaction active.
Connect-WSMan	Se connecte au service WinRM sur un ordinateur distant.

ConvertFrom-Csv	Convertit les propriétés d'objet au format CSV (valeurs séparées par des virgules) en versions CSV des objets d'origine.
ConvertFrom-SecureString	Convertit une chaîne sécurisée en chaîne standard chiffrée.
ConvertFrom-StringData	Convertit une chaîne contenant une ou plusieurs paires clé/valeur en une table de hachage.
Convert-Path	Convertit un chemin d'accès Windows PowerShell en chemin d'accès à un fournisseur Windows PowerShell.
ConvertTo-Csv	Convertit des objets Microsoft .NET Framework en une série de chaînes de longueurs variables au format CSV (valeurs séparées par des virgules).
ConvertTo-Html	Convertit des objets Microsoft .NET Framework au format HTML pouvant être affiché dans un navigateur web.
ConvertTo-SecureString	Convertit des chaînes standards chiffrées en chaînes sécurisées. Elle peut aussi convertir du texte brut en chaînes sécurisées. Elle est utilisée avec ConvertFrom-SecureString et Read-Host.
ConvertTo-Xml	Crée une représentation XML d'un objet.
Copy-Item	Copie un élément d'un emplacement vers un autre dans un espace de noms.
Copy-ItemProperty	Copie une propriété et une valeur d'un emplacement spécifié vers un autre emplacement.
D	
Debug-Process	Débogue un ou plusieurs processus en cours d'exécution sur l'ordinateur local.
Disable-ComputerRestore	Désactive la fonctionnalité *Restauration du système* sur le lecteur de système de fichiers spécifié.
Disable-PSBreakpoint	Désactive les points d'arrêt de la console actuelle.
Disable-PSRemoting	Désactive l'ordinateur pour recevoir des commandes distantes.
Disable-PSSessionConfiguration	Refuse l'accès aux configurations de session sur l'ordinateur local.
Disable-WSManCredSSP	Désactive l'authentification CredSSP sur un ordinateur client.
Disconnect-WSMan	Déconnecte le client du service WinRM sur un ordinateur distant.
E	
Enable-ComputerRestore	Active la fonctionnalité *Restauration du système* sur le lecteur de système de fichiers spécifié.
Enable-PSBreakpoint	Active les points d'arrêt de la console actuelle.
Enable-PSRemoting	Configure l'ordinateur pour recevoir des commandes distantes.
Enable-PSSessionConfiguration	Active les configurations de session sur l'ordinateur local.
Enable-WSManCredSSP	Active l'authentification CredSSP sur un ordinateur client.
Enter-PSSession	Démarre une session interactive avec un ordinateur distant.
Exit-PSSession	Met fin à une session interactive avec un ordinateur distant.
Export-Alias	Exporte vers un fichier les informations sur les alias actuellement définis.
Export-Clixml	Crée une représentation XML d'un ou de plusieurs objets et la stocke dans un fichier.
Export-Console	Exporte les noms des composants logiciels enfichables de la session active vers un fichier console.
Export-Counter	L'applet de commande Export-Counter accepte des objets PerformanceCounterSampleSet et les exporte en tant que fichiers journaux de compteur.
Export-Csv	Convertit les objets Microsoft .NET Framework en une série de chaînes de longueurs variables séparées par des virgules (CSV), puis enregistre ces chaînes dans un fichier CSV.

Export-FormatData	Enregistre les données de mise en forme de la session active dans un fichier de mise en forme.
Export-ModuleMember	Spécifie les membres de module exportés.
Export-PSSession	Importe des commandes à partir d'une autre session et les enregistre dans un module Windows PowerShell.
F	
ForEach-Object	Exécute une opération en fonction de chacun des jeux d'objets d'entrée.
Format-Custom	Utilise un affichage personnalisé pour mettre en forme la sortie.
Format-List	Met en forme la sortie en tant que liste de propriétés dans laquelle chaque propriété apparaît sur une nouvelle ligne.
Format-Table	Met en forme la sortie en tant que tableau.
Format-Wide	Met en forme les objets en tant que large table qui affiche une seule propriété de chaque objet.
G	
Get-Acl	Obtient le descripteur de sécurité d'une ressource, comme un fichier ou une clé de registre.
Get-Alias	Obtient les alias pour la session active.
Get-AuthenticodeSignature	Obtient les informations relatives à la signature Authenticode d'un fichier.
Get-ChildItem	Obtient les éléments et les éléments enfants à un ou plusieurs emplacements spécifiés.
Get-Command	Obtient des informations de base sur les applets de commande et d'autres éléments des commandes Windows PowerShell.
Get-ComputerRestorePoint	Obtient les points de restauration présents sur l'ordinateur local.
Get-Content	Obtient le contenu de l'élément à l'emplacement spécifié.
Get-Counter	Obtient des données de compteur de performance à partir des ordinateurs locaux et distants.
Get-Credential	Obtient un objet credential (informations d'identification) basé sur les nom et mot de passe d'un utilisateur.
Get-Culture	Obtient le jeu de cultures actuel du système d'exploitation.
Get-Date	Obtient l'heure et la date actuelles.
Get-Event	Obtient les événements de la file d'attente d'événements.
Get-EventLog	Obtient les événements d'un journal d'événements ou la liste des journaux d'événements présents sur les ordinateurs locaux ou distants.
Get-EventSubscriber	Obtient tous les abonnés aux événements de la session active.
Get-ExecutionPolicy	Obtient les stratégies d'exécution pour la session active.
Get-FormatData	Obtient les données de mise en forme de la session active.
Get-Help	Affiche des informations sur les commandes et les concepts Windows PowerShell.
Get-History	Obtient la liste des commandes entrées pendant la session active.
Get-Host	Obtient un objet qui représente le programme hôte actuel. Affiche en outre la version de Windows PowerShell et les informations régionales par défaut.
Get-HotFix	Obtient les correctifs logiciels qui ont été appliqués aux ordinateurs locaux et distants.
Get-Item	Obtient l'élément à l'emplacement spécifié.
Get-ItemProperty	Obtient les propriétés de l'élément spécifié.
Get-Job	Obtient les tâches en arrière-plan Windows PowerShell qui s'exécutent dans la session active.

Get-Location	Obtient des informations à propos de l'emplacement de travail actif.
Get-Member	Obtient les propriétés et méthodes des objets.
Get-Module	Obtient les modules qui ont été importés ou peuvent être importés dans la session active.
Get-PfxCertificate	Obtient des informations sur les fichiers de certificat .pfx de l'ordinateur.
Get-Process	Obtient les processus qui s'exécutent sur l'ordinateur local ou un ordinateur distant.
Get-PSBreakpoint	Obtient les points d'arrêt définis dans la session active.
Get-PSCallStack	Affiche la pile des appels actuelle.
Get-PSDrive	Obtient les lecteurs Windows PowerShell présents dans la session active.
Get-PSProvider	Obtient des informations se rapportant au fournisseur Windows PowerShell spécifié.
Get-PSSession	Obtient les sessions Windows PowerShell (PSSession) dans la session active.
Get-PSSessionConfiguration	Obtient les configurations de session inscrites sur l'ordinateur.
Get-PSSnapin	Obtient les composants logiciels enfichables Windows PowerShell situés sur l'ordinateur.
Get-Random	Obtient un nombre aléatoire ou sélectionne aléatoirement des objets dans une collection.
Get-Service	Obtient les services présents sur un ordinateur local ou distant.
Get-TraceSource	Obtient les composants Windows PowerShell qui sont instrumentés pour le traçage.
Get-Transaction	Obtient la transaction actuelle (active).
Get-UICulture	Obtient les paramètres de la culture d'interface utilisateur actuelle définis dans le système d'exploitation.
Get-Unique	Retourne les éléments uniques dans une liste triée.
Get-Variable	Obtient les variables de la console actuelle.
Get-WinEvent	Obtient des événements à partir des journaux d'événements et des fichiers journaux de suivi d'événements présents sur les ordinateurs locaux et distants.
Get-WmiObject	Obtient des instances de classes WMI (*Windows Management Instrumentation*) ou des informations sur les classes disponibles.
Get-WSManCredSSP	Obtient la configuration CredSSP du client.
Get-WSManInstance	Affiche les informations de gestion pour une instance de ressource spécifiée par un URI de ressource.
Group-Object	Regroupe les objets qui contiennent la même valeur pour les propriétés spécifiées.
H	
help	Affiche des informations sur les commandes et les concepts Windows PowerShell.
I	
Import-Alias	Importe une liste d'alias à partir d'un fichier.
Import-Clixml	Importe un fichier CLIXML et crée des objets correspondants dans Windows PowerShell.
Import-Counter	Importe des fichiers journaux de compteur de performance (.blg, .csv, .tsv) et crée les objets qui représentent chaque échantillon de compteur dans le journal.
Import-Csv	Convertit les propriétés d'objet d'un fichier CSV (fichier de valeurs séparées par des virgules) en versions CSV des objets d'origine.
Import-LocalizedData	Importe des données spécifiques à une langue dans des scripts et fonctions selon la culture d'interface utilisateur sélectionnée pour le système d'exploitation.

Import-Module	Ajoute des modules à la session active.
Import-PSSession	Importe des commandes à partir d'une autre session dans la session active.
ImportSystemModules	
Invoke-Command	Exécute les commandes sur des ordinateurs locaux et distants.
Invoke-Expression	Exécute les commandes ou les expressions sur l'ordinateur local.
Invoke-History	Exécute les commandes depuis l'historique de la session.
Invoke-Item	Exécute l'action par défaut sur l'élément spécifié.
Invoke-WmiMethod	Appelle des méthodes *Windows Management Instrumentation* (WMI).
Invoke-WSManAction	Appelle une action sur l'objet spécifié par l'URI de ressource et les sélecteurs.
J	
Join-Path	Combine un chemin d'accès et un chemin d'accès d'enfant en un seul chemin d'accès. Le fournisseur fournit les séparateurs de chemin d'accès.
L	
Limit-EventLog	Définit les propriétés de journal d'événements qui limitent la taille du journal d'événements et l'ancienneté de ses entrées.
M	
Measure-Command	Mesure le temps qu'il faut pour exécuter des blocs de script et des applets de commande.
Measure-Object	Calcule les propriétés numériques des objets, ainsi que les caractères, mots et lignes des objets chaînes, tels que les fichiers de texte.
mkdir	Crée un élément.
Move-Item	Déplace un élément d'un emplacement à un autre.
Move-ItemProperty	Déplace une propriété d'un emplacement à un autre.
N	
New-Alias	Crée un alias.
New-Event	Crée un événement.
New-EventLog	Crée un journal d'événements et une source d'événements sur un ordinateur local ou distant.
New-Item	Crée un élément.
New-ItemProperty	Crée une propriété pour un élément et définit sa valeur. Par exemple, vous pouvez utiliser New-ItemProperty pour créer et modifier des données et des valeurs de registre qui sont les propriétés d'une clé de registre.
New-Module	Crée un module dynamique qui existe uniquement en mémoire.
New-ModuleManifest	Crée un manifeste de module.
New-Object	Crée une instance d'un objet Microsoft .NET Framework ou COM.
New-PSDrive	Crée un lecteur Windows PowerShell dans la session active.
New-PSSession	Crée une connexion permanente à un ordinateur local ou distant.
New-PSSessionOption	Crée un objet qui contient les options avancées d'une session PSSession.
New-Service	Crée un service Windows.
New-TimeSpan	Crée un objet TimeSpan.
New-Variable	Crée une variable.

New-WebServiceProxy	Crée un objet proxy de service web qui vous permet d'utiliser et de gérer le service web dans Windows PowerShell.
New-WSManInstance	Crée une nouvelle instance d'une ressource de gestion.
New-WSManSessionOption	Crée une table de hachage d'options de session de gestion des services web à utiliser comme paramètres d'entrée pour les applets de commande de gestion des services web : Get-WSManInstance Set-WSManInstance Invoke-WSManAction Connect-WSMan
O	
Out-Default	Envoie la sortie au formateur par défaut et à l'applet de commande de sortie par défaut.
Out-File	Envoie la sortie à un fichier.
Out-GridView	Envoie la sortie vers une table interactive dans une fenêtre distincte.
Out-Host	Envoie la sortie à la ligne de commande.
Out-Null	Supprime la sortie au lieu de l'envoyer à la console.
Out-Printer	Envoie la sortie à une imprimante.
Out-String	Envoie des objets à l'hôte en tant que série de chaînes.
P	
Pop-Location	Définit l'emplacement actuel sur le dernier emplacement placé sur la pile. Vous pouvez extraire l'emplacement à partir de la pile par défaut ou d'une pile créée à l'aide de l'applet de commande Push-Location.
Push-Location	Ajoute l'emplacement actuel au sommet d'une liste d'emplacements (appelée pile).
R	
Read-Host	Lit une ligne d'entrée à partir de la console.
Receive-Job	Obtient les résultats des tâches en arrière-plan de Windows PowerShell dans la session active.
Register-EngineEvent	Crée un abonnement aux événements générés par le moteur Windows PowerShell et par l'applet de commande New-Event.
Register-ObjectEvent	Crée un abonnement aux événements générés par un objet Microsoft .NET Framework.
Register-PSSessionConfiguration	Crée et inscrit une nouvelle configuration de session.
Register-WmiEvent	S'abonne à un événement *Windows Management Instrumentation* (WMI).
Remove-Computer	Supprime l'ordinateur local d'un groupe de travail ou d'un domaine.
Remove-Event	Supprime des événements de la file d'attente d'événements.
Remove-EventLog	Supprime un journal d'événements ou annule l'inscription d'une source d'événements.
Remove-Item	Supprime les éléments spécifiés.
Remove-ItemProperty	Supprime la propriété et la valeur d'un élément.
Remove-Job	Supprime une tâche en arrière-plan de Windows PowerShell.
Remove-Module	Supprime des modules de la session active.
Remove-PSBreakpoint	Supprime des points d'arrêt de la console actuelle.
Remove-PSDrive	Supprime un lecteur Windows PowerShell de son emplacement.
Remove-PSSession	Ferme une ou plusieurs sessions Windows PowerShell (PSSession).

Remove-PSSnapin	Supprime les composants logiciels enfichables Windows PowerShell de la session active.
Remove-Variable	Supprime une variable et sa valeur.
Remove-WmiObject	Supprime une instance d'une classe *Windows Management Instrumentation* (WMI) existante.
Remove-WSManInstance	Supprime une instance de ressource de gestion.
Rename-Item	Renomme un élément dans un espace de noms du fournisseur de Windows PowerShell.
Rename-ItemProperty	Renomme la propriété d'un élément.
Reset-ComputerMachinePassword	Réinitialise le mot de passe du compte ordinateur de l'ordinateur.
Resolve-Path	Résout les caractères génériques inclus dans un chemin d'accès et affiche le contenu de ce dernier.
Restart-Computer	Redémarre le système d'exploitation sur les ordinateurs locaux et distants.
Restart-Service	Arrête, puis démarre un ou plusieurs services.
Restore-Computer	Démarre une restauration système sur l'ordinateur local.
Resume-Service	Reprend un ou plusieurs services interrompus (suspendus).
S	
Select-Object	Sélectionne des propriétés spécifiées d'un objet ou d'un jeu d'objets. Elle peut également sélectionner des objets uniques d'un tableau d'objets, ou sélectionner un nombre spécifié d'objets à partir du début ou de la fin d'un tableau d'objets.
Select-String	Recherche du texte dans des chaînes et des fichiers.
Select-Xml	Recherche du texte dans un document ou une chaîne XML.
Send-MailMessage	Envoie un message électronique.
Set-AuthenticodeSignature	Ajoute une signature Authenticode à un script Windows PowerShell ou à un autre fichier.
Set-Content	Écrit ou remplace le contenu d'un élément par un nouveau contenu.
Set-Date	Modifie l'heure système sur l'ordinateur en la remplaçant par l'heure que vous spécifiez.
Set-ExecutionPolicy	Modifie la préférence utilisateur de la stratégie d'exécution Windows PowerShell.
Set-Item	Remplace la valeur d'un élément par la valeur spécifiée dans la commande.
Set-ItemProperty	Crée ou modifie la valeur d'une propriété d'un élément.
Set-Location	Définit l'emplacement de travail actif sur un emplacement spécifié.
Set-PSBreakpoint	Définit un point d'arrêt sur une ligne, commande ou variable.
Set-PSDebug	Active et désactive les fonctions de débogage de script, définit le niveau de trace et active/désactive le mode strict.
Set-Acl	Modifie le descripteur de sécurité de la ressource spécifiée, telle qu'un fichier ou une clé de registre.
Set-Alias	Crée ou modifie un alias (autre nom) pour une applet de commande ou un autre élément de commande dans la session Windows PowerShell actuelle.
Set-PSSessionConfiguration	Ajoute une signature Authenticode à un script Windows PowerShell ou à un autre fichier.
Set-Service	Démarre, arrête et interrompt un service, puis modifie ses propriétés.
Set-StrictMode	Établit et met en vigueur des règles de codage dans les expressions, scripts et blocs de script.
Set-TraceSource	Configure, démarre et arrête une trace des composants Windows PowerShell.
Set-Variable	Définit la valeur d'une variable. Crée la variable s'il n'existe aucune variable portant le nom demandé.

Set-WmiInstance	Crée ou met à jour une instance d'une classe WMI (*Windows Management Instrumentation*) existante.
Set-WSManInstance	Modifie les informations de gestion qui sont associées à une ressource.
Set-WSManQuickConfig	Configure l'ordinateur local pour l'administration à distance.
Show-EventLog	Affiche les journaux d'événements de l'ordinateur local ou d'un ordinateur distant dans l'observateur d'événements.
Sort-Object	Trie les objets par les valeurs de propriétés.
Split-Path	Retourne la partie spécifiée d'un chemin d'accès.
Start-Job	Démarre une tâche Windows PowerShell en arrière-plan.
Start-Process	Démarre un ou plusieurs processus sur l'ordinateur local.
Start-Service	Démarre un ou plusieurs services arrêtés.
Start-Sleep	Suspend l'activité d'un script ou d'une session pendant l'intervalle de temps spécifié.
Start-Transaction	Démarre une transaction.
Start-Transcript	Crée un enregistrement de tout ou partie d'une session Windows PowerShell dans un fichier texte.
Stop-Computer	Arrête les ordinateurs locaux et distants.
Stop-Job	Arrête une tâche Windows PowerShell en arrière-plan.
Stop-Process	Arrête un ou plusieurs processus en cours d'exécution.
Stop-Service	Arrête un ou plusieurs services en cours d'exécution.
Stop-Transcript	Arrête une transcription.
Suspend-Service	Interrompt (suspend) un ou plusieurs services en cours d'exécution.
T	
Tee-Object	Enregistre la sortie de la commande dans un fichier ou une variable, puis l'affiche dans la console.
Test-ComputerSecureChannel	Teste et répare le canal sécurisé entre l'ordinateur local et son domaine.
Test-Connection	Envoie les paquets de demande d'écho ICMP (*pings*) à un ou plusieurs ordinateurs.
Test-ModuleManifest	Vérifie qu'un fichier manifeste de module décrit précisément le contenu d'un module.
Test-Path	Détermine si tous les éléments d'un chemin d'accès existent.
Test-WSMan	Teste si le service WinRM s'exécute sur un ordinateur local ou distant.
Trace-Command	Configure et démarre une trace de l'expression ou de la commande spécifiée.
U	
Undo-Transaction	Restaure la transaction active.
Unregister-Event	Restaure la transaction active.
Unregister-PSSessionConfiguration	Supprime les configurations de session inscrites de l'ordinateur.
Update-FormatData	Met à jour les données de mise en forme de la session active.
Update-List	Ajoute et supprime des éléments dans une valeur de propriété contenant une collection d'objets.
Update-TypeData	Met à jour la configuration de type étendu actuelle en rechargeant en mémoire les fichiers *.types.ps1xml.
Use-Transaction	Ajoute le bloc de script à la transaction active.

W	
Wait-Event	Attend qu'un événement particulier soit déclenché avant de poursuivre l'exécution.
Wait-Job	Supprime l'invite de commandes jusqu'à ce qu'une des tâches ou toutes les tâches en arrière-plan de Windows PowerShell s'exécutant dans la session soient terminées.
Wait-Process	Attend l'arrêt des processus avant d'accepter une autre entrée.
Where-Object	Crée un filtre qui contrôle les objets qui seront passés le long d'un pipeline de commande.
Write-Debug	Écrit un message de débogage sur la console.
Write-Error	Écrit un objet dans le flux d'erreurs.
Write-EventLog	Écrit un événement dans un journal d'événements.
Write-Host	Écrit la sortie personnalisée sur un hôte.
Write-Output	Envoie les objets spécifiés à la commande suivante dans le pipeline. Si la commande est la dernière du pipeline, les objets sont affichés sur la console.
Write-Progress	Affiche une barre de progression dans une fenêtre de commande Windows PowerShell.
Write-Verbose	Écrit le texte dans le flux de messages commentés.
Write-Warning	Écrit un message d'avertissement.

Liste des alias

Alias	Commande équivalente
%	ForEach-Object
?	Where-Object
ac	Add-Content
asnp	Add-PSSnapIn
cat	Get-Content
cd	Set-Location
chdir	Set-Location
clc	Clear-Content
clear	Clear-Host
clhy	Clear-History
cli	Clear-Item
clp	Clear-ItemProperty
cls	Clear-Host
clv	Clear-Variable
compare	Compare-Object
copy	Copy-Item
cp	Copy-Item

Alias	Commande équivalente
cpi	Copy-Item
cpp	Copy-ItemProperty
cvpa	Convert-Path
dbp	Disable-PSBreakpoint
del	Remove-Item
diff	Compare-Object
dir	Get-ChildItem
ebp	Enable-PSBreakpoint
echo	Write-Output
epal	Export-
epcsv	Export-Csv
epsn	Export-PSSession
erase	Remove-Item
etsn	Enter-PSSession
exsn	Exit-PSSession
fc	Format-Custom
fl	Format-List
foreach	ForEach-Object
ft	Format-Table
fw	Format-Wide
gal	Get-
gbp	Get-PSBreakpoint
gc	Get-Content
gci	Get-ChildItem
gcm	Get-Command
gcs	Get-PSCallStack
gdr	Get-PSDrive
ghy	Get-History
gi	Get-Item
gjb	Get-Job
gl	Get-Location
gm	Get-Member
gmo	Get-Module
gp	Get-ItemProperty
gps	Get-Process
group	Group-Object

Alias	Commande équivalente
gsn	Get-PSSession
gsnp	Get-PSSnapIn
gsv	Get-Service
gu	Get-Unique
gv	Get-Variable
gwmi	Get-WmiObject
h	Get-History
history	Get-History
icm	Invoke-Command
iex	Invoke-Expression
ihy	Invoke-History
ii	Invoke-Item
ipal	Import-
ipcsv	Import-Csv
ipmo	Import-Module
ipsn	Import-PSSession
ise	powershell_ise.exe
iwmi	Invoke-WMIMethod
kill	Stop-Process
lp	Out-Printer
ls	Get-ChildItem
man	help
md	mkdir
measure	Measure-Object
mi	Move-Item
mount	New-PSDrive
move	Move-Item
mp	Move-ItemProperty
mv	Move-Item
nal	New-
ndr	New-PSDrive
ni	New-Item
nmo	New-Module
nsn	New-PSSession
nv	New-Variable
ogv	Out-GridView

Alias	Commande équivalente
oh	Out-Host
popd	Pop-Location
ps	Get-Process
pushd	Push-Location
pwd	Get-Location
r	Invoke-History
rbp	Remove-PSBreakpoint
rcjb	Receive-Job
rd	Remove-Item
rdr	Remove-PSDrive
ren	Rename-Item
ri	Remove-Item
rjb	Remove-Job
rm	Remove-Item
rmdir	Remove-Item
rmo	Remove-Module
rni	Rename-Item
rnp	Rename-ItemProperty
rp	Remove-ItemProperty
rsn	Remove-PSSession
rsnp	Remove-PSSnapin
rv	Remove-Variable
rvpa	Resolve-Path
rwmi	Remove-WMIObject
sajb	Start-Job
sal	Set-
saps	Start-Process
sasv	Start-Service
sbp	Set-PSBreakpoint
sc	Set-Content
select	Select-Object
set	Set-Variable
si	Set-Item
sl	Set-Location
sleep	Start-Sleep
sort	Sort-Object

Alias	Commande équivalente
sp	Set-ItemProperty
spjb	Stop-Job
spps	Stop-Process
spsv	Stop-Service
start	Start-Process
sv	Set-Variable
swmi	Set-WMIInstance
tee	Tee-Object
type	Get-Content
where	Where-Object
wjb	Wait-Job
write	Write-Output

La plate-forme .NET

C

La plate-forme .NET (prononcez point net ou *dot net* en anglais) est un ensemble d'outils pour les développeurs de logiciels. Ce socle unique contient un très grand nombre de modules et d'API qui leur permet de développer des applications pour l'ordinateur ou bien des applications Internet.

Cette plate-forme existe réellement depuis les années 2000. Sa gamme de fonctionnalités ne fait que croître et s'impose peu à peu dans le monde de l'informatique. D'abord destiné à des applications de type Windows, la plate-forme .NET est portée sous Linux via le projet Mono, puis s'ouvre vers Internet tout d'abord grâce à l'ASP.NET, puis via SilverLight avant de s'intégrer aux systèmes d'exploitation. Mise en avant par Microsoft, cette plate-forme fait également l'objet d'un projet ambitieux destiné à créer un système d'exploitation entièrement basé sur .NET : le projet Midori.

Une architecture particulière

Plate-forme logicielle, .NET met en relation différentes applications et ressources, comme la communication entre le matériel de votre ordinateur et vos applications. Si cela ressemble au rôle tenu par votre système d'exploitation, les différences portent sur le fond. En effet, le processus de mise en relation a été facilité et les possibilités sont bien plus nombreuses, aboutissant à la création d'applications toujours plus complètes et proposant une meilleure expérience utilisateur (simplicité, rapidité, sécurité, etc.).

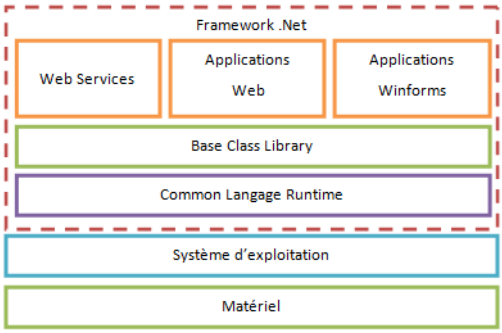


Figure C-1
Vue d'ensemble de .NET

EN SAVOIR PLUS Le projet Mono

Si vous souhaitez en apprendre plus sur la plate-forme Mono, l'équivalent libre de .NET pour la plate-forme Linux, rendez-vous à l'adresse suivante :

- http://www.mono-project.com

La plate-forme .NET s'appuie sur :

- une machine d'exécution basée sur la CLI (*Common Langage Infrastructure*) portable et surtout multi-langages ;
- la possibilité d'utiliser son langage de programmation préféré afin d'arriver au même résultat final ;
- un framework très complet comprenant des milliers de classes et fonctions toutes prêtes ;
- des protocoles de communication propres au framework .NET, tels que WCF (*Windows Communication Foundation*) ;
- des technologies d'interfaces applicatives évoluées telles que WPF (*Windows Presentation Foundation*) ou SilverLight pour les applications web ;
- une portabilité (Windows, Windows Mobile, UNIX/Linux via le projet Mono) ;
- une ouverture vers les autres technologies Microsoft (Windows Live ID, Windows Azure, etc.) ;
- des outils de développements comme Visual Studio.

Soit en résumé, la plate-forme de développement la plus plébiscitée du moment du fait des possibilités qu'elle apporte.

Un langage de développement pas comme les autres

La spécificité de .NET est son langage de programmation, ou plutôt, ses langages de programmation, pour être tout à fait exact. En effet, il met en œuvre des bibliothèques de classes et de fonctions (appelées *Base Class Library*) utilisables par différents langages tels que C#, VB.NET mais également Ada, APL, C++, Cobol, Eifell, Fortran, Haskell, ML, J#, Jscript, Mercury, Oberon, Objective Caml, Oz, Pascal, Perl, Python,

Scheme, SmallTalk, Visual Basic, et d'autres. Tous ces langages appliquent la spécification *Common Langage Specification* afin de respecter la norme CLI (*Common Langage Infrastructure*) qui décrit l'environnement d'exécution de la machine virtuelle .NET.

Ce rapprochement via la norme CLI permet aux différents langages de s'accorder sur les types de base (représentation d'un nombre, d'un nombre à virgule, d'une chaîne, d'un bit, etc.), de produire à partir d'un compilateur particulier un langage intermédiaire commun et identique pour tous. Ainsi, un même code, écrit en C# ou en C++ CLI, produit exactement le même code intermédiaire et a le même comportement, ce qui n'était jusqu'alors pas garanti avec les anciens langages existants.

Ce langage intermédiaire (CIL, *Common Intermediate Langage*) bytecode est alors compilé par un second compilateur CLR (*Common Langage Runtime*) afin de produire du code machine (01001011101). Les commandes décrites par l'application sont alors gérées par le système d'exploitation. Tout ceci se produit de manière entièrement transparente pour le développeur.

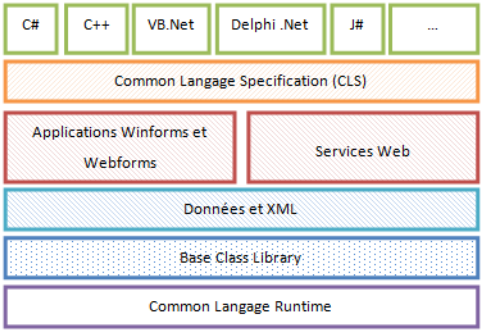


Figure C-2
Les différentes briques de .NET

Également appelées framework .NET, les bibliothèques de base de la plate-forme fournissent les éléments de base à la création d'applications évoluées. Si l'architecture n'a pas été modifiée depuis la création de la plate-forme, le framework évolue constamment, impliquant à chaque fois de nouvelles technologies.

Framework

La traduction littérale de ce terme est cadre de travail. Il s'agit d'un ensemble d'outils ou de modules qui doivent permettre au développeur de créer plus facilement ses applications tout en y adjoignant un maximum de fonctionnalités.

Des technologies innovantes

La plate-forme évolue vite : une nouvelle version sort tous les 18 mois en moyenne. Chaque nouvelle version apporte son lot de nouveautés ciblant d'une part les développeurs en leur permettant de développer toujours plus vite et plus facilement, et d'autre part les utilisateurs en

PRÉCISION **Version actuelle**

À l'heure où ce livre est mis sous presse, la version 4.0 est déjà en cours de développement.

proposant un pack de fonctionnalités complet que les développeurs n'ont plus qu'à intégrer au sein de leurs applications. Le tableau C-1 présente les grandes phases de l'évolution de .NET.

Tableau C-1 Nouveautés apportées par les différentes versions de .NET

Version	Nouveautés
Version 2.0	Support des plates-formes 64 bits. Contrôles web avancés améliorant les interfaces graphiques des applications web. Micro Framework, version allégée de la plate-forme utilisable sur des micropuces.
Version 3.0	Windows Presentation Foundation : nouvelles interfaces graphiques entièrement repensées. Windows Communication Foundation : système de communication avancé et plus sécurisé. Windows Workflow Foundation : permet la construction de processus métier à l'aide de workflows. Windows CardSpace : logiciel de gestion des identités utilisateur et des informations associées.
Version 3.5	Évolution des langages C# 3.0 et VB.NET 9.0. Nouveaux protocoles de communication d'applications pair-à-pair (*peer-to-peer*). API de synchronisation de données. API pour les fonctionnalités réseau en accès asynchrone.

Un avantage pour l'administrateur système

Sans le savoir, l'administrateur système bénéficie également de .NET. En effet, de plus en plus d'outils qu'il utilise ou tout simplement certaines parties du système d'exploitation sont basés sur cette plate-forme, puis des technologies comme PowerShell, présenté au cours de ce livre, peuvent également en tirer profit.

Index

64 bits 16, 19

A

ACL (Access Control List) 9, 104, 194, 288
ActiveX 97
adresse IP 184
adware 245
Aero 11, 13, 218
Aero Glass 16
affichage multiple 85
Agile VPN 13
alerte planifiée 299
alimentation 234
  portable 234
Allen, Paul 10
allocation 31, 106
  extensible 31
  fixe 31
analyse
  heuristique 248
  MSRT 249
  pare-feu 259
  Windows Defender 246
antivirus 248, 318
  méthode de fonctionnement 248
  MSRT 249
appareil photo 55
applet
  créer 322
  GUID 322
  icône 326
AppLocker 15, 17, 96, 97, 165
  configurer 98
  DLL 99
  programme système 100
assistance à distance 53, 314, 317
attribut 194
  étendu 194
audio 80
  configurer les périphériques 81
  sons Windows 83
  volume 80
audit
  accès aux fichiers
    paramétrer 200
    règle 201
authentification
  FTP 282
autorisations 194, 317
  FTP 288
  modifier 194, 199
  NTFS 194
  partage 206
Autoruns 225

B

base de registre 94
BCD (Boot Configuration Data) 33
bibliothèque 317
BitLocker 13, 17, 112, 113, 165
BitLocker To Go 14, 17, 115
Boot Loader 33
boot.ini 33
bootloader 49, 310
bootscreen 310
bot 245
BranchCache 13, 17
BSOD (Blue Screen of Death) 311
bureau à distance 53

C

cache 71, 277
  BranchCache 13
carte
  graphique 216
  réseau 183
    adressage IP 184
CCleaner 94, 318
CD-Rom 55
centre
  de maintenance 242, 296
  de mobilité 87
  de synchronisation 156
  réseau et partage 172, 210
certificat 259, 278
cheval de Troie 245
chiffrer
  clé USB 14
  disque
    externe 14
    interne 13
Cipher.exe 110
ClamWin 318
clavier 76
clé
  produit 25
  registre 317

USB 55
compte
administrateur 133, 136
créer 131
bloquer 132
console d'administration 130
mot de passe 132
partagé 132
utilisateur
créer 131
mot de passe 133
verrouiller 163
verrouiller 132
concentrateur 69
configuration minimale requise 24
Conseiller de mise à niveau 24
console
changer le mot de passe utilisateur 133
d'administration IIS 270
gestion 47
des disques 104
des journaux d'événements 306
des services Internet 280
des stratégies de sécurité locale 98
MMC 253
contrôle
à distance 316
parental 135
activer 136
application 138
avancé 140
Web 140
utilisateur 141, 244
niveau 143
principe 142
stratégie 144
CSS (Cascading Style Sheets) 269

D

date 46
defrag.exe 231
défragmenter 228, 317
démarrage 310
emplacement des applications 49
logiciel 317
options 53
paramétrer 48
problème 310
réparation 313
déni de service 14, 245
dernière bonne configuration connue 311
désinstaller Windows 35
DHCP 184
Direct Access 13
DirectX 13
DiskPart 106
disque
de base 104
défragmenter 230
dur
formater 27
non reconnu 27
partitionner 28
virtuel 25
dynamique 104, 107
limiter l'espace 159
mirroring 104
nettoyer 226
partition 105
quota 158
activer la gestion 158
bonnes pratiques 159
personnaliser 159
virtuel (VHD) 30
DLL 95, 99, 322
DNSSEC (Domaine Name System Security Extension) 14
document hors connexion 155
dossier public, partage 186
driver 9
driverquery 67
droits 9
AppLocker 15

E

Easy Connect 314
écouteur 306
écran
bleu 311
double 85
non détecté 87
résolution 86
édition de Windows 7 15
Entreprise 17
Familiale 16
Familiale Premium 16
Intégrale 18
Professionnelle 17
Starter 16
effet visuel 52
EFS (Encrypting File System) 9, 104, 110, 111
élévation de privilèges 327
ENIAC 9
espace disque
point de restauration 293
évaluation de l'ordinateur 50
exécution automatique 55, 56
exFAT 104, 106

F

FAT32 104, 107
fichier
audit d'accès 199
autorisations 194
d'échange 237
de pagination 237
hors connexion 153
hors ligne 154
partagé
cacher 205
propriétaire 194
synchroniser 156
temporaire 226, 318
version 157
versionné, prévisualiser 157
filtrage web 140
fonctionnalité Windows
ajouter 95
gestionnaire 95
force brute 132
framework .NET 276, 336
FTP (File Transfert Protocol) 279
authentification 282
autorisation 288
compte utilisateur 281
connexion passive 287
dossier racine 281
exploration des répertoires 283
filtre 283
groupe utilisateur 281
héritage d'autorisation 281, 288
isolation d'utilisateur 284
journal 284
règle 288
répertoire invisible 283

G

Gates, Bill 10
gestionnaire
de fonctionnalités Windows 95
de périphériques 53, 65

panneau Périphériques et imprimantes 71
groupe
administrateur 131
par défaut, supprimer 134
résidentiel
créer 188
mot de passe 188, 190
paramètres 189, 190
rejoindre 189
utilitaire de résolution des problèmes 191
utilisateur 194
créer 134
propriétés 134
GUID (Globally Unique Identifier) 35, 322
GUIDGEN.exe 323

H

hachage de fichier 99
HCL (Hardware Compatiblity List) 24
heure 46
histoire de Windows 10
Home 133
Home Group 12
HTML (Hypertext Markup Language) 269
éditeur 268

I

IIS (Internet Information Services) 266, 280
activer 266
image disque 149, 152
imprimante 71
connexion à une imprimante partagée 210
installer 73
modifier les propriétés 73
non USB 73
options avancées 74
par défaut 75
partager 209
pilote 73
spool 75
tester la configuration 74
Wi-Fi 212
index de stabilité 296
indexation des fichiers 118
indice de performance 217
consulter 217
installation
à partir de Windows XP 24, 26
complète standard 26
mise à niveau (depuis Windows Vista) 26
sur un disque virtuel (VHD) 30
installeur 92
interception de paquet 14
IP 184, 256
ipconfig 181
IPSec 165, 256

J

jeton 141, 144
journal 202, 244, 276, 284
aide à distance 315
audit d'accès aux fichiers 200
d'audit 164
d'événements 297, 300
abonnement 307, 309
applicatif 300
archiver 309
de performance 223
diagnostic 298
ordinateur distant 306
système 300
tâche automatique 303
tâche planifiée 308
taille du fichier 309
vide 308
vue filtrée 301, 308
pare-feu 260

K

Kompozer 268

L

lecteur
réseau 133, 154
Windows Media 55, 186
listener 306
live CD Windows 110
Live Mesh 156
localhost 268
log 297
logiciel
associer à un type de fichier 53
par défaut 53
logonscreen 310

M

malware 162, 244, 245, 317, 318
Master 229
mémoire 222
cache 235
diagnostic 313
physique 9, 216
swap 9
virtuelle 9, 52, 237
menu
contextuel
afficher le libellé Chiffrer 330
ajouter des fonctionnalités 329
personnaliser 328
rendre visible 330
démarrage
alternatif 310
réparer 33
Mes documents 133
MIME 278
mirroring 104, 109
mise à jour
appliquer 57
désinstaller 59
disponibilité 57, 58
effacer de la liste 59
fréquence 60
manuelle 57
niveau 58
paramétrer Windows Update 59
pilote 67
sélectionner 59
MKDIR 283
MMC (Microsoft Management Console) 167, 297
mode sans échec 310, 311, 312
modèle
créer 167
de sécurité
appliquer 169
base de données 168
tester 168
moindre privilège 141
moniteur
de fiabilité 296
de ressources 222
mot de passe 131, 163, 187, 188
MSConfig 225
msconfig.exe 48
MSDN (Microsoft Developer Network) 322
MS-DOS 10
MSRT (Malicious Software Removal

Tool) 249
multi-boot 33, 35

N

nom de l'ordinateur 53
NTBackup.exe 26
NTFS (New Technology File System) 9, 104, 106, 107, 158, 229
  autorisations 194
  sécurité 199

O

observateur d'événements 298
Orbe 34

P

panneau
  de configuration 40
    affichage 40
    personnaliser 40, 322
paramètres visuels 232
pare-feu 244, 250, 306, 307, 309
  administration 251
  connexion sécurisée 255
    règle 256
  console MMC 253
  FTP 287
  journal 260
  profil 251, 254
  programme autorisé 252
  règle 255
  trafic
    entrant 254
    sortant 255
partage
  assistant partage 203
  autorisations 206
  avancé 204
  dossier
    caché 205
    public 186
  fichier sur Internet 271
  invite de commandes 207
  permissions 206
  supprimer 207, 208
  voir les dossiers partagés 205
  web
    authentification 274
    filtrage 276
    journal 276
    visibilité des fichiers 272
partition 27, 318
  activer la protection 293
  compression 123
  créer 28
  étendre 28, 106
  format 106
  formater 27
  principale, ajouter 105
  redimensionner 106
  système de fichiers 107
  type 105
Path 53
Patterson, Tim 10
perfmon.exe 219
performances
  analyser 216
  en temps réel 221
  indice 217
  optimiser 232, 235
  système 216
périphérique 53
  démonter 70
  désactiver 67, 68
  installer 68, 71
  lister les pilotes installés 67
  mettre à jour les pilotes 67
  pilote 66, 67, 71
  plug and play 67
  problème 66
  USB, consommation 69
pilote 9, 312
  signature 64
planificateur de tâches 41
plug and play 67
point
  de montage 109
  de raccordement 66
  de restauration 148, 292
    espace disque 293
    forcer la création 293
    supprimer 228
  de sauvegarde
    restaurer 294
portable 79, 87
PowerShell 15
  alias 338
  commandes 337
  expression 341
  pipeline 339
  registre 344
  script 334
processeur 19
profil utilisateur 52, 132
Program Files 92
programme 92
  autoriser 139, 165
  bloquer 96
  démarrage 224, 225
  désinstaller 92
  indésirable 244
  installer 92
  non désinstallable 93
propriétaire (d'un fichier ou dossier) 198
protection du système 292

Q

quota utilisateur 104

R

raccordement 66
RAID-5 109
RAM (Random Access Memory) 9, 216
rapport d'activité 140
RDP (Remote Desktop Protocol) 13
ReadyBoost 235
récupération système 313
Recuva 148
redémarrage automatique 312
réécriture d'URL 276
registre 93, 94, 235, 292, 317, 318, 323, 325, 344
  nettoyer 94
  sous-clé 327
règle d'application 99
réseau
  imprimante 186
  nom SSID 176
  open 175
  partage 185
  statut 180
  VPN 176
    déconnecter 180
  Wi-Fi
    ajouter manuellement 175
    détecter 174
    difficulté de connexion 175
    état de la connexion 175
    modifier les paramètres 176
    renommer la connexion 182
    sécurité 174
restauration 292, 313
  point de sauvegarde 294
  recommandée 294
  sélective 294

rootkit 318

S

SACL (System Access Control List) 200
SafeGuard 15
sauvegarde 25, 148
  automatique 149
script
  ouverture de session 132
secpol.msc 166
sécurité 98, 110, 244
  connexion open 175
serveur
  DHCP 184
  FTP
    dossier racine 281
    pare-feu 287
    SSL 286
    variable utilisateur 286
  IIS 266
  impression 209
  web 95, 266, 271
    ajouter module 277
service 47, 49, 312
  en cours d'exécution 222
  FTP 280
  Internet, IIS 267
  partage
    activer 202
  Windows 343
SFC (System File Checker) 313
shadow copy 157
signature 99, 246, 248, 259
  pilote 64
snap-in 167, 297
son système 83
souris 77
  bouton, comportement 77
  pointeur 78
  roulette 79
Spybot 318
SpyNet 247
spyware 245
SRP (Software Restriction Policy) 97
SSL (Secure Socket Layer) 278, 281, 286
stabilité 298, 313
  index 296
stratégie
  compte utilisateur 144
  de droits
    utilisateur 163
  de groupe 17, 98
  de restriction logicielle 165
  de sécurité 162
    audit 164
    compte 162
    droits utilisateur 163
    secpol 166
    Windows 162
  locale 131, 143, 247
streaming 252
surface d'attaque 95
swap 9, 237
SysInternals 317
système
  d'exploitation, principe de fonctionnement 8
  de fichiers 9
    changer 107
  propriétés 50
  propriétés avancées 51

T

tâche planifiée 41
  créer 41
  déclencheur 42
  modifier 43
task-list 11
TCP (Transmission Control Protocol) 252
TechNet 322
tentative d'intrusion, détecter 164
type de fichier 54

U

UAC (User Account Control) 14, 141, 200, 327
UDP (User Datagram Protocol) 252
Ultimate Boot CD 318
UltraVNC 317
URL (Uniform Resource Locator) 268
  refusée 283
UsersPublic 186
usurpation d'identité 163
utilitaire de résolution des problèmes 72
  groupe résidentiel 191

V

versionner 149
VHD (Virtual Hard Disk) 30
vidéo projecteur 13, 84
virtual store 125
virtualisation 17
  virtual store 125
virus 49, 92, 141, 162, 241, 245, 248, 317
volume 80, 108
  agrégé par bande 108
  en miroir 109
  fractionné 108
  RAID-5 109
  simple 108
VPN (Virtual Private Network) 13, 176

W

W3C 266
WAMP 267
WEP (Wired Equivalent Privacy) 174
Wi-Fi 173
  ad hoc 175
WIM (Windows Image Format) 29
Windows Defender 244, 245
  analyse 246
  paramétrer 247
Windows Event Collector 307
Windows Management Instrumentation 334
Windows Search 119
Windows Update 57, 64, 67, 73, 244
  niveau des mises à jour 58
  paramétrer 57, 59
Windows Vista, Service Pack 1 26
Windows XP 25
Windows.old 25
winload.exe 33
WinRM (Windows Remote Management) 306, 307
WMI (Windows Management Instrumentation) 47, 306, 307, 341
WPA (Wi-Fi Protected Access) 174
WQL (WMI Query Language) 307

X

XPath 302