



<http://WWW.CABARE.NET> ©

Système Windows 7 Seven Sp1 – sys 20 – Cours -

Cours Système Windows 7 Seven Sp1

Michel Cabaré – Ver 2.3 – Juin 2011-

**Système Windows 7 – Seven Sp1
Cours**

Michel Cabaré – Ver 2.3 – Juin 2011

www.cabare.net ©

Ce Support a pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion de réseaux locaux

Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

En effet, **et c'est là sa vocation première**, ce document doit "**servir de support à la prise de notes en formation, et sera donc avantageusement complété par vos soins**". Son but est de permettre une présentation de vos notes plus structurée et donc plus facilement utilisable ensuite.

Bon Travail

Michel Cabaré

TABLE DES MATIÈRES

WINDOWS XP & SEVEN	8
POSITIONNEMENT DANS LA FAMILLE MICROSOFT :	8
DUREE DU SUPPORT CHEZ MICROSOFT :	9
FONCTIONNALITES SEVEN :	10
CONFIGURATION MATERIELLE	11
CONFIGURATION REQUISE :	11
HARDWARE COMPATIBILITY LIST :	11
QU' EST-CE QU'UN SERVICE PACK :	12
INSTALLER UN SERVICE PACK :	14
PATCHES:	14
CENTRE DE PROFIL MICROSOFT :	16
MBSA 2.2 GRAPHIQUE:	17
MBSA ET ANALYSE DISTANTE:	19
MBSACLI INVITE DE COMMANDE:	19
NOTIONS POUR INSTALLER SEVEN	21
FICHIERS D'INSTALLATION IMAGE - WIM :	21
LA HAL - HARDWARE ABSTRACTION LAYER	21
Sous Windows NT/2K/XP,	22
Sous SEVEN	22
LES CATEGORIES DE PARTITION SUR SYSTEME INTEL:	23
SYSTEME DE FICHIER NTFS :	25
INSTALLATION NOUVELLE/ M.A.J.	26
MISE A NIVEAU - INSTALL COMPLETE:	26
INSTALL COMPLETE DEPUIS DVD:	27
Paramètre régionaux :	27
Installer / Réparer	28
Licence	28
Mise à Jour / Installation Avancée	29
Création des Partitions	29
Copie des fichiers	30
Décompression des fichiers	31
Fin d'installation des fichiers	31
Assistant premier démarrage	31
WINPE 3.1	34
WINDOWS PREINSTALLATION ENVIRONMENT:	34
UTILISER WINDOWS PE LORS DE L'INSTALLATION SEVEN:	34
UTILISER UN MEDIA AMORÇABLE WINDOWS PE:	35
SÉQUENCE BOOT & MULTI-BOOT	36
BOOT XP & NTLDR:	36
BOOT SEVEN & BOOTMGR :	37
MULTI-BOOT SEVEN (BOOTMGR) - XP (NTLDR) :	38

BCDEDIT	39
BCDEDIT ET GESTION DU MAGASIN :	39
<i>Sauvegarde du magasin complet :</i>	39
<i>Structure du magasin:</i>	40
BCDEDIT COMMANDE :	41
<i>Copier-Dupliquer une entrée du magasin:</i>	42
<i>Supprimer une entrée du magasin:</i>	42
BCDEDIT ET GESTIONNAIRE DE DEMARRAGE – BOOT MANAGER :	42
<i>Système par défaut:</i>	43
<i>Time-out:</i>	43
<i>Forcer l’affichage du menu de boot:</i>	43
BCDEDIT ET CHARGEUR DE DEMARRAGE – BOAT LOADER :	44
<i>Renommer une entrée :</i>	44
BCDEDIT ET CHARGEUR ANCIEN SYSTEME – LEGACY BOAT LOADER :	45
<i>Renommer une entrée :</i>	45
BCDEDIT OPTION /STORE :	45
UTILITAIRE BOOTSECT & CHANGEMENT BCDEDIT / NTLDR:	46
INSTALLER SEVEN A COTE DE XP (MULTI-BOOT).....	46
<i>même disque, autre partition :</i>	46
<i>autre disque :</i>	46
INSTALLER XP A COTE DE SEVEN.....	47
SUPPRIMER UN BOOT SEVEN (RETOUR BOOT XP):	48
SUPPRIMER UN BOOT XP (RETOUR BOOT SEVEN):	49
LES PROCESSUS SOUS SEVEN	51
SEQUENCE POST : POWER ON SELF TEST	51
SEQUENCE DEMARRAGE BOOTMGR.....	51
VOCABULAIRE SYSTEME SOUS SEVEN :	52
LISTER LES PROCESSUS EN COURS :	53
<i>Interface classique graphique:</i>	53
<i>Tasklist (SEVEN - XP):</i>	54
<i>Taskkill (SEVEN - XP):</i>	55
QUELQUES PROCESSUS DE BASE	55
GESTIONNAIRE DE SERVICES.....	55
DRIVERS.....	57
LES ANCIENS TYPES VXD - SYS - WDM :	57
LES DRIVERS VISTA SEVEN WDF :	58
MAGASIN DE DRIVERS :	58
<i>Mise en place du pilote dans le magasin.....</i>	59
<i>Installation du pilote lors du P&P par SEVEN.....</i>	59
STRATEGIES DE GESTION DE DRIVERS :	59
DRIVERS CERTIFIES :	60
INSTALLATION DE PILOTES NON CERTIFIES :	60
GESTIONNAIRE DE PERIPHERIQUE:	61
VERSIONS - INSTALLATION DE PILOTES :	61
INSTALLATION DRIVER VIA UPDATE :	62
INSTALLATION DRIVER VIA FICHIERS LOCAUX :	62
METHODE PAR DEFAUT INSTALLATION DE DRIVERS :	65
SIGVERIF VERIFICATION DRIVERS SIGNES:	65
DRIVERQUERY VERIFICATION DRIVERS SIGNES:.....	67
INTÉGRITÉ SEVEN.....	68
LES DLL (DYNAMIC LINK LIBRARIES) :	68
WRP PROTECTION DES DLL :	68
<i>sfc - system file checker</i>	69

UAC- USER ACCOUNT CONTROL	70
OBJECTIF VISE :	70
IL – INTEGRITY LEVEL :	70
DESACTIVATION DE L'UAC (Panneau de configuration):	72
GESTION DE L'UAC (STRATEGIES LOCALES):	73
<i>Désactivation de l'UAC :</i>	<i>73</i>
<i>Désactivation de l'UAC pour les Administrateur :</i>	<i>73</i>
<i>Désactivation l'UAC pour les Utilisateurs :</i>	<i>73</i>
<i>Activation l'UAC pour le compte Administrateur Root :</i>	<i>73</i>
INSTALLATIONS ET VIRTUALISATION.....	75
PRECONISATION MICROSOFT :	75
VIRTUALISATION DES PROCESSUS :	75
COMPATIBILITE AVANT SEVEN	77
EXECUTER EN MODE COMPATIBILITE:	77
INSTALLER EN MODE COMPATIBILITE:.....	77
PROTECTION DEP	78
PRINCIPE DEP DATA EXECUTION PREVENTION:.....	78
DESACTIVATION COMPLETE DE DEP :	78
DESACTIVATION POUR UNE APPLICATION DE DEP :	78
WINDOWS RE (CONSOLE DE RECUPERATION).....	80
WINDOWS RECOVERY ENVIRONNEMENT:	80
DEMARRER L'ENVIRONNEMENT DE RECUPERATION WINRE:.....	81
ETAPE 1 SEQUENCE POST – BARRE DE PROGRESSION	82
<i>Problèmes hardware</i>	<i>82</i>
<i>Problèmes partition- mbr-fichiers manquants</i>	<i>83</i>
ETAPE 2 BARRE DE PROGRESSION AVANT SESSION	83
ETAPE 3 APRES L'OUVERTURE DE SESSION	84
WINDOWS RE INVITE DE COMMANDE	85
INVITE DE COMMANDE:	85
MODIFIER LES PARTITIONS - UTILITAIRE DISKPART	86
SHRINK DISKPART – REDUIRE UNE PARTITION.....	86
EXTEND DISKPART – ETENDRE UNE PARTITION	87
CD REPARATION – VS CONSOLE.....	88
CREATION CD DE REPARATION	88
OPTIONS DE DEMARRAGE – F8	89
DEMANDER F8 LORS DU DEMARRAGE :	89
REPARER SANS REINSTALLER.....	91
REINSTALLER LE SYSTEME :	91
REINSTALLER COMPLETEMENT.....	93
REINSTALLER LE SYSTEME :	93

LA RESTAURATION SEVEN	94
PRINCIPE RESTAURATION - DESACTIVATION-	94
DESACTIVATION DE LA RESTAURATION	94
CREATION D'UN POINT DE RESTAURATION	95
UTILISER ANNULER UN POINT DE RESTAURATION	95
TYPES DE POINT DE RESTAURATION	96
PARAMETRAGES DES POINT DE RESTAURATION : VSSADMIN	97
SAUVEGARDE SYSTEME - FICHIERS	98
DEUX OUTILS DE SAUVEGARDE :	98
IMAGE SYSTEME - VHD :	98
AUTOMATISER VIA WBADMIN	100
REALISER UNE RESTAURATION INTEGRALE SYSTEME	100
REALISER UNE SAUVEGARDE FICHIERS-	102
REALISER UNE RESTAURATION DE FICHIERS-	104
COMPTES UTILISATEURS	105
COMPTE D'UTILISATEURS – SESSION:	105
CONNEXION MULTIPLES UTILISATEUR	106
SID SECURITY IDENTIFIER :	108
WHOAMI :	108
COMPTES PRE-DEFINIS :	109
EXECUTER EN TANT QUE:	109
UTILISATEURS LOCAUX:	109
GESTION DES COMPTES:	110
RE-DEFINITION DE MOT DE PASSE	111
DESACTIVER LA BASCULE RAPIDE UTILISATEUR	107
CACHER LE DERNIER UTILISATEUR	111
GROUPE LOCAUX	112
NOTIONS DE GROUPE :	112
GROUPE LOCAUX PREDEFINIS :	112
PROFILS UTILISATEURS	113
LIENS SYMBOLIQUES – RACCOURCIS – JONCTIONS :	113
OBJECTIF :	113
PROFIL LOCAL:	114
EMPLACEMENT PROFILS LOCAUX SEVEN:	114
STRUCTURE DES PROFILS SEVEN:	115
STRUCTURE D'UN PROFIL UTILISATEUR	116
PROFIL PAR DEFAULT	117
<i>Méthode Certifiée pour modifier le profil par défaut.....</i>	<i>117</i>
<i>Méthode Non Certifiée pour modifier le profil par défaut</i>	<i>117</i>
PROFIL PUBLIC	119
SUPPRIMER TOUS LES PROFILS LOCAUX SEVEN:	120
INTERFACE SEVEN – XP/2000.....	121
RETROUVER L'INTERFACE XP 2000:.....	121
<i>Menu Démarrer (modification organisationnelle):.....</i>	<i>121</i>
<i>Panneau de configuration (modification organisationnelle):</i>	<i>122</i>
<i>Aspect des fenêtres (modification esthétique):</i>	<i>122</i>
L'EXPLORATEUR WINDOWS:	123

AERO – PERFORMANCES SEVEN	125
INTERFACE AERO:	125
NOTE SEVEN:.....	126
COMPROMIS PERFORMANCES :.....	127
MESSAGES DU CENTRE DE MAINTENANCE :	127
SLMGR – ACTIVATION LICENCE	128
INSTALLER SEVEN SANS CLE:.....	128
REACTIVER SEVEN - UTILITAIRE SLMGR:	128
<i>Réactivation période de grâce.....</i>	<i>129</i>
TRANSFERT – RE-SAISIE LICENCE:	130
SAISIE LICENCE SLUI 3:.....	130
INCLASSABLES DE SEVEN.....	131
MENU ETENDUS (INVITE DE COMMANDE):	131
OPTIONS DEMARRAGE MSCONFIG.EXE :	131
OUTILS DXDIAG:	133
OUTILS MSINFO32:	133
OUTILS SHUTDOWN:	134
WHOAMI:	135
CONSOLE MMC.....	136
MICROSOFT MANAGEMENT CONSOLE:	136
CREER UNE CONSOLE PERSONNALISEE:	136
LIMITER LES FONCTIONS D’UN COMPOSANT LOGICIEL :.....	138
ENREGISTRER LA CONSOLE UTILISATEUR :.....	139
ANNEXE : ECRAN BLEU.....	140
LES ECRANS BLEU – ERREUR KERNEL DE DEMARRAGE:.....	140
LES ECRANS BLEU "ALEATOIRES":	140
WINDG" INSTALLATION ET PARAMETRAGE	141
FICHER MINI-DUMP.....	142
REMONTER UNE ERREUR	142
GENERER UN BSOD	144
SYSPREP	145
VERSIONS DE SYSPREP:	145
SYSPREP 3.14 POUR SEVEN-2008:	145
SYSPREP MODE GRAPHIQUE:	146
SYSPREP /GENERALIZE:	146
MINI INSTALLATION PASSE OOBE:	147
SYSPREP /UNATTEND:C:\FICHER.XML:	147
SYSPREP /UNATTEND COPYPROFILE	148
ACTIVATION ET SKIPREARM	149
EXEMPLE DE FICHER DE REPONSE	149

WINDOWS XP & SEVEN

Positionnement dans la famille Microsoft :

Une fois mis de côté MsDOS (jusqu'à la version 6.22 de 1994) et Windows (jusqu'à la version 3.10) deux fonctions ont été ajoutés aux systèmes d'exploitation personnels microsoft, la gestion intégrée de la notion de réseaux poste à poste, (windows workgroup 3.11), et une structure multi-tâche écrite en code 32 bits (Windows 95)

- système d'exploitation personnel polyvalent et facile à administrer, mais non sécurisé, on utilisera Windows 9.x... :
 - ✓ **3.11** wrkgrp en 1993 extension workgroup
 - ✓ **95** en aout 1995 intégration Tcp/Ip (et ses mises à jours telles que 95OSR1, 95 OSR2, 98, 98 SP1, 98 SE et «millenium» !)

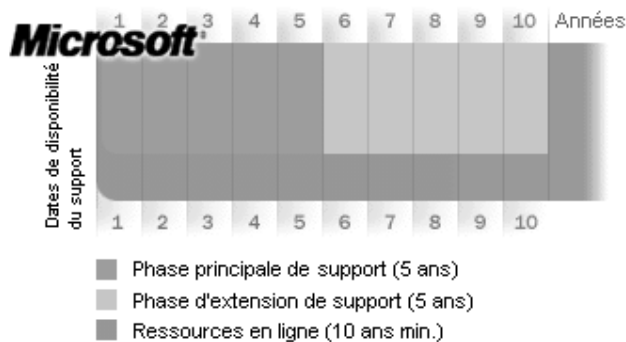
Puis, dans la lignée de windows 9.x **au niveau de l'interface**, mais **radicalement différentes au niveau du code**, baptisées de **NT** pour "New Technologie" pour les démarquer de ce qui existait précédemment :

- système d'exploitation 32 bits multi-tâche, **WINDOWS NT**:
 - ✓ **4.0** en juillet 96 : Version Workstation et Server
01/01/2005 : arrêt complet du support
- Une mise à jour majeure du système d'exploitation **Windows 2000**:
 - ✓ **5.0** dit **2000** en fév 2000 Version Pro, Server, Advanced Server
16/06/2003 : arrêt complet du support
 - Une mise à jour **Windows XP**: starter, familiale, pro, intégrale
 - ✓ **5.1** en sept 2001 Professionnel, Home, Embedded
08/04/2014 : arrêt complet du support
- Une mise à jour majeure du système d'exploitation dit **Vista**:
 - ✓ **6.0** en janvier 2007 dit **Vista**, Version Home Basic, Home Premium, Business-Pro, Business-Enterprise, (Ultimate...)
Une mise à jour **7 - Seven**: starter, familiale, pro, intégrale
 - ✓ **6.1** en octobre 2009 ...
Une mise à jour **Windows - 8**: RT, 8, pro, entreprise
 - ✓ **6.2** en octobre 2012 ...

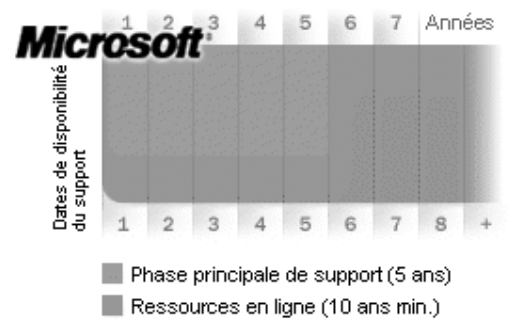
Durée du support chez Microsoft :

Grosso modo, 5 ans pour Seven Family, et 10 ans pour Seven Professionnel

Logiciels Entreprise et développement



Grand public/Matériel/Multimédia



La phase principale de support inclut :

- Support à l'incident (assistance utilisateur, support payant, garantie)
- Support pour les mises à jour de sécurité
- La possibilité de faire des demandes de hotfixes hors sécurité

N.B: La durée de la phase principale de support est de 3 ans au minimum pour les produits

La phase d'extension de support inclut :

- Support payant
- Support pour les mises à jour de sécurité, sans frais additionnels
- Support des hot-fixes non relatifs à la sécurité nécessite la souscription à une extension de contrat de support spécifique. Un paiement au correctif peut aussi s'appliquer.
- Pas de demandes de support gratuit, de changements de code ou de nouvelles fonctionnalités durant la phase d'extension de support.

Systèmes d'exploitation d'ordinateur	Dernier Service Pack	Fin du support standard	Fin du support étendu
Windows XP	Service Pack 3	14 avril 2009	8 avril 2014
Windows Vista	Service Pack 2	10 avril 2012	11 avril 2017
Windows 7	Service Pack 1	12 janvier 2015	14 janvier 2020

Fonctionnalités Seven :

Les éditions **N** de Windows 7 sont identiques aux éditions standard, à l'exception du Lecteur Windows Media et des technologies associées (Windows Media Center ou Création de DVD)

Pour pouvoir utiliser **Windows XP Mode**, vous devez le préinstaller dans une version OEM ou le télécharger. Windows XP Mode fonctionne uniquement sur les versions Professionnel et Intégrale de Windows 7, et utilise la technologie de virtualisation, Virtual PC. Vous pouvez télécharger à la fois Windows XP Mode et Windows Virtual PC.

Les versions sont starter, familiale, pro, intégrale

La différence entre les versions Pro (business) et intégrale se résume aux fonctionnalités suivantes :

- Pack Multilingue
- BitLocker

CONFIGURATION MATERIELLE

Configuration requise :

Voilà les données pour une utilisation de **Seven**

- Un processeur 32 bits (x86) ou 64 bits (x64) de 1 gigahertz (GHz) ou plus rapide
- Une RAM de 1 gigaoctet (Go) (32 bits) ou de 2 Go (64 bits)
- Un espace disque disponible de 16 Go (32 bits) ou de 20 Go (64 bits)
- Un périphérique graphique DirectX 9 avec un lecteur WDDM 1.0 ou supérieur

N.B: Le Mode Windows XP requiert une RAM supplémentaire de 1 Go, un espace disque supplémentaire de 15 Go et un processeur permettant une virtualisation du matériel avec Intel VT ou AMD-V activé dans le BIOS...

Et voilà un rappel les données pour une utilisation de **Vista-Seven**

7 Capable	7 Ready	En pratique
Proc type P4 minimum 800 Mghz	Proc type P4 minimum 1 Ghz	
512 Mg de RAM	1 Giga de RAM	
Vidéo DirectX 9.0	Vidéo DirectX 9.0 - pilote WDDM – 128 MB ram	Vidéo DirectX 10.0 - pilote WDDM – 256 MB ram
6 Giga libres DD	15 Giga libres DD	

Hardware Compatibility List :

Dans Seven (mais depuis NT), les applications ne peuvent accéder directement au matériel car c'est lui qui contrôle directement l'intégralité du HARD, c'est pour cette raison que SEVEN à priori ne **supporte** aucun driver non certifié, et qu'il est impératif de vérifier avant toute installation que tout le matériel (y compris les cartes vidéo, cartes réseau, lecteur de CD-ROM, disques ...) soit référencé dans la HCL

Désormais les listes Windows 7 et 8 sont disponibles

<http://www.microsoft.com/fr-fr/windows/compatibility/win7/CompatCenter/Home>



Lorsque l'on fait une recherche, on peut obtenir

 L'icône « **Compatible** » signifie que le produit est conçu pour fonctionner avec Windows 8, Windows RT ou Windows 7. En règle générale, vous n'aurez rien à faire pour garantir la compatibilité, et la mention « Aucune action requise » s'affichera sous « Compatible » sur la page de détails du produit. En revanche, si un fabricant ou un éditeur propose une version plus récente ou requiert un logiciel supplémentaire, vous trouverez un lien supplémentaire vers le site Web de l'éditeur.

 L'icône d'avertissement « **Action recommandée** » indique que vous devez peut-être trouver une solution pour assurer la compatibilité d'un produit avec Windows. La plupart du temps, une mise à niveau gratuite est disponible, mais certains éditeurs peuvent requérir une mise à niveau payante pour l'obtention de la dernière version. Dans les deux cas, vous trouverez sous « Action recommandée » un lien vers le site Web de l'éditeur.

 L'icône « **Non compatible** » signifie que le produit n'est pas compatible ou n'est pas conçu pour fonctionner avec Windows. Vous pouvez ces [étapes de dépannage de compatibilité](#) ou visitez le [forum Communauté Microsoft](#) pour obtenir des conseils supplémentaires dans la communauté.

 La certification « Compatible - Windows 8 » signifie que le produit satisfait les exigences en matière de test de Microsoft pour la compatibilité avec Windows 8 64 bits et 32 bits. Pour obtenir le logo « Compatible avec Windows 8 », les logiciels et matériels doivent réussir des tests d'installation, de performances, de fiabilité et de sécurité conçus par Microsoft de manière à garantir leur compatibilité avec Windows 8.

 La certification « Compatible - Windows 8 et Windows RT » signifie que le produit satisfait aux exigences des tests de Microsoft pour la compatibilité avec Windows 8 et Windows RT. Pour obtenir le logo « Compatible avec Windows 8 et Windows RT », les périphériques doivent réussir des tests d'installation, de performances, de fiabilité et de sécurité conçus par Microsoft de manière à garantir leur compatibilité avec Windows 8 et Windows RT.

 La certification « Compatible - Windows 7 » signifie que le produit satisfait les exigences en matière de test de Microsoft pour la compatibilité avec Windows 7 64 bits et 32 bits. Pour obtenir le logo « Compatible avec Windows 7 », les logiciels et matériels doivent réussir des tests d'installation, de performances, de fiabilité et de sécurité conçus par Microsoft de manière à garantir leur compatibilité avec Windows 7.

à noter que beaucoup de matériels restent simplement « compatible » et non pas certifiés...

Qu'est-ce qu'un Service Pack :

Dans un premier temps on installe Windows mais il faut ensuite impérativement appliquer le service pack existant faute de quoi le fonctionnement correct peut être gravement compromis

IL NE S'AGIT PAS DE CORRECTION MINEURES, MAIS SOUVENT D'IMPÉRATIF FONCTIONNELS !

Sans rentrer dans le détail des listes d'erreurs corrigés par ces services packs, il reste à dire que normalement

2000 livré 02/2000	5.00.build 2195	SP4 final juin 2003
XP livré 09/2001	5.10.build 2600	SP3 final mai 2008
Vista livré 01/2007	6.00.build 6000	SP2 final mai 2009
Seven livré 07/2009	6.10.build 7600	SP1 mars 2011 build 7601
8 livré 10/2012	6.20.build 9200	SP1 à venir

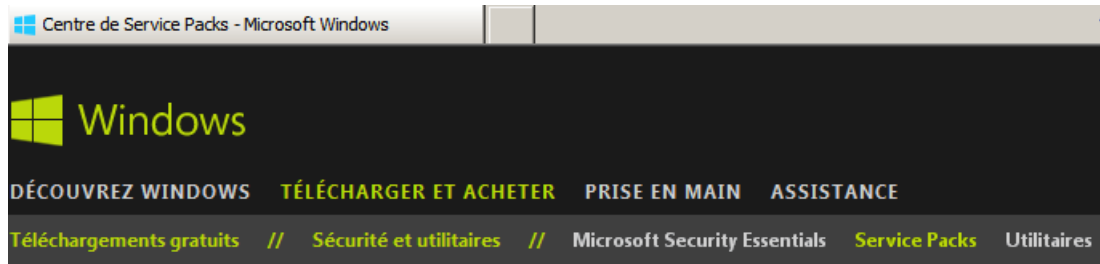
On peut vérifier quel service pack est correct, effectuer une recherche sur internet avec « Service Pack Windows » et par exemple on trouve

Centre de Service Packs - Microsoft Windows

windows.microsoft.com > ... > Microsoft Security Essentials

Découvrez les **Service Packs** Windows et téléchargez les derniers SP pour ... **Service Packs** consiste à activer Windows Update pour Windows 8, **Windows 7** et ...

Ce qui donne



Centre de Service Packs

Procurez-vous le dernier Service Pack pour votre version de Windows

Un Service Pack (SP) est une mise à jour de Windows, combinant souvent des mises à jour déjà parues, qui vient renforts fournis gratuitement* sur cette page, peuvent contenir des améliorations en matière de sécurité et de performances, matériel. Veillez à installer le dernier Service Pack afin de maintenir votre version de Windows à jour. Environ 30 minutes vous devrez redémarrer votre ordinateur vers le milieu de l'installation.

Le moyen recommandé (et le plus facile) pour se procurer des Service Packs consiste à activer **Windows Update** pour **Mises à jour automatiques** pour Windows XP. Windows vous avertira lorsque les Service Packs dont vous avez besoin jour automatique est une opération simple et rapide qui peut vous faire gagner du temps et économiser de l'espace.

Apprenez à identifier la version de Windows et du Service Pack que vous possédez

Windows 8 **Windows 7** **Windows Vista** **Windows XP**

Et on peut télécharger

Résumé

Version : 976932 Date de publication : 15/03/2011
Modifier la langue : Français

Articles de la Base de connaissances : [KB976932](#)

Fichiers contenus dans ce téléchargement

Les liens figurant dans cette section correspondent aux fichiers disponibles pour ce téléchargement. Téléchargez les fichiers qui vous conviennent.

Nom du fichier	Taille
7601.17514.101119-1850_Update_Sp_Wave1-GRMSP1.1_DVD.iso	1.9 GB

TÉLÉCHARGER

N.B : Si on ne peut plus faire de « slimstream », on peut télécharger une version incorporant directement le Service Pack.

Installer un Service Pack :

Il faut de l'espace disque car le programme **Update.exe** crée une copie des fichiers modifiés dans **\$NTServicepackUninstall\$,** sous **%systemroot%.** :

Cela nécessite dans le pire des cas, 7500 Méga!

Espace disque nécessaire pour Windows 7 SP1

Méthode d'installation	Estimation de l'espace disque requis
Windows Update	La mise à jour automatique nécessite un espace disque minimal et elle est recommandée pour obtenir Windows 7 SP1. • 32 bits (x86) : 750 Mo • 64 bits (x64) : 1050 Mo
Téléchargement de Windows 7 SP1 à partir du site Web Microsoft	Vous pouvez également télécharger Windows 7 SP1 à partir du site Web Microsoft. Cette méthode nécessite plus d'espace disque qu'en utilisant Windows Update. • 32 bits (x86) : 4 Go • 64 bits (x64) : 7,2 Go

Espace disque nécessaire pour Windows Server 2008 R2 SP1

Méthode d'installation	Estimation de l'espace disque requis
Windows Update	La mise à jour automatique nécessite un espace disque minimal et elle est recommandée pour obtenir Windows Server 2008 R2 SP1. • 32 bits (x86) : 850 Mo • 64 bits (x64) : Non disponible
Téléchargement de Windows Server 2008 R2 SP1 à partir du site Web Microsoft	Vous pouvez également télécharger Windows Server 2008 R2 SP1 à partir du site Web Microsoft. Cette méthode nécessite plus d'espace disque qu'en utilisant Windows Update. • 32 bits (x86) : 3,5 Go • 64 bits (x64) : 7,2 Go

Patches:

Si on peut raisonnablement installer les services packs au fur et à mesure de leur sortie (environ tous les 6-10 mois), cela n'empêche pas la sortie d'autres "patches" ou type de mises à jour :

- les **Hot Fixes** : qui sont des correctifs très spécifiques accessibles uniquement après traitement d'un incident auprès du support technique.
- les **Patches** : qui sont des correctifs ponctuels de bug ou de défaillance aillant fait l'objet d'un patch particulier et isolé uniquement pour ce problème

Il est possible d'être informé un peu à l'avance de la sortie des Mises à jours et patches via une lettre d'information via le centre

<http://www.microsoft.com/france/core/newsletters.aspx>

Newsletters de Microsoft France

Vous êtes novice ou expert ? Revendeur ou utilisateur ? Professionnel ou particulier ? Parmi les **newsletters diffusées** par Microsoft France, il y en a forcément **une qui vous correspond** et qui vous aidera à mieux utiliser vos logiciels :

Newsletter France

Newsletter produits

Newsletters professionnels de l'informatique

Newsletter pour l'éducation

Newsletter entreprise

Toutes les newsletters

Un identifiant **passport microsoft** peut être nécessaire...


Windows Live ID

Connexion à Site Web Windows Live ID

Aide

Adr. de messagerie :

Mot de passe :

[Mot de passe oublié ?](#)

Connexion

Connexion

Connectez-vous maintenant pour consulter ou modifier les paramètres de votre compte.

Pour vous connecter au site à partir duquel vous avez cliqué sur le lien Espace Utilisateurs, cliquez sur le bouton Précédent de votre navigateur, puis connectez-vous.

Liens

- [Ouvrir un compte](#)

Puis on gère ses inscriptions...

2 lettres sont particulièrement intéressantes :

TechNet



Newsletter TechNet

Ce bulletin est une synthèse de l'actualité TechNet, la source d'information technique de référence pour évaluer, déployer et supporter les produits Microsoft.

Toutes les deux semaines | [Inscription à la Newsletter TechNet](#) | [Un exemplaire de la Newsletter TechNet](#)

Alertes de Sécurité



Alertes de sécurité

Recevez les synthèses des bulletins de sécurité Microsoft (en anglais). Elles présentent les dernières failles de sécurité découvertes, les risques encourus ainsi que les solutions pour y remédier.

Dès qu'une alerte se présente | [Inscription aux bulletins de sécurité](#)

Donnant ensuite la possibilité de s'inscrire

Microsoft

France

Modifier

Centre de Sécurité

Protection du PC, de la vie privée et de la famille

Accueil | **Sécurité** | Confidentialité | Sécurité familiale | Ressources

Mises à jour

Newsletter Sécurité

Comment...

- Obtenir un outil ou une mise à jour de sécurité
- Mises à jour de sécurité
- Logiciel anti-virus, anti-espion gratuit
- Analyse gratuite de

Lettres d'information et alertes Sécurité Microsoft

Retrouvez chaque mois les dernières informations et ressources techniques pour vous aider à sécuriser vos infrastructures et applications.

Bulletins et Avis de sécurité Microsoft



Bulletins de sécurité
 Recevez par message électronique la synthèse des articles techniques présentant les dernières mises à jour et solutions pour s'en protéger.





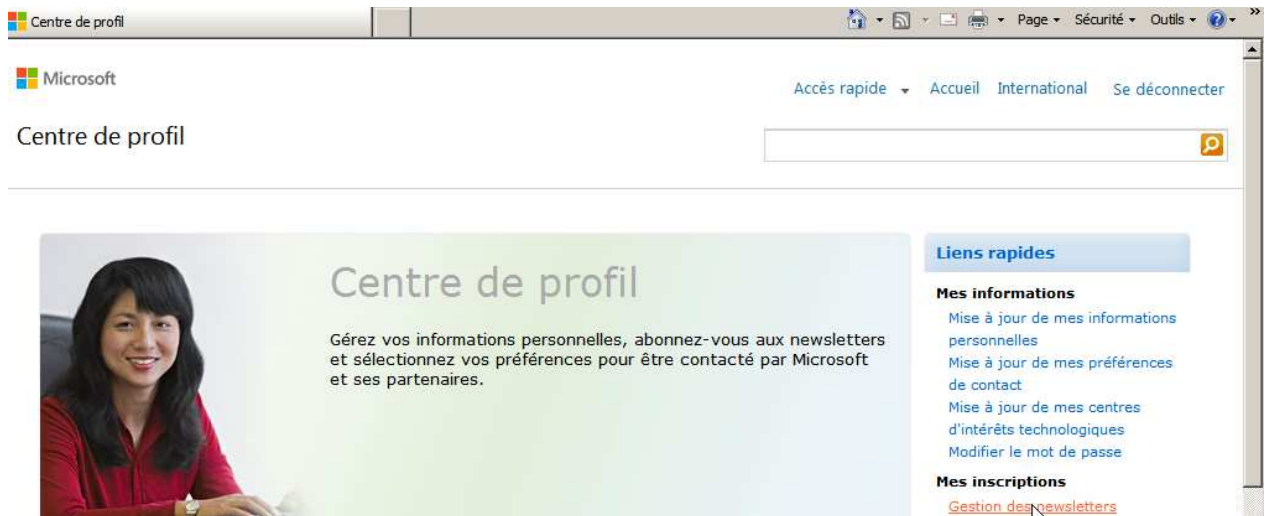
Système Windows 7 - Seven
- Cours - ver 2.3 -

<http://www.cabare.net> Page 15
- Michel Cabaré -

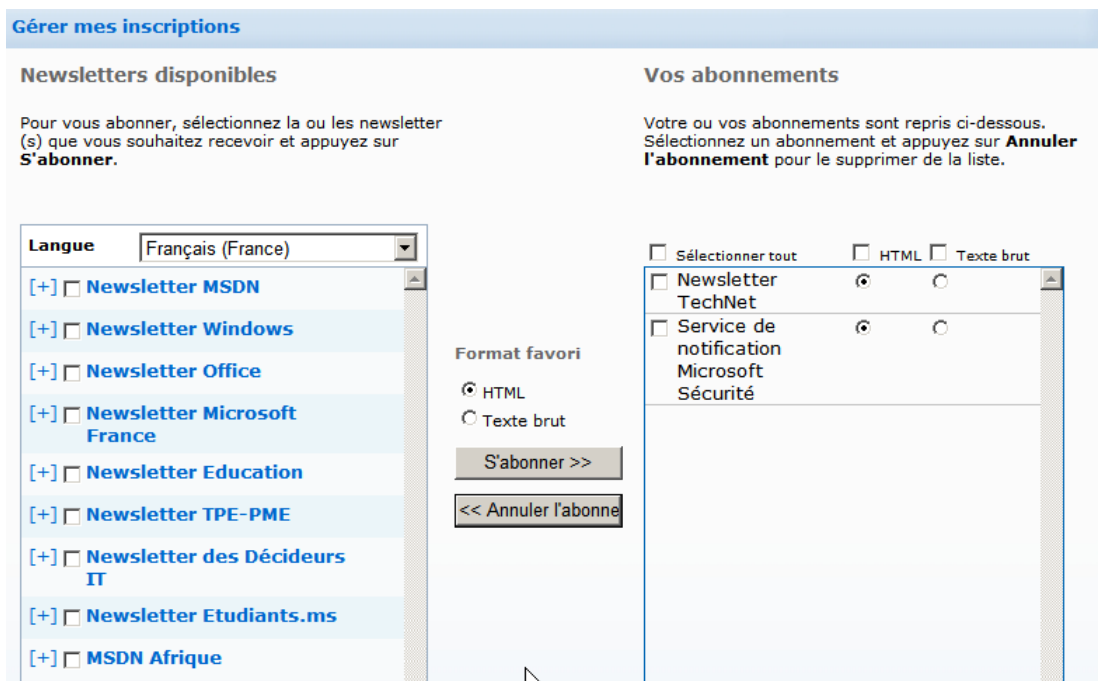
Centre de profil Microsoft :

Une autre manière d'accéder à l'information est de se créer un profil Microsoft, donnant ensuite la possibilité de s'inscrire globalement sur des newsletters.

On fait une recherche avec « profil microsoft » et on peut se logger avec un compte Passeport Microsoft – Microsoft Live



Dans les inscriptions, on demande ensuite Technet et Notification Sécurité.



MBSA 2.2 graphique:

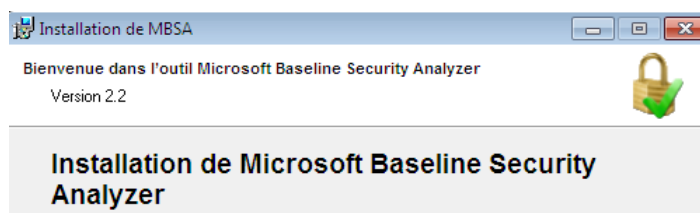
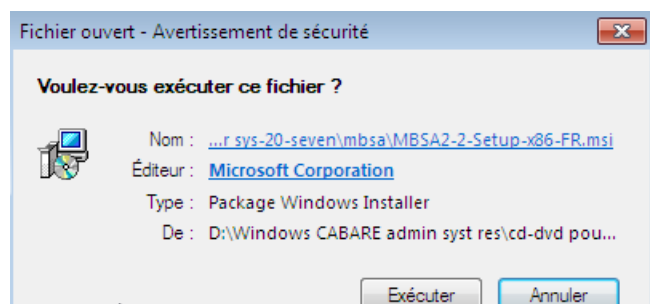
Microsoft Baseline Security Analyzer 2.2 (for IT Professionals) - Français

MBSASetup-x64-FR.msi	1.7 Mo	Télécharger
MBSASetup-x86-FR.msi	1.6 Mo	Télécharger
MBSASetup-x86-JA.msi	1.6 Mo	Télécharger

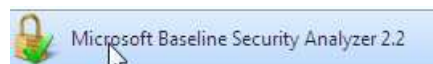
Résumé

Version: 2.2
Date de publication : 06/08/2010
Langue : Français [Modifier](#)

Il faut donc exécuter ce fichier...



La version 2.2 de MBSA comprend une interface graphique



qui peut effectuer l'analyse locale de systèmes Windows SEVEN



Peu de réglages sont indispensables à ce niveau

Quel ordinateur voulez-vous analyser ?

Entrez le nom de l'ordinateur ou son adresse IP.

Nom de l'ordinateur : (cet ordinateur)

Adresse IP :

Nom du rapport de sécurité :

%D% = domaine, %C% = ordinateur, %T% = date et heure, %IP% = Adresse IP

Options :

- ☒ Rechercher les vulnérabilités d'administration de Windows
- ☒ Rechercher les mots de passe vulnérables
- ☐ Rechercher les vulnérabilités d'administration de IIS
- ☐ Rechercher les vulnérabilités d'administration de SQL
- ☒ Rechercher les mises à jour de sécurité
- ☐ Configurer les ordinateurs pour Microsoft Update et la configuration minimale requise pour les analyses
- ☐ Options avancées des services de mise à jour :
 - ☐ Analyser en n'utilisant que les serveurs Windows Server Update Services(WSUS) assignés
 - ☐ Analyser en n'utilisant que Microsoft Update
 - ☐ Analyser avec le catalogue hors connexion uniquement

Après téléchargement d'une base de signature depuis le site de microsoft,
Une analyse est rendue



Détails du rapport pour WORKGROUP - TEST-PC (2010-02-23 09:13:08)



Évaluation de la sécurité :
Risque important (Un ou plusieurs tests critiques ont échoué.)

Nom de l'ordinateur : WORKGROUP\TEST-PC
Adresse IP : 192.168.1.201
Nom du rapport de sécurité : WORKGROUP - TEST-PC (23-02-2010 09:13)
Date d'analyse : 23/02/2010 09:13
Analysé avec MBSA version : 2.1.2112.0
Date de synchronisation du catalogue :
Catalogue des mises à jour de sécurité : Microsoft Update

Un résultat est donné avec des indications sur les actions éventuelles

Résultats de l'analyse des mises à jour de sécurité

Score	Catégorie	Résultat
	Windows - Mises à jour de sécurité	9 mises à jour de sécurité sont absentes. 4 Service Packs ou correctifs cumulatifs sont absents. Afficher les ressources analysées Détails Comment corriger le problème
	Office - Mises à jour de sécurité	1 Service Packs ou correctifs cumulatifs sont absents. Afficher les ressources analysées Détails Comment corriger le problème
	SQL Server - Mises à jour de sécurité	Aucune mise à jour de sécurité n'est absente. Afficher les ressources analysées Détails

On peut quasiment se laisser porter par l'interface...

9 mises à jour de sécurité sont absentes. 4 Service Packs ou correctifs cumulatifs sont absents.

Détails pour Windows

Mises à jour de sécurité

Les éléments marqués d'un  sont des confirmés comme manquants. Les éléments marqués d'un  sont des confirmés comme manquants et n'ont pas été approuvés par l'administrateur système.

Score	ID	Description	Gravité maximale	Télécharger
	MS10-013	Mise à jour de sécurité pour Windows 7 (KB975560)	Critique	
	MS10-002	Mise à jour de sécurité cumulative pour Internet Explorer 8 pour Windows 7 (KB978207)	Critique	
	MS10-006	Mise à jour de sécurité pour Windows 7 (KB978251)	Critique	

MBSA et analyse distante:

l'analyse peut être faite à distance si on installe sur les postes un Windows Update Agent,

 WindowsUpdateAgent30-x86.exe)

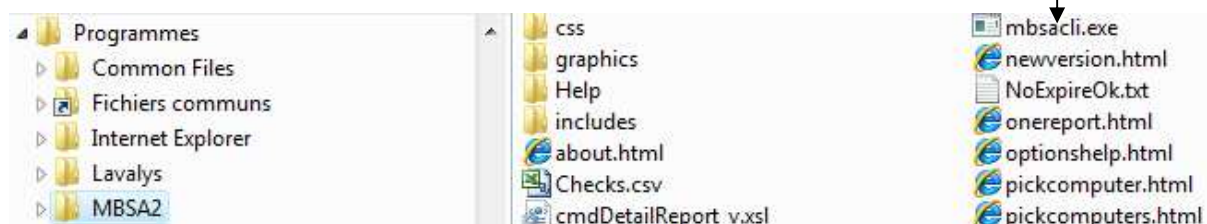
Cela suppose dans la manière la plus simple, que :

- Le compte utilisé soit administrateur sur les 2 postes utilisé
- Le pare-feu soit désactivé
- Les partages fichiers/imprimantes soient autorisés dans le profil réseau
- Le service Registre à distance soit démarré

MBSACLI invite de commande:

La version 2.1 de MBSA comprend aussi une interface de ligne de commande disponible via la commande **mbsacli** depuis le dossier dans lequel MBSA est installé

En général %programmes%\ Microsoft Baseline Analyser 2\



Il faut y ouvrir une invite de commande pour lancer ensuite

Mbsacli

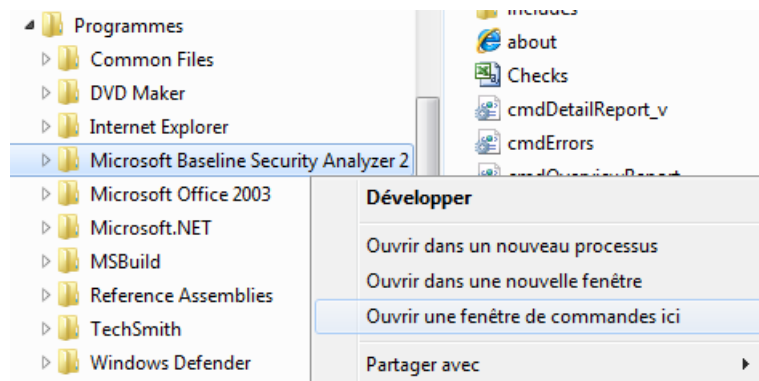
```
Administrateur : C:\Windows\system32\cmd.exe
C:\Program Files\Microsoft Baseline Security Analyzer 2>mbsacli /?
Microsoft Baseline Security Analyzer
Version 2.1.1 (2.1.2112.0)
(C) Copyright 2002-2009 Microsoft Corporation. Tous droits réservés.

MBSACLI [/target : /r : /d domaine] [/n option] [/o fichier] [/qp] [/qel] [/qr]
[/qt] [/listfile fichier] [/xmlout] [/wa : /wil] [/catalog fichier] [/nvc]
[/ial] [/mul] [/nd] [/rd répertoire] [/?]

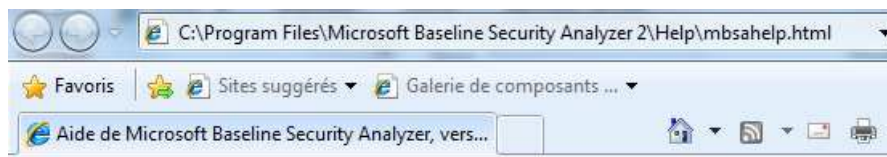
MBSACLI [/ll] [/ls] [/lr fichier] [/ld fichier] [/unicode] [/nvc] [/?]

Description :
Outil ligne de commande pour Microsoft Baseline Security Analyzer
```

NB : pour ouvrir une invite de commande on peut utiliser **SHIFT + Clic Droit / Ouvrir une fenêtre de commande ici**



Une aide en ligne substantielle se trouve soit dans le fichier **mbsahelp.html** du dossier **HELP**, soit en demandant l'aide en invite graphique



Microsoft Baseline Security Analyzer

Microsoft Aide de Microsoft Baseline Security Analyzer

Sommaire

- [Notes de publication pour MBSA 2.1](#)
- [Mise en route](#)
 - [Configuration système requise](#)
 - [Options d'analyse](#)
 - [Vérifications de sécurité](#)
 - [Outil de ligne de commande de MBSA](#)
 - [Remarques générales](#)

Outil de ligne de commande

Vous pouvez utiliser l'outil de ligne de commande de MBSA au lieu de l'interface utilisateur graphique de MBSA pour effectuer des analyses de sécurité locales ou à distance et également pour afficher des rapports d'analyses précédentes. Cet outil se trouve dans le répertoire d'installation de MBSA 2.1 (par défaut : %programfiles%\Microsoft Baseline Security Analyzer 2).

Syntaxe

Pour effectuer une analyse complète d'un ou de plusieurs ordinateurs :

```
MBSACLI [/target {[domaine\]ordinateur | IP} | /r IP-IP | /d domaine] [/n option[+option...]]  
[ /o modèle] [/qp] [/qr] [/qe] [/qt] [/q] [/listfile fichier] [/wa | /wi]  
[ /catalog fichier] [/nvc] [/ia] [/mu] [/nd] [/u nom_d'utilisateur /p mot de passe] [/rd répertoire]
```

Pour analyser l'ordinateur local et vérifier uniquement les mises à jour, en envoyant les résultats vers la sortie standard (STDOUT) au format XML :

NOTIONS POUR INSTALLER SEVEN

Fichiers d'installation Image - WIM :

Désormais Seven ne s'installe plus depuis une distribution de fichiers stockés dans une arborescence du CD-DVD d'installation (traditionnellement un dossier i386...), mais depuis une image au format **WIM Windows Imaging format**

Ce format **Wim** présente les avantages suivants :

- Réduction considérable de la taille due à la structure mono-fichier de la distribution
- Indépendance du matériel, deux distributions suffiront à couvrir tous le parc, une 32 bits et (éventuellement une 64 bits)
- Orienté fichier, et non secteurs disques, il peut s'installer sans reformater le disque sur des partitions existantes (et garder l'existant)
- Stockage des différentes images dans un fichier Wim, permettant de déployer différentes topologies en économisant de la place car les fichiers communs aux différentes images ne sont stockés qu'une fois
- Démarrage de l'installation avec **Windows PE 2.0**, (boot.Wim) permettant de préparer (si besoin) disques et partition...

Il est possible d'installer Seven de 2 manières :

- En mode manuel, depuis le CD depuis **install.WIM** (en y ajoutant éventuellement un fichier de réponse **unattended.XML**)
- En mode automatique on déploie les images via un nouvel outil **IMAGEX**, ou mieux avec un serveur d'installation (ex RIS) rebaptisé en **WDS Windows Deployment System**. (depuis le SP2 de 2003 serveur)

La HAL - Hardware Abstraction Layer

C'est ce que l'on appelle la Couche d'Abstraction Matérielle

Depuis NT, tous les logiciels doivent obligatoirement passer par le noyau pour accéder au matériel (contrairement à DOS/W31/W9x où un pilote ou une appli "maison" pouvaient accéder directement au matériel). Ceci a été mis en place pour des raisons de stabilité

La HAL sert justement à cette tâche (Accès direct sans passer par les pilotes de l'OS, mais sans court-circuiter le noyau pour autant) !

Sous Windows NT/2K/XP,

il y avait plusieurs **HAL** de disponibles (sans compter celles que peuvent développer les constructeurs de PCs) selon :

- gestion de l'énergie: ACPI (Advanced Configuration and Power Interface) - Standard (Non-ACPI)
- APIC (Advanced Processor Interrupt Controller)
- MPS (MultiProcessor Systems)
- processeurs : mono-pro - multi-pro

A chaque HAL correspond une DLL de setup, renommée HAL.DLL à l'install:

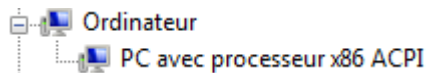
- hal.dll standard (Non-ACPI) PC
- halaacpi.dll ACPI Uniprocessor PC
- halmacpi.dll ACPI Multiprocessor PC

Ceci en liaison avec les 2 fichiers kernel principaux (NTOSKRNL.EXE et NTKRNLP.A.EXE) qui changent à l'install en fonction du type noyau

Sous SEVEN

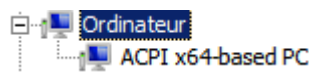
une seule HAL est désormais détectée, dénommée

PC avec processeur x86 ACPI



Ou

PC avec processeur x64 ACPI



Seven se déployant à partir d'image, la détection de la base HARDWARE peut se faire directement au lancement de l'OS (et non plus lors de l'installation). On peut forcer la détection de la HAL à travers via 2 nouvelles commandes disponible, dans la section windows boot loader :

detecthal Yes

usefirmwarepcsettings No

```
Chargeur de démarrage Windows
-----
identificateur            {current}
device                   partition=C:
path                     \Windows\system32\winload.exe
description              Microsoft Windows Vista
locale                   fr-FR
inherit                  {bootloadersettings}
osdevice                partition=C:
systemroot               \Windows
resumeobject            {06ac77b7-f447-11dc-a37d-dbb378e90123}
nx                       OptIn
detecthal                Yes
usefirmwarepcsettings   No
```

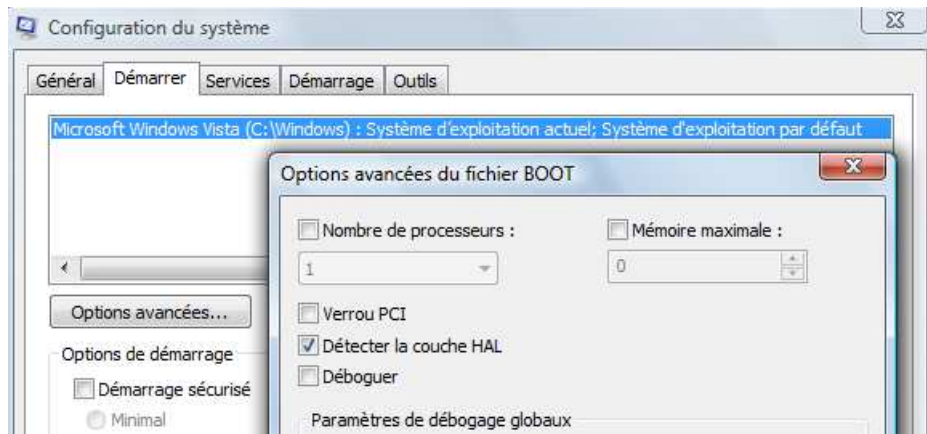
Donc

Bcdedit /set {current} detecthal yes

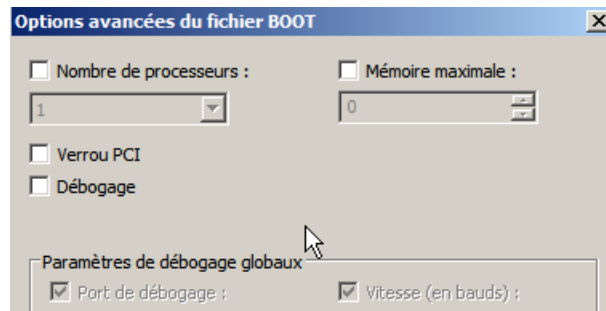
Et **Bcdedit /set {current} detecthal no**

Cette option était aussi gérable initialement à travers msconfig (Version RC):

Démarrer / Options avancées.../Détecter couche HAL



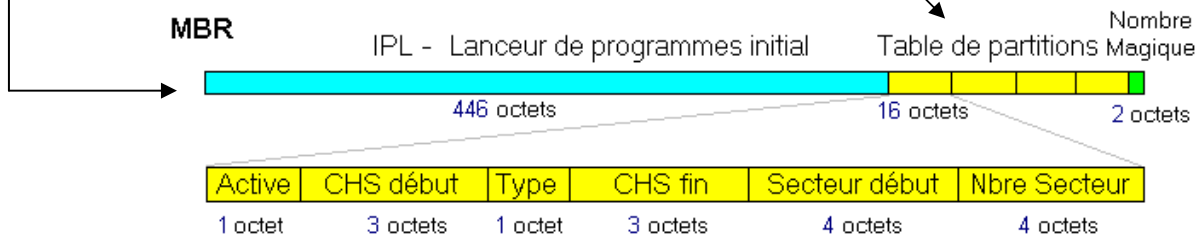
Mais supprimé depuis la version RTM...



Les catégories de partition sur système INTEL:

Un disque contient une table des partitions (**MBR Master Boot Record**).

Les **446** premiers octets sont réservés au code du programme (ce code, lui dépend toutefois du système d'exploitation sous lequel la MBR a été créée). Les **64** octets suivants offrent la place nécessaire à une table de partition pouvant contenir jusqu'à quatre entrées.



Chaque entrée dans la table des partitions peut correspondre soit à une partition **primaire** (dite aussi **principale**) soit à une partition **étendue**, (qui elle même peut contenir des partitions dites **logiques**)

Les 3 catégories de partition **primaires** (ou **principales**), **étendues** et **logiques** sont des notions INDEPENDANTES de tout système d'exploitation. La notion est liée UNIQUEMENT à la plate-forme matérielle, à savoir INTEL (et compatibles)

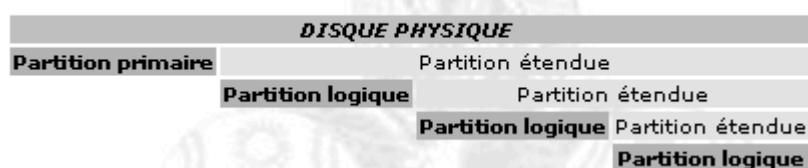
On peut répartir ces catégories de partitions en 2 groupes logiques :

- Les partitions "conteneur" = qui sont essentiellement d'un seul type :
 - o **étendues** (définissant une table de partition "hors MBR" dans ce que l'on nomme une **EBR**)
- Les partitions "contenus" = qui sont de deux types :

- o **primaires** (définies exclusivement dans une table de partition dite **MBR Master Boot record**) au nombre de **4 maximum** par disque physique
- o **logiques** (définies exclusivement dans la **EBR Extended Boot Record d'une partition étendue**)

Le problème (historique) est qu'au départ seulement 4 "rayonnages" au maximum ont été prévus. Toujours pour des questions historiques (au départ, les disques étaient tous petits, comparés à ceux de maintenant), on ne peut créer que **un ou deux** compartiments, le 2ème étant alors un nouveau tiroir, "emboîté" dans un compartiment. Et ce "petit" tiroir peut à **nouveau** contenir 2 compartiments, un pour du rangement (=partition LOGIQUE), et un autre pour un nouveau tiroir, et ainsi de suite, à l'infini (jusqu'à ce qu'il n'y ait plus de place du tout)

Donc un disque pourra avoir la structure suivante :



Ce disque possède 1 partition **PRIMAIRE** (celle où on va stocker le système d'exploitation généralement), et 3 partitions **LOGIQUES** (ici ce sont les seules qui nous intéressent : les "contenus", les partitions **ÉTENDUES** n'étant que des "contenants")

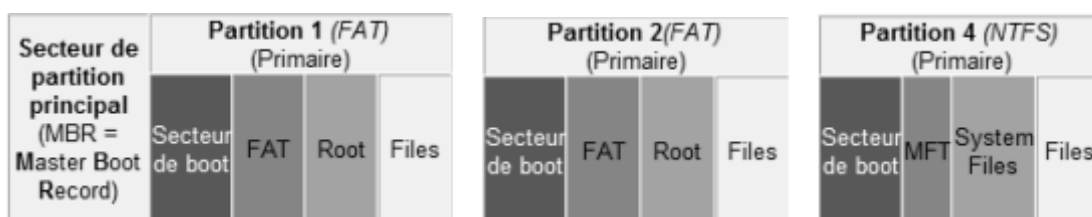
NB : Une table de partition (que ce soit celle du MBR ou celle d'une partition étendue) ne peut pas contenir plus de 4 entrées.

N.B : De plus, avec les outils DOS/Windows, une table de partition ne "pointe" au plus que vers 2 partitions (une logique et éventuellement une étendue), alors qu'elle pourrait en contenir 4.

Par conséquent, sous FDISK ou avec l'administrateur de disque NT4, seule est affichée la 1ère partition étendue, suivie de toutes les autres partitions logiques comme si elles étaient directement à l'intérieur de cette partition étendue.

N.B : Si vous créez des partitions principales multiples, seule une partition principale peut être active à la fois.

N.B : La plupart des systèmes d'exploitation ne peuvent être amorcés qu'à partir d'une partition principale (qui peut contenir un secteur de boot)



Système de Fichier NTFS :

- Une sécurité d'accès pour les fichiers.
- Pour implémenter **Active Directory** sur un serveur
- Cryptage des fichiers : via **EFS** notamment.
- Quotas de disque : Analyse / contrôle d'espace utilisée par personne.
- La prise en charge de disques durs de très grande capacité très largement supérieure à celle des systèmes FAT32

Comparaison avec l'ancien système FAT-FAT32

	NTFS	FAT – FAT32 – FAT32X
Sécurité	Utilisateurs / Groupes bénéficient des différents accès à un fichier - dossier.	Les fichiers ne sont pas protégés.
Journal des activités	journal des activités	pas de journal.
Services	Cryptage, Quota...	Aucun service
Compression de fichier	Prend en charge	pas prise en charge.

Comparaison des tailles de disques et de fichiers

NTFS	FAT	FAT32-FAT32X
taille minimale recommandée 10 Go	Volumes compris entre la taille d'une disquette et 2 Go	Volumes compris entre 512 Mo et 32 Go
taille maxi recommandée 2 Téraoctets		
Ne peut pas être utilisé sur des disquettes		formate jusqu'à 32 Go (peut lire plus...)
La taille des fichiers est limitée que par la taille du volume	Taille maximale des fichiers : 2 Go	Taille maximale des fichiers : 4 Go

INSTALLATION NOUVELLE/ M.A.J.

Mise à niveau - Install Complète:

L'une des premières décisions que vous devez prendre est soit de mettre à niveau votre système d'exploitation actuel, soit de procéder à une installation entièrement nouvelle, soit encore de procéder à un multi-boot.

- Au cours d'une **mise à niveau**, le programme d'installation **remplace** les fichiers Windows existants mais essaye de conserver vos paramètres et applications actuels. Il est bien sûr possible que certaines applications ne soient pas compatibles avec Windows Seven

N.B: Après une **mise à niveau**, aucun moyen de revenir version antérieure !

Upgrade FROM :	Windows 7 Home Premium	Windows 7 Professional	Windows 7 Ultimate
Windows XP*	Custom Install		
Any 32-bit version to 64-bit, or vice-versa	Custom Install		
Windows Vista Home Basic	In-Place Upgrade	In-Place Upgrade + Windows Anytime Upgrade	In-Place Upgrade
Windows Vista Home Premium	In-Place Upgrade	In-Place Upgrade + Windows Anytime Upgrade	In-Place Upgrade
Windows Vista Business	Custom Install	In-Place Upgrade	In-Place Upgrade
Windows Vista Ultimate	Custom Install	Custom Install	In-Place Upgrade

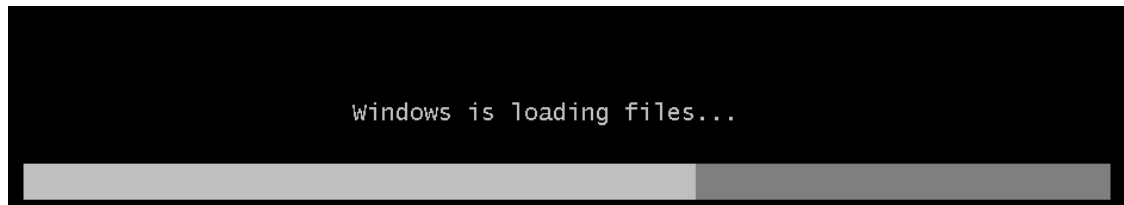
- Si vous choisissez une **installation complète**, vous devez réinstaller vos applications et redéfinir vos préférences.
Une installation complète sur une autre partition donnera un système en dual-boot, automatiquement.

Evidemment, un seul credo opérationnel : « Pour passer de XP à Seven, il faudra sauvegarder les données puis réinstaller entièrement le système et les fichiers

Install Complète depuis DVD:

En bootant depuis un DVD, c'est la manière normale d'installation... On passe tout de suite en interface graphique...

Il est conseillé de ne pas courir plusieurs lièvres à la fois, d'autant plus que faire une installation ne nécessite pas de connexion internet...



On passe avec une interface graphique de manière quasi immédiate...

Paramètre régionaux :

Il suffit d'indiquer le pays, code clavier, les symboles numériques que l'on souhaite utiliser

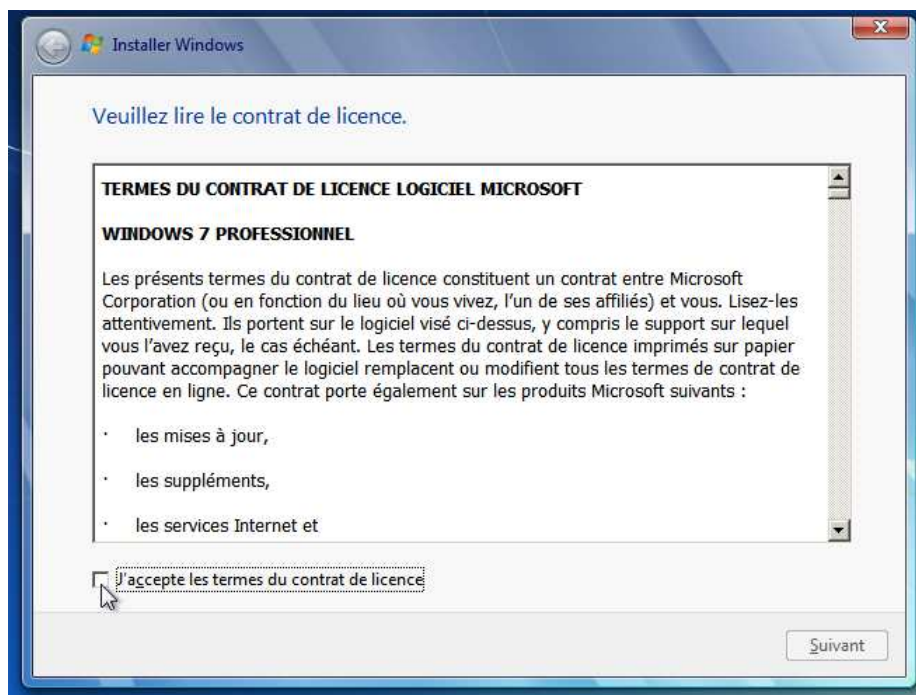


Installer / Réparer

Il faut demander d'**Installer** Seven



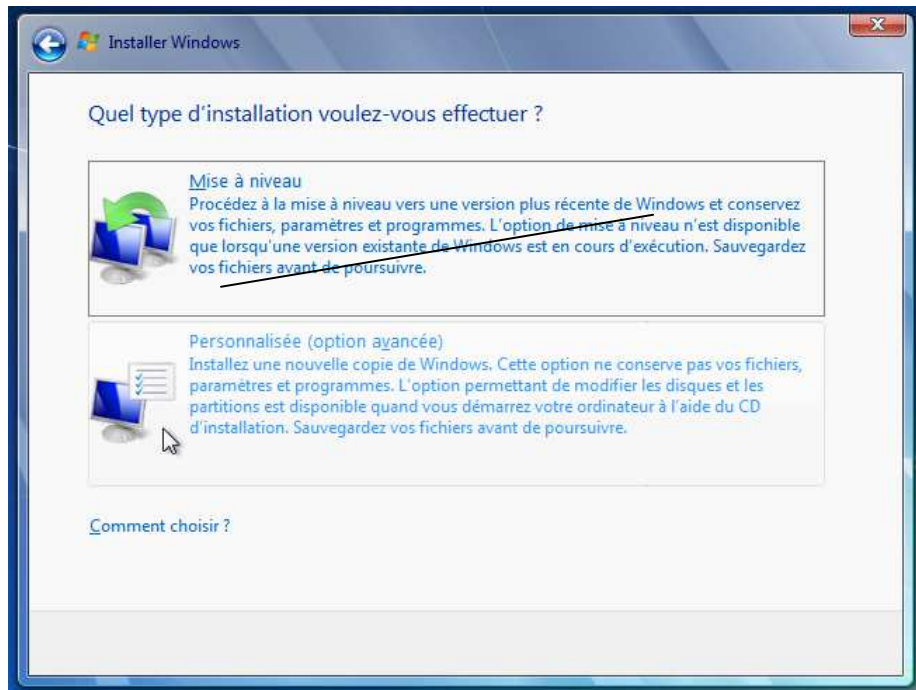
Licence



Il faut accepter la licence

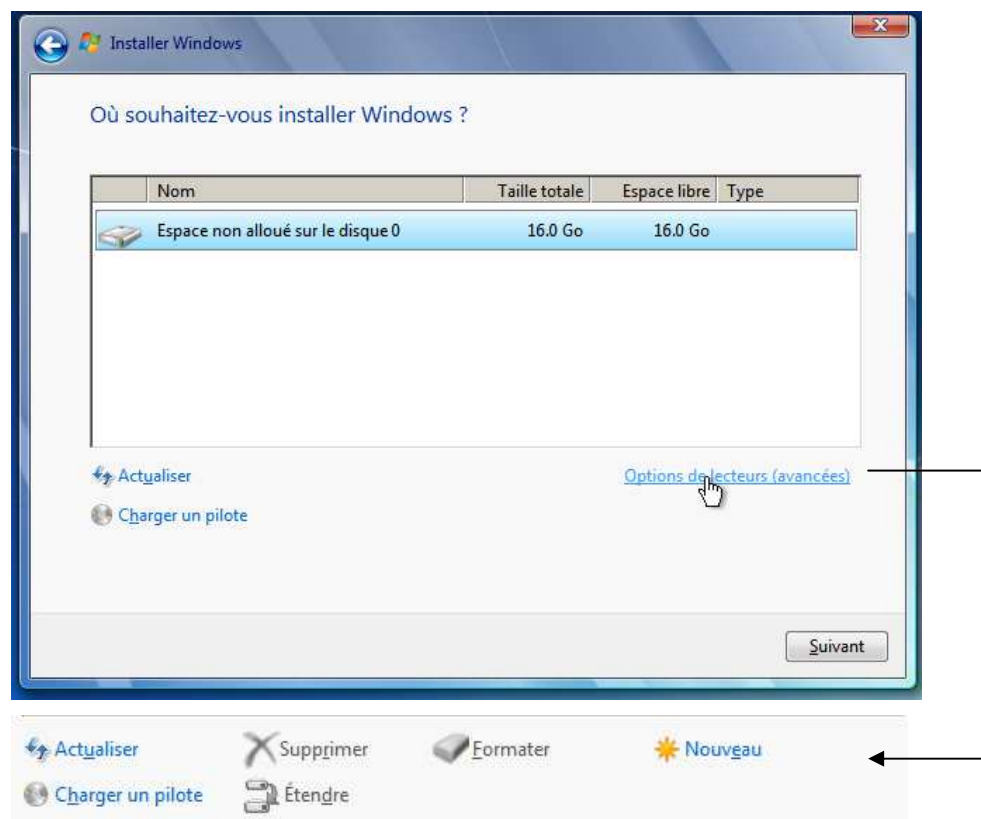
Mise à Jour / Installation Avancée

La mise à jour est souvent désactivée (car elle n'est disponible que si on démarre la procédure d'installation depuis l'ancien OS XP par exemple), et donc on demande une Installation **Personnalisée (option avancée)**.



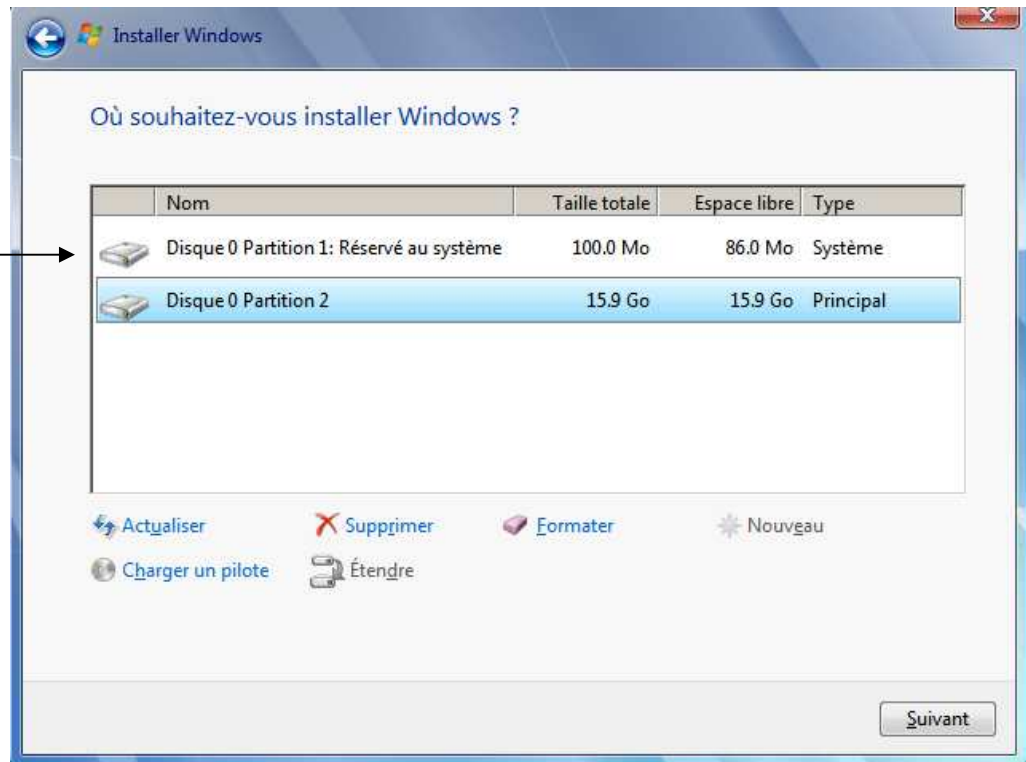
Création des Partitions

Lorsque l'on crée des partitions, ce sont des partitions Principales qui sont montées. Le formatage ne donne pas ici le choix du type de système de fichier, et un système NTFS est obligatoirement utilisé.



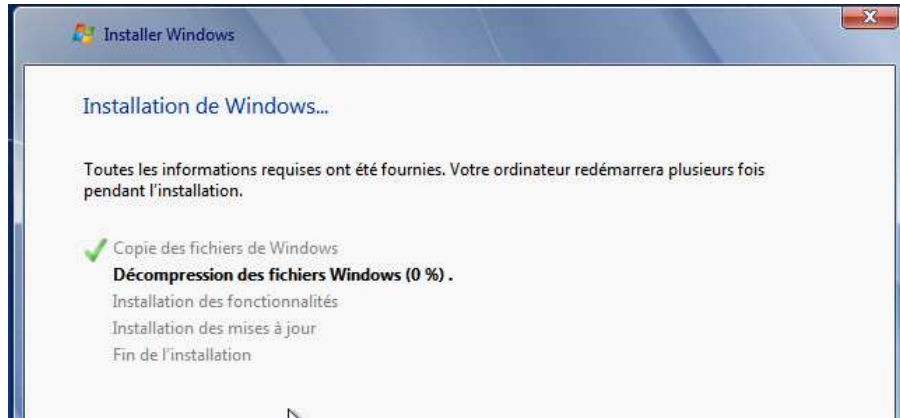
Beaucoup plus d'options sont disponibles en invite de commande via **MAJ+F10** puis utilitaire **diskpart...**

Une partition « cachée » système est créée pour stocker des outils de récupération en cas de crash système

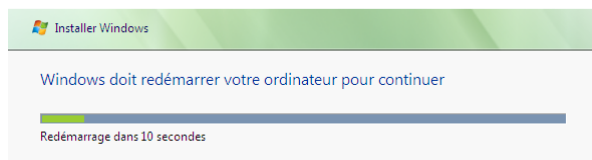


Copie des fichiers

Le programme d'installation poursuit,

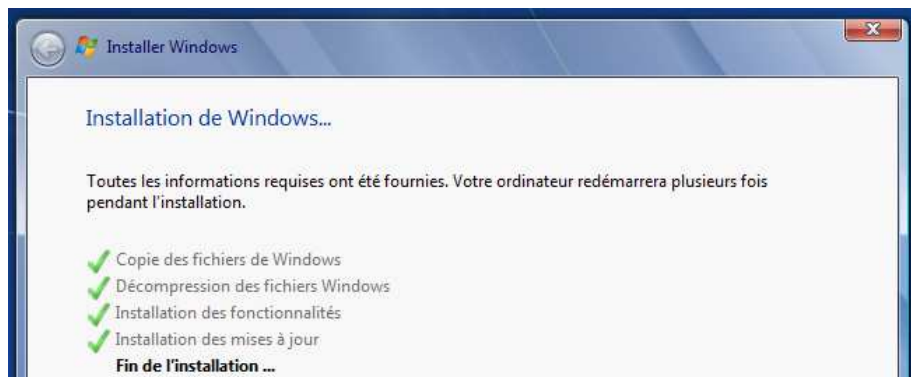


et génère un premier Re-Boot



Décompression des fichiers

Le programme d'installation décompresse les fichiers, commence la copie des fichiers et génère un deuxième Re-Boot



Fin d'installation des fichiers

Le programme d'installation termine la copie des fichiers et génère un troisième Re-Boot

Assistant premier démarrage

Il demande successivement :

- un compte utilisateur (qui aura des droits d'administration)
- Le nom machine

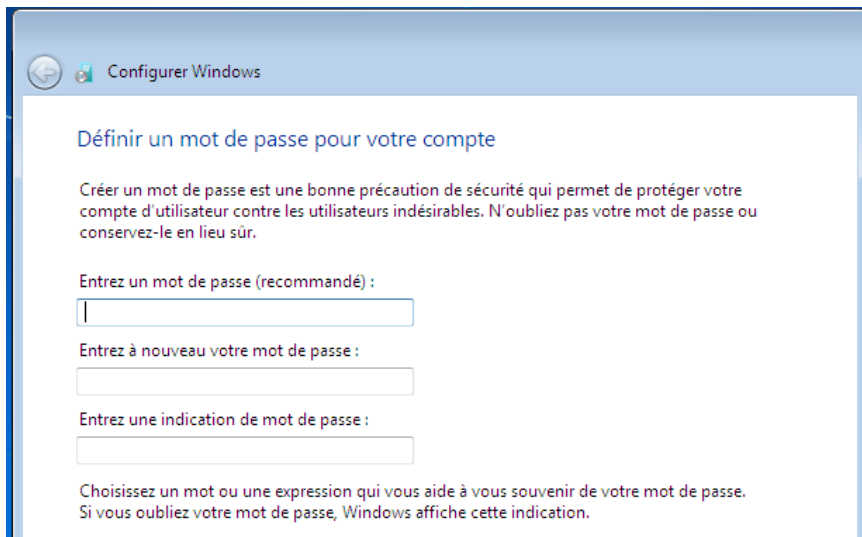
Entrez un nom d'ordinateur unique qui soit différent des autres noms d'ordinateur, de groupe de travail ou de domaine utilisés sur votre réseau

La longueur maximale pour un nom d'ordinateur est de **63 caractères**.

N.B : Les ordinateurs antérieurs à Windows 2000 reconnaissent les 15 premiers caractères du nom uniquement. Si vous utilisez VISTA sur un réseau qui compte des ordinateurs antérieurs à Windows 2000 La longueur maximale est **15 caractères**. Utilisez uniquement les caractères suivant : les **chiffres de 0 à 9**, les **lettres majuscules et minuscules de A à Z** et le **trait d'union (-)**.

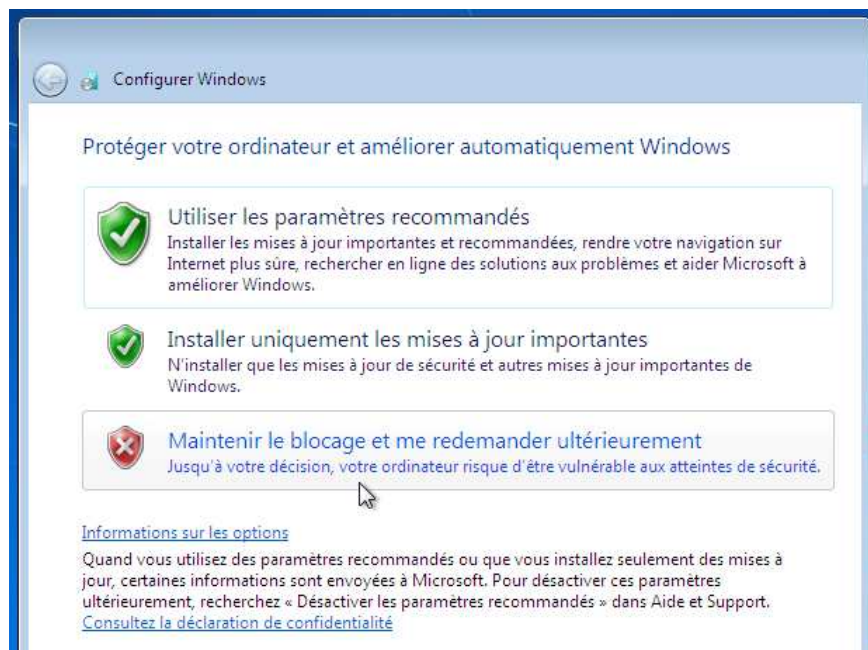
N.B : Vous pourrez toujours y revenir en demandant dans le **panneau de configuration** l'icône **système**



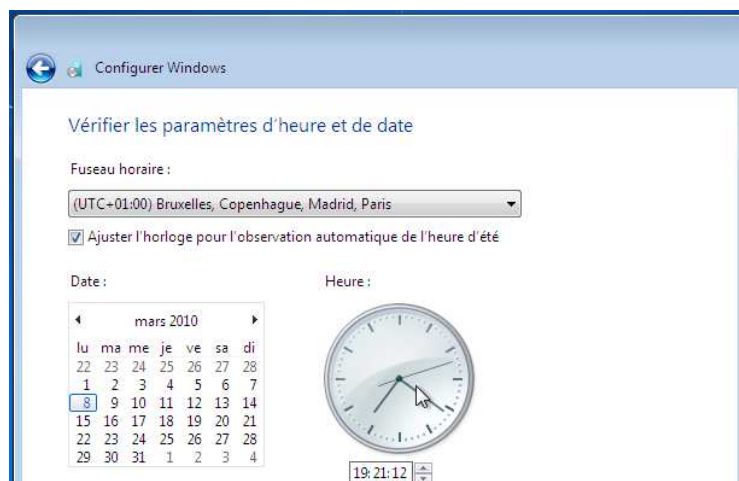


Le mot de passe peut contenir jusqu'à **127 caractères**.

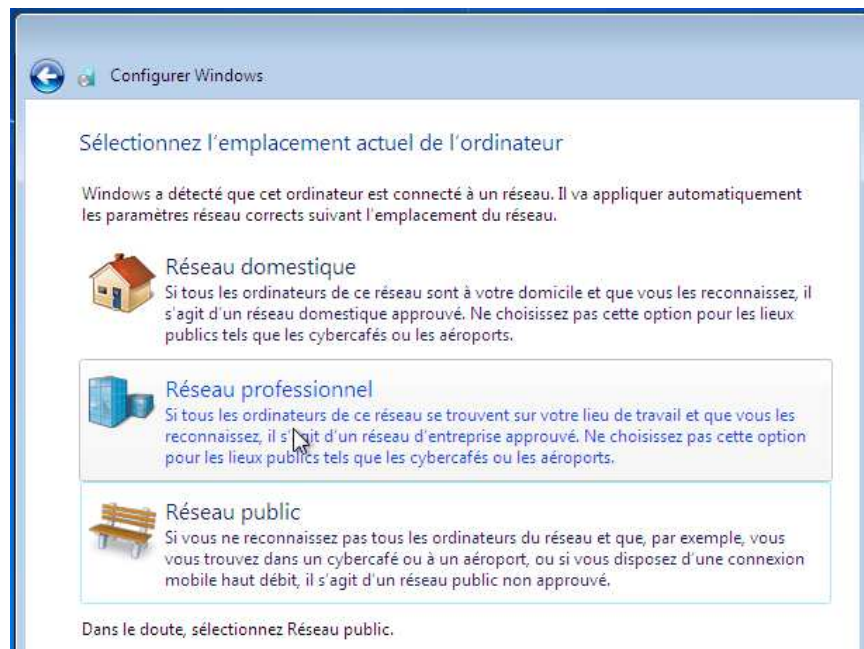
- La politique de maj de Windows et de gestions de toute la sécurité



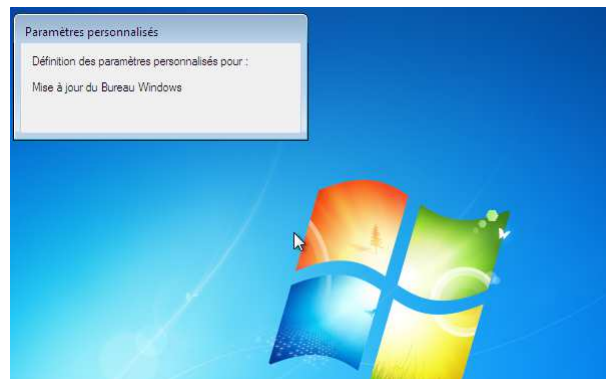
- Le fuseau Horaire



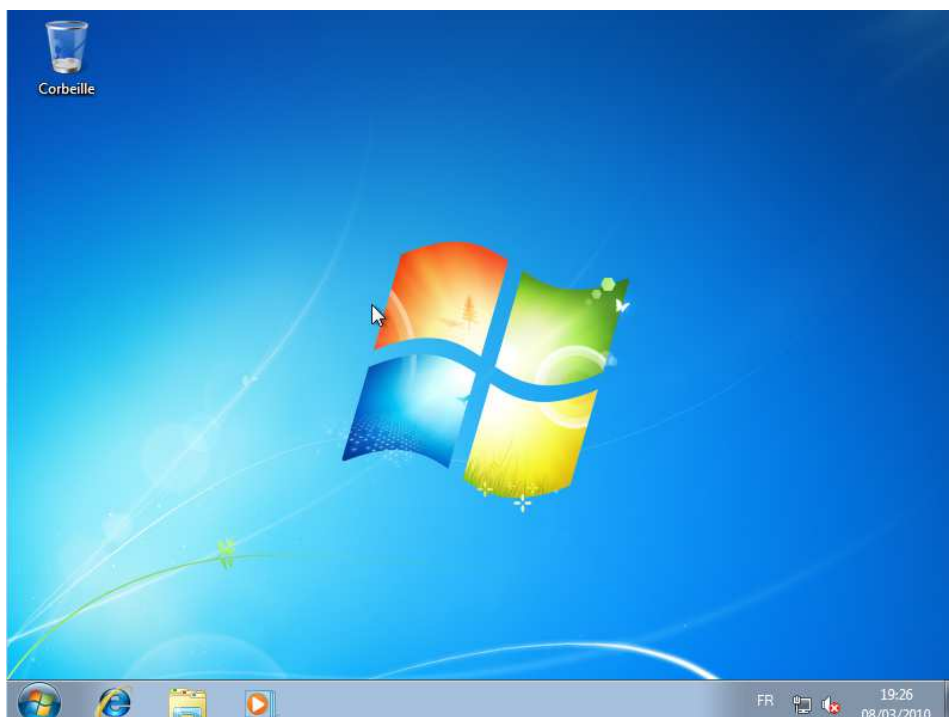
- Si une carte réseau est détectée alors il faut choisir un « type » réseau



Et ensuite un profil de l'utilisateur est créé à partir du profil par défaut



Et l'installation est terminée



WINPE 3.1

Windows Preinstallation Environment:

Avec l'avènement de Windows Vista, puis SEVEN et 2008, Microsoft a fondamentalement modifié sa stratégie d'installation, en donnant à l'utilisateur une interface graphique. Cette version basique de Windows, est dénommée **PE**, pour **Preinstallation Environment**,

Windows PE 2.0 est basé sur le noyau de Vista, en plus compact.

Windows PE 3.0 est basé sur le noyau de Seven. Avec Windows PE on peut:

- Accéder en lecture et écriture aux lecteurs formatés NTFS
- disposer d'une gamme de pilotes matériels, tant en 32- qu'en 64-bit,
- Avoir d'une couche réseau TCP-IP et Netbios
- Faire fonctionner des applications en 32- et 64-bit.

Windows PE 3.0 n'est pas uniquement destiné à l'installation de Seven, mais il peut être dissocié de ce dernier, et devenir à son tour un outil de dépannage et de diagnostic autonome !

Windows PE 3.1 intègre une mise à jours des hotfix de winpe3.0 et, quelques drivers réseaux supplémentaires

- Ce n'est pas une version Embedded de Windows (reboot automatique toutes les 72h)

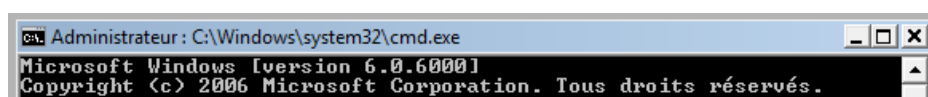
Il est possible de récupérer une copie de Windows PE soit :

- En l'extrayant d'un DVD d'installation de SEVEN
- En téléchargeant auprès de Microsoft un kit automatisé d'installation de Windows (**WAIK**, pour **Windows Automated Installation Kit**)

Utiliser Windows PE lors de l'installation Seven:

Au démarrage apparaît l'écran qui vous accueille lorsque vous installez Windows Seven,

Mais la combinaison de Touche **MAJ+F10** permettra d'ouvrir une fenêtre d'invite de commande (en plus de l'habituel wizard d'installation...)



Utiliser un média amorçable Windows PE:

le CD Seven contient déjà un environnement de démarrage sous Windows PE. Utiliser un média contenant uniquement Windows PE peut être assez pratique car :

1. Il permet de démarrer n'importe quelle machine, y compris un poste sous Windows 2000 ou sous Windows XP sans utiliser une copie de Seven
2. Grâce à la très petite taille de l'environnement Windows PE 3.1, il est envisageable de le placer sur une simple clef USB.
N.B : un minimum de 256 Mo de RAM est nécessaire
3. Il est naturellement possible d'ajouter ses propres outils à l'image ISO générée par les outils Windows PE.

Un CD ou une clef Windows PE au sein d'une entreprise est un outil puissant car depuis la ligne de commandes il est en effet possible d'accéder à toutes les données contenues sur le disque dur, et ce sans aucun contrôle du statut d'administrateur de l'utilisateur et sans aucun contrôle de compte.

En effet, les commandes saisies depuis l'interface Windows PE s'exécutent par défaut en mode administrateur

SÉQUENCE BOOT & MULTI-BOOT

Boot XP & ntldr:

Depuis Windows NT, windows installe son secteur d'amorçage et quelques fichiers cachés sur la **Partition Principale Active** mais autorise l'installation de son répertoire \WINNT ailleurs. L'installation peut créer des partitions Fat-NTFS.

Windows NT4 ne reconnaît pas les partitions formatées en FAT32.

Windows 2000 reconnaît les partitions Fat32 et FAT32x (disque de plus de 8.4Giga) de Windows 9.x mais pas leurs volumes compressés.

Le programme de partition, identifie la partition active, charge le secteur de boot inscrit dans la MBR et lance le programme de boot qu'il contient. Ce programme cherche sur le disque un (ou deux) autre(s) programme(s) et leur passe la main. Ces programmes sont :

pour DOS :	IO.SYS et MSDOS.SYS (ou IBM....COM)
pour Window 95/98 :	IO.SYS et MSDOS.SYS (fichier texte config)
pour NT –2000 – XP :	NTLDR ("NT" Loader)

Donc le secteur de boot de la MBR charge le programme NT Loader (**NTLDR**). Ce dernier affiche un menu de sélection basé sur le fichier de configuration **BOOT.INI**. La structure de ce fichier texte est relativement simple. Les fichiers suivants sont copiés dans le répertoire racine de la partition principale active :

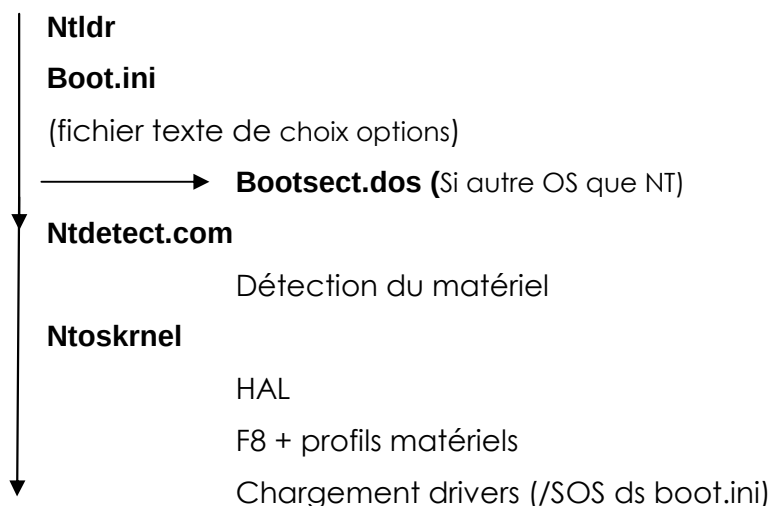
Boot.ini	fichier de menu de lancement NT-2000
Ntldr	fichier systeme NT-2000
Ntldetect.com	fichier systeme NT-2000
Bootfont.bin	police systeme pour affichage écran
Ntbootdd.sys	si vous disposez d'un disque SCSI qui n'est pas visible à partir de MS-DOS (non détecté par le BIOS)
Bootsect.dos	(si un autre système d'exploitation se trouvait sur votre ordinateur, image du secteur de boot)

Ces fichiers ne doivent en aucun cas être supprimés, car ils sont indispensables au démarrage de NT. Ces fichiers sont tous des fichiers système cachés, en lecture seule. Si l'un d'entre eux ne se trouve pas sur votre système, utiliser une disquette amorçable pour réparer...

Après la séquence **POST Power on Self Test** , que tous PC déroule, indépendamment du système qui peut être installé. Le **BIOS** du PC vérifie la présence du matériels, (mémoire, disque, périphériques) le périphérique de démarrage est localisé dans la MBR, et charge alors le programme lanceur

Sur une PC avec un **BIOS**, voici la séquence d'amorçage via **Ntldr**

Mise sous tension « Séquence POST »



Boot Seven & Bootmgr :

Le BIOS actuel peut disparaître au profit d'une technologie baptisée **EFI Extensible Firmware Interface**, utilisant un gestionnaire de boot non plus inscrit dans la MBR mais dans une mémoire non volatile NVRAM. Les options de démarrage de Windows **Seven** ne sont plus stockées dans le fichier boot.ini mais dans une branche du registre nommée **BCD, Boot Configuration Database**.

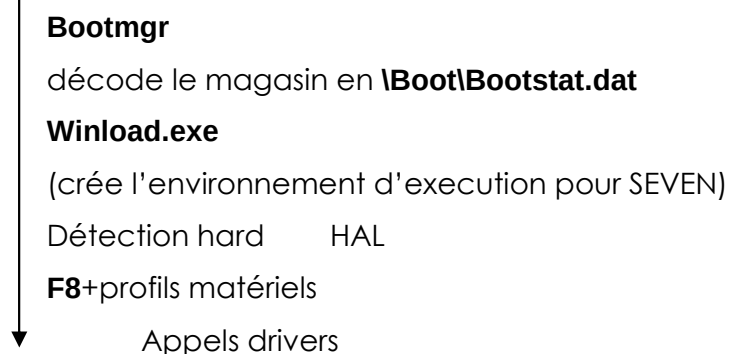
N.B : Ce **BCD** bien que stocké dans une partie de la base de registre, ne peut être modifié que par l'appel de l'utilitaire **bcdedit.exe**. (ou par programmation via des API de WMI qui peuvent modifier ce registre)

Les fichiers suivants sont copiés dans le répertoire racine de la partition principale active

autoexec.bat	fichier de compatibilité pour VDM et NT
config.sys	fichier de compatibilité ms-dos & windows
bootmgr	fichier de démarrage de Seven
pagefile.sys	fichier de swap Seven
hiberfil.sys	fichier gestion mode hibernation de Seven
un dossier Boot	stocké à la racine de la partition principale active et contenant la branche de la base de registre bootstat.dat

Sur un PC avec un **BIOS** ou **EFI**, la séquence d'amorçage via **Bootmgr**

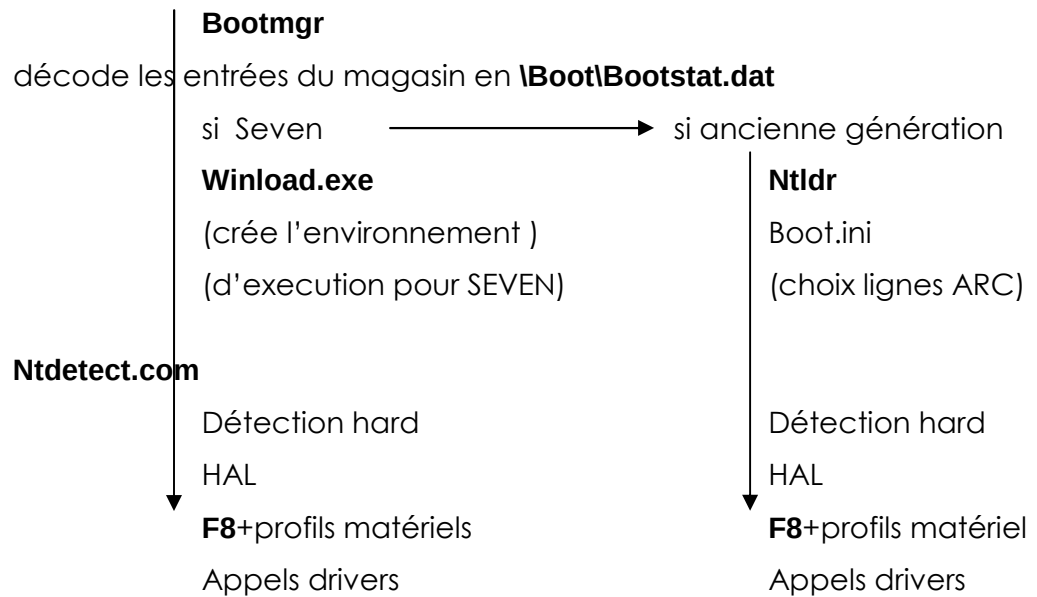
Mise sous tension « Séquence POST »



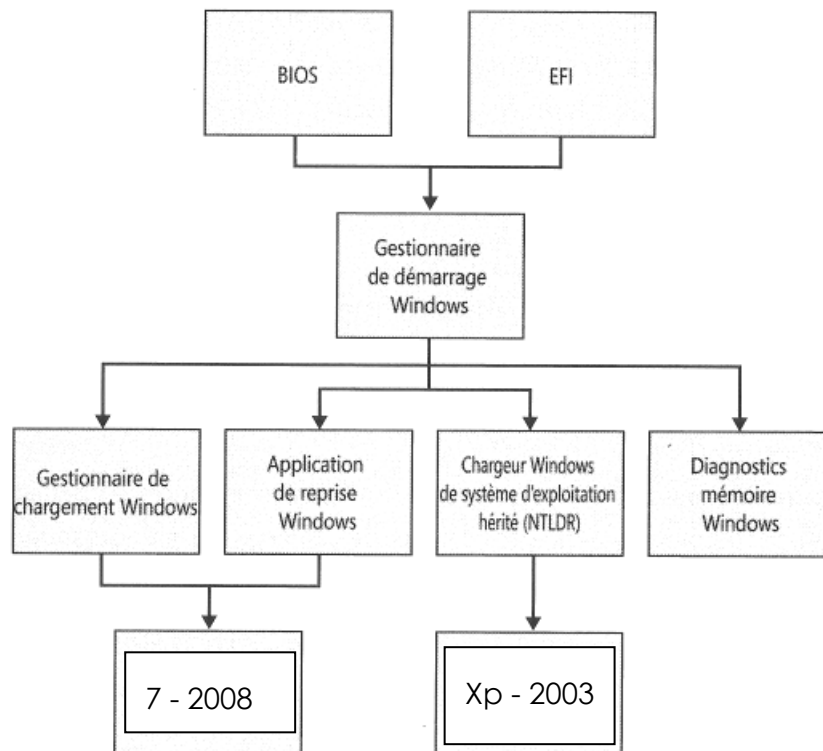
Multi-Boot Seven (bootmgr) - XP (ntldr) :

Sur un PC avec un **BIOS** ou **EFI**, la séquence d'amorçage Multi-Boot SEVEN-XP

Mise sous tension « Séquence POST »



Ce qui au final, avec les outils de récupération Seven et de diagnostic mémoire, pourrait donner le schéma suivant :



Structure du magasin:

Section Gestionnaire de démarrage :

Bootmgr il permet de gérer le boot et les multi-boot.

Section Legacy (éventuellement)

renvoi à NTLDR et ancien boot.ini

Section Chargeur démarrage Windows

Winload.exe existe pour chaque version de Seven - 2008 installée

```
C:\Users\test>bcdedit

Gestionnaire de démarrage Windows
-----
identificateur      {bootmgr}
device              partition=D:
description         Windows Boot Manager
locale              fr-FR
inherit              {globalsettings}
default              {current}
resumeobject        {324e1371-5d1b-11dc-8bf1-d6f4bef89e58}
displayorder        {ntldr}
toolsdisplayorder   {memdiag}
timeout             30

Chargeur de système d'exploitation Windows d'ancienne génération
-----
identificateur      {ntldr}
device              partition=D:
path                \ntldr
description          Version antérieure de Windows

Chargeur de démarrage Windows
-----
identificateur      {current}
device              partition=C:
path                \Windows\system32\winload.exe
description          Microsoft Windows Vista
locale              fr-FR
inherit              {bootloadersettings}
no integritychecks   No
osdevice             partition=C:
systemroot           \Windows
resumeobject        {324e1371-5d1b-11dc-8bf1-d6f4bef89e58}
nx                  OptIn
```

Dans le magasin, chaque section est repérée par un identificateur {xxxxxx}

- **Gestionnaire de démarrage / Windows Boot Manager** : (toujours unique, Stocké à la racine de la partition active)

```
Gestionnaire de démarrage Windows
-----
identificateur      {bootmgr}
```

contenant notamment les éléments : **Device - Description - Default - DisplayOrder - Timeout**

- **Chargeur ancienne génération /Legacy Boot Loader**: (Si besoin... renvois à NTLDR et ancien boot.ini)

```
Chargeur de système d'exploitation Windows d'ancienne génération
-----
identificateur      {ntldr}
```

contenant notamment les éléments : **Device - Path - Description**

- **Chargeur démarrage Windows / Windows Boot Loader**: (un pour chaque installation de Seven Vista, stocké dans \Windows\system32)

```
Chargeur de démarrage Windows
-----
identificateur      {current}
```

N.B: s'il y a plusieurs installations de SEVEN VISTA alors on aurait plusieurs sections **Chargeur de démarrage Windows** mais avec comme identificateur des GUID du genre

```
{cbd971bf-b7b8-4885-951a-fa03044f5d71}
```

contenant notamment les éléments : **Device - Path - Description - Osdevice - Systemroot**

BCDEDIT commande :

Une aide en ligne est disponible via

Bcdedit / ?

et les commandes sont nombreuses :

```
Administrateur : C:\Windows\system32\cmd.exe
C:\>bcdedit /? /TOPICS

RUBRIQUE DE CE FICHIER D'AIDE

Pour afficher l'aide d'une rubrique, exécutez « bcdedit /? <rubrique> », où
<rubrique> représente l'une des valeurs suivantes :

bootdebug          Commande /bootdebug.
bootems            Commande /bootems.
bootsequence       Commande /bootsequence.
copy               Commande /copy.
create             Commande /create.
createstore        Commande /createstore.
dbgsettings        Commande /dbgsettings.
debug              Commande /debug.
default            Commande /default.
delete             Commande /delete.
deletevalue        Commande /deletevalue.
displayorder       Commande /displayorder.
ems                Commande /ems.
emssettings        Commande /emssettings.
enum               Commande /enum.
export             Commande /export.
FORMATS            Formats pour les types.
ID                 Identificateurs pour les entrées.
import             Commande /import.
set                Commande /set.
store              Option de ligne de commande /store.
timeout            Commande /timeout.
toolsdisplayorder  Commande /toolsdisplayorder.
TYPES              Types qui s'appliquent à toutes les entrées.
TYPES BOOTAPP      Types relatifs aux applications de démarrage. Parmi elles
                   figurent le gestionnaire de démarrage, l'application de
```

La commande **bcdedit / ? types** Permet de connaître les entrées utilisables en ligne de commande

```
Entrées
=====
DESCRIPTION <string>   Définit la description d'une entrée.
PATH <string>           Définit le chemin d'accès à l'application.
DEVICE <device>         Définit le périphérique sur lequel réside
                         l'application.
INHERIT <list>          Définit la liste des entrées à hériter.
```

La commande **bcdedit / ? formats** indique les valeurs de données possibles

```
bool    Valeur booléenne. Les valeurs suivantes correspondent à TRUE (vrai) :
        1, ON, YES, TRUE

        Les valeurs suivantes correspondent à FALSE (faux) :
        0, OFF, NO, FALSE

device  Périphérique, qui peut être de l'un des types suivants :
        BOOT
        PARTITION=<lecteur>
        FILE=[<parent>]<chemin>
        RAMDISK=[<parent>]<chemin>.<idoptions>

        Les options pour ces types sont :
        <lecteur>   Lettre de lecteur suivie d'un deux-points
                     et sans barre oblique inverse à la fin.
        <parent>    <Obligatoire> Peut représenter BOOT ou une lettre de
                     lecteur avec un deux-points. Les crochets n'indiquent
                     pas qu'il est facultatif mais constituent des éléments
                     littéraux de la syntaxe.
        <chemin>    Chemin d'accès au fichier <ou au fichier .wim> à partir
                     de la racine du périphérique parent.
        <idoptions> Identificateur de l'entrée d'option de périphérique
                     qui contient les options d'image de déploiement du
                     système <SDI> du disque virtuel. Il s'agit en général
                     de <ramdisksdioptions>.

id       Identificateur d'entrée qui fait référence à une entrée du magasin
des données de configuration de démarrage. Exécutez « bcdedit /? ID »
pour plus d'informations sur les identificateurs.
```

Copier-Dupliquer une entrée du magasin:

Dans notre magasin, avant de modifier l'entrée de seven (par exemple), nous souhaitons en effectuer une copie...

La commande **bcdedit /copy / ?** nous donne toutes les options. Si on veut copier la section repérée comme **{current}** il faut taper

bcdedit /copy {current} /d "copie du boot loader de seven"

```
C:\>bcdedit /copy {current} /d "copie du boot loader de seven"
L'entrée a été correctement copiée dans {6900ba1f-1c65-11df-9c4e-9f716fb9c591}.
```

l'affichage du magasin devrait faire apparaître

```
Chargeur de démarrage Windows
-----
identificateur      {6900ba1f-1c65-11df-9c4e-9f716fb9c591}
device             partition=C:
path               \Windows\system32\winload.exe
description         copie du boot loader de seven
locale             fr-FR
inherit             {bootloadersettings}
```

Identificateur
général

Supprimer une entrée du magasin:

Il faut bien sur indiquer l'identificateur, ce qui n'est pas toujours commode !

La commande **bcdedit /delete / ?** nous donne toutes les options. Il suffit alors pour nous si on veut supprimer la section repérée comme

{81e8e7e5-60fc-11dc-b302-000102fb28b7} de taper

```
C:\Users\test>bcdedit /delete {81e8e7e5-60fc-11dc-b302-000102fb28b7}
Opération réussie.
```

l'affichage du magasin ne devrait plus faire apparaître cette entrée

N.B : dans le cas où l'on voudrait supprimer une entrée avec un descripteur « bien connu », comme **{ntldr}** il faut ajouter l'option **/f** comme dans

```
bcdedit /delete {ntldr} /f
```

Un descripteur bien connu c'est un descripteur autre que un GUID. Donc, **ntldr** – **bootmgr** – **current** sont des descripteurs bien connus !

BCDEDIT et Gestionnaire de démarrage – Boot Manager :

L'entrée du magasin correspondant au boot manager est **{bootmgr}**

- cette entrée existe toujours,
- et elle est unique

```
Gestionnaire de démarrage Windows
-----
identificateur      {bootmgr}
device             partition=\Device\HarddiskVolume1
description         Windows Boot Manager
locale             fr-FR
inherit             {globalsettings}
default             {current}
resumeobject        {6900ba1f-1c65-11df-9c4e-9f716fb9c591}
displayorder        {current}
toolsdisplayorder   {memdiag}
timeout            30
```

un certain nombre de types spécifiques s'appliquent au gestionnaire de démarrage, affichables via la commande

bcdedit / ? types bootmgr

Démarrage =====	
BOOTSEQUENCE <liste>	Définit la séquence de démarrage unique.
DEFAULT <identificateur>	Définit l'entrée de démarrage par défaut.
TIMEOUT <entier>	Définit le temps d'attente du gestionnaire de démarrage en secondes avant que le gestionnaire de démarrage sélectionne une entrée par défaut.
Reprise =====	
RESUME <booléen>	Indique qu'une opération de reprise doit être tentée.
RESUMEOBJECT <identificateur>	Fournit l'identificateur de l'objet d'application de reprise.
Affichage =====	
DISPLAYBOOTMENU <booléen>	Active l'affichage du menu de démarrage.
DISPLAYORDER <liste>	Définit la liste d'ordre d'affichage du gestionnaire de démarrage.
TOOLSDISPLAYORDER <liste>	Définit la liste d'ordre d'affichage des outils du gestionnaire de démarrage.

Système par défaut:

Il faut changer la valeur **default** {identificateur}

Aide avec **bcdedit /default / ?**

```
C:\Users\test>bcdedit /default {ntldr}
Opération réussie.
```

Time-out:

Il faut changer la valeur **timeout** {entier}

```
C:\Users\test>bcdedit /timeout 45
Opération réussie.
```

Forcer l'affichage du menu de boot:

C'est la commande **Set** qui permet de définir une valeur dans le magasin

Avec le type voulu derrière

```
C:\>bcdedit /set /?

Cette commande définit une valeur d'option d'entrée dans le magasin des données
de configuration de démarrage.

bcdedit [/store <nomfichier>] /set [[<id>]] <typedonnées> <valeur>

<nomfichier>   Spécifie le magasin à utiliser. Si cette option n'est pas
                spécifiée, le magasin système est utilisé. Pour plus
                d'informations, entrez « bcdedit /? store ».

<id>           Spécifie l'identificateur de l'entrée à modifier. S'il n'est
                pas spécifié, <current> est utilisé. Pour plus d'informations
                sur les identificateurs, entrez « bcdedit /? ID ».

<typedonnées>  Spécifie le type de données de l'option qui sera créée
                ou modifiée. Entrez « bcdedit /? TYPES » pour plus
                d'informations sur les types de données.

<valeur>       Spécifie la valeur à affecter à l'option. Le format de
                <valeur> dépend du type de données spécifié. Entrez
                « bcdedit /? FORMATS » pour plus d'informations sur les
                formats de données.
```

Si on veut faire apparaître le menu de boot (même si il y a un seul OS) par exemple pour laisser le temps de voir les options disponibles avec F8, alors il faut mettre ON dans le type **DISPLAYBOOTMENU** de la section {bootmgr}

Comme dans

Bcdedit /set {bootmgr} displaybootmenu on

BCDEDIT et Chargeur de démarrage – Boat Loader :

L'entrée du magasin correspondante est **{current}**

- cette entrée existe toujours,
- et elle est dupliquée pour chaque installation de Seven Vista ou Serveur2008, dans ce cas elle n'est pas identifiée par **{current}** mais plutôt par un **{xxxguidxxx}**

```
Chargeur de démarrage Windows
-----
identificateur      {current}
device              partition=C:
path                \Windows\system32\winload.exe
description          Microsoft Windows Vista
locale              fr-FR
inherit              <bootloadersettings>
nointegritychecks   No
osdevice             partition=C:
systemroot           \Windows
resumeobject        <324e1371-5d1b-11dc-8bf1-d6f4bef89e58>
nx                  OptIn
```

Renommer une entrée :

Et le type **Description** est une chaîne de caractère

Comme dans

Bcdedit /set {current} description « Windows Seven Pro »

```
C:\>bcdedit /set {current} description "Windows Seven Pro"
L'opération a réussi.
```

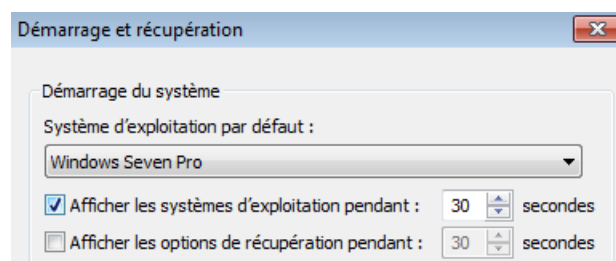
N.B : Pour nous ici, s'il s'agit de renommer l'entrée de notre Seven actuel (en cours), <id> pourra prendre la valeur absente, car cela vaudra **current** !
L'écriture simplifiée pourrait être

Bcdedit /set description « Windows Seven Pro »

donc cela donne

```
Chargeur de démarrage Windows
-----
identificateur      {current}
device              partition=C:
path                \Windows\system32\winload.exe
description          Windows Seven Pro
locale              fr-FR
inherit              <bootloadersettings>
recoverysequence    <6900ba1d-1c65-11df-9c4e-9f716fb9c591>
recoveryenabled      Yes
osdevice             partition=C:
systemroot           \Windows
resumeobject        <6900ba1b-1c65-11df-9c4e-9f716fb9c591>
nx                  OptIn
```

et dans l'interface graphique on retrouve



BCDEDIT et Chargeur ancien système – Legacy Boot Loader :

L'entrée du magasin correspondante est {ntldr}

- cette entrée n'existe pas toujours, uniquement si on utilise une installation en Dual-Boot avec des système NT-2000-XP
- dans le cas où elle existe, elle est unique

Renommer une entrée :

On veut renommer notre « Ancien Windows »

```
Chargeur de système d'exploitation Windows d'ancienne génération
-----
identificateur      {ntldr}
device              partition=D:
path                \ntldr
description          Version antérieure de Windows
```

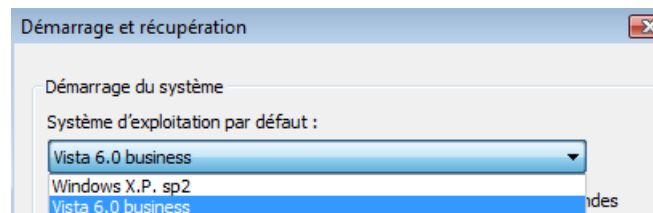
donc <id> devra prendre la valeur {ntldr}

```
C:\>bcdedit /set {ntldr} DESCRIPTION "Windows X.P. sp2"
Opération réussie.
```

donc cela donne

```
Chargeur de système d'exploitation Windows d'ancienne génération
-----
identificateur      {ntldr}
device              partition=D:
path                \ntldr
description          Windows X.P. sp2
```

et dans l'interface graphique on retrouve



BCDEDIT option /store :

Si Bcdedit fonctionne par défaut avec l'entrée en cours d'utilisation, on peut lui indiquer avec quel magasin il doit travailler. C'est l'option **/store** qui permet cela.... Et elle est utilisable avec pratiquement toutes les commandes bcdedit existantes.

Imaginons effectuer une copie de notre magasin...

```
C:\Users\Administrateur>bcdedit /export "d:\backup-bcd\testbcd"
L'opération a réussi.
```

Au lieu de travailler sur l'original, on peut travailler sur la copie si on rajoute dans toutes les commandes l'option **/store "d:\backup-bcd\testbcd"**...

On peut donc par exemple visualiser le magasin sauvegardé par...

```
C:\Users\Administrateur>bcdedit /store "d:\backup-bcd\testbcd" /enum
```

Dupliquer une entrée...

```
C:\Users\Administrateur>bcdedit /store "d:\backup-bcd\testbcd" /copy {default} /d "copie du boot"
L'entrée a été correctement copiée dans {73a1cebe-86e0-11e0-b2a7-0004769b1b3b}.
```

Utilitaire Bootsect & changement bcdedit / ntldr:

Sur une machine Multi-Boot XP – Seven ou entre deux systèmes famille ntldr et bcdedit, on peut arriver à un plantage complet, et à une non information dans la MBR du lanceur à aller chercher dans le secteur de boot de la partition principale

- ✓ on peut utiliser **Bootsect.exe** pour restaurer la MBR du disque et le secteur de boot qui va chercher bootmgr (donc restauration boot seven....)
- ✓ on peut utiliser **Bootsect.exe** pour restaurer la MBR du disque et le secteur de boot qui va chercher ntldr (donc restauration boot Xp....)

Cet utilitaire est disponible sur le Media d'installation de Seven, dans un dossier **lboot**. Il est également disponible dans le kit **Waik** de microsoft

l'utilisation de cet utilitaire permet de faire face, soit depuis la **console RE** de vista, soit depuis la **console de récupération** XP... à une perte de l'amorçage selon le système voulut dans la MBR...

Installer Seven à coté de XP (multi-boot)

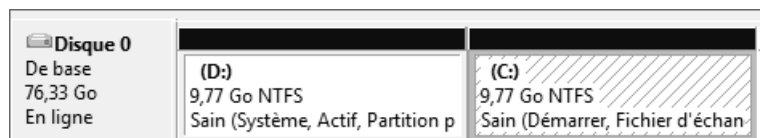
C'est une procédure simple, si l'on suit l'ordre des versions, car microsoft a développé des systèmes à compatibilité ascendante:

- Windows XP étant installé sur la première partition Active...
- Il faut installer Seven dans une autre partition principale (voire un autre disque), ayant au mois 12 Giga de libre
Il n'est plus possible de faire cohabiter Seven et Xp dans une même partition.
- Il faut booter sur le CD de Seven (pour désactiver la mise à niveau) et demander d'installer avec les options avancées
- Il faut choisir une nouvelle partition, la formater et lancer l'installation

N.B : il est conseillé de préparer sa partition disque dur depuis XP, en effet le Setup d'installation de Seven ne donne pas toutes les possibilités de création de partions de reformatage voulues, et parfois refusera une installation sur un disque non préparé (volume dynamiques...)

même disque, autre partition :

Le résultat fonctionne, la partition active est inchangée ! (mais le lettrage est modifié dans Seven qui se trouve en C : et la partition principale active passe en D :...)



- ✓ Ce qui amènera aussi également la présence sur D : du dossier **lboot** et du fichier **bootmgr** (qui se stockent sur la partition active...)
- ✓ le lecteur de Seven est déclaré en C :

autre disque :

Ce sera sans doute le cas le plus fréquent.

On ajoute un deuxième disque dans la machine, et on le prépare depuis XP (partitionnement)

Volume	Disposition	Type	Système de fichiers	Statut	Capacité
(D:)	Partition	De base	NTFS	Sain	38,2
disque-xp (C:)	Partition	De base	NTFS	Sain (Système)	37,2

The screenshot shows the Disk Management console. Disk 0 (38,28 Go) has a primary partition (D:) of 38,28 Go, NTFS, and is healthy. Disk 1 (37,26 Go) has a primary partition (disque-xp (C:)) of 37,26 Go, NTFS, and is healthy. A legend indicates that the blue bar represents the 'Partition principale' (Primary Partition).

Le résultat fonctionne, la partition **active** est inchangée ! (mais le lettrage est surprenant dans Seven qui se trouve installé en C : et avec la partition principale active décalée en D : ...)

- ✓ Ce qui amènera aussi également la présence sur D : du dossier **lboot** et du fichier **bootmgr** (qui se stockent sur la partition active...)
- ✓ Le lecteur de Seven est déclaré en C :

Volume	Disposition	Type	Système de fichiers	Statut
(C:)	Simple	De base	NTFS	Sain (Dé
disque-xp (D:)	Simple	De base	NTFS	Sain (Sy
LRMBVOL_FR_CD1 (E:)	Simple	De base	CDFS	Sain (Pa

The screenshot shows the Disk Management console. Disk 0 (38,29 Go) has a primary partition (C:) of 38,28 Go, NTFS, and is healthy. Disk 1 (37,27 Go) has a primary partition (disque-xp (D:)) of 37,26 Go, NTFS, and is healthy. A legend indicates that the blue bar represents the 'Partition principale' (Primary Partition).

Installer XP à coté de Seven

Si vous voulez installer une version antérieure du système d'exploitation Windows sur un ordinateur Windows Seven, c'est beaucoup plus complexe, et non garanti sur la fiabilité de l'opération !

En effet le programme d'installation remplace tout le contenu de la MBR, du secteur de démarrage et des fichiers de démarrage. Par conséquent, la version antérieure du système d'exploitation Windows perd sa compatibilité en aval avec Windows Seven.

1. pour installer Windows Xp il faut impérativement prévoir une partition différente de celle où Seven est installée, ou (rajouter un disque)

N.B : Si on veut pouvoir "désinstaller" Seven et laisser ensuite uniquement Xp, il faut que la partition sur laquelle on installe Xp soit principale (sinon elle ne sera pas amorçable...) par conséquent il est préférable de créer cette partition au préalable, en effet l'installation de Xp sur un système ayant déjà une partition, crée par défaut une partition étendue...

2. Il faut booter sur le CD de XP et lancer une installation, dans laquelle on demande d'installer Xp sur la partition voulue, en la formatant. on se retrouve avec un XP sans trace de Seven au boot...

N.B : il se peut que lors de la phase d'installation, un message d'erreur apparaisse..... cela vient du fait que l'installation « casse » la MBR et l'appel au secteur de boot. (dans ce cas passer à l'étape 3)

3. Utilisez **Bootsect.exe** pour restaurer le MBR Windows Seven et le code de démarrage qui transmet le contrôle au Gestionnaire de démarrage.

En invite de commandes :

lecteur:\boot\Bootsect.exe /NT60 All

N.B : lecteur représente le lecteur dans lequel se trouve le media d'installation de Windows Seven.
(Le dossier de démarrage figure sur le lecteur de CD-DVD.)

Maintenant on à de nouveau Seven !, mais sans XP...

4. Il faut utiliser **Bcdedit.exe** pour créer manuellement une entrée dans le magasin permettant de lancer la version antérieure du système d'exploitation Windows.

En invite de commandes :

Bcdedit /create {ntldr} -d " xxxx "

N.B : Dans cette commande, xxxx peut être remplacé par le texte de votre choix. Par exemple « Windows XP »

Bcdedit /set {ntldr} device partition=x:

N.B : Dans cette commande, x: correspond à la lettre qui désigne le lecteur de la partition active.

Bcdedit /set {ntldr} path \ntldr

Bcdedit /displayorder {ntldr} -addlast

5. Redémarrez l'ordinateur

Supprimer un boot Seven (retour boot Xp):

Sur une machine Multi-Boot XP – Seven comme crée précédemment, on souhaite ne pas garder Seven et retrouver la machine native XP

- ✓ Il faut utiliser **Bootsect.exe** pour restaurer la MBR du disque et le secteur de boot qui transmet le contrôle au Gestionnaire de démarrage Windows ancienne version (NTLDR).
- ✓ Il faut effacer toutes traces de SEVEN

On pourrait imaginer le mode opératoire suivant :

1. En invite de commandes :

lecteur:\Boot\ Bootsect.exe -NT52 All

N.B : lecteur représente le lecteur dans lequel se trouve le media d'installation de Windows Seven.

(Le dossier **\Boot** figure sur le Média Seven.)

2. Redémarrez l'ordinateur
et donc uniquement Xp apparaît au boot.
3. Supprimer la partition sur laquelle Seven était installé
4. Faire le ménage des fichiers amenés par Seven sur la partition qui reste
(ou se trouve Windows XP) notamment :
 - un dossier **\boot** à la racine (il faut d'abords s'approprier le dossier en NTFS, pour se donner les droits dessus)
 - un fichier **bootmgr** à la racine (il faut d'abords s'approprier le dossier en NTFS, pour se donner les droits dessus)

Supprimer un boot XP (retour boot Seven):

Sur une machine Multi-Boot XP – Seven comme crée précédemment, on souhaite garder Seven et supprimer définitivement XP.

- ✓ Il faut utiliser **Bootsect.exe** pour restaurer la MBR du disque et le secteur de boot qui va chercher bootmgr
- ✓ Il faut effacer toutes traces de XP

1. il faut transférer sur la future partition active les fichiers nécessaire au boot vista (actuellement stockés dans la partition active qui contient xp, vue en D : ...) c'est à dire le dossier **\boot** et le fichier **bootmgr**

N.B : (Le dossier **\Boot** contient une partie de la base de registre sur laquelle Seven est lancé, il faut faire cette manipulation depuis la console de recup Seven Pour que la base ne soit pas lue)

N.B : La « console » se lance en bootant sur le CD Seven puis - **réparer l'ordinateur** - dans la boîte de dialogue « options de récupération système » suivant, puis **invite de commande...**

N.B : toujours dans La « console » vérifier le lettrage utilisé, en fait il faut repérer les lettre qui correspondent a telle ou telle partition, car ce ne sont pas forcément les mêmes qu'utilise Seven en mode OS normal !

Donc sachant que

dir /A (affiche fichier– dossier cachés)

il faut vérifier en console de récupération qui apparaît avec quel lecteur logique, avant d'effectuer les opérations suivantes :

mkdir C:\Boot (creation du dossier receptacle)

D :

xcopy D:\Boot C:\Boot /c /h /o /s /e (copie de tout le dossier)

xcopy D:\bootmgr C:\ /h (copie du fichier)

On sort de la console et on redémarre....

2. Il faut activer la future partition active C : (à la place de l'ancienne D :)
Via dans le gestionnaire de disque, menu contextuel en pointant la partition **Marquer la partition comme active**

3. Il faut pour cette partition restaurer un secteur de boot amorçant Seven (et non pas XP comme il l'est actuellement) :

lecteur:\Boot\ Bootsect.exe -NT60 All

N.B : lecteur représente le lecteur dans lequel se trouve le media d'installation de Windows Seven.
(Le dossier **\Boot** figure sur le Média Seven.)

Pour que le changement soit effectif, redémarrer le poste

4. Il faut nettoyer le gestionnaire d'amorçage via **bcdedit** pour supprimer l'entrée XP et indiquer le nouveau chemin du lanceur **bootmgr**

Bcdedit /delete {ntldr} /f

Bcdedit /set {bootmgr} device partition=c:

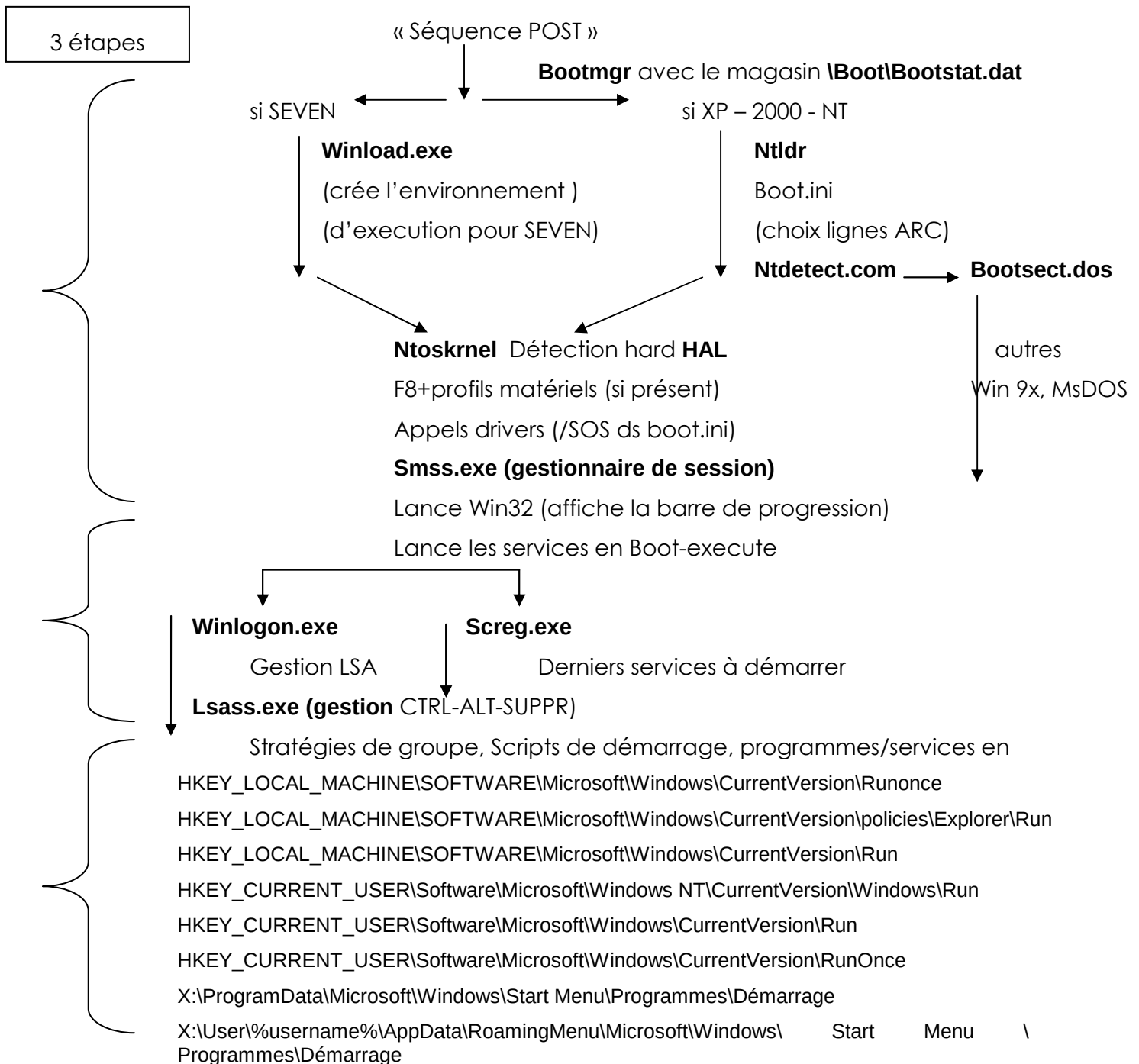
5. Il est possible de récupérer la place prise par l'ancien XP, le plus simple étant de supprimer le volume et de recréer une partition...(ou enlever le disque...)

LES PROCESSUS SOUS SEVEN

Séquence POST : Power On Self Test

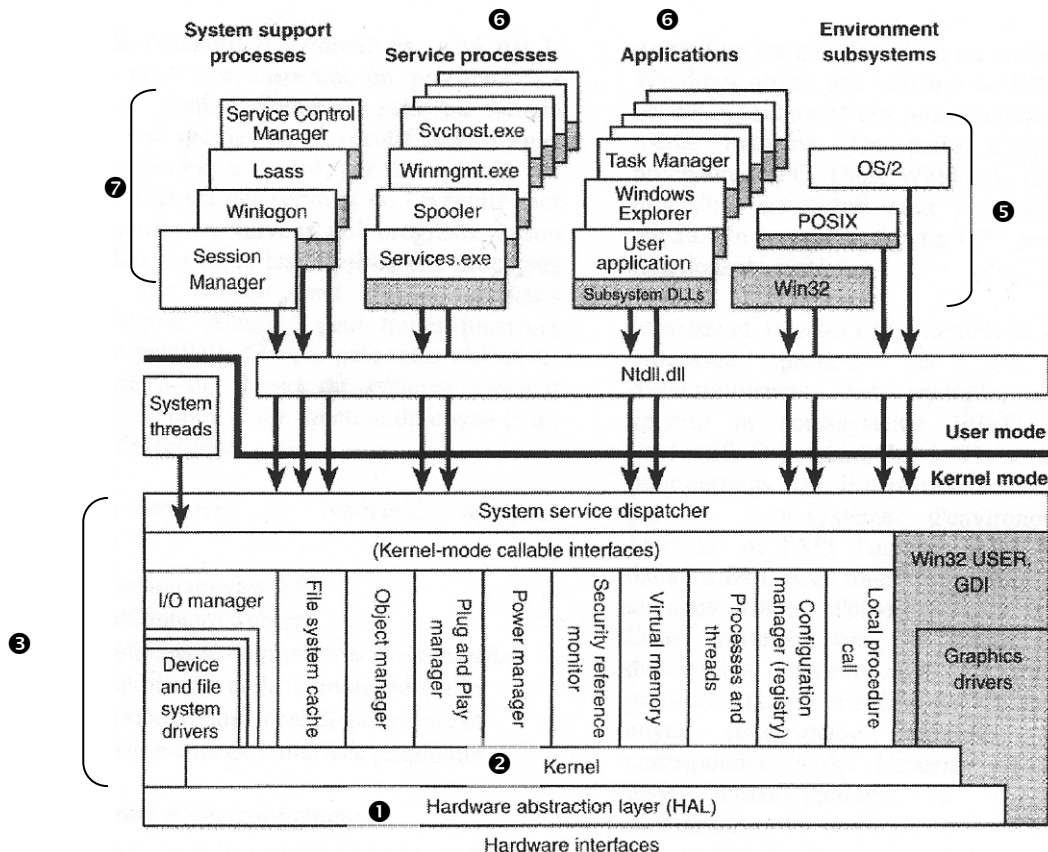
C'est la séquence que tous PC déroule, indépendamment du système. Le **BIOS** ou le **EFI** du PC vérifient la présence de certains matériels, (mémoire, disque, périphériques). Après cette séquence l'ordinateur doit trouver le gestionnaire de démarrage Vista nommé **Bootmgr**.

Séquence démarrage Bootmgr



Vocabulaire système sous SEVEN :

Très schématiquement on peut distinguer :



- LA **HAL ①** ou couche d'abstraction matérielle : fournit des fonctions pour contrôler le bus système, canaux DMA, déclenchement des interruptions, horloge système... toutes ces fonctions sont utilisées dans les autres parties du noyau
- Le **Kernel ②** (micro kernel) : c'est le noyau toujours en mémoire, traite les interruptions, permet au CPU d'allouer du temps aux différents processus, appelé aussi **threads**.
- **L'exécutif ③** (serveur noyaux) : c'est l'ensemble des services système de gestion mémoire – périphériques – fichiers – appelé donc threads système. Chaque service système progresse à son propre rythme
- les **services noyaux sous systèmes environnement ④** : il s'agit de supporter différentes interfaces... : win32 – posix – Os2... par exemple l'exécutif de windows définit un ensemble de fonction nommée **API (Access Programming Interface)**. ⑤ Un programme utilisateur fait appel à des API système pour dialoguer avec l'OS.
- les **services noyaux systèmes ⑥** nécessaires comme le spool d'impression, task manager ... et les **services de sécurité** associés ⑦
- Certaines applications peuvent utiliser directement des **DLL Dynamic Link Library**... qui elles feront appel si nécessaire aux API système

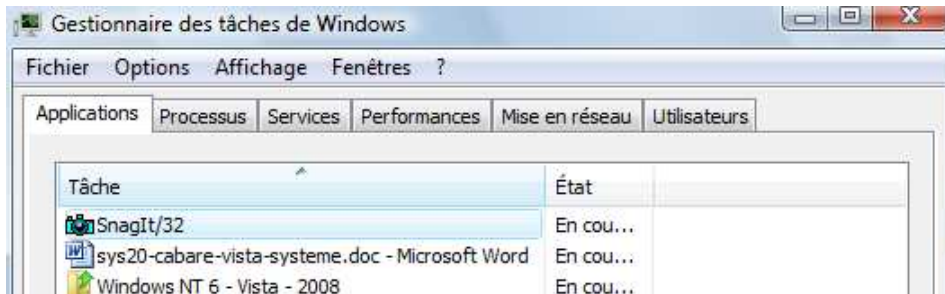
Les appels entre ces programmes sont nommés **LPC Local Procedure Call** s'ils se font sur une machine, ou **RPC Remote Procedure Call** à distance.

Lister les Processus en cours :

Il existe une interface graphique, et une invite de commande plus complète...

Interface classique graphique:

Appelable via **CTRL+ALT+SUPPR** ou via les propriétés de la barre des tâches, le **Gestionnaire des tâches** donne une vision plus complète de la chose !



3 onglets sont disponibles, **Applications / Processus / Services** :

Application :

Programme lancé par l'utilisateur, ou lancé automatiquement au démarrage de Windows. Tourne dans une interface fenêtre, normalement sans incidence sur le fonctionnement de SEVEN

Processus :

Correspond à des programmes vus par le système d'exploitation. Un processus est caractérisé par le fait qu'il a une identification (**PID**) au niveau du système, des dépendances et une priorité d'exécution. Il peut contenir plusieurs services.

Services :

Programme géré par le système d'exploitation comme "partie intégrante du système". Un service est caractérisé par le fait qu'il peut se gérer via le gestionnaire de service Seven et est lancé dans un processus, souvent avec d'autres services.

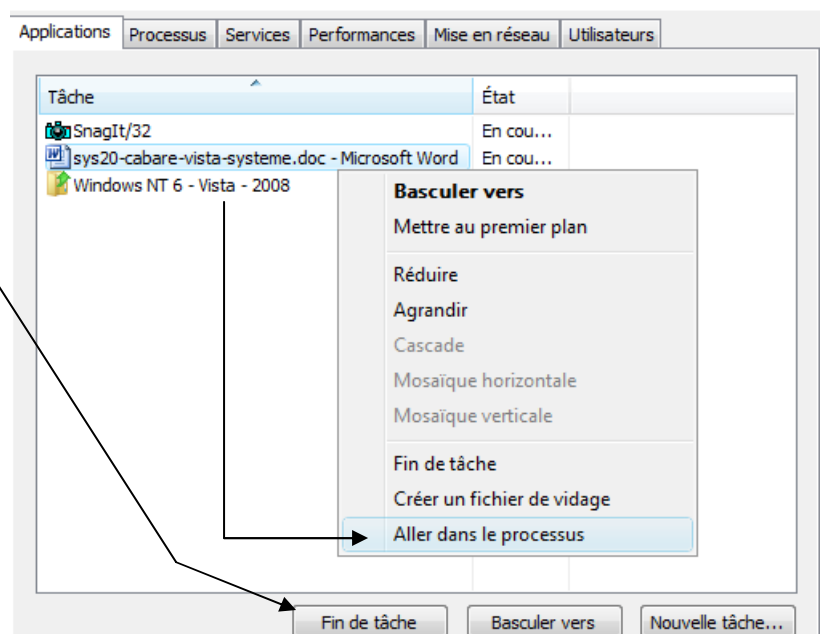
Onglet Application :

Dans l'onglet **Application** on peut

Fin de tâche : arrête d'un programme planté

Si impossible, on peut demander **Aller dans le processus**

et arrêter le processus



Onglet Processus :

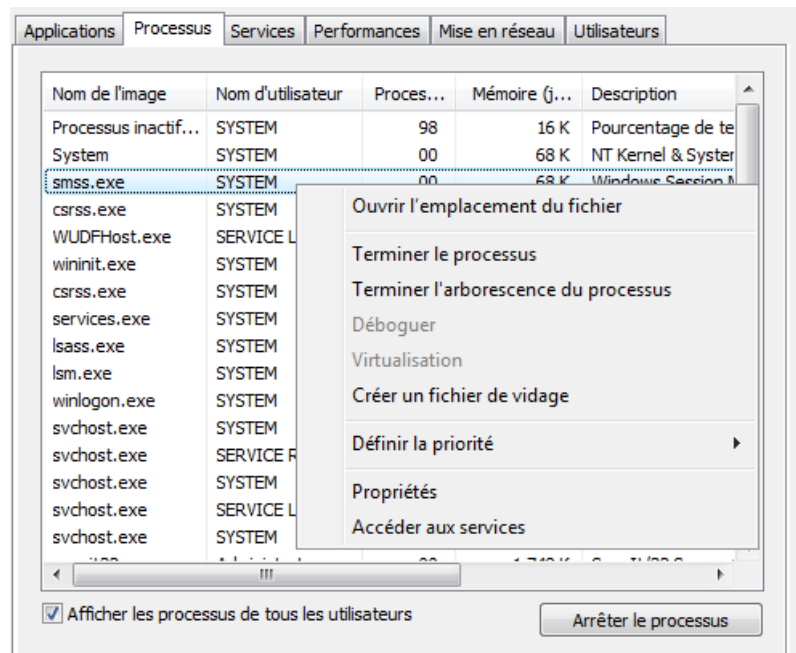
Dans l'onglet **Processus** on peut

Arrêter le processus : ou l'arborescence du processus via clic droit

Ouvrir l'emplacement du fichier via clic droit

Définir la priorité du processus

on peut demander **Afficher le PID** via le menu affichage / sélectionner les colonnes (et tuer le PID via **TaskKill**)



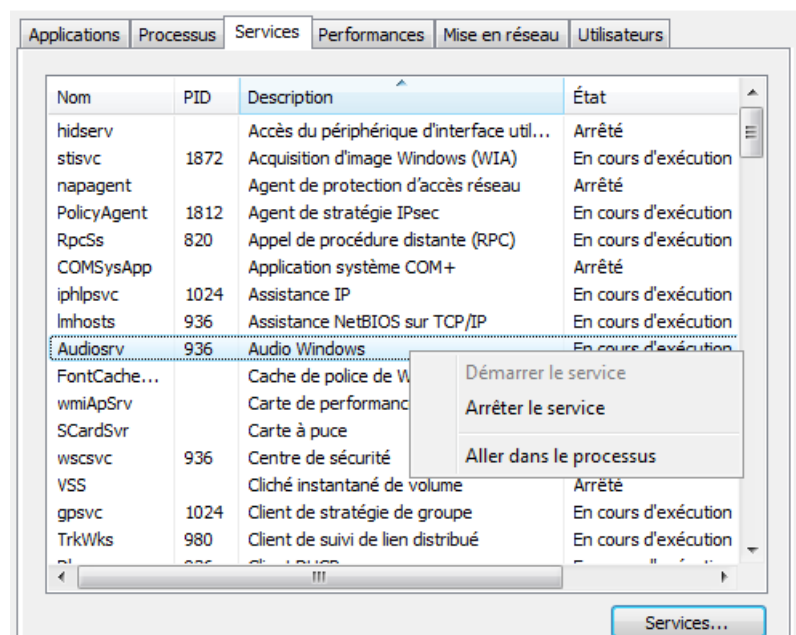
Onglet Services :

Dans l'onglet **Services** on peut

Arrêter/Démarrer un service: selon son état

Accéder à la gestion des services **via Services...**

Parfois "remonter" dans le processus qui héberge le service via **Aller dans le processus**



Tasklist (SEVEN - XP):

```
C:\Documents and Settings\Administrateur>tasklist /?  
TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]  
          [/M [module] : /SVC : /UI [/FI filtre] [/FO format] [/NH]
```

Cette commande porte pas mal de zone d'ombre...

Tasklist et Tasklist /SVC

Si cette option fonctionne, les autres options on l'air plus délicates à utiliser...

Taskkill (SEVEN - XP):

```
C:\Documents and Settings\Administrateur>taskkill /?  
TASKKILL [/S système] [/U utilisateur [/P mot_de_passe]]  
< [/FI filtre] [/PID ID_processus : /IM image] > [/F] [/T]
```

Taskkill /PID x

Et

Taskkill /PID x /F

Et

Taskkill /PID x /F /T

fonctionnent, les autres options on l'air plus délicates à utiliser...

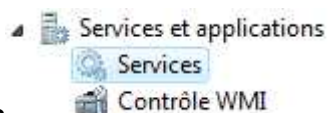
Quelques Processus de base

Depuis les premiers processus vitaux lancé par le système... on peut retrouver

Processus	Type Arrêt	Commentaires
Smss.exe	Vital pour l'OS	Gestionnaire de session, lancé par le système et appelant à son tour Csrss.exe et Winlogon
Csrss.exe -	Vital pour l'OS	Portion de sous système
Winlogon	Vital pour l'OS	Demande d'identification
Lsass.exe	Arrêt par PID unique	Serveur authentification local, génère pour winlogon à l'aide de msgina.dll un jeton...
Svchost.exe	Arrêt par PID unique	Processus générique servant d'hôte pour d'autres processus... On peut fouiller avec tasklist...
Services	Arrêt par PID unique	Gestionnaire de contrôle des services
Spoolsv.exe	Arrêt par PID unique	Gestion des tâches d'impression

Gestionnaire de Services

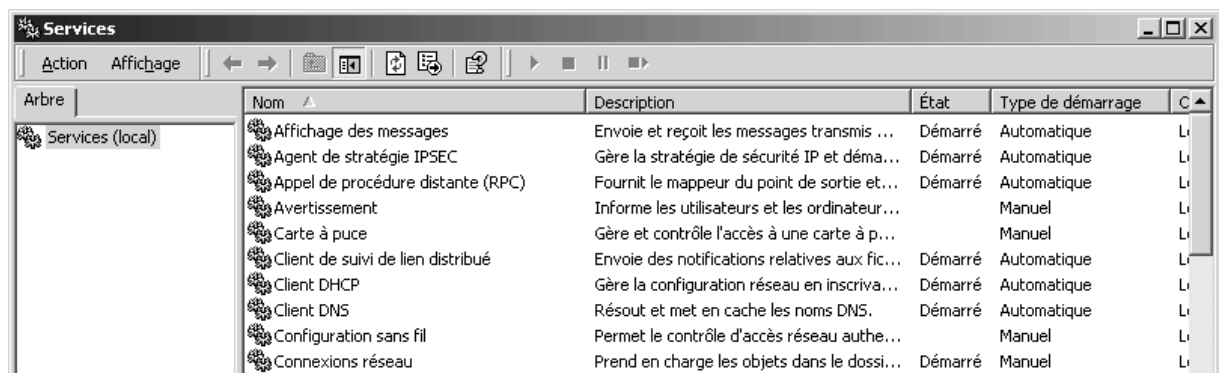
Ces processus correspondent à des services qui peuvent se gérer via une interface graphique, accessibles via



Clic droit - **ordinateur** / **Gérer** / **Services**



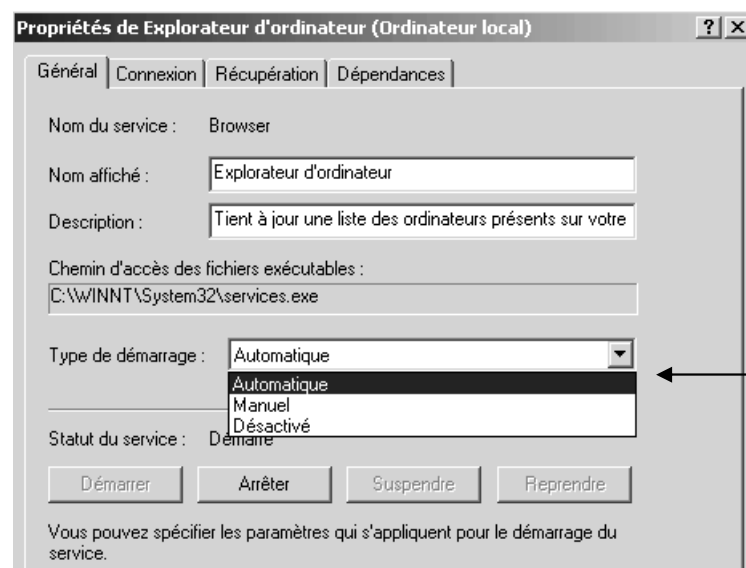
panneau de configuration / **Outils d'administration** /



Sur un service particulier

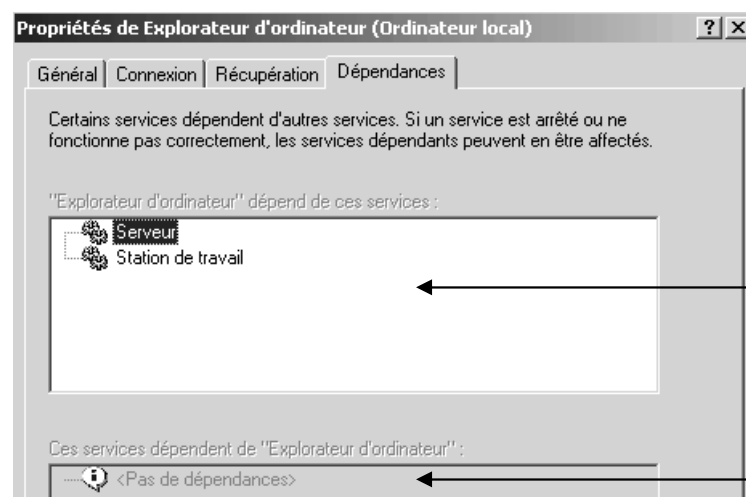


on demande via les propriétés



Essentiellement pour le prochain démarrage du poste

et on peut avoir une idée des dépendances...



De qui ce service dépend...

Qui dépend de ce service...

DRIVERS

les anciens types vxd - sys - wdm :

Windows9x - vxd

Successeur du vieux DOS à 16 bits. Lors de la conception de ce système d'exploitation, la compatibilité en amont était une condition incontournable. Windows9x permet un accès direct au matériel

En ce sens, ce genre de dispositifs comportent une série de contrôleurs virtuels (dont l'extension est **.vxd**) qui ne sont pas compatibles avec Windows 2000. Ces pilotes ont un nom **VxD** pour **Virtual x Device** et x pouvant valoir D=Display – P=Printer – T=timer – X=inconnu.

Windows NT - sys

Nouveau système, nouveaux type de drivers (dont l'extension est **.sys**) qui ne sont pas compatibles avec Windows 2000

Windows 2000 – wdm

Introduit le nouveau modèle de contrôleurs de Windows fondés sur Windows Driver Model (**WDM**) qui permet aux systèmes d'exploitation Windows98 d'utiliser théoriquement les mêmes contrôleurs !

Cependant, les différences dans la conception et le développement des deux systèmes empêchent tout driver WDM contenant des parties de son code à 16 bits de fonctionner sous Windows 2000 et donc VISTA

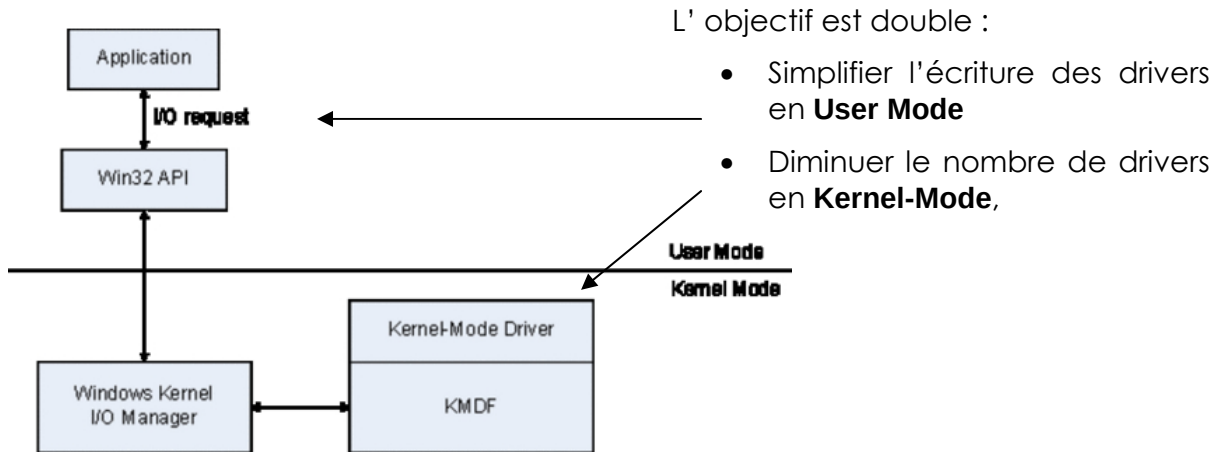
Pour communiquer avec le système, le pilote passe par une interface que l'on appelle communément **device-driver interface** ou **DDI**. De même, ces DDI sont très proches du noyau et leur modification implique souvent une recompilation des pilotes les utilisant. Ces DDI sont critiquées par les développeurs qui les trouvent trop compliquées à utiliser lorsqu'il s'agit de gérer le Plug and Play, les entrées / sorties asynchrones ou la gestion de l'énergie.

De plus, lors de la création de son modèle, Microsoft n'avait pas prévu tous ces développements de drivers annexes, et, afin de garantir des performances optimales, les **DDI** ont été rattachées au noyau. L'inconvénient, c'est qu'un driver instable, peut corrompre le système et le bloquer

Les Drivers Vista Seven WDF :

Pour Vista, a créer un nouveau modèle de pilotes séparé de la base de son système. C'est la naissance de la **Windows Driver Foundation** ou **WDF**. Ce modèle contient trois composants principaux

- Le Kernel-Mode Driver Framework (KMDF)
- Le User-Mode Driver Framework (UMDF)
- Des outils de vérification des pilotes



Lorsqu'une application envoie une requête d'entrée / sortie à un pilote basé sur les **MDF**, cette requête arrive d'abord à l'API Win32 qui se charge de la transmettre au noyau du système. Dans les cas des pilotes en espace utilisateur, cette gestion est dévolue au framework et le code s'en trouve allégé. Comme les pilotes s'exécutent en espace utilisateur, ils se retrouvent un peu dans le cas d'un programme quelconque et n'ont accès qu'à l'espace mémoire qui a été alloué à leur processus. Un plantage du pilote ne corrompra plus l'ensemble du système, qui pourra redémarrer le pilote par la suite comme un programme utilisateur classique.

Magasin de drivers :

Sous XP, il fallait installer le périphérique avant le driver

1. on connectait le périphérique
2. le service Plug and Play le détectait
3. XP cherchait le pilote dans les chemins fournis (ou connaissait le driver)
4. installation

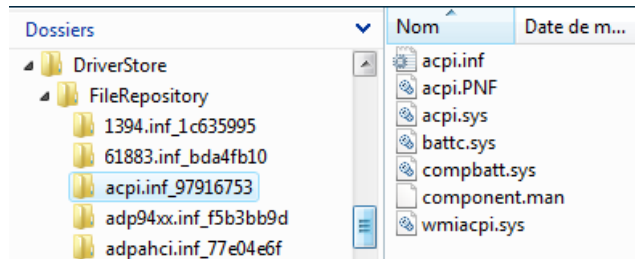
Sous SEVEN, il existe deux étapes distinctes

1. mise en place du driver (intégration des pilotes) dans le magasin de pilotes
2. installation du pilote depuis le magasin lorsque le service plug and play de SEVEN détecte le périphérique

l'objectif est de dissocier mise à disposition d'un driver (nécessitant des droits d'administration, et avec une procédure vérifiant la qualité du Driver) , et installation du périphérique (que l'on peut faire sans avoir de Droits élevés).

Mise en place du pilote dans le magasin

Le magasin se trouve en **c:\windows\system32\DriverStore**



Et contient tous les périphériques qu'il gère nativement. Outre les pilotes que SEVEN connaît, la mise en place de nouveaux drivers peut se faire

- Si le périphérique n'est pas connecté par des outils comme **pnputil.exe**, **drvload.exe**, ou en utilisant des outils de déploiement genre **WAIK**
- Si le périphérique est connecté, "à la volée" avec le disque et l'assistant ajout de matériel (mais avec des droits d'administration)

Installation du pilote lors du P&P par SEVEN

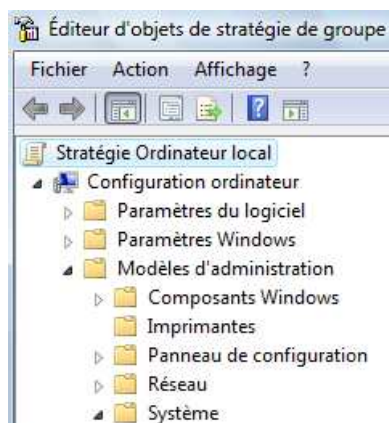
1. on connecte le périphérique
2. le service Plug and Play le détecte
3. SEVEN cherche le pilote dans le magasin, si un pilote est présent, il installe le périphérique sans autres formes de procédure.
4. Si un pilote n'est pas présent, SEVEN cherche dans les chemins fournis MAIS vérifie que l'utilisateur dispose des autorisations nécessaires, et vérifie à la volée le Drivers, avant de le stocker dans le magasin, Puis de l'installer.

Stratégies de gestion de drivers :

Comme désormais il est possible d'installer potentiellement un périphérique sans avoir de Droits élevé, de nouvelles **Stratégies** sont disponibles dans

gpedit.msc... Puis

Configuration ordinateur \Modèles d'administration\Systeme



Deux entrées nouvelles

- Installation de périphériques
- Restrictions d'installation de périphériques
- Installation de pilotes

Drivers certifiés :

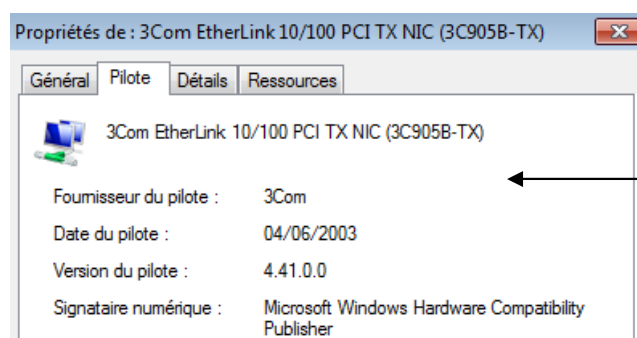
Les fichiers des pilotes de périphériques et du système d'exploitation fournis avec Windows ont une signature numérique Microsoft.

La signature numérique indique qu'un pilote ou fichier précis a atteint un certain niveau de test et qu'il n'a pas été modifié - endommagé - ou remplacé par le processus d'installation d'un autre programme.

on parle de pilotes certifiés **WHQL: Windows Hardware Quality Labs**.

Il en va de même pour un grand nombre de fichiers indispensables au bon fonctionnement du système d'exploitation

Seven accepte par défaut uniquement des pilotes certifiés, mais pas forcément conçus pour lui ! (Certifier ne veut pas dire développer pour...)



Voici un driver accepté par SEVEN datant de 2003 !

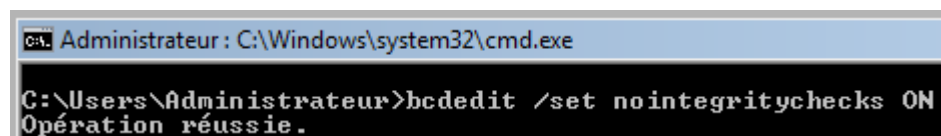
Installation de pilotes non certifiés :

Soit au démarrage par la touche **F8** puis on demande l'option de démarrage

- **Désactiver le contrôle obligatoire de la signature des pilotes**

Soit en invite de commande

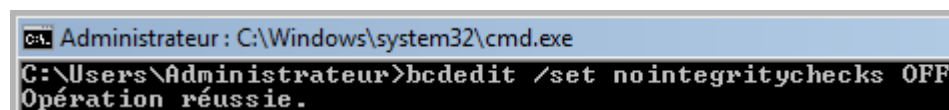
Bcdedit /set nointegritychecks ON



Puis redémarrage, installation du driver

Pour re-protéger du système

Bcdedit /set nointegritychecks OFF



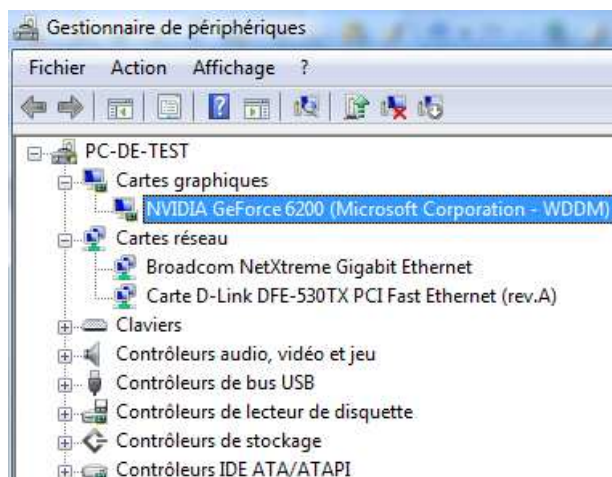
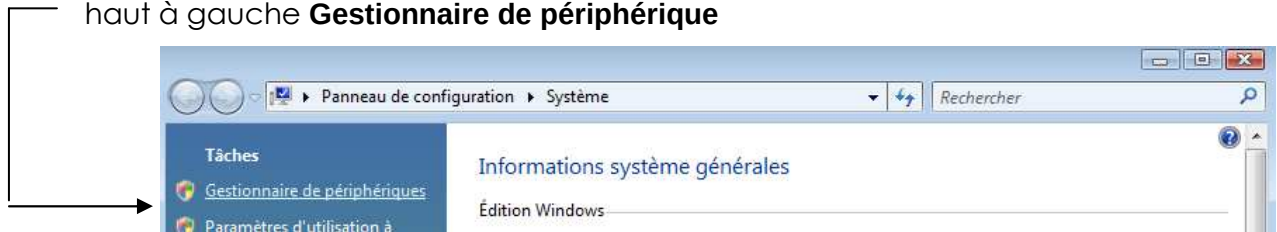
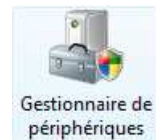
et redémarrage

Gestionnaire de périphérique:

Cela peut se faire de différentes manières, la manière « préconisée » par microsoft étant de faire apparaître via le

panneau de configuration le gestionnaire de périphérique :

on peut aussi y accéder par le propriété du bureau, puis en haut à gauche **Gestionnaire de périphérique**

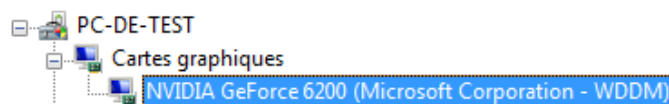


Les familles de périphériques sont listées (par exemple Cartes graphiques)

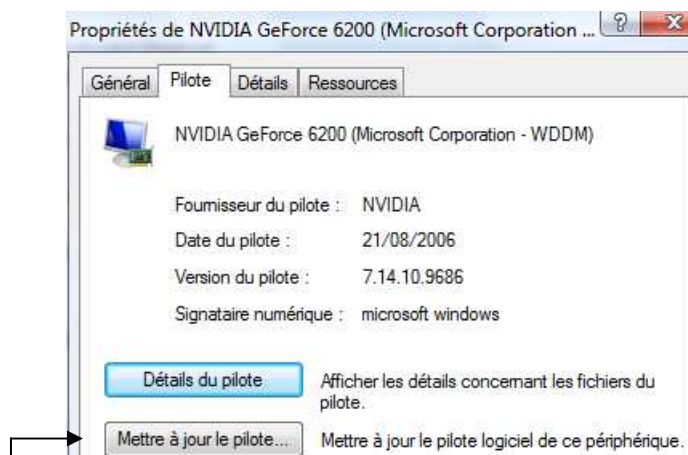
Ainsi que leurs composants (par exemple NVIDIA GeForce 6200)

Versions - Installation de pilotes :

On demande les propriétés du composant sélectionné



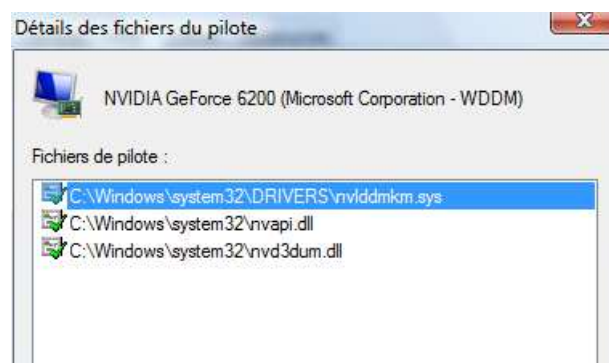
pour obtenir



On peut facilement mettre à jours le pilote

On peut aussi avoir des renseignements sur le driver installé actuellement, et savoir les fichiers utilisés via

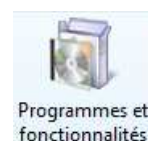
Détails du pilote



Installation driver via Update :

On demande les propriétés du composant sélectionné

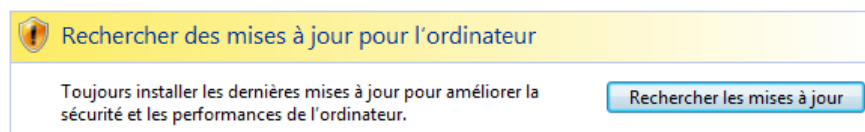
On peut avoir une idée de la provenance du pilote. Dans le panneau de configuration on demande **Programmes et fonctionnalités**



Puis **Afficher les mises à jour installées**

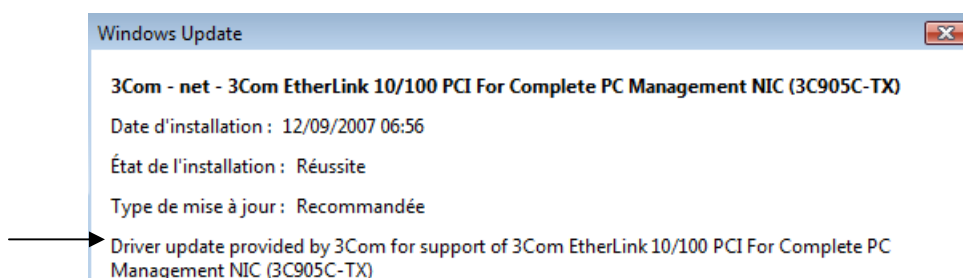
Windows Update / Afficher l'historique des mises à jour

Windows Update

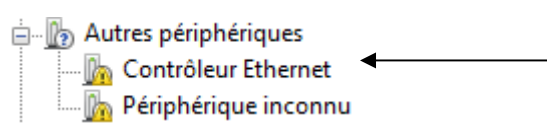


Dernière recherche de mises à jour : Hier à 10:27
Des mises à jour ont été installées : Hier à 10:28. [Afficher l'historique des mises à jour](#)
Vous avez configuré Windows pour : Installer automatiquement les nouvelles mises à jour chaque jour à 03:00 (recommandé)
Vous recevez les mises à jour : Pour Windows et d'autres produits à partir de Microsoft Update

dans la liste, sur une mise à jour, (driver) on demande **afficher les détails**



Installation driver via Fichiers locaux :

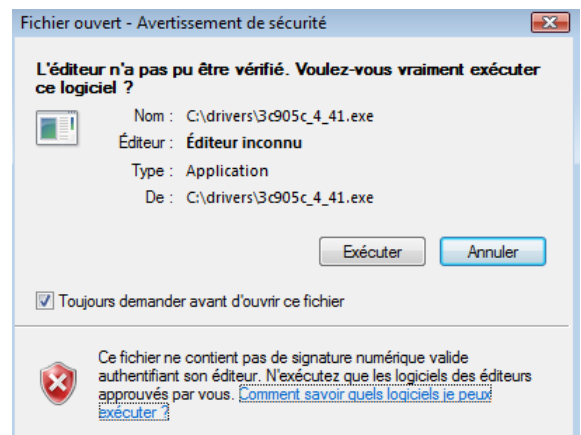


On veut récupérer un driver pour notre carte **3Com 3C905...**

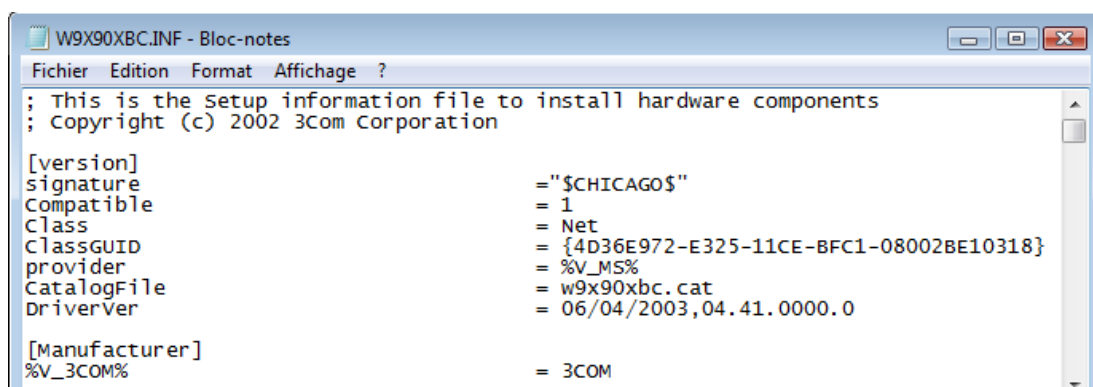
Il faut déjà obtenir un package du driver correct, et l'installer quelque part sur notre poste... Cela peut faire apparaître des mises en garde du au format auto-extractible de ces packages !

Si le constructeur travaille bien, il fournit un fichier **xxx.inf**

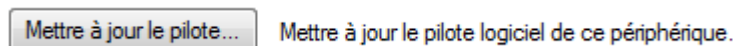
Nom	Date de modificati...
EL90XBC4.SY_	04/06/2003 18:49
EL90XBC5.SY_	04/06/2003 18:37
W9X90XBC.CAT	18/06/2003 17:35
W9X90XBC.INF	05/06/2003 11:44



Contenant la définition du driver et son installation



Ce package il faut ensuite l'installer via **mettre à jour le pilote** :



SEVEN nous demande de choisir, il faut lui indiquer que l'on dispose du package localement

- ➔ Rechercher automatiquement un pilote logiciel mis à jour
Windows va rechercher sur votre ordinateur et sur Internet le pilote logiciel le plus récent pour votre périphérique.
- ➔ Rechercher un pilote logiciel sur mon ordinateur
Recherchez et installez manuellement le pilote logiciel.

Ne pas demander **Rechercher auto...** car cela revient à **Windows Update**

Si il n'y a pas d'ambiguïté sur le nom du dossier dans lequel vous avez votre package, et si le driver est simple (pas de choix entre différents modèles) alors on peut indiquer un emplacement

Rechercher le pilote logiciel sur votre ordinateur

Rechercher les pilotes logiciels à cet emplacement :

F:\3Com\4.41

Parcourir...

☒ Inclure les sous-dossiers

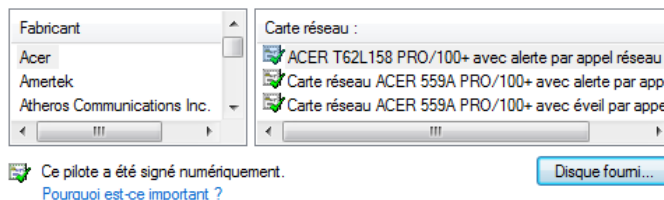
→ Me laisser choisir parmi une liste de pilotes de périphériques sur mon ordinateur
Cette liste affichera les pilotes logiciels installés et compatibles avec le périphérique, ainsi que tous les pilotes logiciels dans la même catégorie que le périphérique.

Si on veut être plus progressif, on demande alors **Me laisser choisir...**

Sélectionnez la carte réseau



Cliquez sur la carte réseau correspondant à votre matériel puis cliquez sur OK. Si vous disposez d'un disque d'installation pour ce composant, cliquez sur Disque fourni.



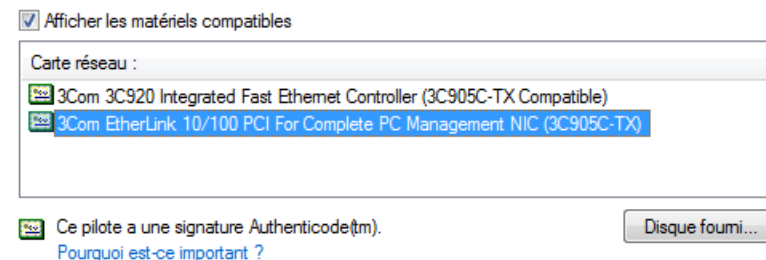
En demandant **Disque fourni** il faut repérer notre fichier **xxx.inf**

Nom du fichier : *.inf
Types de fichiers : Setup Information (*.inf)

4.41	
Nom	Date de modification...
W9X90XBC.INF	05/06/2003 11:44

A ce moment la SEVEN décode le **xxx.inf**

Et si nécessaire nous propose un choix



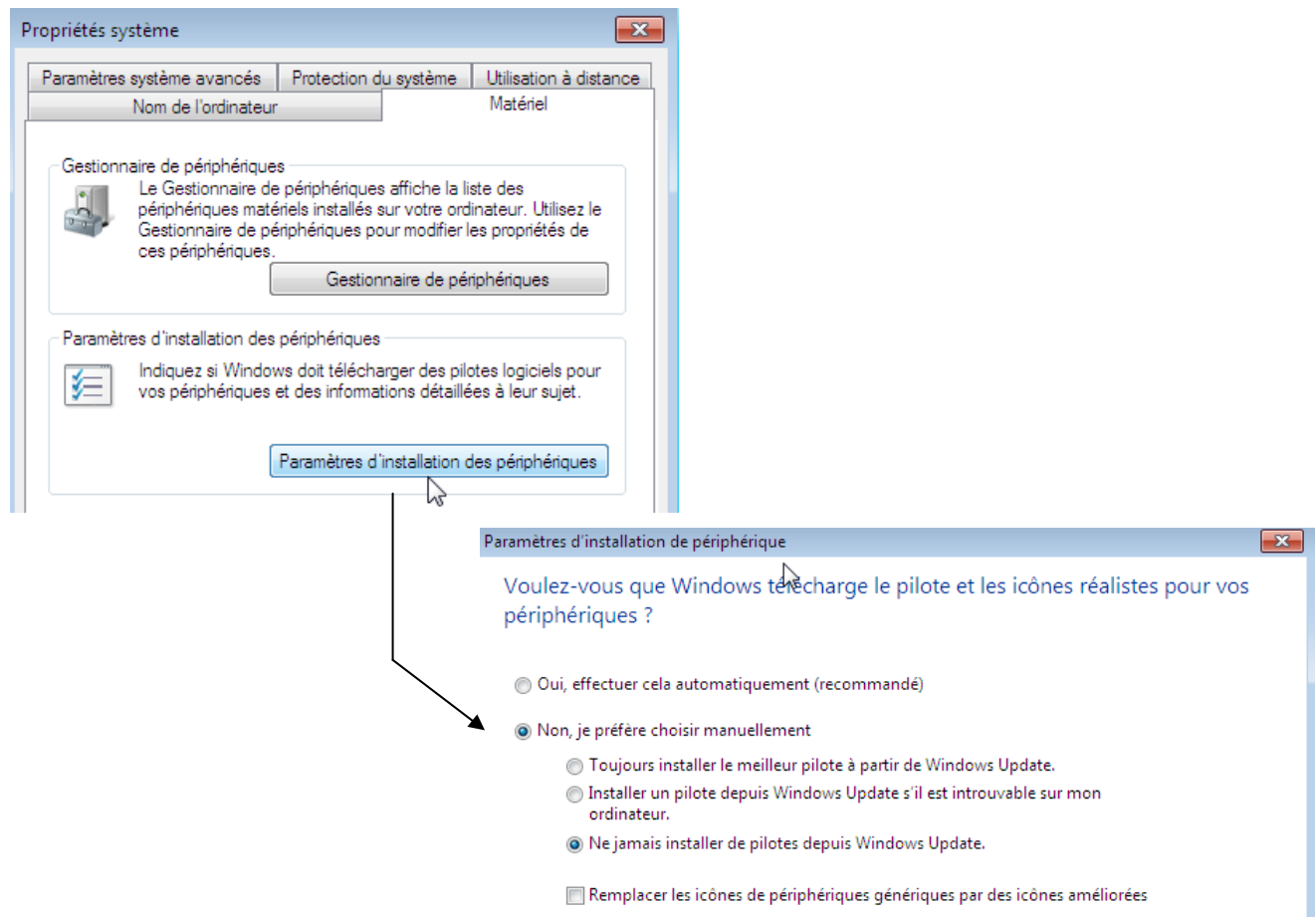
ok

Méthode par défaut installation de drivers :

Réglable dans les propriétés du poste de travail, **paramètres systèmes avancé**
(pour atteindre la boîte de dialogue **propriétés systèmes**)

puis onglet **Matériel**

Paramètres d'installation des périphériques

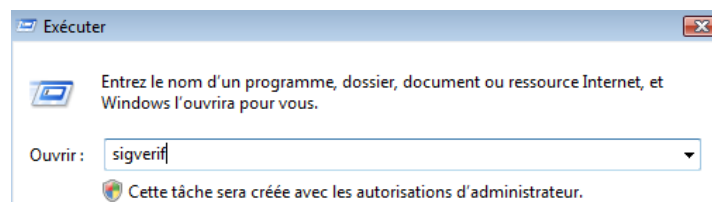


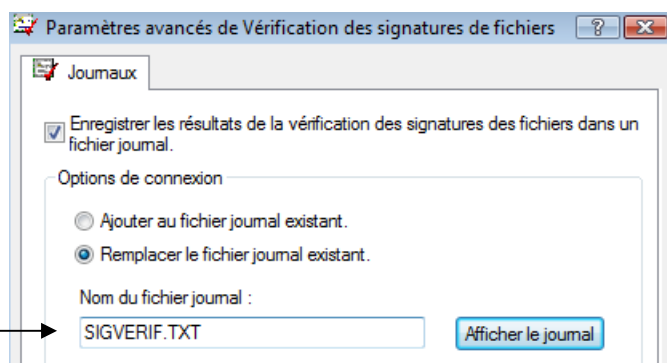
Sigverif vérification drivers signés:

On peut aussi à tout moment demander d'effectuer une vérification sur une machine installée, et sur laquelle on aurait laissé un certain nombre d'installation se faire...

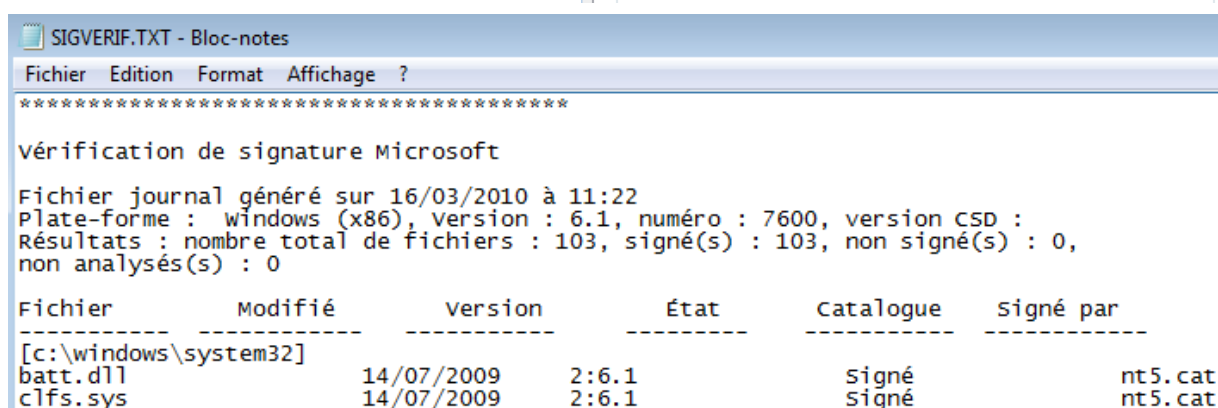
cette vérification peut se faire à partir d'une commande que l'on lance en direct lors d'une session...par la ligne de commande

sigverif





on a le résultat dans un fichier journal



il existe des fichiers signés d'origine (nt5.cat) ou apportés (ici ... microsoft !)

Fichier	Modifié	Version	État	Catalogue	signé par	
[c:\windows\system32]						
batt.dll	14/07/2009	2:6.1	Signé	nt5.cat	Microsoft windows	
clfs.sys	14/07/2009	2:6.1	Signé	nt5.cat	Microsoft windows	
nvd3dum.dll	14/07/2009	2:5.1	Signé	Microsoft-windows-cl	Microsoft windows	
nvgf2um.dll	14/07/2009	2:5.1	Signé	Microsoft-windows-cl	Microsoft windows	
storprop.dll	14/07/2009	2:6.1	Signé	nt5.cat	Microsoft windows	
e190xbc5.sys	04/06/2003	1:4.90,2:5.00	Signé	w9x90xbc.cat	Microsoft windows Hardware Compatibility	

Et on peut trouver des fichiers assez anciens, surtout dans les driver

[c:\windows\system32\drivers]						
acpi.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
afd.sys	14/07/2009	2:6.1	Signé	nt5.cat		
agilevpn.sys	14/07/2009	2:6.1	Signé	nt5.cat		
asynchmac.sys	14/07/2009	2:6.1	Signé	nt5.cat		
atapi.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
ataport.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
blbdrive.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
cdrom.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
cng.sys	14/07/2009	2:6.1	Signé	nt5.cat		
compositebus.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-cl		
csc.sys	14/07/2009	2:5.1,2:5.2,2:6.0,2:	Signé	Microsoft-windows-Of		
discache.sys	14/07/2009	2:6.1	Signé	nt5.cat		
disk.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
drmk.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-cl		
drmkaud.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-cl		
dxgkrnl.sys	14/07/2009	2:6.1	Signé	nt5.cat		
e190xbc5.sys	04/06/2003	1:4.90,2:5.00	Signé	w9x90xbc.cat		
fdc.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		
flpydisk.sys	14/07/2009	2:5.1	Signé	Microsoft-windows-Co		

Ici un driver 3c905 de carte réseau 3COM datant de 2003 !

DriverQuery vérification drivers signés:

Depuis Seven et 2008R2 on dispose d'une commande similaire dans l'esprit, mais qui peut analyser une machine à distance. **DriverQuery**

Syntaxe

```
DRIVERQUERY [/s <System> [/u [<Domain> \] <Username> [/p <Password>]]] [/fo {table | liste | csv}] [/nh] [/v | /si]
```

Les paramètres les plus intéressants étant

Paramètre	Description
/s <System>	Spécifie le nom ou l'adresse IP d'un ordinateur distant. N'utilisez pas de barres obliques inverses. La valeur par défaut est l'ordinateur local.
/u [<Domain> \] <Username>	Exécute la commande avec les informations d'identification du compte d'utilisateur comme spécifié par <i>l'utilisateur</i> ou le <i>domaine\utilisateur</i> . Par défaut, /s utilise les informations d'identification de l'utilisateur actuellement connecté à l'ordinateur qui émet la commande. /u ne peut pas être utilisée sauf si /s est spécifié.
/p <Password>	Spécifie le mot de passe du compte d'utilisateur qui est spécifié dans le paramètre /u . /p ne peut pas être utilisé sauf si /u est spécifié.
/si	Fournit des informations sur les pilotes signés.

Ainsi **Driverquery /SI** donnerait pour tous les drivers du poste courant l'information s'ils sont signés ou non

```
C:\Users\util>driverquery /si
```

DeviceName	InfName	IsSigned	Manufacturer
Volume générique	volume.inf	TRUE	Microsoft
Gestionnaire de volume	machine.inf	TRUE	(Périphérique système st
Pilote d'énumérateur de lecteur	machine.inf	TRUE	(Périphérique système st
...	...	...	...

Dans l'exemple ci-dessous, on teste les drivers d'une machine en **192.168.1.10** avec un login **administrateur** et un mot de passe **local**.

```
C:\Users\util>driverquery /s 192.168.1.10 /u administrateur /p zk29 /si
```

DeviceName	InfName	IsSigned	Manufacturer
Volume générique	volume.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft

Dans l'exemple ci-dessous, on teste les drivers d'une machine en **192.168.1.111** avec un login de domaine **cabare-intra\administrateur** et un mot de passe **zk281**.

```
C:\Users\util>driverquery /s 192.168.1.111 /u cabare-intra\administrateur /p zk281 /si
```

DeviceName	InfName	IsSigned	Manufacturer
Volume générique	volume.inf	TRUE	Microsoft
Volume générique	volume.inf	TRUE	Microsoft

Bien sûr encore faut-il que soit le pare-feu soit désactivé, soit que l'on ait autorisé comme règles la **gestion des services à distance...** la **gestion à distance des tâches planifiées...**

- | | |
|--|-----------------------------------|
| ✓ Gestion à distance des tâches planifiées (RPC) | Gestion à distance des tâches ... |
| ✓ Gestion à distance des tâches planifiées (RPC-EPMAP) | Gestion à distance des tâches ... |
| ✓ Gestion à distance du Pare-feu Windows (RPC) | Gestion à distance du Pare-fe... |
| ✓ Gestion à distance du Pare-feu Windows (RPC-EPMAP) | Gestion à distance du Pare-fe... |
| ✓ Gestion des services à distance (NP-Entrée) | Gestion des services à distance |
| ✓ Gestion des services à distance (RPC) | Gestion des services à distance |
| ✓ Gestion des services à distance (RPC-EPMAP) | Gestion des services à distance |

INTEGRITE SEVEN

les DLL (Dynamic Link Libraries) :

les **DLL** sont des bibliothèques de routines (fonctions ou procédures) chargées en mémoire au moment de leur appel (contrairement à un programme EXE qui se charge entièrement avant même de s'exécuter).

Plusieurs avantages sont présents :

- En cas de modification de la bibliothèque de routines, il n'est donc pas nécessaire de recompiler tout le programme, le remplacement du fichier DLL est suffisant. Le programme utilise automatiquement les fonctions modifiées au prochain lancement.
- Les fonctions issues de la DLL ne sont alors plus chargées plusieurs fois, car plusieurs programmes peuvent se référer simultanément à une instance de la DLL présente en mémoire

Des inconvénients existent :

- La gestion des versions de DLL est complexe...
- Il faut éviter la mise à jours sauvage, et la gestion des packages pour garantir une stabilité du système

Il est toujours difficile de connaître la liste des DLL nécessaires (ou plus nécessaires au bon fonctionnement d'un programme). On peut utiliser des utilitaires mais la tâche reste complexe.

A cet effet, un gestionnaire d'installation, à partir de win98, travaille normalement à partir des fichiers **.msi** pour maintenir cette liste à jour. Mais les applications ne prévoient pas forcément une procédure correcte....

WRP Protection des DLL :

Il existe un mécanisme intégré à windows permettant de vérifier les versions protégés de certains fichiers (.sys .dll .exe .ttf .fon .ocx) et de remplacer a la volée par leur version d'origine pour assurer l'intégrité du système. Ce mécanisme nommé **WRP (windows Ressource protection)** qui remplace la version 2000-XP de **WFP (windows File protection)** évite l'écrasement de fichier sensibles par des applications peut scrupuleuses...

A cet effet un cache contenant une "copie" d'origine des fichier existe en

%systemroot%\Winsxs

En cas d'écrasement d'un fichier, WFP puisera de l'aide dans :

1. le dossier **Winsxs**,
2. le Média d'origine,
3. le point d'installation réseau...

Le remplacement/mise à jour des fichiers système protégés est pris en charge uniquement dans les cas suivants :

1. installation de Service Pack ou de correctifs à l'aide d'Update.exe ;
2. mises à niveau du système d'exploitation à l'aide de Winnt32.exe ;
3. Windows Update.
4. A travers une API spéciale

sfc - system file checker

il existe une invite en ligne de commande **Sfc** permettant le forcer la vérification de l'intégrité du système SEVEN (sans attendre la vérification en tâche de fond)

```
C:\Users\Administrateur>sfc /help
Vérificateur de ressources Microsoft(R) Windows(R) version 6.0
Copyright (c) Microsoft Corporation. Tous droits réservés.

Analyse l'intégrité de tous les fichiers système protégés et remplace
les versions incorrectes par les versions Microsoft appropriées.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<fichier>]
    [/VERIFYFILE=<fichier>]
    [/OFFWINDIR=<répertoire Windows hors connexion>]
    [/OFFBOOTDIR=<répertoire Windows hors connexion>]

/SCANNOW      Analyse l'intégrité de tous les fichiers système
              protégés et répare les fichiers endommagés dès que
              possible.
/VERIFYONLY   Analyse l'intégrité de tous les fichiers système
              protégés. Aucune réparation n'est effectuée.
/SCANFILE     Analyse l'intégrité du fichier référencé et le répare
              si des problèmes ont été identifiés. Spécifiez le
              chemin d'accès complet dans <fichier>.
/VERIFYFILE   Vérifie l'intégrité du fichier ayant comme chemin
              complet <fichier>. Aucune réparation n'est effectuée.
/OFFBOOTDIR   Pour les réparations hors connexion, spécifier
              l'emplacement du répertoire de démarrage hors
              connexion.
/OFFWINDIR    Pour les réparations hors connexion, spécifier
              l'emplacement du répertoire Windows hors connexion.
```

N.B: Cette commande peut provoquer l'accès au Media de Windows

UAC- USER ACCOUNT CONTROL

Objectif Visé :

Ce n'est pas un moyen de se protéger contre les virus infaillible, mais plutôt une manière d'éduquer les utilisateurs et développeurs d'applications.

Sur Vista le compte par défaut fait partie du groupe des Administrateurs mais à des droits d'accès restreints au système.

Le principe est de lancer toutes les tâches en tant qu'utilisateur standard, que vous soyez administrateur ou non !

- ✓ Lorsque une opération requière des droits élevés, une boîte de dialogue demande l'élévation des droits pour ce processus. (une simple confirmation)
- ✓ Si l'utilisateur ne fait pas partie du groupe des administrateurs, la boîte de dialogue lui demande alors un compte et un mot de passe ayant des droits d'administration...

N.B : seul le compte administrateur d'origine, (désactivé par défaut lors de l'installation) ne subit pas l'UAC !

IL – Integrity Level :

Lorsque vous ouvrez une session de manière générale avec Windows, le service de sécurité LSASS va créer un jeton qui contiendra le SID de l'utilisateur. C'est ce jeton qui sera utilisé pour lancer des applications.

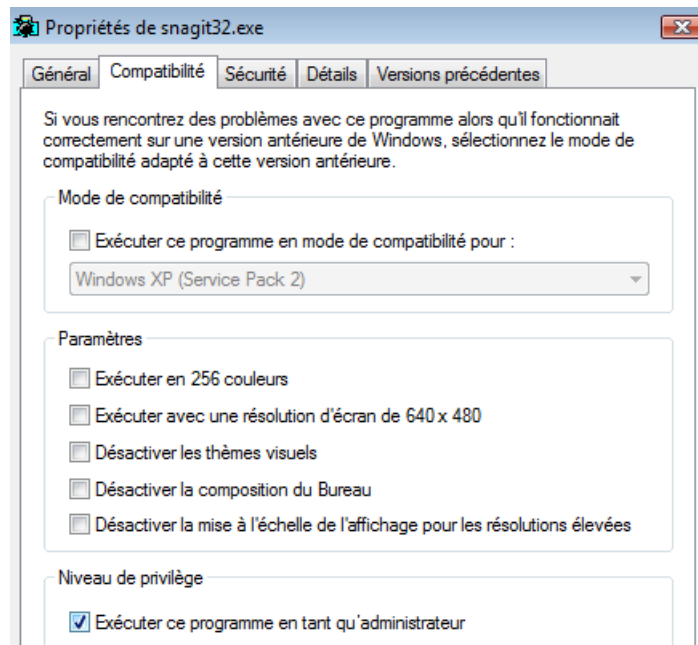
Avec Vista, lorsque vous ouvrez une session, LSASS va créer deux jetons. Un qui va contenir toutes les informations comme dans Windows XP et un autre jeton "restreint" qui ne contiendra que les privilèges d'un utilisateur standard.

Chacun de ces jetons possède le même **SID** utilisateur plus, un SID de type **S-1-5-40-xx** où xx représente le niveau d'intégrité afin de les isoler.

C'est donc grâce à ces niveaux d'intégrité obligatoire et interchangeable durant leur durée de vie que va se baser toute la partie contrôle d'intégrité

C'est donc ce deuxième jeton qui sera utilisé pour lancer les différentes applications. Pour utiliser le premier jeton, celui avec tous les privilèges, vous devrez passer par une élévation de privilège

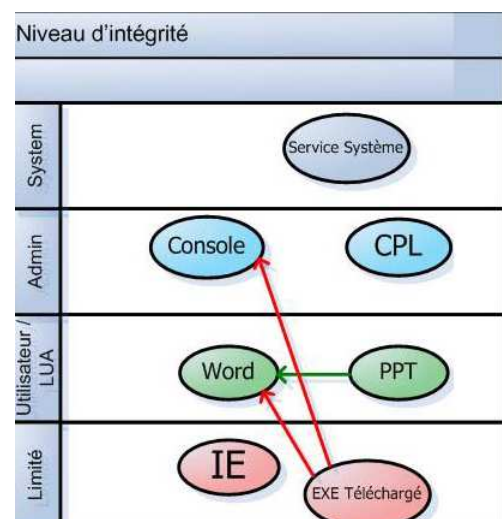
N.B : pour lancer ses applications en utilisant tout le temps le jeton avec tous les privilèges. Il suffit de cocher une case dans les propriétés de l'exécutable



L'UAC repose aussi sur un nouvel attribut dont sont dotés les processus, les fichiers les clés du registre : le niveau d'intégrité. Dit **IL** pour **Integrity Level**.

Les principaux niveaux **IL** : **Limité** – **Utilisateur** - **Administrateur** – **System**

- Il faut savoir que les processus Utilisateur / LUA ne peuvent pas modifier les processus s'exécutant dans un niveau d'intégrité supérieur. (mais ils peuvent les lire pour obtenir des infos...)
- Le groupe des administrateurs à un **IL** élevé
- Pour un utilisateur, les processus qu'il lance et ses fichiers ont un **IL** niveau moyen



Dans cette optique par exemple, lorsque l'on lance IE (par exemple) on lance en fait 2 processus, avec des niveaux IL différents...

ieuser : avec un **IL** d'utilisateur (pour stocker ses favoris...)

ieexplorer : avec un **IL** bas pour exécuter lesactivex et autres...

Fichier Options Affichage ?						
Applications Processus Services Performances Mise en réseau Utilisateurs						
Nom de l'image	Nom d'utilisateur	Processeur	Mémoire ...	Priorité	Virtualisa...	Description
explorer.exe	test	00	15 684 K	Normale	Désactivé	Explorateur Win...
ieuser.exe	test	00	2 092 K	Normale	Activé	Internet Explorer
ieexplore.exe	test	00	5 788 K	Normale	Activé	Internet Explorer
lsass.exe	SYSTEM	00	696 K	Normale	Non aut...	Processus de l'a...

Autre exemple: lorsque l'on récupère une pièce jointe, et que on la stocke, si c'est un exécutable, sont application a un IL de bas niveau, dont ne peut interférer avec les processus système ayant un IL élevé...

Désactivation de l'UAC (panneau de configuration):

Le seul compte exempt de l'UAC étant le compte Administrateur (créé lors de l'installation) il faut essayer de gérer les effets de l'UAC

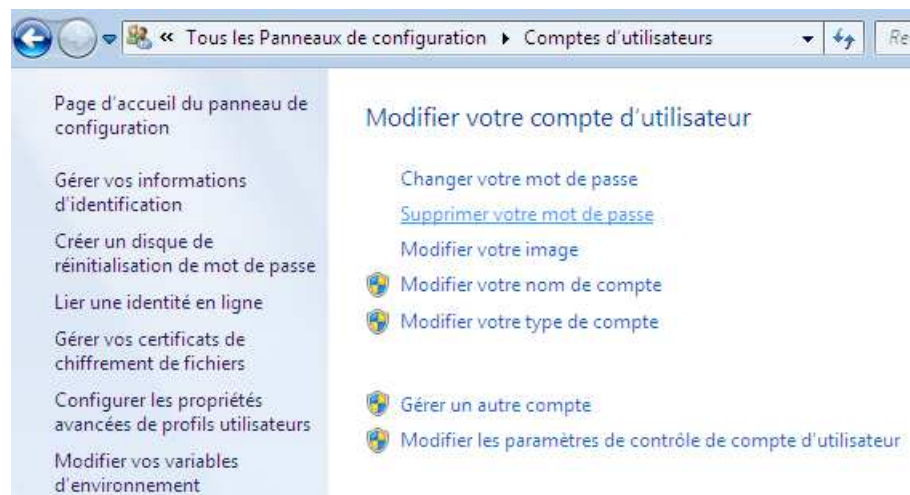
Il est recommandé de ne pas désactiver les invites du contrôle de compte d'utilisateur dans les paramètres de stratégie de groupe ou en agissant sur le curseur.

Bien que l'invite d'élévation soit la partie la plus visible du contrôle de compte d'utilisateur, celui-ci fournit également les composants sous-jacents comme :

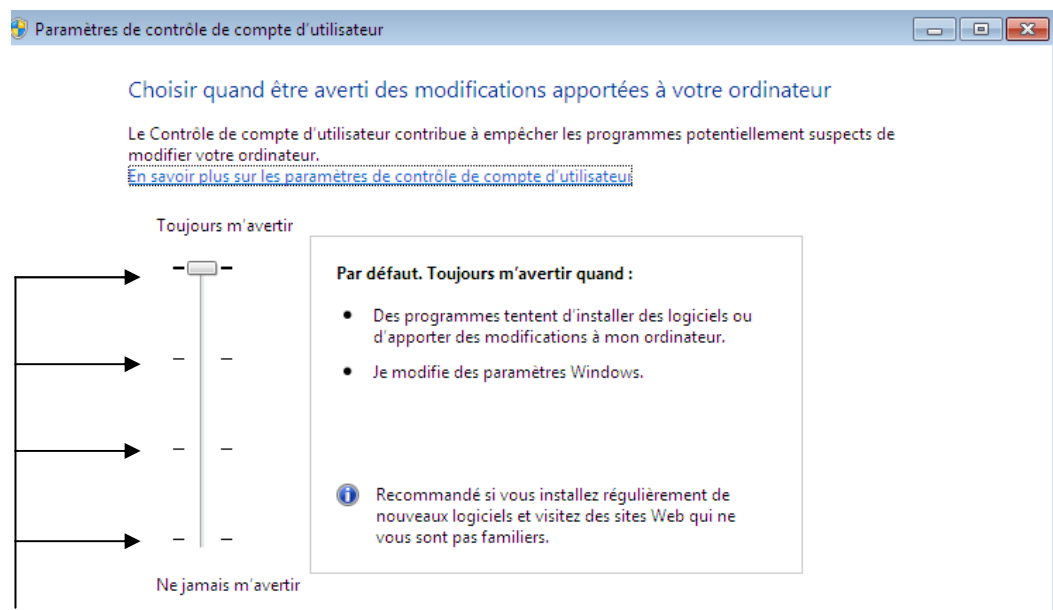
- Mode protégé d'Internet Explorer
- Virtualisation de fichiers système et du Registre

Cependant si on veut paramétrer cette gestion (...) via l'interface graphique il faut demander dans

Panneau de configuration / Comptes d'utilisateurs



la commande **Modifier les paramètres de contrôle de compte d'utilisateur**



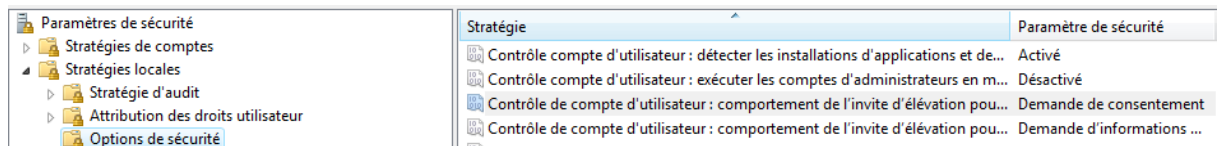
la prise en compte de cette commande peut demander un redémarrage.

Gestion de l'UAC (stratégies locales):

Dans les stratégies locales de sécurité, se retrouvent les réglages de l'UAC

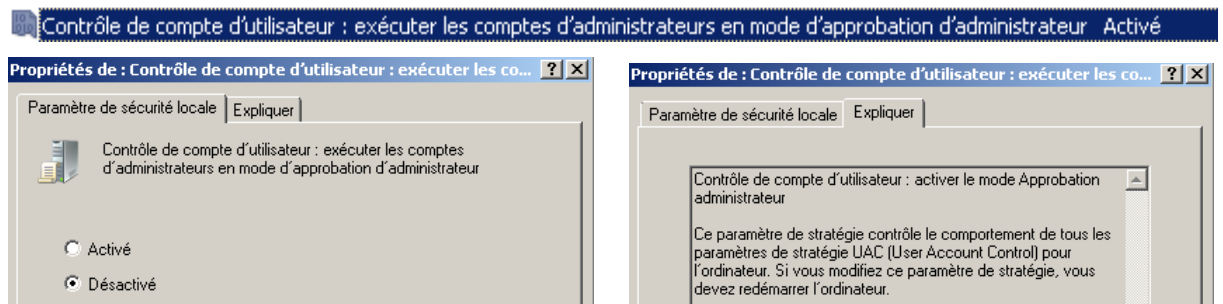
Dans le **Panneau de Configuration / Outils d'administration / Stratégies de sécurité locales**

Puis dans les **Stratégies locales / Options de sécurité**



Désactivation de l'UAC :

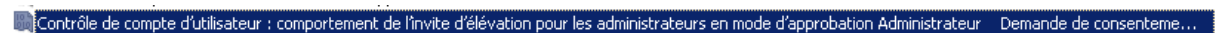
Sans doute le plus ... radical



Désactivation de l'UAC pour les Administrateur :

Il existe un moyen de préserver L'UAC et d'enlever cette boîte de dialogue lors d'une demande d'approbation administrateur

Double cliquez sur "**Contrôle compte d'utilisateur: comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur**".



La valeur par défaut est "**Demande de consentement**". Elle permet à l'administrateur de choisir entre "**Autoriser**" ou "**Refuser**".

- ✓ - La valeur "**Demande d'informations d'identification**" permet de demander à l'administrateur de renseigner son nom d'utilisateur et son mot de passe.
- ✓ - La valeur "**Elever les privilèges sans invite utilisateur**" permet d'élever les privilèges sans aucune demande, il n'y aura donc plus de boîte de dialogue !.

Désactivation l'UAC pour les Utilisateurs :

L'équivalent pour les utilisateurs



Activation l'UAC pour le compte Administrateur Root :

Cela permet de généraliser l'UAC au compte Administrateur d'origine (!!!).



Paramètre de curseur	Paramètres de stratégie de groupe équivalents
Toujours m'avertir	- Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Demande de consentement sur le bureau sécurisé. - Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est activé.
M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur (valeur par défaut)	- Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Demande de consentement pour les binaires non Windows. - Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est activé.
M'avertir uniquement quand des programmes tentent d'apporter des modifications à mon ordinateur (avec bureau sécurisé)	- Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Demande de consentement pour les binaires non Windows. - Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est désactivé.
Ne jamais m'avertir  Remarque Ce paramètre requiert un redémarrage pour entrer en vigueur.	- Le paramètre de stratégie comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur a la valeur Élever les privilèges sans invite utilisateur. - Le paramètre de stratégie Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation est désactivé. - Le paramètre de stratégie Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur est désactivé. - Le contrôle de compte d'utilisateur est désactivé.

DONC... il ne faut jamais utiliser le compte Administrateur intégré pour travailler avec SEVEN, puisque un compte administrateur "autre" bénéficiera de l'effet protecteur de l'UAC sans occasionner de gêne.

On peut demander une invite d'élévation automatique, mais il faut laisser l'UAC faire son travail...

N.B : une modification des réglages de l'UAC nécessite le plus souvent un redémarrage du poste pour être sûr de la prise en compte des nouveaux paramètres.

INSTALLATIONS ET VIRTUALISATION

Préconisation microsoft :

Microsoft recommande que les programmes d'installation d'application globaux s'exécutent avec les droits administratifs et

- ✓ créent un répertoire sous le répertoire **%ProgramFiles%** (pour stocker les fichiers de l'application exécutables et les données auxiliaires)
- ✓ créent une clé sous **HKEY_LOCAL_MACHINE\Software** (pour leurs paramètres d'application.)

Lorsqu'une application s'exécute, elle peut le faire dans différents comptes utilisateur et devrait donc

- ✓ enregistrer les données spécifiques à l'utilisateur dans un répertoire **%AppData%** (propre à chaque utilisateur)
- ✓ enregistrer des paramètres propres à chaque utilisateur dans le profil d'annuaire de l'utilisateur sous **HKEY_CURRENT_USER\ Software**.

Les comptes utilisateur standard n'ont pas de droits d'écriture dans le répertoire **%ProgramFiles%** ou dans **HKEY_LOCAL_MACHINE\Software**, Mais puisque la plupart des systèmes de Windows sont à utilisateur unique et que la majorité des utilisateurs étaient administrateurs..., les applications qui enregistrent de façon inexacte des données utilisateur et des paramètres à ces emplacements fonctionnaient quand même.

Virtualisation des processus :

Si un programme d'installation se lance sans tous les droits administrateurs comme il va tenter d'écrire dans des dossiers systèmes ou protégés il court à l'échec

Pour prévoir ce type de problème, Microsoft a créé tout un système de virtualisation de dossier dans Windows Seven.

- Sous Windows XP, dans un environnement limité, vous lanciez l'installation jusqu'au moment où un fichier a besoin d'être écrit dans un espace protégé Cette opération va faire "crasher" l'installation rendant le logiciel à moitié installé et donc inutilisable
- Seven déroule toute l'installation pour savoir si il a besoin d'aller écrire dans les dossiers système ou des parties réservées du registre. Si c'est le cas, et que l'installateur n'a pas les autorisations suffisantes, alors un système de dossiers virtuels est mis en place.

En effet, au final toutes les applications peuvent écrire dans les dossiers systèmes et sécurisés de Windows. Seulement, parfois, ce ne sont pas les vrais dossiers systèmes de Windows. Ce sont en fait des dossiers virtualisés situés dans le profil de l'utilisateur. ... **AppData\local\VirtualStore\...**

Ensuite une application, devant être exécutée avec les privilèges administrateur parce qu'elle va écrire dans **Program Files** ou dans la clef de

registre **HKLM**, est exécutée avec un jeton "restreint", il n'y aura aucune erreur de la part du système.

Lors du lancement de l'application, celle-ci ira dans un premier temps regarder dans le dossier virtuel du profil, et si elle ne trouve rien, elle chargera les paramètres dans le Program Files réel.

Grâce à ce système, près de 90% des applications non réécrites pour Vista allant écrire dans **Program Files** ou dans des dossiers systèmes fonctionnent.

On parle de « **programmes hérités** »

Seven traite un processus comme « virtualisable » si :

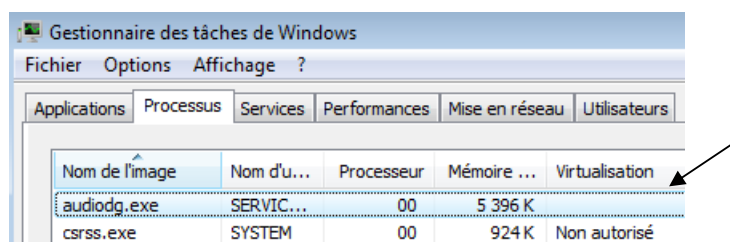
- il fait 32 bits (et non 64 bits),
- il ne s'exécute pas avec les droits administratifs,
- il n'a pas un fichier de signature spécifique pour Windows Seven

Les emplacements de système de fichiers qui sont virtualisés pour les processus d'héritage sont

- %ProgramFiles%
- %ProgramData%
- %SystemRoot%

Cependant, tous les fichiers possédant une extension exécutable, y compris .exe, .bat, .scr, .vbs et autres, sont exclus par défaut de la virtualisation. (Cela signifie que les programmes qui se mettent à jour à partir d'un compte utilisateur standard échouent au lieu de créer des versions privées de leurs exécutables)

N.B : on peut vérifier si une application est virtualisable dans le gestionnaire de tâche, en ajoutant la colonne ☒ Virtualisation



N.B : Comme les informations sont stockées dans le répertoire utilisateur, cela peut être gênant. Par exemple, pour une application qui stocke les meilleurs scores : l'utilisateur fera toujours le meilleur score !

N.B : Il faut également noter que ce système de dossier virtuel est utilisé pour les contrôles ActiveX d'Internet Explorer 7

Dans un répertoire contenant des fichiers virtualisés, l'Explorateur affiche un bouton nommé **Fichiers de compatibilité** dans sa barre d'outils. Il renvoie vers le sous-répertoire de VirtualStore contenant les fichiers virtualisés

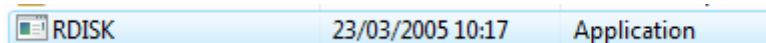


COMPATIBILITE AVANT SEVEN

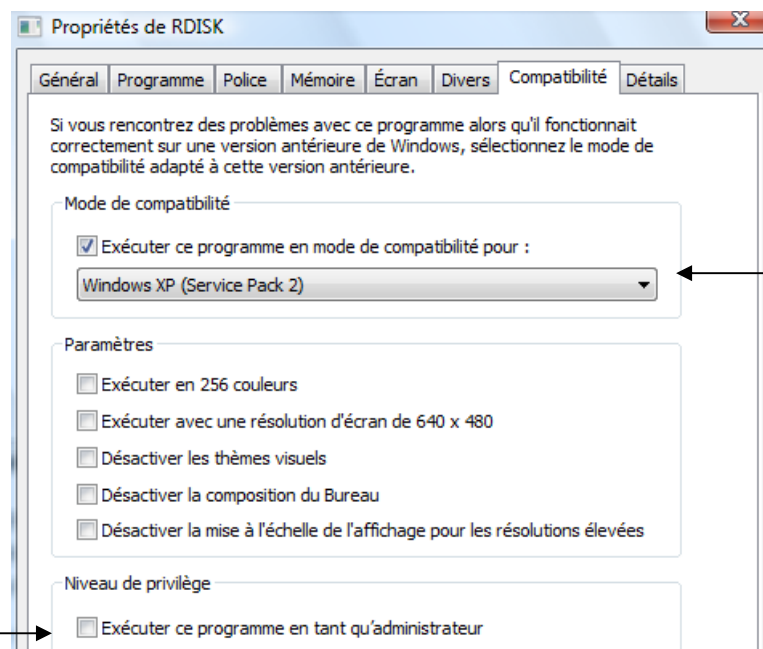
Exécuter en mode compatibilité:

Si un programme fonctionnait correctement sur une version antérieure à SEVEN, et que vous ne disposez pas de la version spécifique à SEVEN, on peut tenter de demander de l'exécuter en mode compatibilité

Par exemple pour l'utilitaire RDISK suivant



On demande clic-droit sur l'exécutable, **propriétés** onglet **Compatibilité**



On spécifie

- si il y à besoin d'exécuter avec un privilège d'administrateur
- On choisit un mode de compatibilité

Windows 95
Windows 98
Windows NT 4
Windows 2000
Windows XP (Service Pack 2)
Windows XP (Service Pack 3)
Windows Server 2003 (Service Pack 1)
Windows Server 2008 (Service Pack 1)
Windows Vista
Windows Vista (Service Pack 1)
Windows Vista (Service Pack 2)

Installer en mode compatibilité:

Parfois in faut demander ce mode sur les fichiers setup d'installation, Puis sur l'exécutable installé...

PROTECTION DEP

Principe DEP Data Execution Prevention:

Il s'agit d'une technologie développée par AMD, connue sous l'appellation **NX** (No eXecute), liée aux adressages **PAE**. (Physical Address Extension))

NX est censée empêcher le "dépassement de mémoire tampon" (*buffer overflow*), une vulnérabilité pouvant être exploitée pour des intrusions à distance ou des attaques virales.

L'objectif est donc de marquer comme non exécutable des emplacements mémoire non occupés par une application, pour éviter que des vers s'auto-répliquent dans le système

Dans XP (Sp2 mini), la fonction qui implémente NX est baptisée **DEP**, pour **Data Execution Prevention**

Désactivation Complète de DEP :

La fonctionnalité DEP, permettant de sécuriser SEVEN contre les virus, peut être responsable de crashes intempestifs sur votre système

bcdedit.exe /set {current} nx AlwaysOff

Puis re démarrage

La réactivation de la protection se fait par

bcdedit.exe /set {current} nx Optin

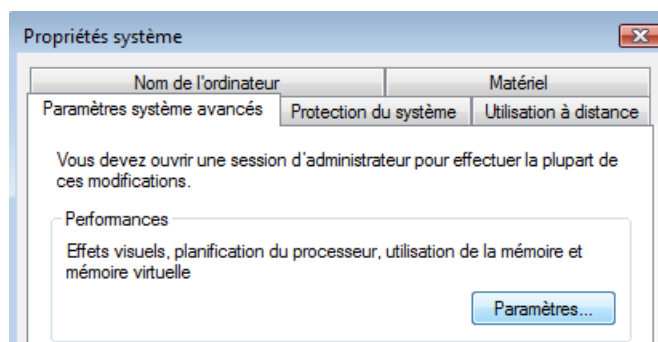
(et re démarrage)

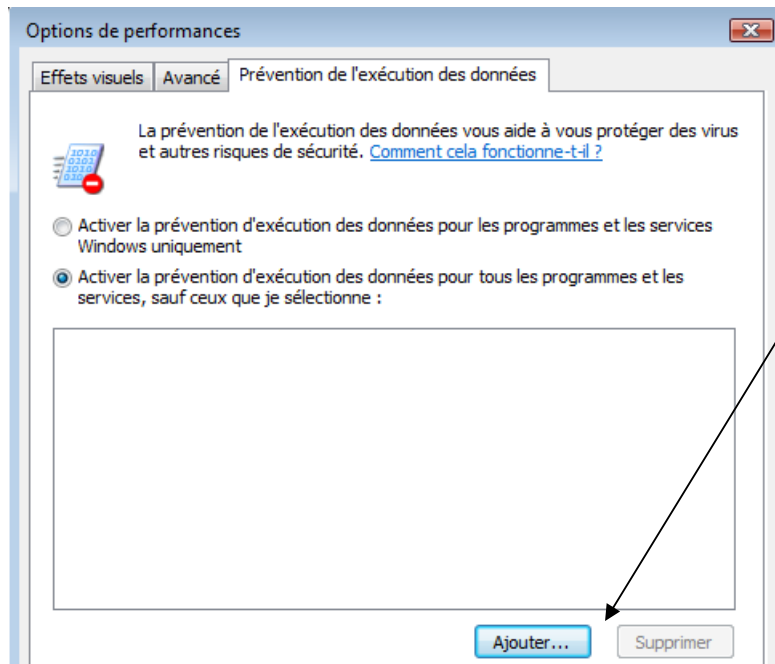
Désactivation pour une application de DEP :

Il est possible de désactiver cette protection uniquement pour une application précise.

Dans les **propriétés de ordinateur /options avancées /performance /paramètres"**

onglet "**prévention de l'exécution des données**".





il est alors possible d'insérer dans la liste présentée les programmes ne devant pas avoir recours à la fonction DEP.

WINDOWS RE (CONSOLE DE RECUPERATION)

Windows Recovery Environnement:

Si la panne n'est pas due à une installation de driver posant problème, mais plutôt à une défaillance matérielle ou à des fichiers manquants ou endommagés, il se peut que l'on n'arrive même pas en F8, il est nécessaire alors d'utiliser L'environnement de récupération.

Basé sur **Windows PE** (Préinstallation Environnement) cet environnement remplace la console qui existait sous XP

Une différence de taille existe entre la version fournie sur SEVEN, et celle existant précédemment :

il n'y a plus de demande d'authentification sur la machine !

Pourquoi ? Les raisons sont multiples :

- L'accès à une procédure de réparation demandant une authentification stockée dans la base de registre du poste à Secourir suppose que celui-ci ne soit pas trop gravement atteint (et que donc sa base de registre soit toujours lisible !)
- La sécurisation des données par mot de passe local ont démontré leurs limites lors des attaques réelles, et donc ne protège pas réellement. Désormais la sécurité des données passe par des procédés de chiffrement

1. renforcement du système EFS
2. Algorithme de chiffrement plus robustes
3. Apparition de BitLocker associant chip TPM et clé USB

N.B: pour des raisons de sécurité, et étant donné que **EFS** et **BitLocker** étant disponible que sur les versions Ultimate, Business Pro et Business Enterprise, les version HOME sont à proscrire.

Démarrer l'environnement de récupération WinRE:

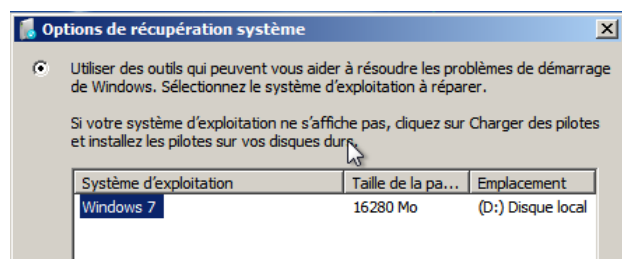
Si l'environnement de Récupération n'est pas pré-installée sur la machine (machine livrée ainsi, avec une pré-installation de secours), alors on peut à partir du CD relancer une pseudo-installation

Appuyez sur n'importe quelle touche pour démarrer du CD-ROM ou DVD-ROM._

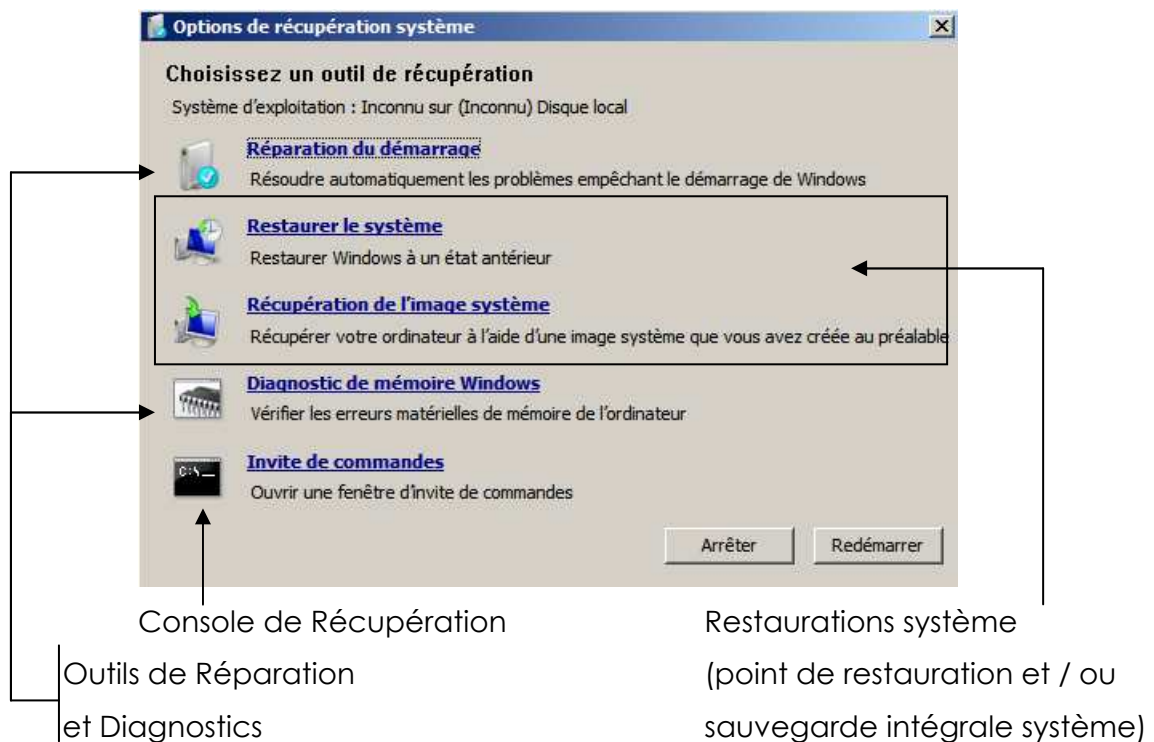
La barre "Windows is loading files" apparaît, puis la barre de progression. On choisit une régionalisation, puis **Suivant** et **Réparer l'ordinateur**



On sélectionne le système SEVEN à réparer (si besoin parmi les différents Systèmes),



et on obtient :



Console de Récupération

Outils de Réparation
et Diagnostics

Restaurations système
(point de restauration et / ou
sauvegarde intégrale système)

Comme on l'a vu dans le chapitre "Les processus sous Seven", on peut distinguer 3 étapes dans le démarrage d'un poste

1. **ETAPE 1** : séquence POST jusqu'à l'affichage Barre de Progression.

à ce niveau on peut avoir des :

- Problème HARDWARE
- Problèmes dans la Partition - MBR du disque
- Fichiers de démarrage absents - endommagés

2. **ETAPE 2** : séquence Barre de Progression jusqu'à l'ouverture de session.

à ce niveau on peut avoir des :

- Problème HARDWARE
- Pilotes – Services defectueux - mal configurés

3. **ETAPE 3** : Après l'ouverture de session.

à ce niveau on peut avoir des :

- Programmes de démarrages
- Programmes instancés automatiquement

Les méthodes de récupérations diffèrent selon les étapes de défaillance

Etape 1 séquence POST – barre de progression

Les problèmes à ce niveau peuvent être matériels ou logiciels:

Problèmes hardware

Les causes fréquentes peuvent être

des problèmes mémoire:

un outil de test RAM est disponible depuis la console Windows RE

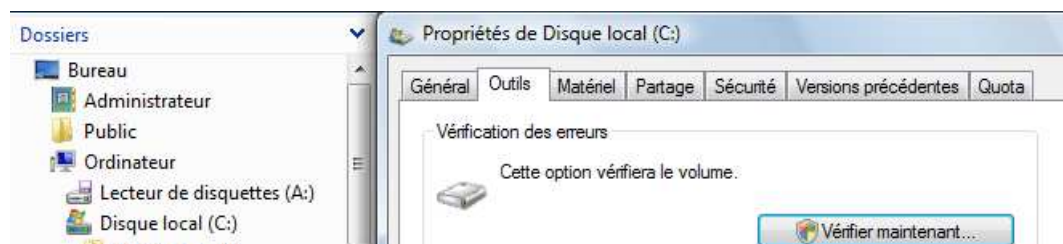


Ou des problèmes de disque dur

On peut essayer de "prévenir" une panne de disque dur... Vista peut s'interfacer avec la technologie SMART des disques récents pour informer l'administrateur de l'état d'un disque dur... dans l'observateur d'évènement on trouve donc une trace des rapport consigné par cette technologie.

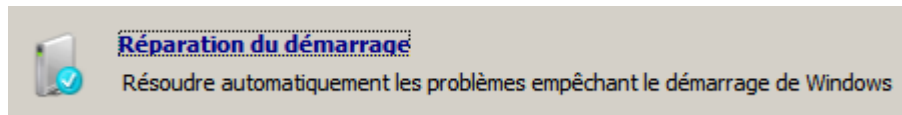
On peut aussi préventivement réaliser des commandes en invite de commande **chkdsk c: /f /r**, (et éventuellement les planifier via un petit batch), moduler le comportement par défaut via **chkntfs...**

soit en interface graphique,



Problèmes partition- mbr-fichiers manquants

Un outil spécifique existe développé pour tester un grand nombre de problème d'amorçage. Sélectionner "**Réparation du démarrage**"...

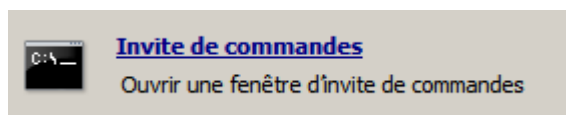


L'exécution de cette procédure lance une suite de tests.

- test du disque système
- diagnostic des défaillances de disque
- test des métadonnées de disque

dont le log est affichable en cliquant sur le lien d'information qui correspond à un journal stocké en **%windir%\system32\LogFiles\SRT\SRTtrail.txt**

Si la procédure automatique échoue, on peut alors passer en **invite de commande**



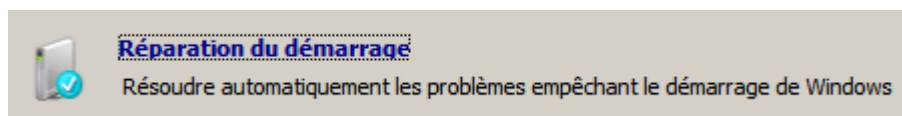
Notamment avec **BootRec.exe** (en invite de commande) suivit des options **/FIXMBR**, **/FIXBOOT** et deux nouvelles **/SCANOS** et **/REBUILDBCD**

Cf chapitre suivant "Utiliser Windows RE en invite de commande"

Etape 2 barre de progression avant session

A ce niveau, le noyau Seven est chargé, les problèmes peuvent être matériels ou logiciels:

On peut tenter de lancer l'outil développé pour les problèmes d'amorçage. Sélectionner "**Réparation du démarrage**"... (peut vraisemblable)



On peut tenter de passer par les "**options de démarrage**" via **F8** (Cf chapitre suivant "Options de démarrage F8") et on demande

- **Dernière configuration connue (option avancée)**
Si c'est un périphérique que l'on vient d'installer.
- **Inscrire les événements de démarrage dans le journal**

Puis lire le fichier log pour voir sur quels drivers on s'arrête.

On peut exclure temporairement des services via **msconfig.exe** (voir chapitre)

Etape 3 après l'ouverture de session

Un programme ou un service lancé automatiquement est probablement la cause de l'erreur...

Stratégies de groupe, Scripts de démarrage, programmes/services en

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

X:\ProgramData\Microsoft\Windows\Start Menu\Programmes\Démarrage

X:\User\%username%\AppData\Roaming\Menu\Microsoft\Windows\Start Menu\Programmes\Démarrage

SHIFT + "Ouverture de session" : ne pas exécuter ces programmes

On peut exclure temporairement tous les programmes de démarrage via **msconfig.exe** (voir chapitre)

WINDOWS RE INVITE DE COMMANDE

invite de commande:

L'accès aux outils manuels est toujours disponible

Les commandes disponibles sous **Windows RE** sont les suivantes :

Console Récupération XP	Windows RE
ATTRIB	
BATCH	
CD	
CHDIR	
CHKDSK	marque les secteurs défectueux
CLS	
COPY	
DEL	
DELETE	
DIR	
DISABLE	Plus disponible
DISKPART	
ENABLE	Plus disponible
EXIT	
EXPAND	
FIXBOOT	BootRec /Fixboot écrire le nouveau code du secteur de démarrage de Windows
FIXMBR	BootRec /FixMbr réparer le secteur de démarrage principal
FORMAT	
HELP	
LISTVC	Plus disponible
LOGON	Plus disponible
MAP	Diskpart
MD	
MKDIR	
MORE	
RD	

REN	
RENAME	
RMDIR	
SYSTEMROOT	
TYPE	

Modifier les partitions - Utilitaire Diskpart

Depuis Vista, il est possible de modifier la taille des partitions sans perdre leur contenu. Cela peut correspondre à divers besoins, comme faire de la place pour une installation de SEVEN sur une machine ou XP utilise tout le disque dur....

L'utilitaire Diskpart en ligne de commande est accessible :

- soit en cours d'installation (au moment du partitionnement **MAJ+F10**)
- soit en invite de commande l'installation terminée **diskpart**

```
C:\Users\Administrateur>diskpart
Microsoft DiskPart version 6.0.6000
Copyright (C) 1999-2007 Microsoft Corporation.
Sur l'ordinateur : PC-DE-TEST
```

On sort de l'utilitaire via **exit**

```
DISKPART> exit
Quitte DiskPart...
C:\Users\Administrateur>
```

Shrink Diskpart – réduire une partition

Une fois **diskpart** lancé, Il faut lister les disques présents sur le poste

```
C:\Users\Administrateur>diskpart
Microsoft DiskPart version 6.0.6000
Copyright (C) 1999-2007 Microsoft Corporation.
Sur l'ordinateur : PC-DE-TEST

DISKPART> list disk

   N° disque   Statut      Taille   Libre   Dyn   GPT
-----
Disque 0      En ligne    37 G octets  1689 K octets
```

Ensuite Il faut sélectionner le disque 0

```
DISKPART> select disk=0
Le disque 0 est maintenant le disque sélectionné.
```

On demande de lister les partitions

```
DISKPART> list partition

   N° partition   Type           Taille   Décalage
-----
Partition 1      Principale      37 G     1024 K
```

Ensuite Il faut sélectionner la partition 1

```
DISKPART> select partition=1
La partition 1 est maintenant la partition sélectionnée.
```

On demande de lister les volumes

```
DISKPART> list volume
```

N° volume	Ltr	Nom	Fs	Type	Taille	Statut	Info
* Volume 0	C		NTFS	Partition	37 G	Sain	Système
Volume 1	D			DUD-ROM	0 o	0 média	

On peut savoir quelle est la taille récupérable en fin de disque

```
DISKPART> shrink querymax
Le nombre maximal d'octets récupérables est : 15 G octets
```

On peut demander de récupérer par exemple 10G via

```
DISKPART> shrink desired=10000
DiskPart a réduit la taille du volume de : 10 G octets
```

Extend Diskpart – étendre une partition

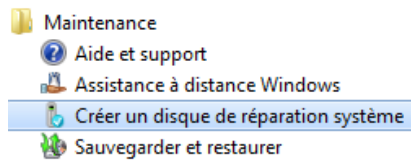
On peut demander d'étendre la partition active (si elle est juste parès la partition sur lequel on est placé. Par exemple ici de 5G via

```
DISKPART> extend size=5000
```

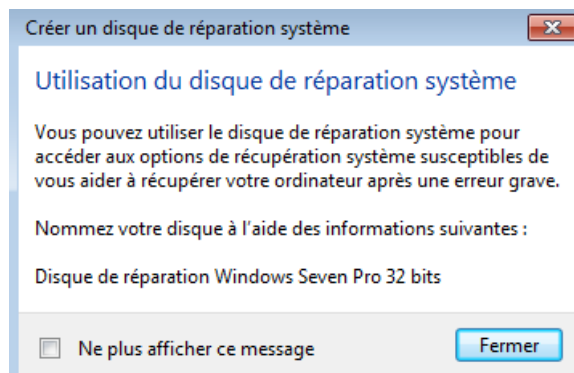
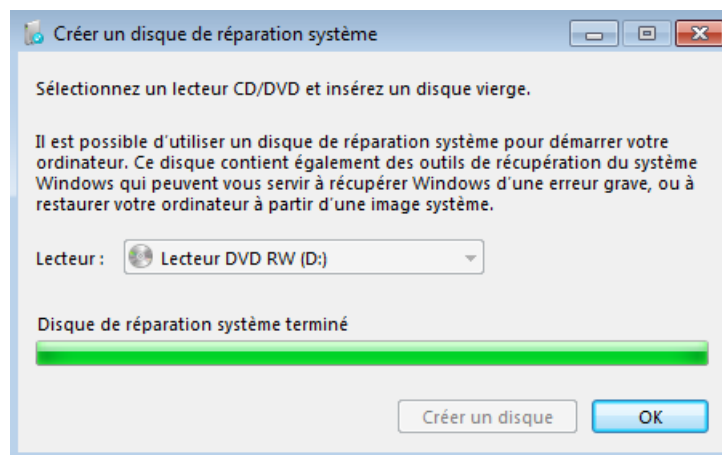

CD REPARATION – VS CONSOLE

Création CD de réparation

Via le menu **Démarrer/ Maintenance / Créer un disque de réparation Système**



Il faut avoir bien sur un graveur DVD...



Vous l'avez compris c'est un CD contenant un Win PE et les outils de réparation présents sur le DVD de SEVEN...

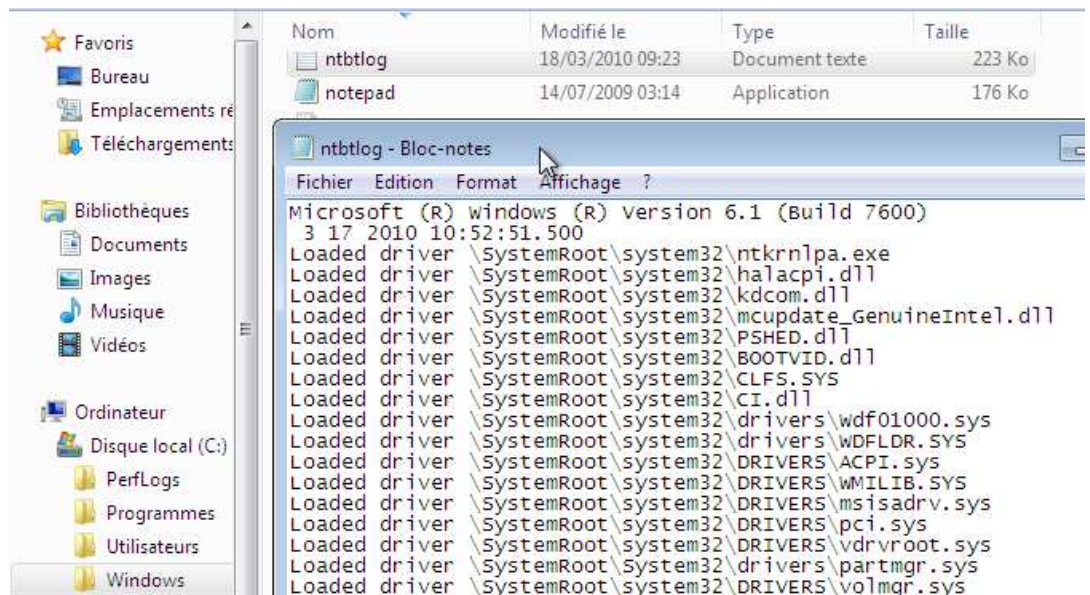
OPTIONS DE DEMARRAGE – F8

Demander F8 lors du démarrage :

Pour obtenir les options avancées de démarrage, il faut appuyer sur **F8** lors de l'amorçage du poste. (après la séquence POST et avant l'apparition de la barre de progression). Cela permet de lancer SEVEN en différents modes, parmi lesquels :

- **Mode sans Echec (avec ou sans réseau)** : permet de lancer uniquement le noyau et les drivers principaux
Utilisation : après une installation posant problème, on peut prendre la main « à minima »
- **Invite de commande en mode sans Echec** : idem ci-dessus mais en dévalisant l'interface graphique...
- **Inscrire les événements de démarrage dans le journal** : permettant de Créer un journal spécifique de tous les pilotes et services chargés ou non par le système

Utilisation : fichier journal **Ntbtlog.txt** dans le dossier racine de SEVEN



- **Activer la video en basse résolution** : pilote VGA en 640x480
- **Dernière bonne configuration connue** : utilise les informations de la dernière configuration correcte consignée dans le registre pour démarrer l'ordinateur
Utilisation : la "dernière bonne configuration connue" est celle qui a permis la dernière ouverture de session, par conséquent si une ouverture de session a été faite depuis l'installation du driver posant problème, cette option ne sert plus à rien !
- **Désactiver le contrôle obligatoire de la signature des pilotes** : permet d'installer des drivers non signés (impossible sur SEVEN64)

TEST MEMOIRE

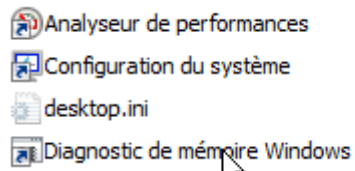
Test Ram depuis WinRE :

Un outil de test RAM est disponible depuis la console Windows RE



Outils d'administration:

On peut aussi le lancer depuis le **panneau de configuration, outils d'administration, diagnostic de mémoire Windows**



REPARER SANS REINSTALLER

Réinstaller le système :

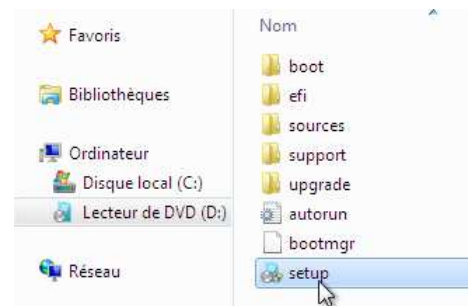
Il est possible de réparer une installation de SEVEN (en raison de l'apparition de dysfonctionnements du système par exemple) tout en conservant l'intégralité des paramètres existants (comptes utilisateurs, personnalisations, logiciels installés).

Si des fichiers de SEVEN sont corrompus, la réparation fonctionnera. Si le malaise se situe dans le registre ou est provoqué par une incompatibilité logicielle, les dysfonctionnements seront toujours présents...

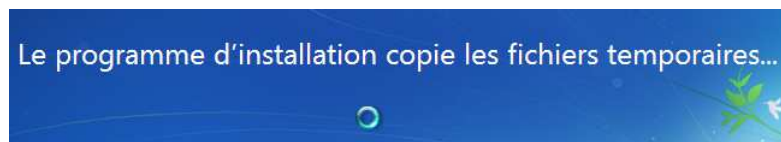
N.B: Avant de lancer la réparation, il est préférable de sauvegarder vos fichiers les plus importants sur une autre partition ou sur DVD.

N.B: Après réparation du système d'exploitation, il peut être nécessaire de réactiver SEVEN auprès de Microsoft

Il ne faut surtout pas Booter sur le CD de SEVEN, mais le lancer DEPUIS SEVEN. C'est-à-dire que on lit le DVD d'installation depuis l'explorateur du SEVEN en cours de fonctionnement



la procédure d'installation classique se déroule.



Puis lorsque l'option "type d'installation" est proposée Il faut absolument demander **Mise à Niveau**



Windows va s'installer comme si c'était une première fois, avec copie préalable de fichiers nécessaires au passage en mode graphique.

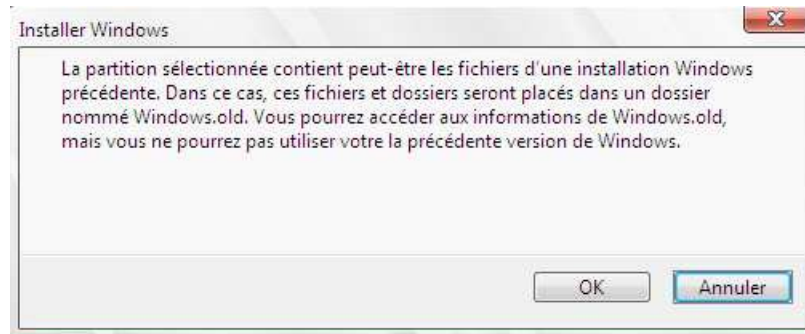


La phase en mode graphique est identique à celle d'une première installation. (Mêmes écrans, mêmes étapes et progression). En particulier, il faudra obligatoirement ressaisir la clef du produit.

REINSTALLER COMPLETEMENT

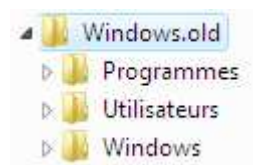
Réinstaller le système :

Il est possible de réinstaller complètement SEVEN (en raison de l'apparition de dysfonctionnements du système par exemple) sans reformater la partition d'origine système



Dans ce cas on dispose d'un nouveau système complet, et :

- L'ancienne structure de SEVEN est automatiquement copiée dans un dossier nommé **Windows.old**



- Tous les dossiers stockés directement à la racine du disque principal sont conservés

Il est donc possible d'aller récupérer manuellement des données dans ces structures préservées.

N.B: Après une **installation complète**, Si vous avez installé SEVEN dans la même partition que votre ancien SEVEN, ou XP, il n'est pas possible de désinstaller le nouveau système.

LA RESTAURATION SEVEN

Principe Restauration - désactivation-

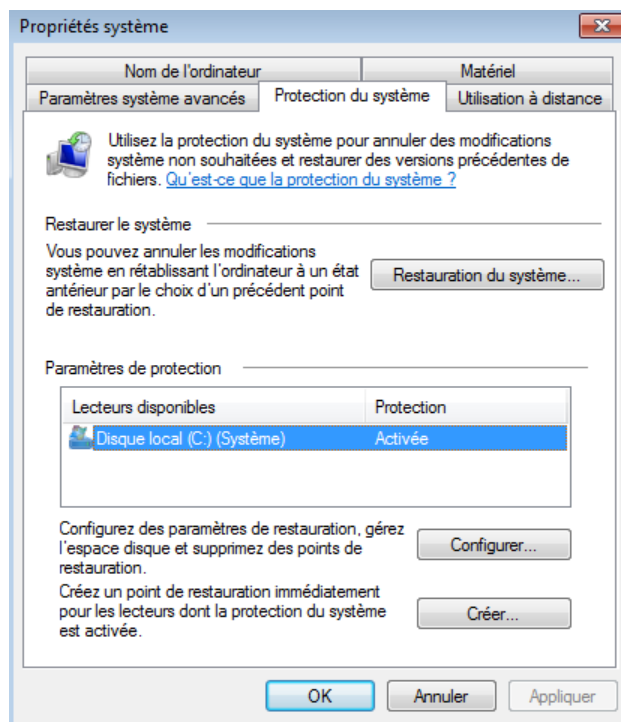
Les points de restauration sont créés par le système, et permettent une mémorisation d'un état du système, à un instant donné. Leur utilisation permet de "retrouver" un système dans un état passé.

L'onglet **Protection du système** est accessible via les **propriétés de Ordinateur**

Chaque lecteur dispose d'un espace disque pour la restauration du système.

N.B : on peut dissocier le lecteur système des lecteurs de données.

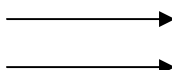
N.B: La restauration du système n'affecte pas les données utilisateurs



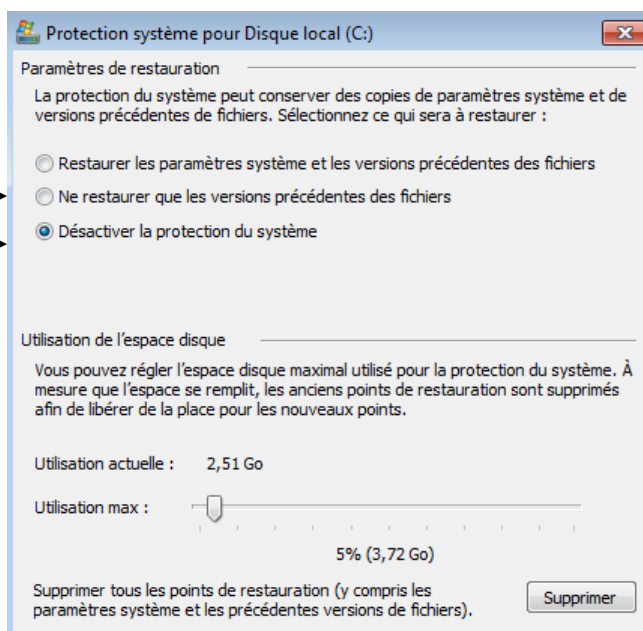
Désactivation de la Restauration

Il faut demander **Configurer...**

Puis au choix



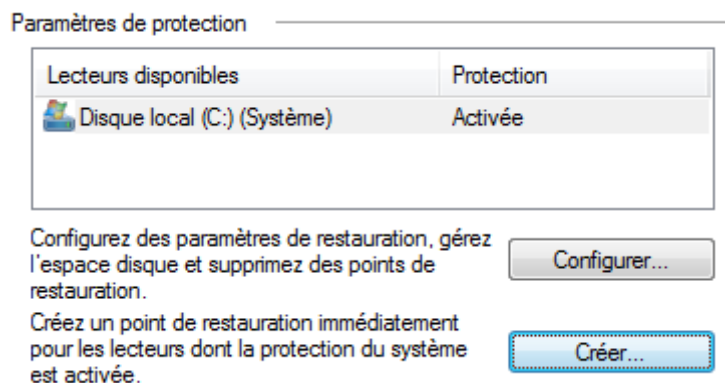
N.B: L'espace disque disponible pour la restauration est ajustable, et détermine le nombre de point de restauration qui peuvent être créés. (la config par défaut peut stocker plusieurs semaines de points de restauration.)



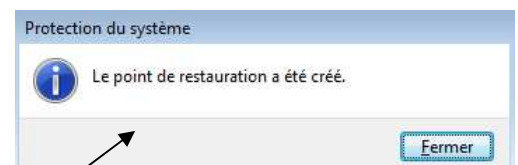
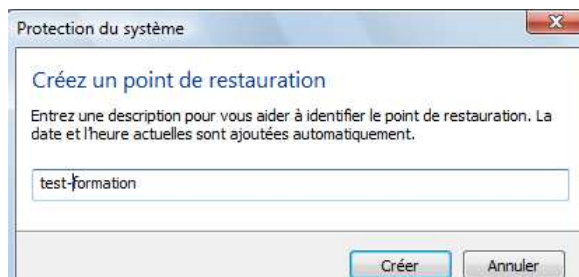
Création d'un point de restauration

Les points de restauration sont créés par le système (lors de l'installation de programme, drivers, mise à jours système...) ou par l'utilisateur

L'onglet **Protection du système** est accessible via les **propriétés** de **Ordinateur**, il suffit de demander ...Créer...



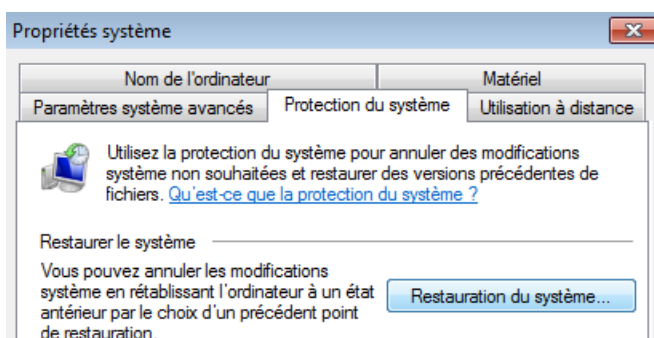
un assistant nous demande de nommer le point



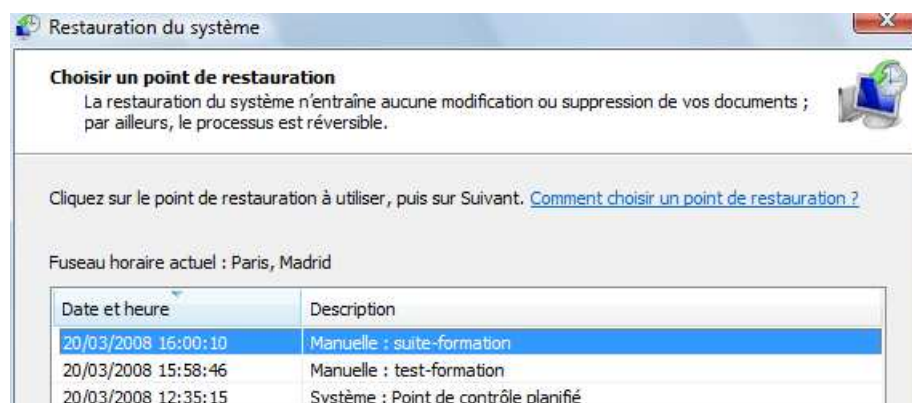
puis on demande **Créer** et on devrait obtenir

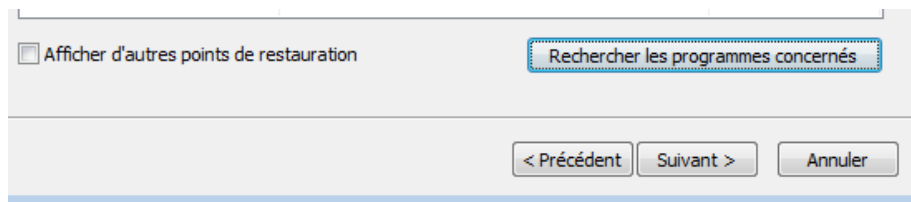
Utiliser Annuler un point de restauration

il suffit de demander ...Restauration du système....



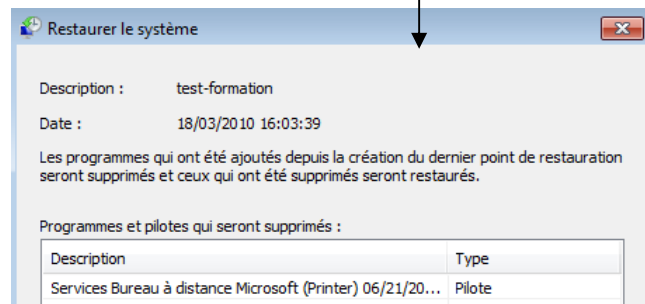
C'est un assistant La liste des points de restauration apparaît ...





A titre d'information, pour aider dans le choix du point de Restauration, le bouton **Rechercher les programmes concernés** est assez utile...

après avoir choisis, il suffit de demander **suivant**



Eventuellement préciser le lecteur, puis confirmer

Annuler une restauration

Dans l'assistant, il suffit de demander ...**Annuler la restauration du système**

Types de point de restauration

3 Types de points de restauration existent

1. **Points contrôle système** : créés toutes les 24 heures, et après 10 heures de fonctionnement à la suite.
2. **Points de restauration d'installation de programmes / pilotes**: créés lors d'une installation de programme, évidemment, mais aussi lors des mises à jours automatiques de Seven, de récupération à l'aide de l'utilitaire de sauvegarde..
N.B: lors de la restauration suite à une installation défaillante, il faut savoir que les fichiers éventuels de l'application ne sont pas supprimés... seules les entrées dans le registre sont effacées.
3. **Points manuels** : crée par l'utilisateur.

Paramétrages des point de restauration : Vssadmin

Ce paramétrage se fait via une commande en ligne

Vssadmin

On peut demander un état des lieux via

Vssadmin list shadowstorage

```
C:\Users\Administrateur>vssadmin list shadowStorage
vssadmin 1.1 - Outil ligne de commande d'administration du service
de cliché instantané de volume
(C) Copyright 2001-2005 Microsoft Corp.

Association de stockage de cliché instantané
  Pour le volume : (C:)\??\Volume{a5248ba1-f05e-11dc-af8a-806e6f6e6963}\
  Volume de stockage de cliché instantané : (C:)\??\Volume{a5248ba1-f05e-11dc-af8a-806e6f6e6963}\
    Espace du volume de stockage de cliché instantané utilisé : 400.016 MB.
    Espace du volume de cliché instantané alloué : 698.563 MB.
    Espace maximal du volume de cliché instantané : 5.59 GB

Association de stockage de cliché instantané
  Pour le volume : (D:)\??\Volume{d99de527-f67a-11dc-8173-0080c8e6c311}\
  Volume de stockage de cliché instantané : (D:)\??\Volume{d99de527-f67a-11dc-8173-0080c8e6c311}\
    Espace du volume de stockage de cliché instantané utilisé : 464 KB.
    Espace du volume de cliché instantané alloué : 300 MB.
    Espace maximal du volume de cliché instantané : 1.465 GB
```

l'option la plus intéressante est

Vssadmin resize shadowstorage

```
C:\Users\Administrateur>vssadmin resize shadowStorage /?
vssadmin 1.1 - Outil ligne de commande d'administration du service
de cliché instantané de volume
(C) Copyright 2001-2005 Microsoft Corp.

Resize ShadowStorage /For=VolumeFor /On=VolumeOn [/MaxSize=TailleMax]
- Modifie la taille maximale d'une association de stockage d'instantanés
entre VolumeFor et VolumeOn. La modification de la taille
d'une association de stockage peut faire disparaître des clichés
instantanés. Si TailleMax n'est pas spécifiée, l'espace utilisable
n'est pas limité. Étant donné que certains clichés instantanés sont
supprimés, l'espace de stockage des clichés sera réduit. TailleMax
doit être supérieure ou égale à 300 Mo et accepte les suffixes suivants :
KB, MB, GB, TB, PB et EB. Vous pouvez également utiliser les suffixes
B, K, M, G, T, P et E. Si aucun suffixe n'est spécifié, TailleMax
est en octets.

Exemple d'utilisation :
vssadmin Resize ShadowStorage /For=C: /On=D: /MaxSize=900MB
```

Comme dans

vssadmin Resize ShadowStorage /For=C: /On=D: /MaxSize=40GB

avec

/For : permet de spécifier sur quel volume on veut mettre en oeuvre

/On : permet de spécifier sur quel volume les points de restauration sont stockés. Sur un système très sollicité, il est bon de dédier un volume spécifique (voire un disque) de 300 MG minimum

/MaxSize= permet de spécifier la taille maximale allouée

SAUVEGARDE SYSTEME - FICHIERS

Deux Outils de Sauvegarde :

SEVEN propose deux nouveaux types de sécurisation pour votre machine:

- Une sauvegarde type image disque (configuration complète)
A L'initiative de l'utilisateur
Automatisable via l'utilitaire **wbadmin.exe**
- Une sauvegarde type fichier (récupération des versions précédentes)
A l'occasion des points de restauration (s'ils sont en place),
Lors de la sauvegarde Seven (si elle est effectuée ou programmée)

Image système - vhd :

Il est donc possible de sauvegarder un volume entier sous forme d'un fichier image disque au format **.vhd**

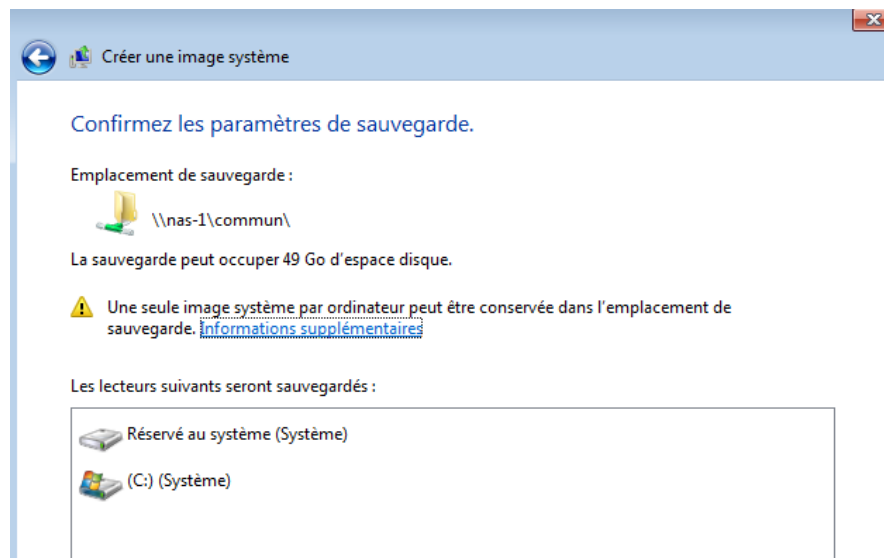
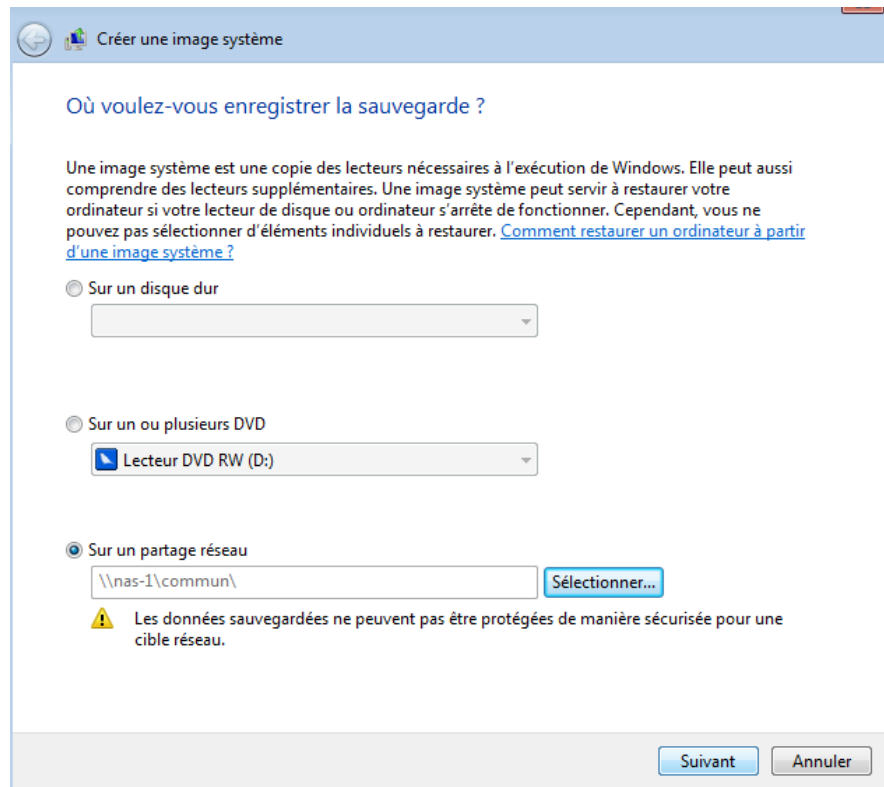
- Avantage : permet de restaurer un ordinateur avec toutes ses applications et données
- Avantage : peut être stocké que sur un lecteur local (CD, DVD, disque amovible...) ou Réseau
- Inconvénient : occupe plus de place, de temps

Accessible via **Démarrer / Programme / Maintenance / Sauvegarder et restaurer**

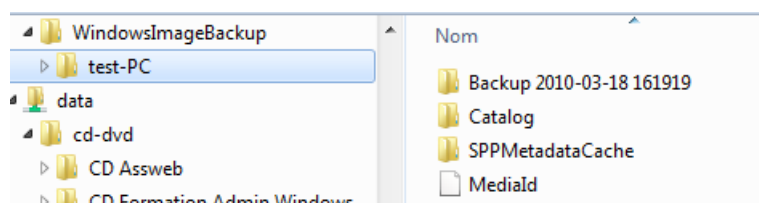


Ici avec **Créer une image système**

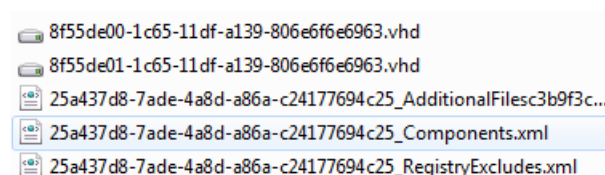
N.B: Ne pas confondre effectuer des sauvegardes, la technique des points de restauration et la création d'une image système de SEVEN...



Cela créera la structure suivante



Avec une nature de fichier .VHD



Automatiser via wbadmin

Pour automatiser la sauvegarde intégrale (à fréquences régulières) il faut utiliser l'utilitaire en invite de commande **wbadmin.exe**

L'option la plus intéressante étant

wbadmin start backup

```
Utilisation : WBADMIN START BACKUP
-backupTarget:<VolumeCible ; PartageRéseauCible>
-include:VolumesÀInclure
[-noVerify]
[-quiet]
```

Pour sauvegarder le lecteur C: dans le lecteur H: il faut alors

wbadmin start backup -backupTarget:H: -include:C: -quiet

cette commande peut aussi permettre de suivre l'évolution d'une sauvegarde lancée graphiquement depuis **Créer une image système**

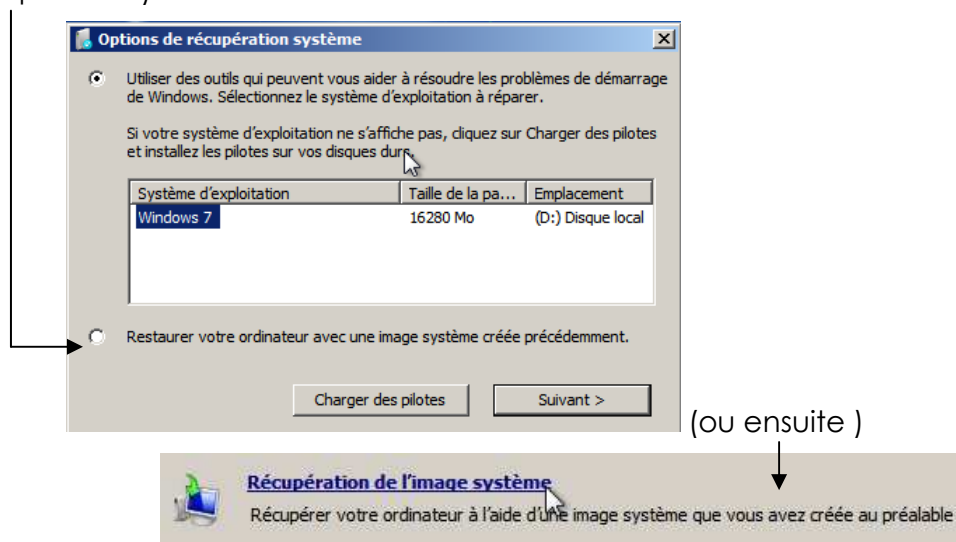
wbadmin get status

```
C:\Users\Administrateur>wbadmin get status
wbadmin 1.0 - Outil de ligne de commande de sauvegarde
(C) Copyright 2004 Microsoft Corp.

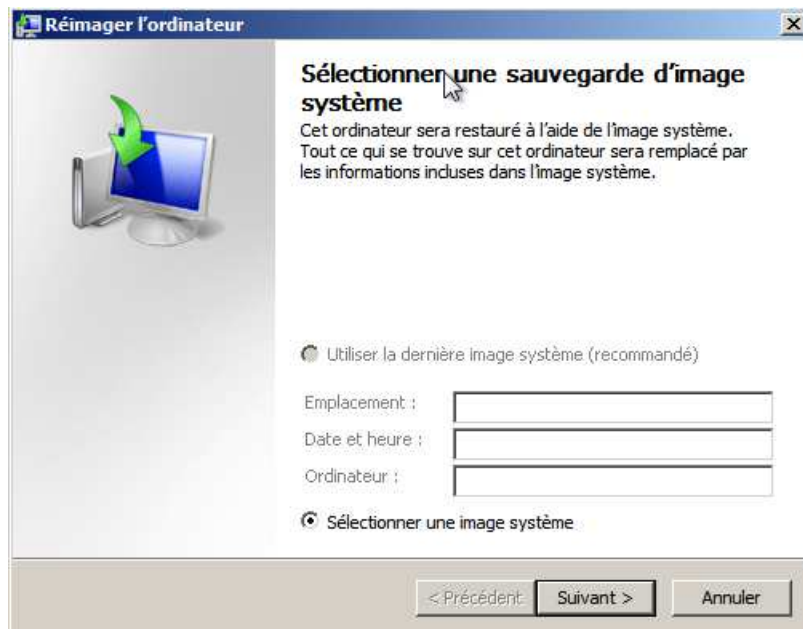
La sauvegarde du volume Réserve au système (100.00 Mo) a abouti.
Création d'une sauvegarde du volume Disque local(C:) en cours, (56%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (56%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (57%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (57%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (57%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (57%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (57%) copiés.
Création d'une sauvegarde du volume Disque local(C:) en cours, (57%) copiés.
```

Réaliser une Restauration Intégrale Système

Cela peut se faire en bootant sur le CD démarrant Windows RE (ou le CD de réparation) et en demandant directement **Restaurer votre ordinateur...**

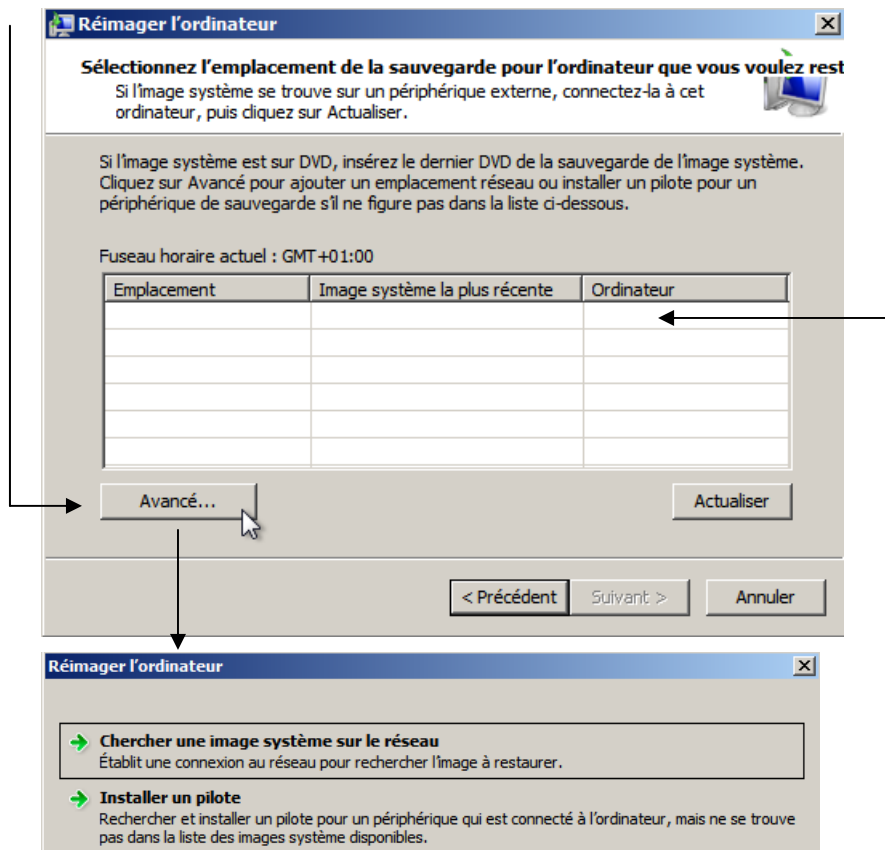


Cela déclenche un assistant

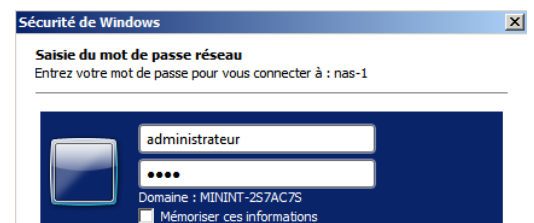
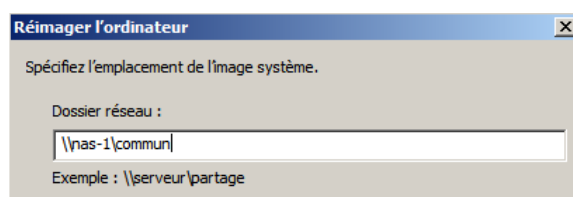


N.B: La dernière image système apparaît si elle est stockée localement...

Soit les images systèmes présentes sur la machine apparaissent...
Soit avec **Avancé...** on va les chercher !



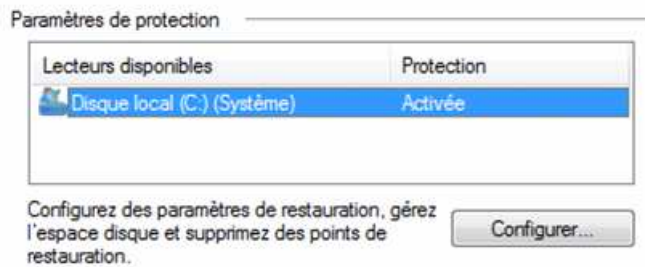
N.B: à ce stade on utilise les drivers réseau connus du Media utilisé ! attention donc au périphériques non reconnus en standard par SEVEN si on utilise le CD de réparation (on incorporera les drivers dans WIN PE)



Réaliser une Sauvegarde Fichiers-

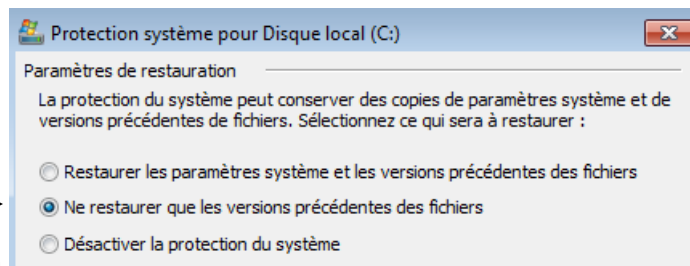
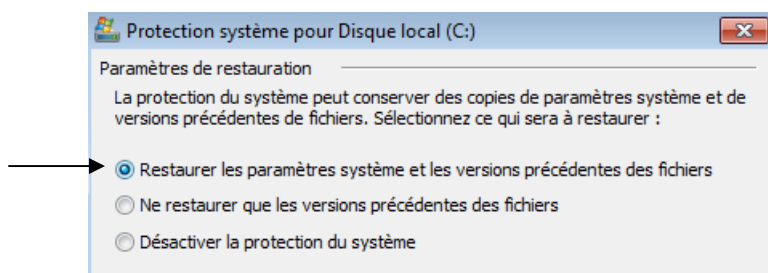
Les sauvegardes de fichiers se font uniquement si :

1. dans l'onglet **Protection du système** qui est accessible via les **propriétés** de **Ordinateur**



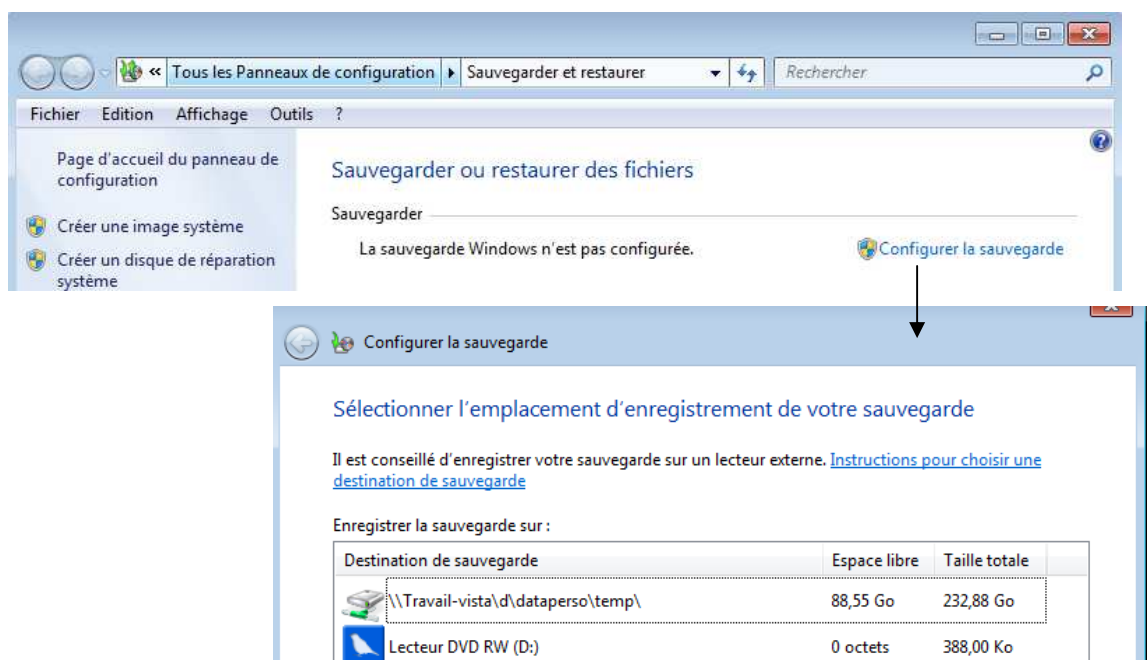
Les paramètres de protection sont activés

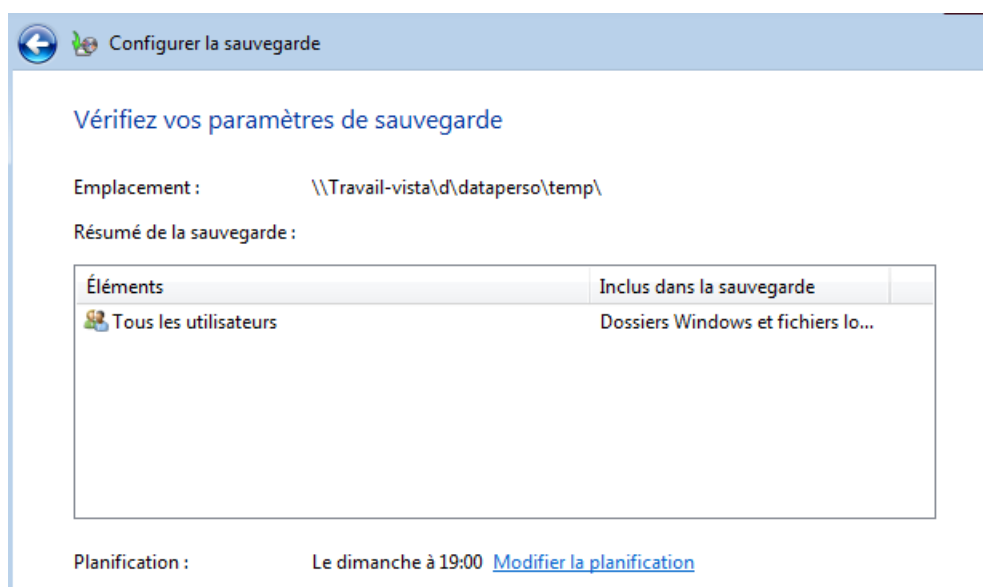
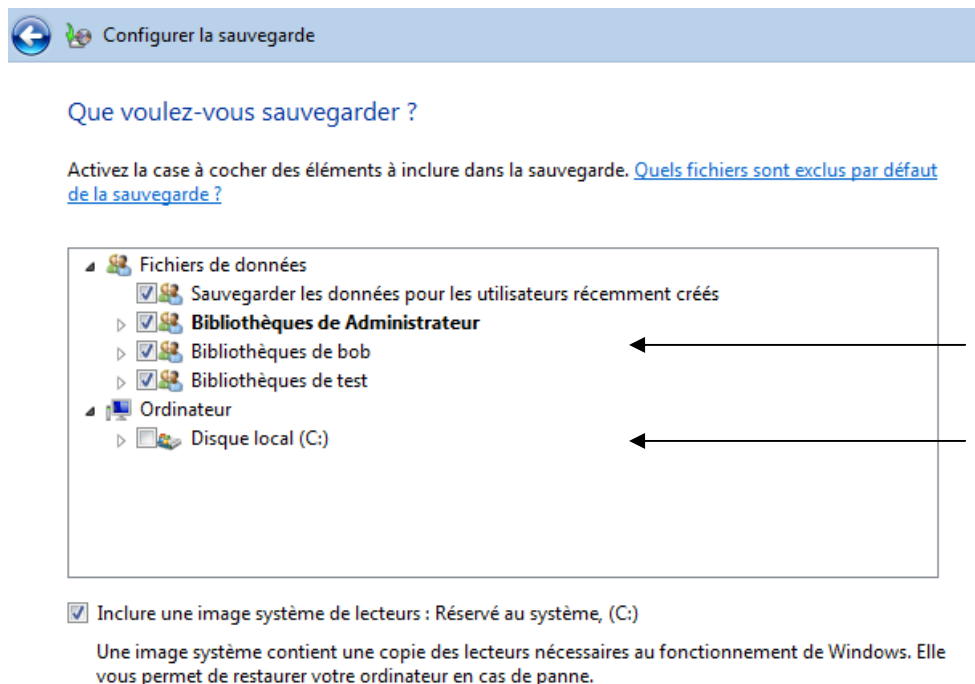
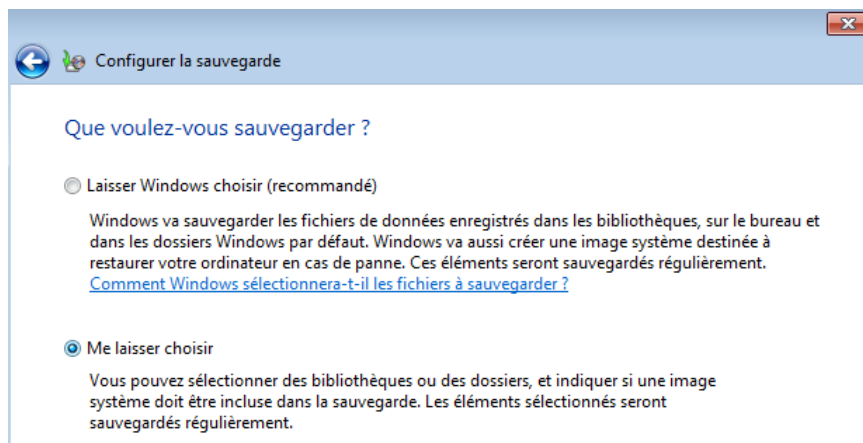
2. Il faut demander **Configurer...** et soit la valeur par défaut



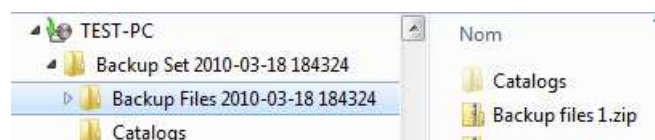
soit au minimum

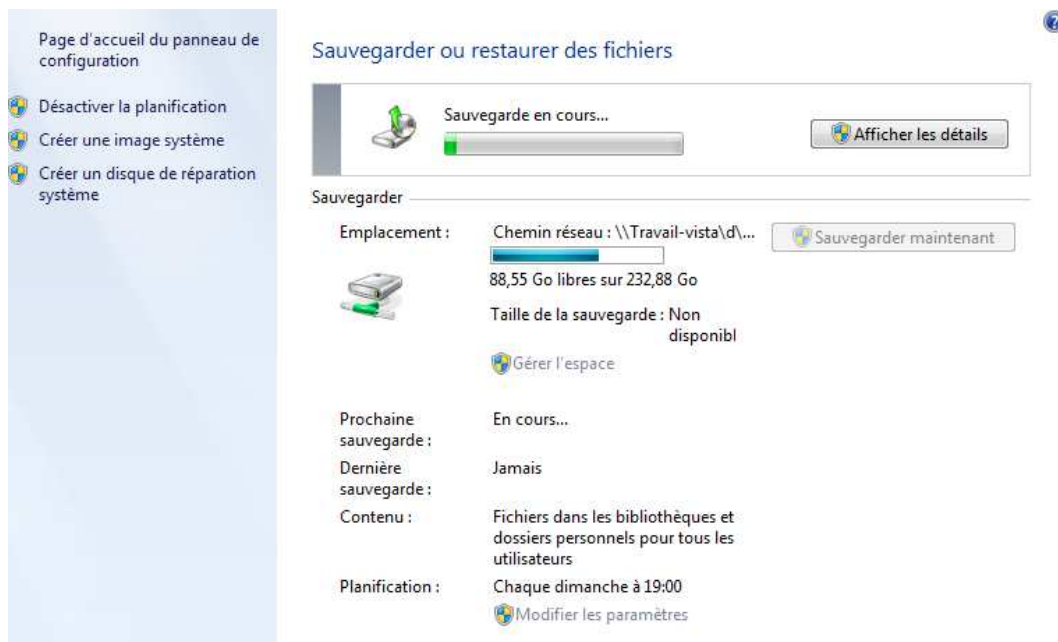
Si les points de restauration sont désactivés, il est évident alors qu'il faut paramétrer la sauvegarde SEVEN...





Cela crée une structure à base de fichier ZIP

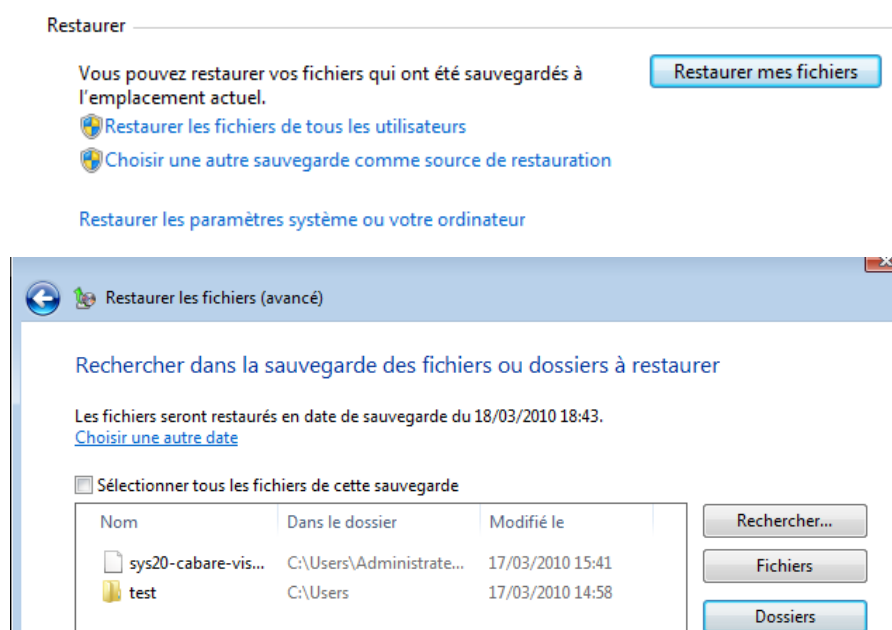




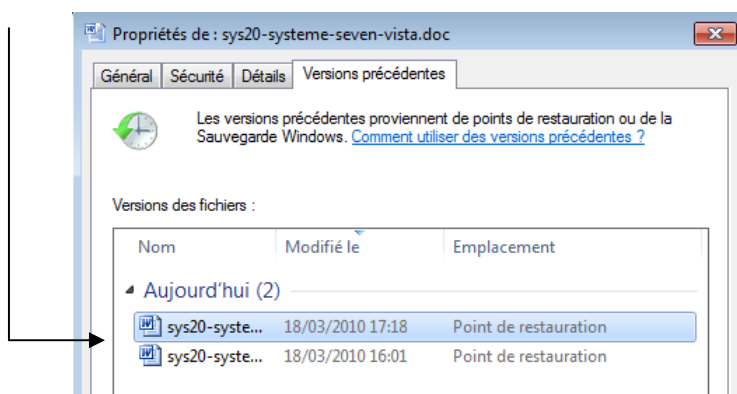
Réaliser une Restauration de Fichiers-

A partir du moment où au moins une sauvegarde a été réalisée, et / ou que les points de restaurations ont été mis en place, il est possible

Soit via **Programme / Maintenance / Sauvegarder et Restaurer**



Soit via les **propriétés** du **fichier / dossier** onglet **Versions précédentes**

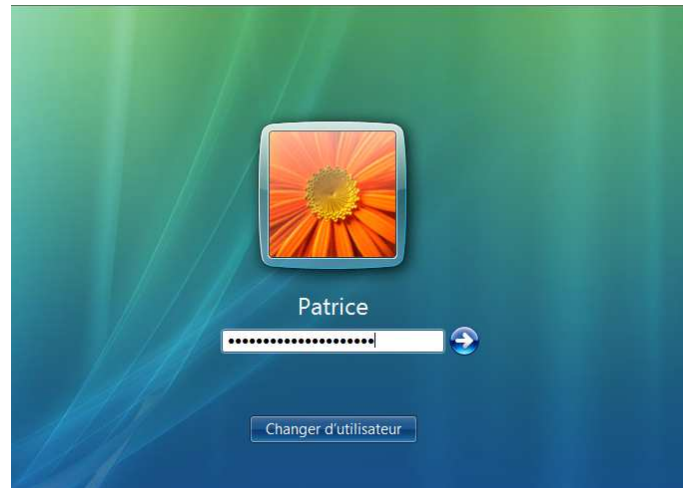


COMPTES UTILISATEURS

Compte d'utilisateurs – session:

On parle de **compte utilisateur** lorsque l'on définit un individu nommé désigné, généralement par un nom d'utilisateur, et un mot de passe et des propriétés

C'est pourquoi toute **session** de travail sur un ordinateur débute par une boîte de dialogue (ou une image à cliquer) demandant un **Nom Utilisateur** et un **Mot de passe** pour reconnaître le compte utilisateur



Le mot de passe peut contenir jusqu'à **127 caractères**

Le nom utilisateur peut contenir jusqu'à **20 caractères**

Attention, le système fait la différence entre **Minuscules /Majuscules** ! et n'accepte pas les caractères suivant: " \ : ; = , + * ? < >

Par sécurité, utilisez un mot de passe d'au moins 7 caractères avec des lettres majuscules et minuscules, des nombres et de la ponctuation...

N.B : Windows 95-98 ne prends en charge que des mots de passe pouvant comporter 14 caractères maxi . Si vous utilisez Windows 2000 XP sur un réseau qui compte aussi des ordinateurs exécutant Windows 95-98 **ne créez pas de mot de passe de plus de 14 caractères**

Winlogon.exe

Ouverture de session

Séquence authentifiée 1

Fermeture de session

Ouverture de session

Séquence authentifiée 2

Fermeture de session

Arrêt Poste

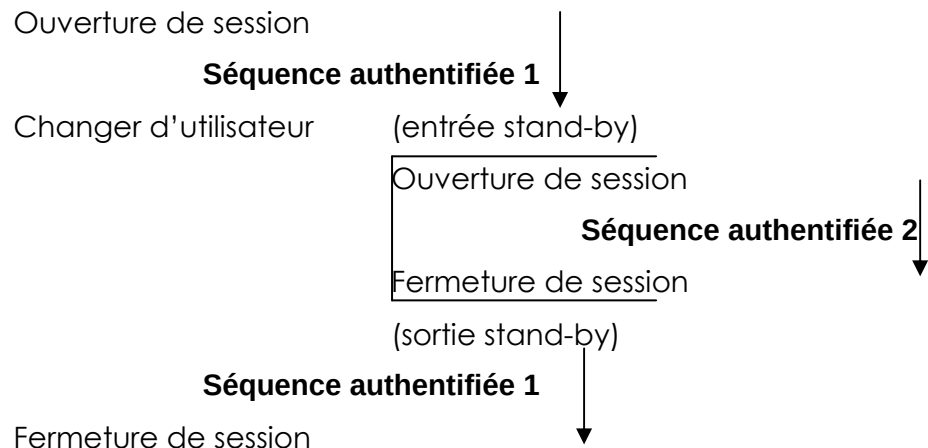
Lorsque l'on ferme une session, tous les travaux en cours ont terminés, et l'on doit pour pouvoir de nouveau travailler, ouvrir une nouvelle session

Connexion multiples Utilisateur

Sur un poste Seven (comme XP) il est possible de changer d'utilisateur connecté sur le poste, sans fermer sa session (les travaux et la tâches initiés continuent...) c'est-à-dire que l'on peut autoriser sur un poste plusieurs sessions en parallèle de différents utilisateurs...

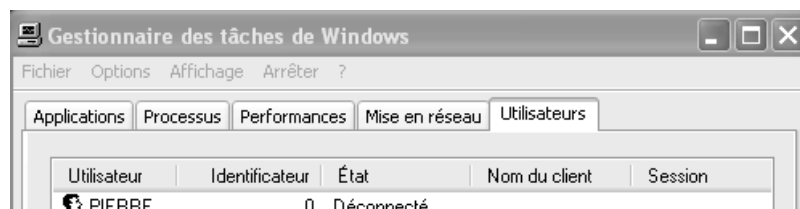
- Il n'est donc plus nécessaire de fermer la session d'un utilisateur pour ouvrir sa propre session....
- Autrement dit deux utilisateurs peuvent ouvrir chacun une session et se passer la connexion sans arrêter leur travaux respectifs....

Winlogon.exe



Arrêt Poste

Pour chaque connexion de chaque session, par exemple Pierre rouvre une connections et recommence à jouer... il à l'impression d'être tout seul...



Mais si l'**Administrateur** ouvre également une connexion, alors il verra toutes les autres connections en cours

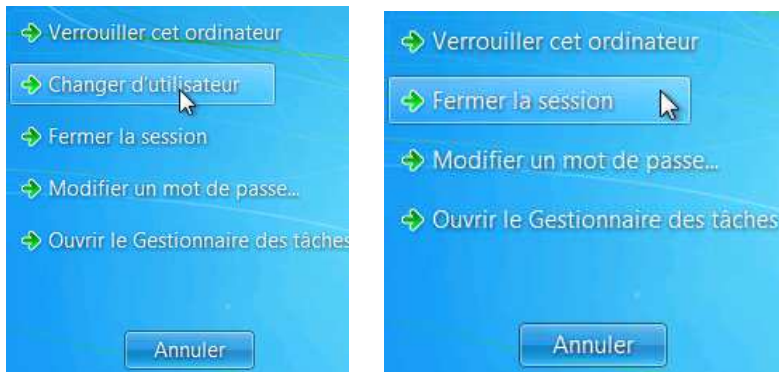


N.B: Cette fonctionnalité, extrêmement gourmande en ressource, pose certains problèmes avec des applications non spécifiquement dessinée pour **XP-Seven**, et entraîne parfois des pertes de donnée lorsqu'un utilisateur éteint la machine sans savoir que d'autres connections sont en cours (par exemple)

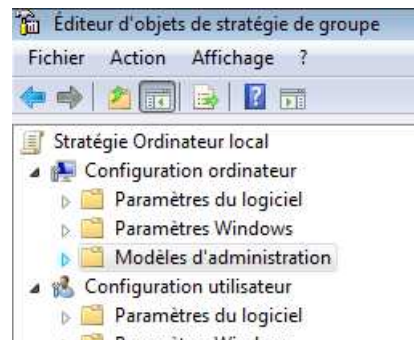
POUR TOUTES CES RAISONS LES CONNEXIONS RAPIDES NE SONT PAS CONSEILLÉES SUR UNE MACHINE A USAGE PROFESSIONNEL !

Désactiver la bascule rapide Utilisateur

Pour faire disparaître **Changer d'utilisateur** (sans fermer la session)

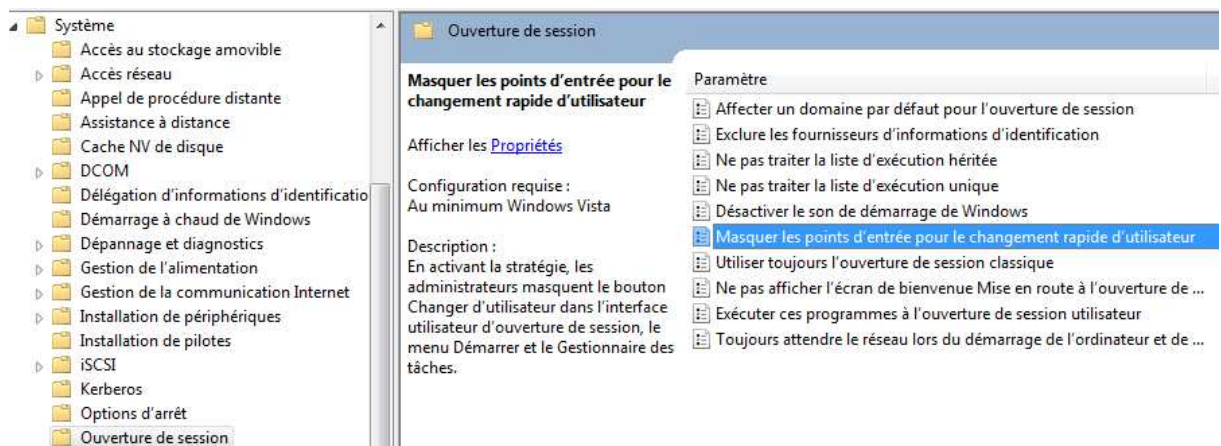


Soit on utilise **gpedit.msc**



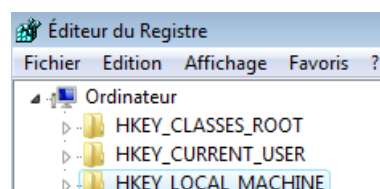
puis

Système/Ouverture de session/Masquer les points d'entrée pour le changement rapide d'utilisateur



ou alors Il faut passer par la base de registre

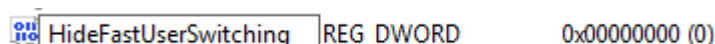
Regedt32.exe



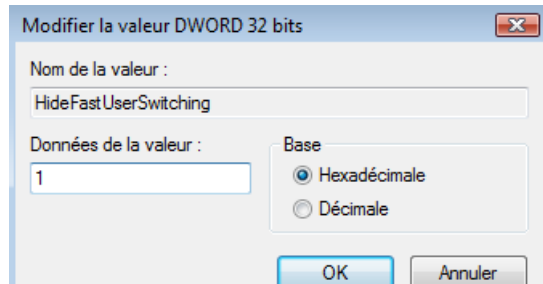
Et dans la clé

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Il faut créer la valeur DWORD : HideFastUserSwitching



Lorsque la valeur Dword vaut 1, alors les sessions multiples sont désactivées.



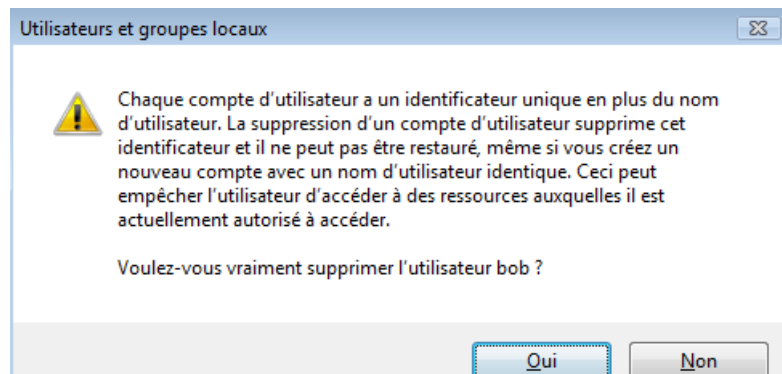
N.B : cette option est automatiquement activée si le poste fait partie d'un domaine. (par défaut la bascule entre utilisateurs locaux est activé sur un poste en workgroup)

SID Sécurité identifier :

Le SID est un numéro d'identification unique sur un poste WindowsT comportant 38 digits et représentant un compte utilisateur ou un nom de groupe. Créé automatiquement à chaque déclaration de nouveau groupe ou utilisateur, il reste stocké dans la machine même si le groupe ou l'utilisateur qui en était à l'origine est supprimé

Ce qui fait que si on supprime puis on recrée un compte ayant le même nom, le SID attribué la deuxième fois sera différent de celui utilisé lors de la 1^{re} création, et par conséquent on ne pourra réutiliser les ressources droits et permissions allouées lors de la première utilisation

Seven se fonde sur les SID et pas sur les noms !



PAR CONSÉQUENT IL EST IMPOSSIBLE DE RECRÉER UN COMPTE UTILISATEUR UNE FOIS QUE CELUI-CI A ÉTÉ EFFACÉ, MEME SI LE MEME NOM EST ATTRIBUÉ ON NE POURRA UTILISER LES RESSOURCES ANCIENNEMENT ALLOUÉES

Whoami :

en tant que quoi on est logué ? **whoami**

```
C:\Users\Administrateur>whoami
util-pc\administrateur
```

et SID à titre d'information **whoami /user**

```
C:\Users\Administrateur>whoami /user

Informations sur l'utilisateur
=====
Nom d'utilisateur      SID
=====
util-pc\administrateur S-1-5-21-1011606315-2156083306-973574392-500
```

Comptes pré-définis :

Il y a un changement important par rapport aux versions précédentes, seuls deux comptes sont créés

Sous **SEVEN** il existe 2 Comptes Utilisateurs prédéfinis

Nom	Nom complet	Description
 Administrateur		Compte d'utilisateur d'administration
 Invité		Compte d'utilisateur invité

Le **Compte Administrateur** (celui d'origine):

C'est la personne qui aura le pouvoir maximal sur la station de travail, et pourra gérer la configuration du système

- Ce compte ne peut être supprimé, mais peut être renommé
- Ce compte par défaut est inactivé

Le **Compte Invité** :

Sert pour des utilisateurs occasionnels ayant un minimum de droits sur le système

- Ce compte par défaut est inactivé

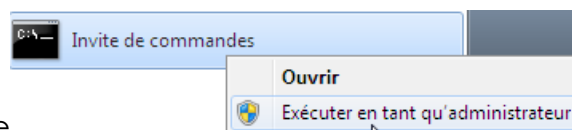
N.B: dans la pratique, lors de l'installation d'un poste Windows 8 hors domaine, un assistant se déroule lors du premier démarrage, demandant les noms des "futurs" utilisateur du poste.... Cela a pour effet de créer des comptes utilisateur – administrateurs !

Ces comptes ayant donc des privilèges forts, puisqu'ils sont membre du groupe des administrateurs du poste.

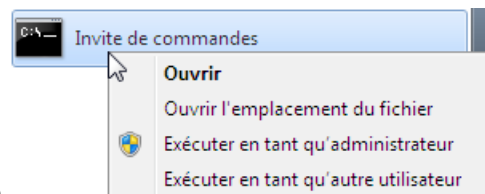
Exécuter en tant que:

On peut lancer une application avec un login autre que celui en cours...

Soit avec le **clic droit** / sur l'invite



Soit avec **MAJ + clic droit** / sur l'invite



Utilisateurs locaux:

Il est possible de créer des comptes utilisateurs sur un poste **SEVEN** on parle alors de comptes locaux, qui n'ont de portée que la machine sur laquelle ils sont créés.

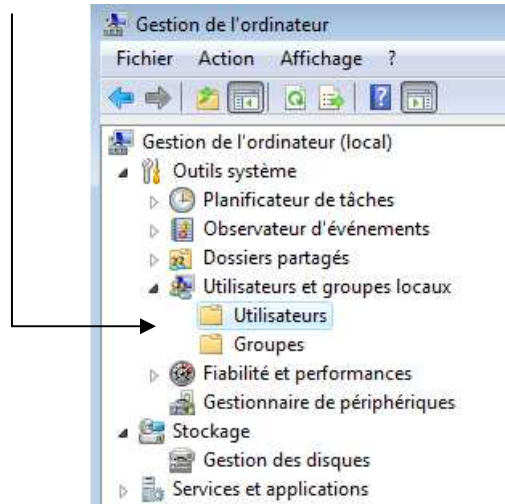
La meilleure façon pour faire cela se trouve dans le menu

**Démarrer / Panneau de configuration (affichage classique)
/ Outils d'Administration/ Gestion de l'ordinateur**

Ou plus rapidement par clic droit sur l'icône **Ordinateur** du bureau

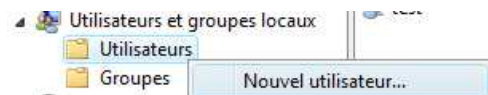


Sur l'icône **Ordinateur** du bureau on demande clic droit **gérer**



Pour créer un nouvel utilisateur
il suffit de demander clic droit
sur le dossier **Utilisateurs**,

Puis **Nouvel utilisateur...**



Nouvel utilisateur

Nom d'utilisateur :

Nom complet :

Description :

Mot de passe :

Confirmer le mot de passe :

☒ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

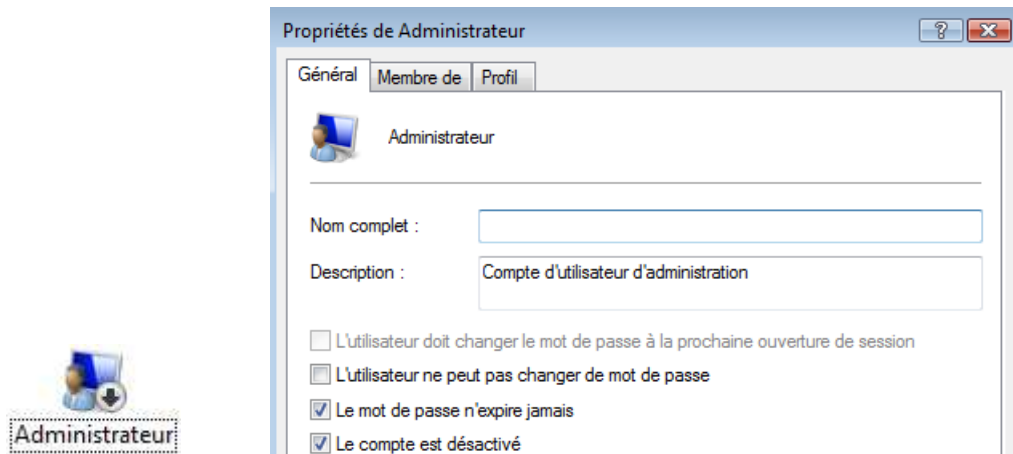
☐ Le mot de passe n'expire jamais

☐ Le compte est désactivé

Gestion des Comptes:

Le compte administrateur d'origine, est désactivé par défaut lors de l'installation.

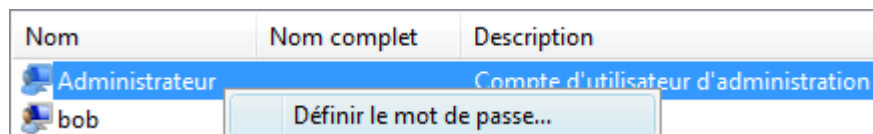
Comme on ne peut pas lui donner un mot de passe lors de l'installation, il faut impérativement lui en donner un lors de son activation !



c'est le seul qui ne subit pas l'**UAC** !

Re-définition de mot de passe

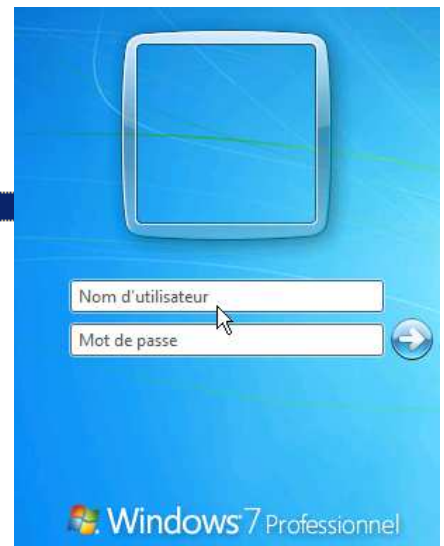
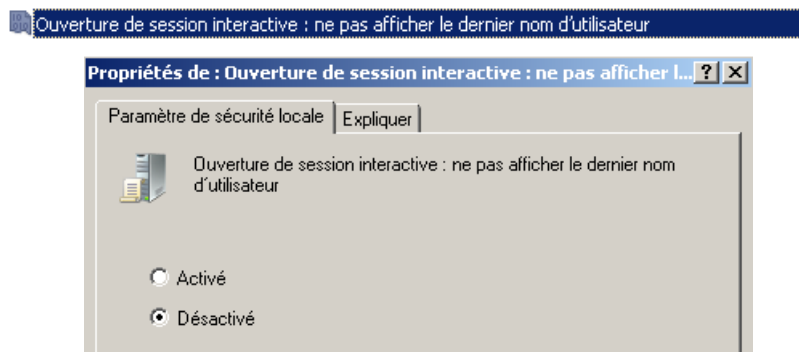
Si on en a les privilèges, on réinitialise le mot de passe d'un compte utilisateur en faisant clic-droit sur le compte à changer, puis on demande **Définir le mot de passe...**



Cacher le dernier Utilisateur

Pour cacher le nom du dernier utilisateur à s'être authentifié...

Stratégies de sécurité locales / Stratégies locales / Options de sécurité



N.B : pour ne pas proposer une liste des utilisateurs locaux existante, et demander un login – mot de passe, il suffit d'activer cette option

GROUPE LOCAUX

Notions de groupes :

On peut aussi définir l'appartenance d'un individu à un groupe (ou à plusieurs groupes) ayant des droits et des permissions bien définies, on dit alors que tel **compte utilisateur** est membre de tel ou tel **groupe**

Toute personne connectée sur le réseau, et à fortiori sur le serveur, est un utilisateur dont on aura forcément prédéfini les actions qu'il est censé faire, et celles qu'il ne peut pas faire, par conséquent toute action sur une machine est déterminée par ce que l'on appelle des "**droits**".

Les droits d'un utilisateur sont souvent déterminés par le groupe auquel il appartient, un **groupe** étant un ensemble d'utilisateur ayant les mêmes droits, ou mieux, un ensemble de droits et de permissions bien définies, dont on bénéficiera lorsque l'on en fait partie.

Un groupe possède un symbole qui est



Groupes Locaux Prédéfinis :

Il existe un certain nombre de **groupes prédéfinis** dans Windows, depuis le groupe Administrateurs (disposant de tous les droits) jusqu'au groupe Invité (ayant les droits les plus faibles, et ne disposant même pas d'un mot de passe...)

Ces groupes prédéfinis, l'administrateur lui-même ne peut les détruire ni les renommer. Autrement dit **ce n'est pas vous qui gérez les groupes prédéfinis, mais vous pouvez vous en servir....**

Dans SEVEN on distingue trois types de comptes utilisateur

- Des comptes utilisateurs standards
- Des comptes utilisateurs administrateurs
- Des comptes utilisateurs invités

PROFILS UTILISATEURS

Liens Symboliques – Raccourcis – Jonctions :

Un lien symbolique c'est un alias avec le dossier/fichier sur lequel on se lie... (si on supprime le lien symbolique, le dossier/fichier n'est pas supprimé)

Un lien réel c'est un autre nom pour le même dossier/fichier (si on supprime le lien réel, le dossier/fichier est supprimé)

Différence entre liens symboliques et raccourcis:

- Un **Raccourci** est une redirection au niveau du système d'exploitation, SEVEN
- Un **Lien symbolique** est une redirection au niveau du système de fichier, NTFS

N.B: on peut lister les liens avec **dir /a** ou mieux **dir /al**

Le lien garde les propriétés du dossier-fichier vers lequel il pointe, ce n'est pas fichier Ink. Ce lien se comporte comme le dossier-fichier "original".

En effet dans les propriétés d'un "raccourci" est-ce utile de savoir que c'est un fichier **Ink** de 800 octets ?, alors qu'avec un lien symbolique, nous pourrions savoir combien pèse le dossier cible, gérer son partage, ses accès... exactement comme si vous regardiez les propriétés du vrai dossier

Par exemple si certains dossiers sont perdus dans l'arborescence complexe de votre système et on veut les gérer depuis le bureau, il vous suffira de créer des liens symboliques sur le bureau avec ces dossiers.

N.B: Les jonctions de répertoire font "double emploi" avec les liens symboliques, simplement elles existent pour des raisons de compatibilité. Elles ne peuvent être données qu'avec des chemins absolus !

Objectif :

Les profils d'utilisateur présentent plusieurs avantages :

- Lorsque les utilisateurs ouvrent une session sur leur station de travail, ils reçoivent les paramètres du bureau tels qu'ils existaient à la fermeture de la dernière session.
- Plusieurs utilisateurs peuvent utiliser le même ordinateur et chacun reçoit un bureau personnalisable lorsqu'il ouvre une session.

Les profils permettent de mémoriser notamment les paramètres suivants:

Explorateur Windows NT	Tous les paramètres définissables par l'utilisateur pour l'Explorateur Windows NT.
Barre des tâches	Tous les groupes de programmes personnels et leurs propriétés, tous les programmes et leurs propriétés, et tous les paramètres de la barre des tâches.
Paramètres d'imprimante	Connexions aux imprimantes du réseau.
Panneau de configuration	tout sauf polices / date-heure / affichage drivers / réseau /
Accessoires	Tous les paramètres d'application spécifiques à l'utilisateur qui affectent l'environnement Windows NT de l'utilisateur, tels que la Calculatrice, l'aspect de l'horloge, le Bloc-notes, Paint

Profil Local:

Le profil est créé automatiquement par défaut pour chaque utilisateur qui ouvre une session sur un poste. Il prend alors le nom de **Profil Local**.

Le profil local peut être créé à partir d'un profil local par défaut (modèle) stocké dans un dossier **Default** (sous Seven) ou **Default User** (sous XP)

Emplacement Profils Locaux Seven:

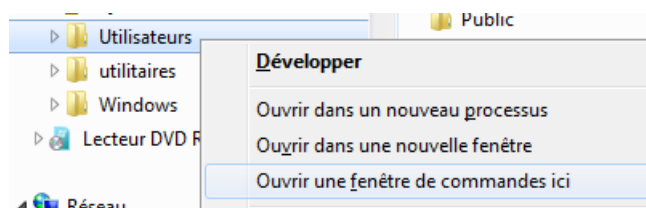
Les Profils Seven ne sont pas stockés comme les profils XP:

XP (Document and Settings)	Seven (Users ou " Utilisateurs ")
-------------------------------------	--

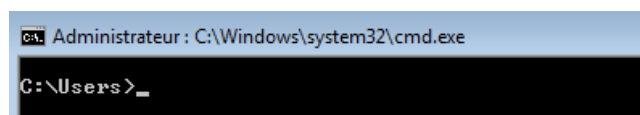
- Le dossier Racine des profils devient « visuellement » le dossier **Utilisateurs** (selon la régionalisation française) mais se trouve être le dossier **Users** (anciennement **Document and Settings**)

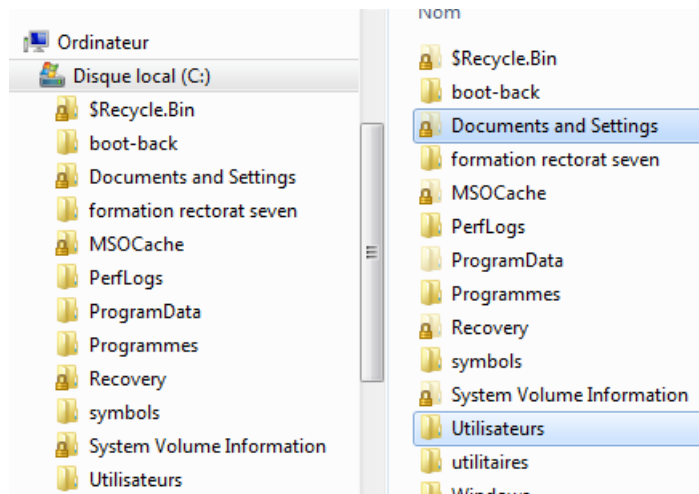
N.B : Avec la régionalisation Seven, le dossier **Users** apparaît dans l'explorateur comme **Utilisateurs**. Mais on le retrouve en demandant

Clic-Droit / Ouvrir une fenêtre de commandes ici

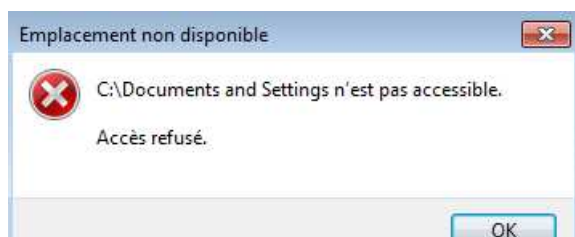


On obtiendra





N.B : on ne peut plus « accéder » à **Documents and Settings...** ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **user...**



La commande en invite

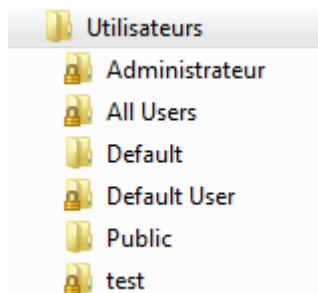
dir /a ou mieux **dir /al** liste les jonctions...

```
C:\>dir /al
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est F2F4-F37C

Répertoire de C:\
14/07/2009 05:53 <JUNCTION> Documents and Settings [C:\Users]
0 fichier(s) 0 octets
```

Structure des Profils Seven:

Dans le dossier **Utilisateurs** (Racine des profils), on trouve désormais



2 nouveaux dossiers système :

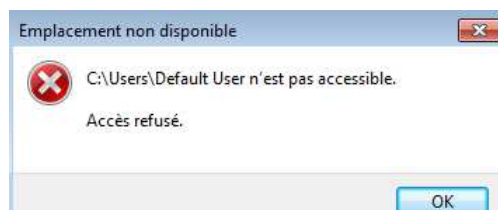
Default et **Public**

2 jonctions pour compatibilité XP-2000 :

Default User et **All Users**

Et les dossier profils des utilisateur créés :
Administrateur , test, xxxx

N.B : on ne peut plus « accéder » à **Default Users...** ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **C:\Users\Default...**



La commande en invite

dir /a ou mieux **dir /al** liste les jonctions...

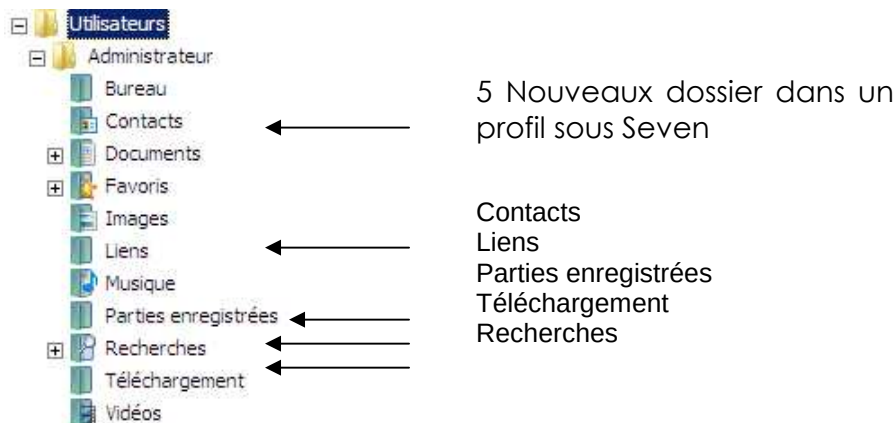
```
Répertoire de C:\Users
14/07/2009 05:53 <SYMLINKD> All Users [C:\ProgramData]
14/07/2009 05:53 <JUNCTION> Default User [C:\Users\Default]
0 fichier(s) 0 octets
2 Rép(s) 6 714 511 360 octets libres
```


Structure d'un profil Utilisateur

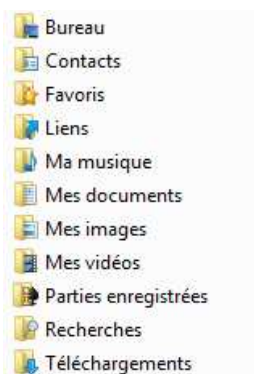
Les principaux changements par rapport aux profils XP sont les suivants :

XP (Document and Settings)	Seven (Users ou " Utilisateurs ")
Pour un compte Donné nommé "Administrateur" Tout se trouve dans Document and Settings \ Administrateur	Pour un compte Donné "Administrateur" Une partie se trouve sous C:\Users\Administrateur Et une partie dans C:\Users\Administrateur \Appdata\Roaming\Microsoft\Windows

- Les préfixes **mes** et **ma** sont supprimés des dossiers **document** ou **musique** (à la place de **mes document** ou **ma musique**)
- Les dossiers **document** ou **musique...** ne sont plus des sous-dossiers du dossier mes documents, mais sont directement créés à la racine du dossier profils (en quelque sorte remise à plat de l'arborescence...)
- 5 nouveaux dossiers apparaissent dans le profil



- Les noms des dossiers physiques ne correspondent pas forcément. Avec la "régionalisation", on peut dire que :



<REP>	Contacts
<REP>	Desktop
<REP>	Documents
<REP>	Downloads
<REP>	Favorites
<REP>	Links
<REP>	Music
<REP>	Pictures
<REP>	Saved Games
<REP>	Searches
<REP>	Videos

Noms réels « hors régionalisation » du gestionnaire de fichier Seven

- certaines entrées stockées sous XP directement dans le profil utilisateur sont maintenant sous SEVEN dans un sous dossier du profil utilisateur **\AppData\Roaming\Microsoft\Windows...** comme par exemple

```

<JUNCTION> Application Data [C:\Users\Administrateur\AppData\Roaming]
<JUNCTION> Cookies [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Cookies]
<JUNCTION> Local Settings [C:\Users\Administrateur\AppData\Local]
<JUNCTION> Menu Démarrer [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Start Menu]
<JUNCTION> Mes documents [C:\Users\Administrateur\Documents]
<JUNCTION> Modèles [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Templates]
<JUNCTION> Recent [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Recent]
<JUNCTION> SendTo [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\SendTo]
<JUNCTION> Voisinage d'impression [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Printer Sho
<JUNCTION> Voisinage réseau [C:\Users\Administrateur\AppData\Roaming\Microsoft\Windows\Network Shortcuts

```

Profil par Défaut

Les principaux changements par rapport aux profils XP sont les suivants :

- Le dossier **Default** correspondant au dossier **Default User** sous XP contient le profil par défaut

```

C:\Users>dir /al
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est 144A-3A67

Répertoire de C:\Users

19/01/2008  15:23    <SYMLINKD>    All Users [C:\ProgramData]
19/01/2008  15:23    <JUNCTION>    Default User [C:\Users\Default]

```

Méthode Certifiée pour modifier le profil par défaut

Il n'est plus possible dans Seven selon Microsoft de modifier le profil par défaut comme on le faisait dans XP

Ceci car certains petits bug apparaissent lorsque on copiait/collait brutalement le profil type dans Default user...

La solution désormais repose sur un fichier **Unattend.xml** contenant une instruction di genre **<copyProfile>true</copyProfile>**

Ce fichier devant être passé en paramètre à un **sysprep** de la machine...

Ceci dit on peut avoir envie de modifier le profil par défaut, dans refaire un sysprep du poste complet, car sysprep ré-initialise bien plus de chose que le simple profil par défaut...

Méthode Non Certifiée pour modifier le profil par défaut

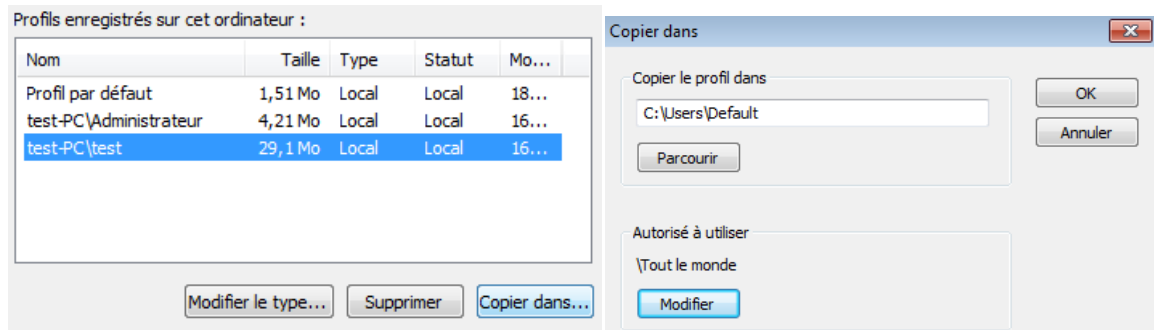
N.B: la méthode de base peut se limiter aux 5 premiers points, car la suite peut demander re-démarrages et attention particulière !!

- Créer un utilisateur "test" (ou mieux "test-xyz") ayant des droits d'administration sur le poste
- Ouvrir une session avec, et faire tout ses réglages...

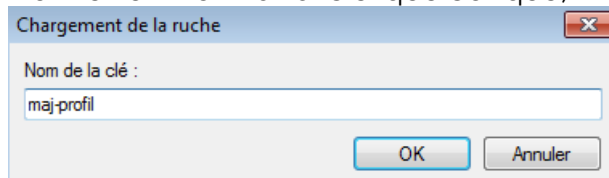
3. Fermer la session de l'utilisateur test et ouvrir une session admin

4. Installer l'utilitaire "**windows enabler**"  et l'activer 

5. Copier le profil test en **C:\Users\Default** avec les droits **Tout le monde**



6. Sélectionner la branche **HKLM** et lancer **regedit**, demander **Fichier / Charger la ruche** et aller chercher la ruche **ntuser.dat** du profil par défaut (donc depuis **c:\user\default**).
Donner un nom à la clé quelconque, mais unique, comme "*maj-profil*"

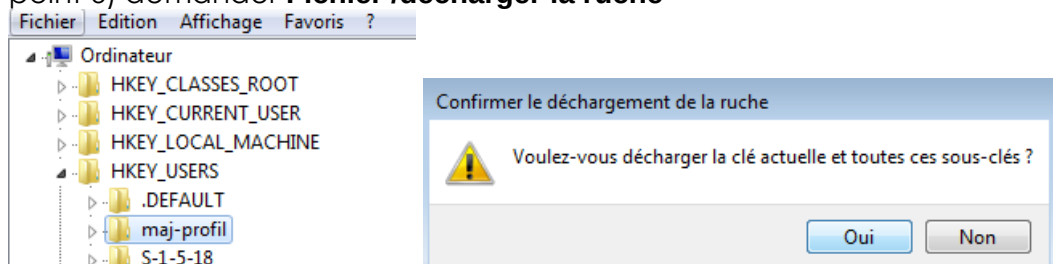


7. dans cette clé, rechercher le nom du profil d'origine du modèle, (donc pour nous "test" (ou mieux *test-xyz*)



effacer toutes les occurrences trouvées...

8. se replacer sur la ruche nettoyée "maj-profil" (si on l'a appelée ainsi au point 6) demander **Fichier /décharger la ruche**



9. reboot du PC

Profil Public

Les principaux changements par rapport aux profils XP sont les suivants :

- les dossiers **ProgramData** et **Users\ Public** correspondent à l'ancien dossier **All User** sous Windows XP

```
C:\Users>dir /al
Le volume dans le lecteur C n'a pas de nom.
Le numéro de série du volume est 144A-3A67

Répertoire de C:\Users

19/01/2008  15:23    <SYMLINK>      All Users [C:\ProgramData]
19/01/2008  15:23    <JUNCTION>     Default User [C:\Users\Default]
```

XP (Document & Settings)	Seven (ProgramData et Users)
All users	En partie dans C:\ProgramData plus exactement C:\ProgramData\Microsoft\Windows\ et C:\Users\Public

Ce dossier **ProgramData** contient tous les liens pour compatibilité antérieure

```
Répertoire de C:\ProgramData

14/07/2009  05:53    <JUNCTION>      Application Data [C:\ProgramData]
18/02/2010  09:25    <JUNCTION>      Bureau [C:\Users\Public\Desktop]
14/07/2009  05:53    <JUNCTION>      Desktop [C:\Users\Public\Desktop]
14/07/2009  05:53    <JUNCTION>      Documents [C:\Users\Public\Documents]
18/02/2010  09:25    <JUNCTION>      Favoris [C:\Users\Public\Favorites]
14/07/2009  05:53    <JUNCTION>      Favorites [C:\Users\Public\Favorites]
18/02/2010  09:25    <JUNCTION>      Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010  09:25    <JUNCTION>      Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009  05:53    <JUNCTION>      Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009  05:53    <JUNCTION>      Templates [C:\ProgramData\Microsoft\Windows\Templates]
```

Et on voit bien que la nouvelle structure de **All-Users** est donc découpée en 2 sections => **ProgramData** & **Users\Public**

1° partie : stockée en **ProgramData\Microsoft\Windows**

```
18/02/2010  09:25    <JUNCTION>      Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010  09:25    <JUNCTION>      Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009  05:53    <JUNCTION>      Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009  05:53    <JUNCTION>      Templates [C:\ProgramData\Microsoft\Windows\Templates]
```

- pour modifier le menu démarrer il faut aller en **c:\ProgramData\Microsoft\Windows\Start Menu**
- pour donner une modèle il faut aller en **c:\ProgramData\Microsoft\Windows\Templates**

2° partie : stockée en **Users\Public**

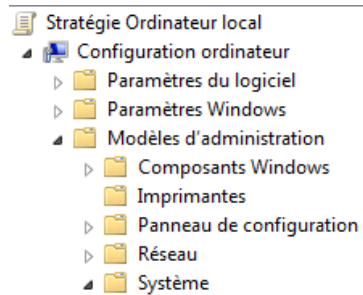
```
18/02/2010  09:25    <JUNCTION>      Bureau [C:\Users\Public\Desktop]
14/07/2009  05:53    <JUNCTION>      Desktop [C:\Users\Public\Desktop]
14/07/2009  05:53    <JUNCTION>      Documents [C:\Users\Public\Documents]
18/02/2010  09:25    <JUNCTION>      Favoris [C:\Users\Public\Favorites]
14/07/2009  05:53    <JUNCTION>      Favorites [C:\Users\Public\Favorites]
```

- pour modifier le Bureau il faut aller en **c:\Users\Public\Desktop**
- pour poser un fichier dans le dossier mes documents il faut aller en **c:\Users\Public\Documents**
- pour poser des favoris de navigation il faut aller en **c:\Users\Public\Favorites**

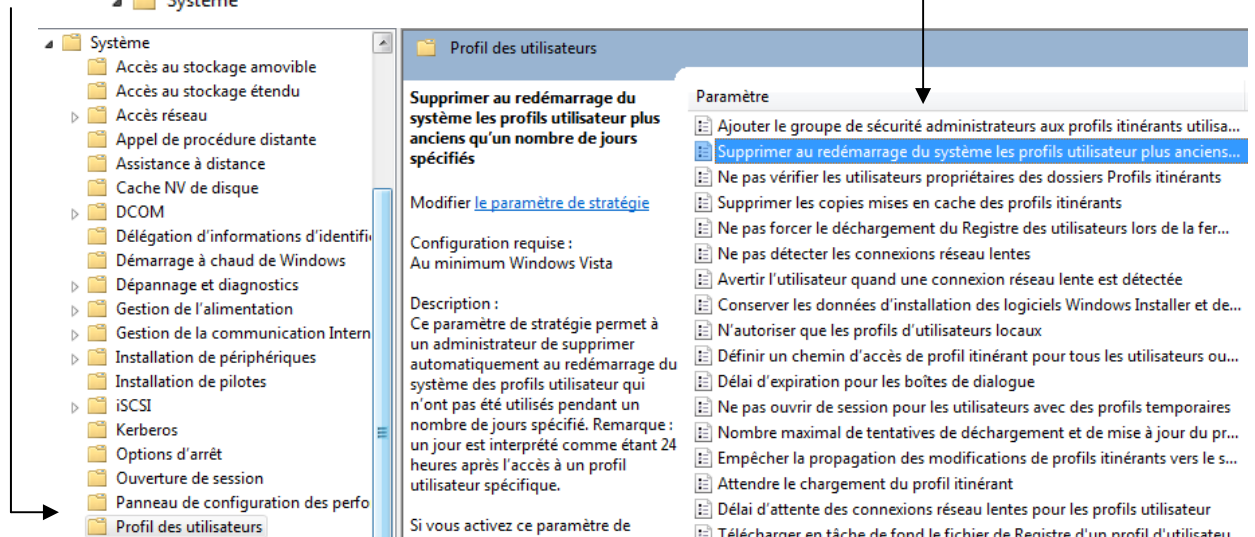
Supprimer tous les profils locaux Seven:

Il faut passer par une GPO, ou bien **Gpedit.msc**

Configuration ordinateur \ modèles d'administration\ Système



Puis **Profil des Utilisateurs \ Supprimer au redémarrage...**



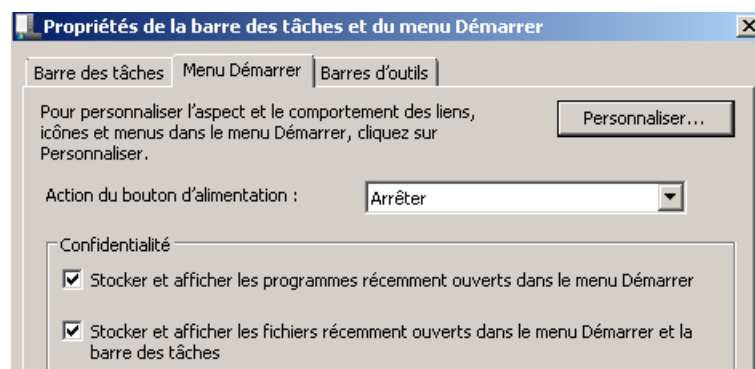
INTERFACE SEVEN – XP/2000

Retrouver l'interface XP 2000:

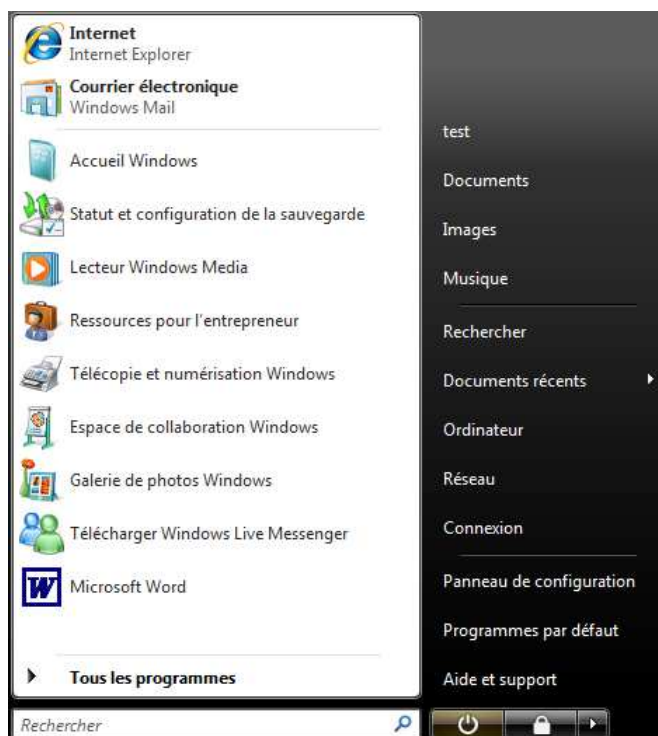
Pour des raisons diverses (habitudes, économie et surtout organisation) on peut vouloir retrouver sous **SEVEN** une interface plus style windows 2000 XP.

Menu Démarrer (modification organisationnelle):

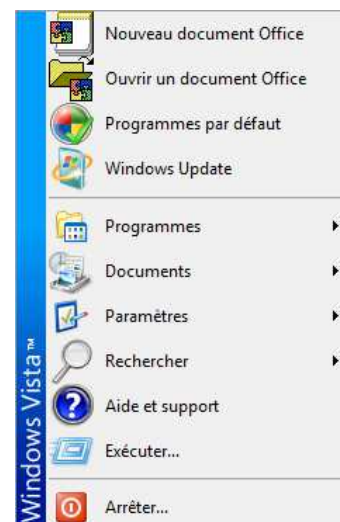
Dans les **propriétés** de la barre des tâches, onglet **Menu Démarrer**



Dans **Personnaliser...** il faut faire ses choix



Affichage **SEVEN** par défaut



Affichage **classique**

Panneau de configuration (modification organisationnelle):

On demande dans **Panneau de configuration**, pour avoir accès à la totalité des options possible, il faut en haut à gauche demander l'affichage icones (et non pas le mode Catégorie)

Affichage **SEVEN** par catégories

Ajuster les paramètres de l'ordinateur

Afficher par : Catégorie ▼



Affichage **SEVEN** par icones

Ajuster les paramètres de l'ordinateur

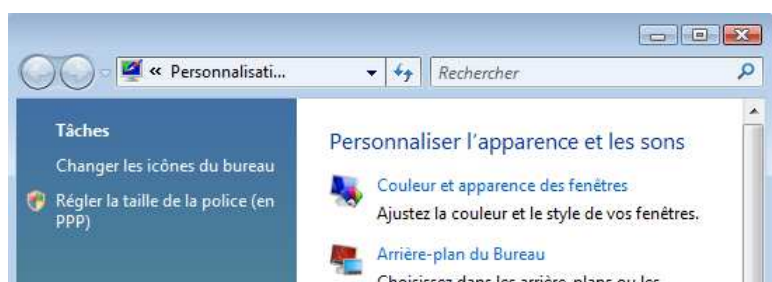
Afficher par : Grandes icônes ▼



Aspect des fenêtres (modification esthétique):

On demande **Personnaliser** par clic droit du **Bureau**

Puis on choisit **Couleur et apparence des fenêtres**



L'explorateur Windows:

On lance l'explorateur via **Explorer** dans la barre des tâches ou via menu contextuel de l'icône démarrage SEVEN (ou via les accessoires...)



Pour ouvrir un dossier ou un lecteur spécifique

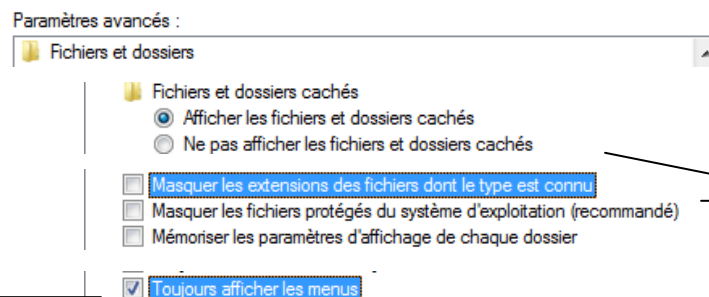
In, (nouvelle fenêtre) et **Ie**, (afficher un dossier) : **c:\data**



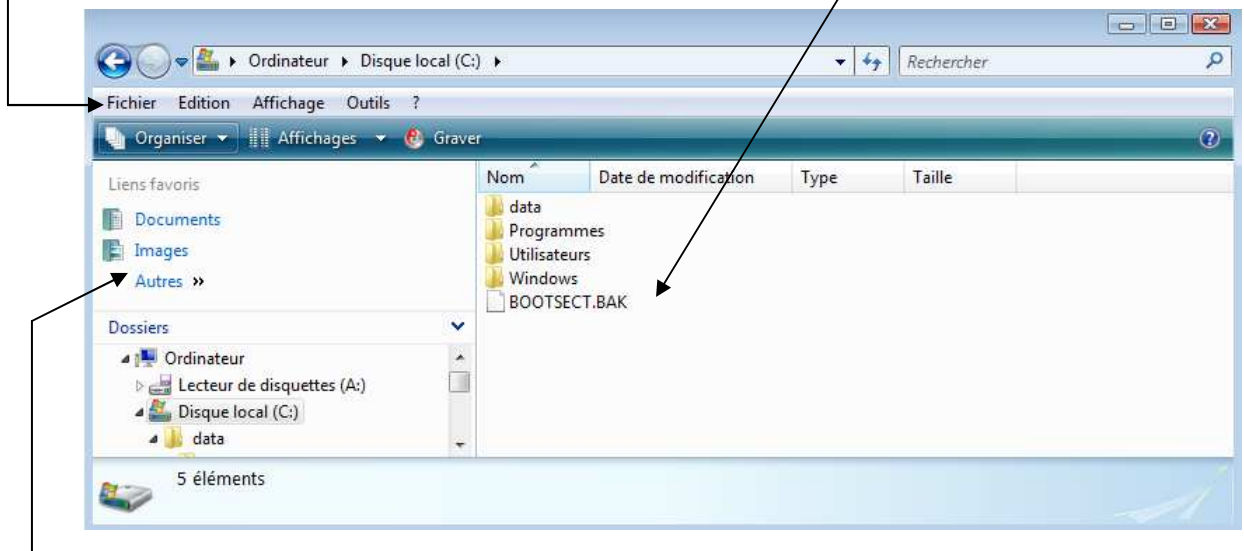
/root, (pour que cela soit vu en tant que racine)



Par rapport à l'aspect par défaut de l'explorateur windows on peut modifier cela via **Organiser / Option des Dossiers et de Recherche**

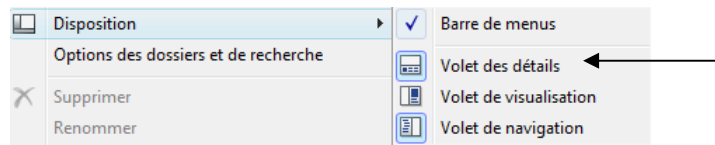


Pour retrouver notamment



La place perdue peut être récupérée via

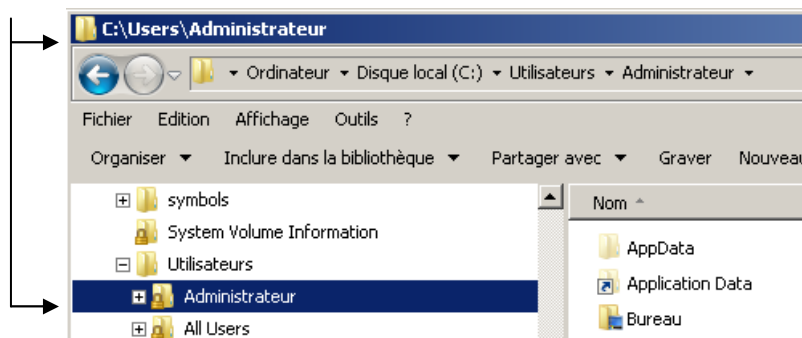
- Réduction de la zone des liens favoris
- La suppression du volet des détails via **Organiser**



Et enfin un dernier réglage peut s'avérer pratique :

- Fichiers et dossiers
- ☒ Afficher l'icône des fichiers sur les miniatures
 - ☒ Afficher la légende des dossiers et des éléments du Bureau
 - ☒ Afficher le chemin complet dans la barre de titre (thème Classique uniquement)
 - ☒ Afficher les dossiers et les fichiers NTFS chiffrés ou compressés en couleur

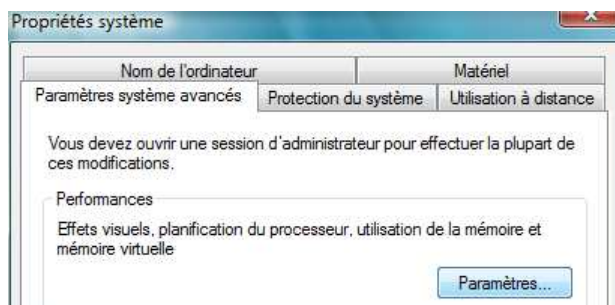
Permettant



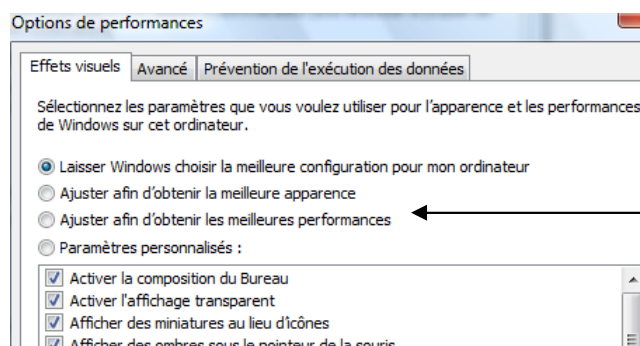
AERO – PERFORMANCES SEVEN

Interface Aero:

Les réglages AERO sont disponibles dans les propriétés ordinateur, dans **Paramètres systèmes avancés - Performances**



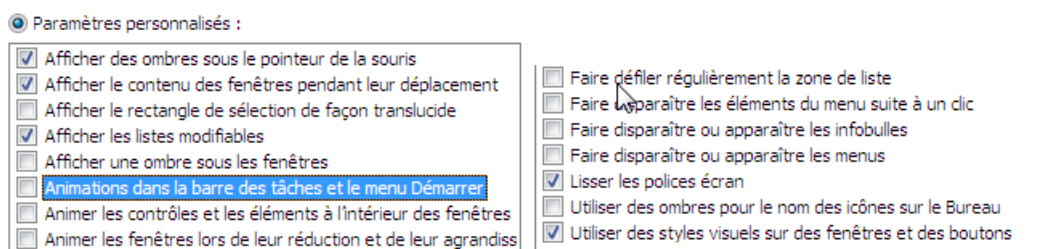
donnant



Pour Désactiver AERO on demande d'obtenir les meilleures performances

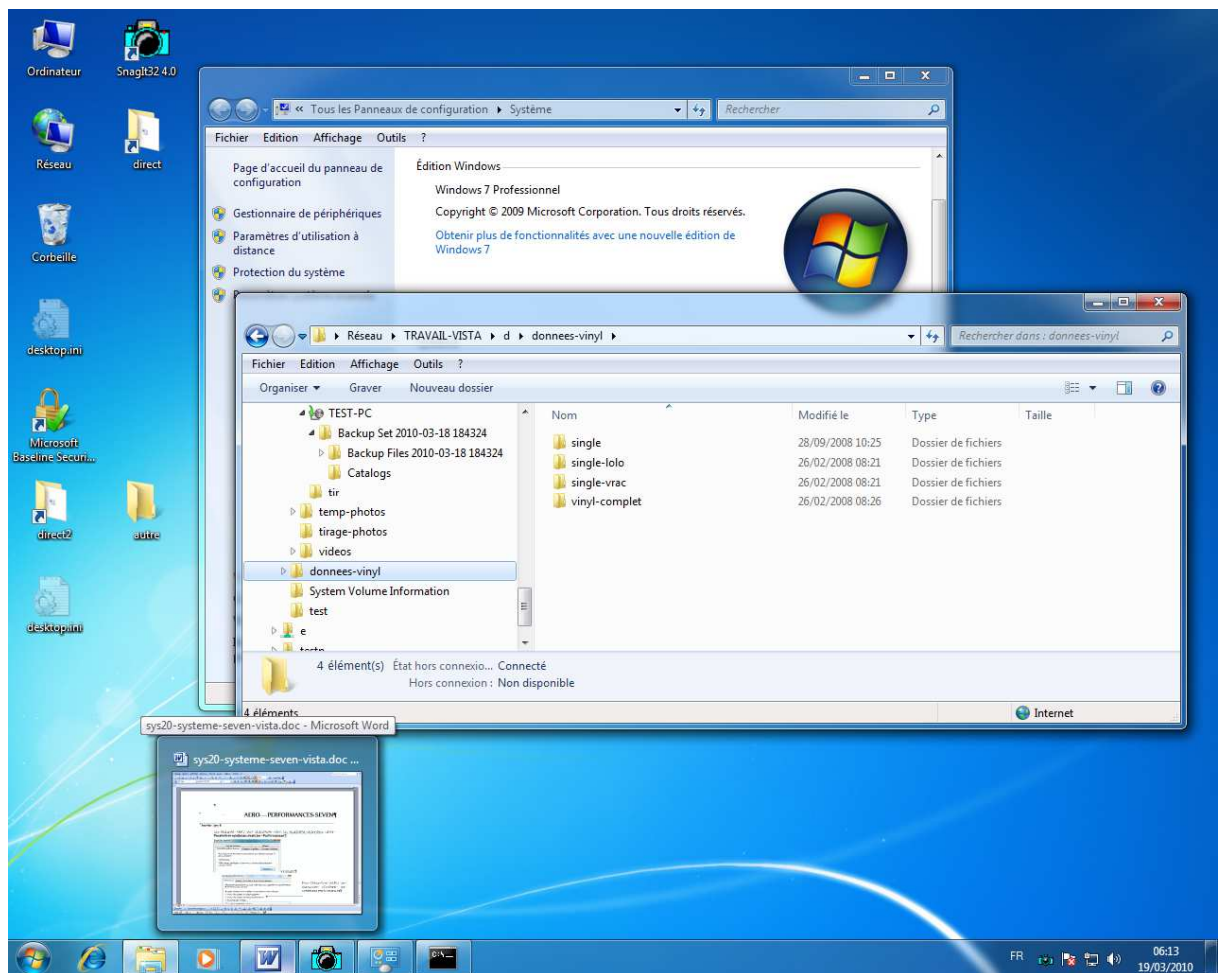
Avec Prévisualisation des écrans correspondants dans programmes en cours dans la barre des tâches, effet 3D à gogo...

Les réglages ci-dessous peuvent être un bon compromis



NB : à noter que dans la commande **ALT+TAB** pour passer d'une application à l'autre désormais le bureau fait partie des programmes sélectionnables...

NB : pour mettre 2 fenêtres cotes-à cotes, on sélectionne les deux boutons dans la barre des tâches (avec CTRL) puis via clic-droit **Afficher les fenêtres côte à côte**



Note Seven:

Dans les **propriétés** de **Ordinateur**

Informations système générales

Édition Windows

Windows 7 Professionnel
Copyright © 2009 Microsoft Corporation. Tous droits réservés.
Obtenir plus de fonctionnalités avec une nouvelle édition de Windows 7



Système

Évaluation :

5,4

Indice de performance Windows

Processeur : Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz 2.67 GHz
Mémoire installée (RAM) : 2,00 Go
Type du système : Système d'exploitation 32 bits

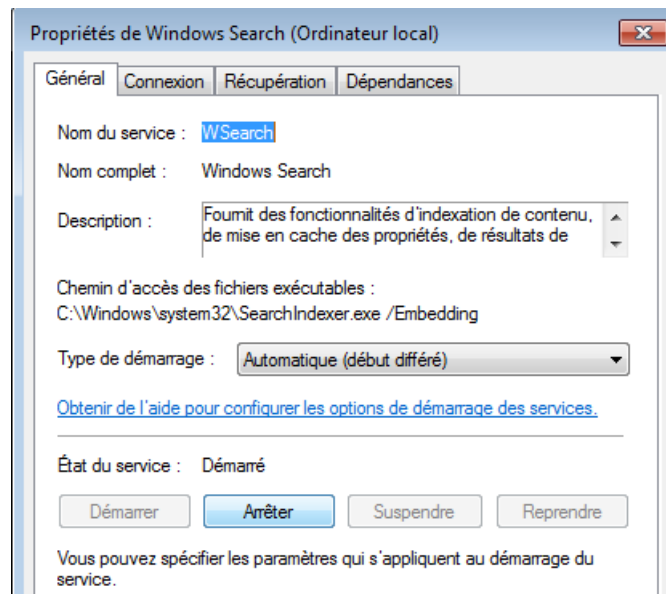
Composant	Ce qui est évalué	Sous-indice	Indice de base
Processeur :	Calculs par seconde	7,2	 Déterminé par le sous-indice le plus bas
Mémoire vive :	Opérations mémoire par seconde	5,5	
Graphiques :	Performances du Bureau pour Windows Aero	5,4	
Graphiques de jeu :	Performances graphiques pour jeux et applications professionnelles 3D	6,4	
Disque dur principal :	Taux de transfert des données sur le disque	5,7	

Compromis Performances :

Certaines fonctionnalités de SEVEN sont « gourmandes », et par conséquent peuvent être désactivées si besoin, comme l'indexation automatique :

Il faut arrêter le service : **Windows Search**

Nom	Description	État	Type de démarrage	Ouvrir une session en tant que
Windows Search	Fournit des ...	Dém...	Automatique (débu...	Système local

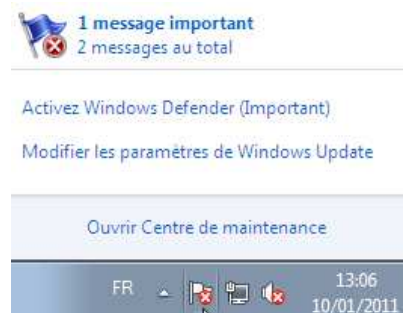


Messages du Centre de Maintenance :

Le "centre de maintenance" de SEVEN peut s'avérer parfois un peu... verbeux

On peut gérer les messages via

Panneau de configuration / Centre de Maintenance / Modifier les paramètres...



Activer ou désactiver les messages

Pour chaque élément sélectionné, Windows va régulièrement rechercher s'il y a des problèmes et vous envoyer un message s'il en trouve. [Comment le Centre de maintenance vérifie-t-il s'il y a des problèmes ?](#)

Messages de sécurité

- | | |
|---|---|
| ☒ Windows Update | ☒ Protection contre les logiciels espions |
| ☒ Paramètres de sécurité Internet | ☒ Contrôle de compte d'utilisateur |
| ☒ Pare-feu du réseau | ☒ Protection antivirus |

Messages de maintenance

- | | |
|--|---|
| ☒ Sauvegarde Windows | ☒ Rechercher les mises à jour |
| ☒ Dépannage de Windows | |

Paramètres associés

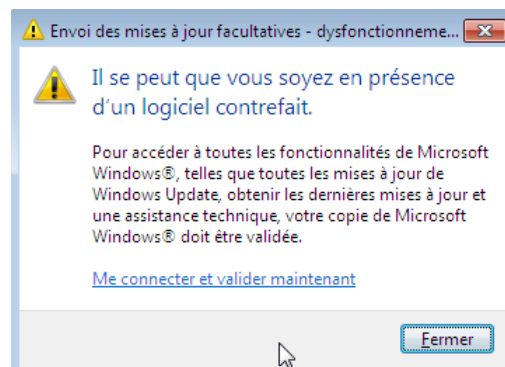
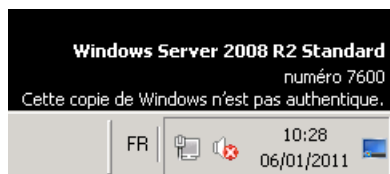
[Paramètres du programme d'amélioration de l'expérience utilisateur](#)

SLMGR – ACTIVATION LICENCE

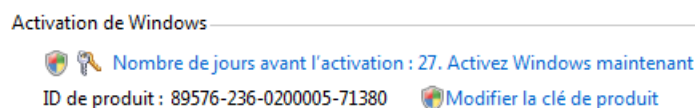
Installer SEVEN sans Clé:

Pour des raisons diverses (habitudes, économie et surtout organisation) on peut vouloir installer **SEVEN** sans saisir de clé

30 jours sont ensuite disponibles sans avoir à rentrer une clé... puis →



Cela peut se vérifier dans les informations système, en bas dans une section Activation de Windows on trouve :



N.B: à part des messages, le poste à un fonctionnement normal !

Réactiver Seven - utilitaire slmgr:

Un outils **slmgr** en ligne de commande est fournit permettant d'avoir des informations plus précises sur la gestion de la licence et de l'activation

Outils de gestion des licences logicielles Windows
Utilisation : slmgr.vbs [NomOrdinateur [Utilisateur MotDePasse] [<Option>]
NomOrdinateur : Nom de l'ordinateur distant (ordinateur local par défaut)
Utilisateur : Compte bénéficiant des privilèges nécessaires sur l'ordinateur distant
MotDePasse : Mot de passe du compte précédent

Options globales :

- ipk <Clé produit>
Installer la clé de produit (remplace la clé existante)
- upk
Désinstaller la clé de produit
- ato
Activation de Windows
- dli [ID d'activation] All
Afficher les informations de la licence (par défaut : licence active)
- dlv [ID d'activation] All
Afficher les informations détaillées de la licence (par défaut : licence active)
- xpr
Date d'expiration de l'état actuel de la licence

Options avancées :

- cpky
Effacer la clé de produit du Registre (évite sa divulgation en cas d'attaque)
- ilc <Fichier de licence>
Installer la licence
- rilc
Réinstaller les fichiers de licence système
- rearm
Réinitialiser l'état de la licence de l'ordinateur

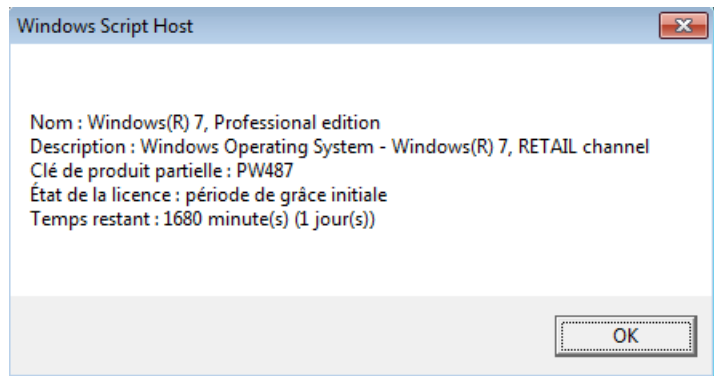
Licences en volume : options du client KMS (Key Management Service) :

- skms <Nom[:Port] | :Port>
Définir le nom et/ou le port de l'ordinateur KMS utilisé par cet ordinateur
- ckms
Effacer le nom de l'ordinateur KMS utilisé (définit le port à sa valeur par défaut)

en tant qu'administrateur, il faut en ligne de commande taper

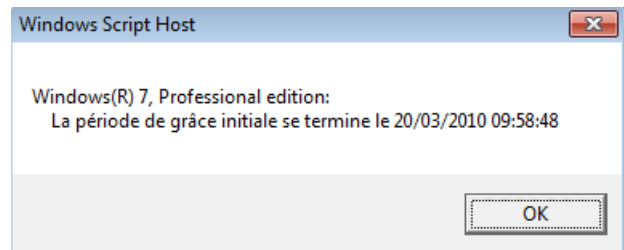
slmgr -dli

donnant par exemple



30 jours sont ensuite disponibles sans avoir à rentrer une clé...et on peut avoir en clair le calcul de « la période de grâce » par

slmgr -xpr

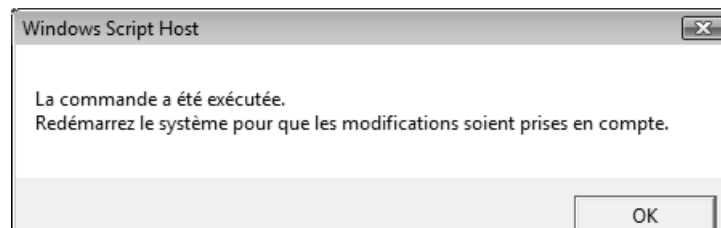


Réactivation période de grâce

il est possible de saisir une instruction en ligne de commande permettant de renouveler ce crédit de 30 jours, et ce un maximum de trois fois ...:

```
C:\Users\Administrateur>slmgr -rearm_
```

après un petit délais on obtient



Ce petit jeu peut être effectué 3 fois, suite à quoi cela ne marche plus...

Dans la base de registre en

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\SL

	Nom	Type	Données
SL	(par défaut)	REG_SZ	(valeur non définie)
SPP	SkipRearm	REG_DWORD	0x00000000 (0) ←
Superfetch	VLActivationInterval	REG_DWORD	0x00000078 (120)
Svchost	VLRenewalInterval	REG_DWORD	0x00002760 (10080)
SystemRestore	WAUSetupLocation	REG_SZ	
Time Zones			
Tracina			

la valeur **SkipRearm** doit valoir 1 pour autoriser le réarmement

Transfert – Re-saisie licence:

slmgr en ligne de commande permet pas mal de manipulations, parmi lesquelles on peut trouver intéressant de désinstaller une clé et la re-installer sur un autre poste.

Pour récupérer la situation actuelle au niveau de la licence

slmgr /dlv

on note l'**ID d'activation**



pour récupérer cette licence et « désactiver » notre poste on tape

slmgr /upk e838d943-63ed-4a0b-9fb1-47152908acc9

pour ré-installer une licence (ne pas confondre une clé d'activation et un n° de licence) sur notre poste on tape

slmgr /ipk 7KBVM-9NWFB-QJVXT-VHV9C-7CBQP-XZK28

puis on l'active via

slmgr /ato

Saisie licence slui 3:

Slui 3 en ligne de commande permet juste de saisir une licence

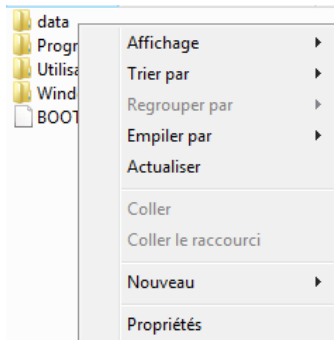


INCLASSABLES DE SEVEN

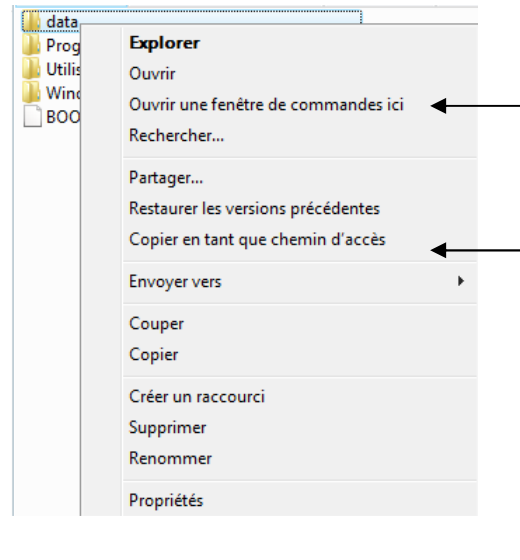
Menu étendus (invite de commande):

On peut avoir des menus "contextuels" complets à l'aide de la touche MAJ

Menu contextuel



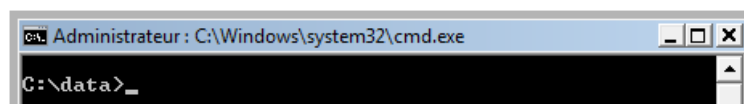
MAJ + Menu contextuel



2 commandes pratiques apparaissent

Ouvrir une fenêtre de commande ici

Permettant de positionner le path local d'une invite de commande directement dans le dossier choisi



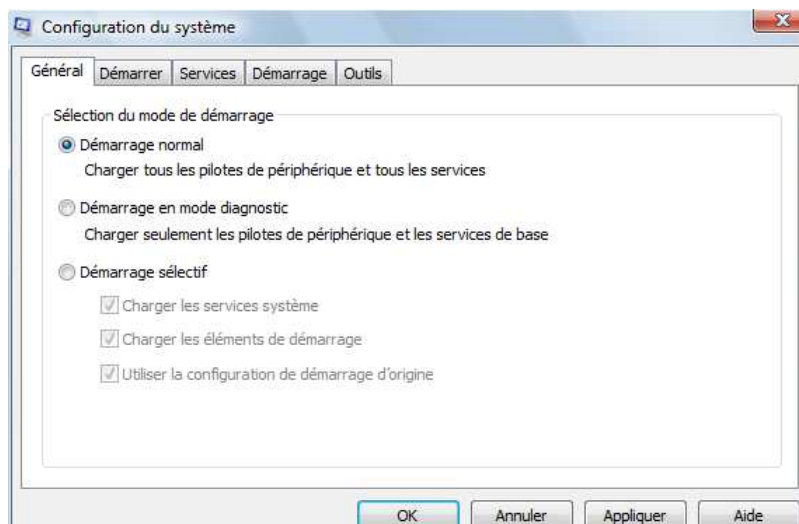
Copier en tant que chemin d'accès

Permettant de récupérer la chaîne entre guillemet du chemin

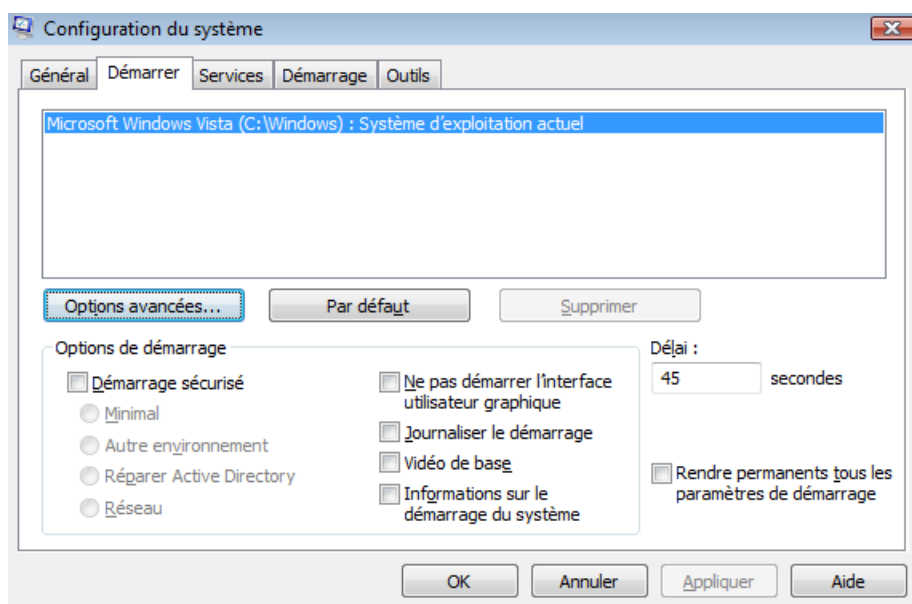
"C:\data"

Options démarrage msconfig.exe :

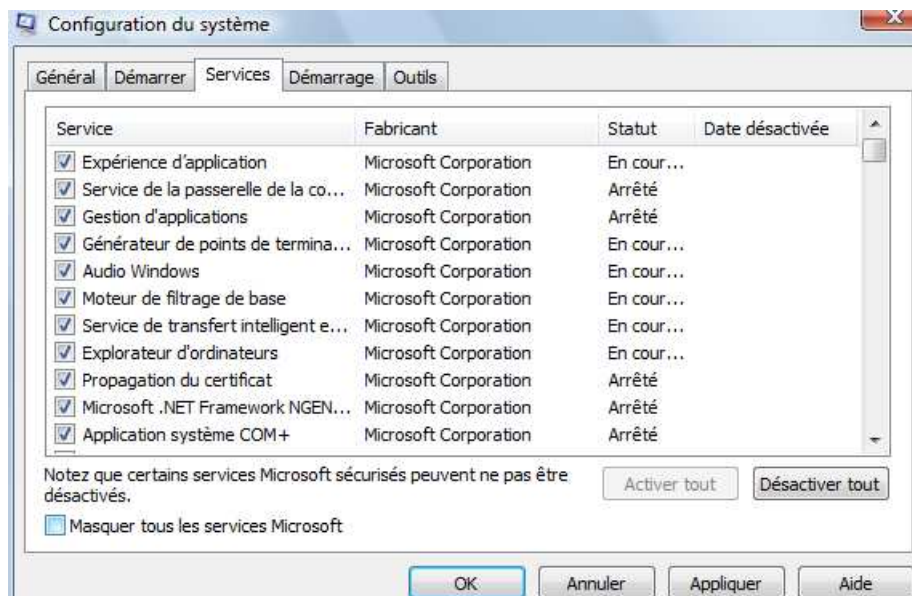
Disposant de 5 onglets fort pratiques **Général**



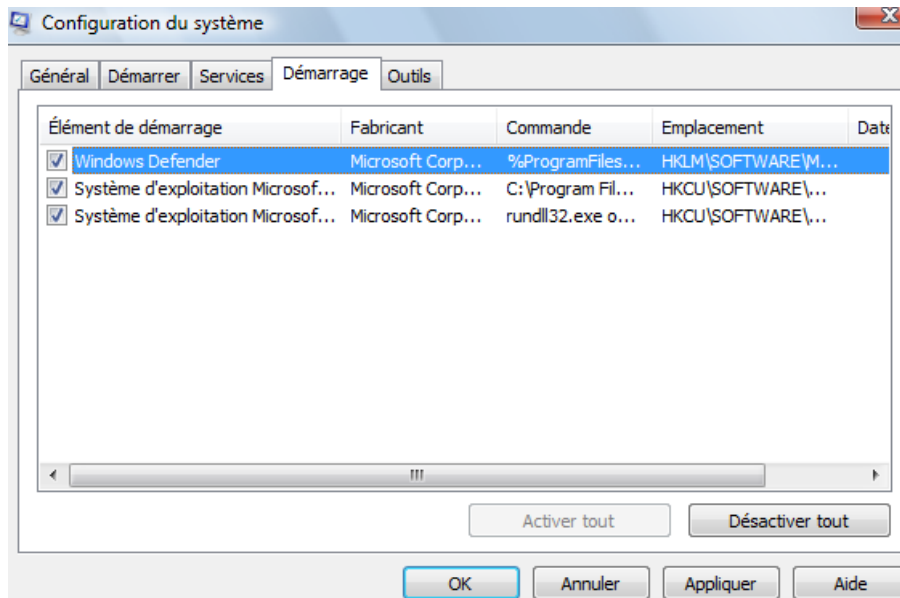
Démarrer



Services

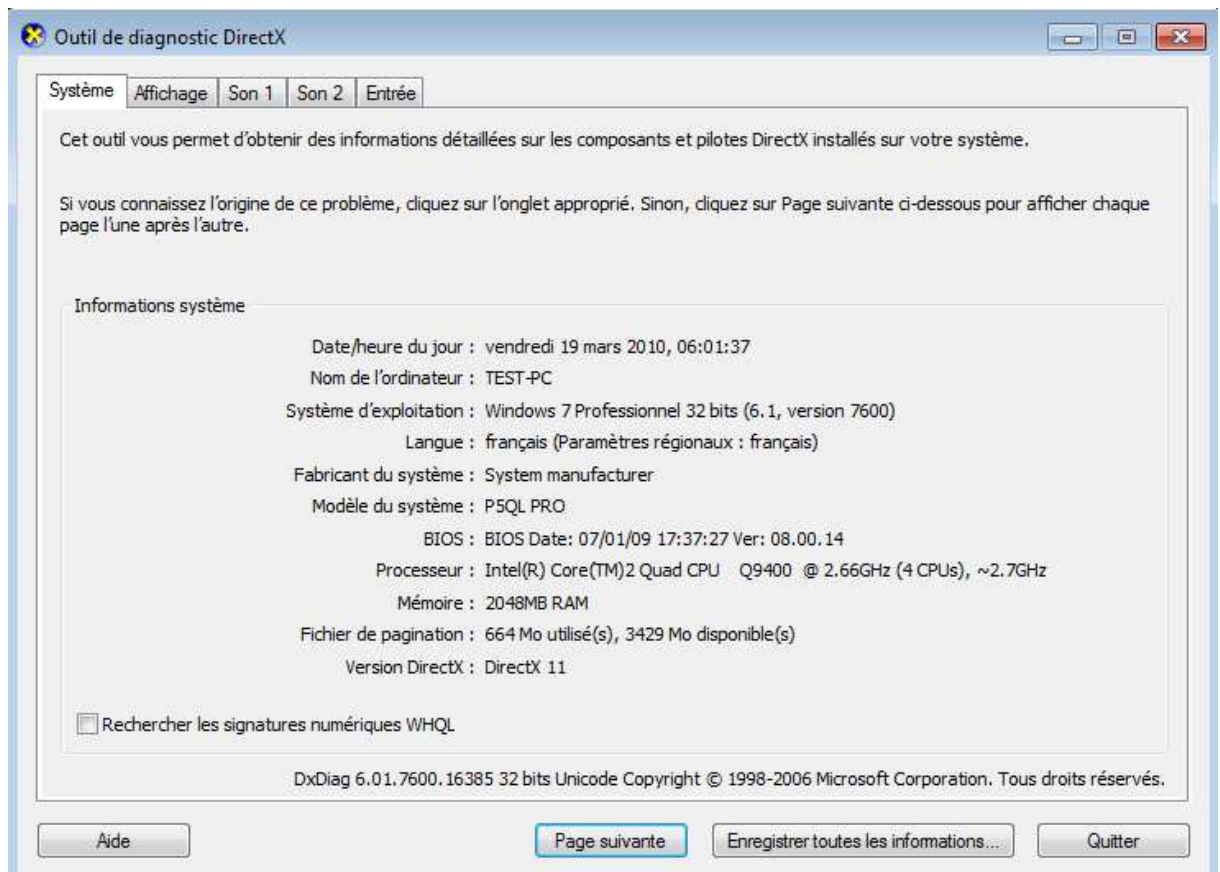


Démarrage



Outils dxdiag:

En ligne de commande **dxdiag**



Outils msinfo32:

En ligne de commande **msinfo32**

Informations système		
Fichier Edition Affichage ?		
Résumé système	Élément	Valeur
- Ressources matérielles - Composants - Environnement logiciel	Nom du système d'exploitation	Microsoft Windows 7 Professionnel
	Versión	6.1.7600 Numéro 7600
	Autre description du système d...	Non disponible
	Fabricant du système d'exploit...	Microsoft Corporation
	Ordinateur	TEST-PC
	Fabricant	System manufacturer
	Modèle	P5QL PRO
	Type	PC à base X86
	Processeur	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz, 2670 MHz, 4 cœur(s), 4 p...
	Versión du BIOS/Date	American Megatrends Inc. 1004, 01/07/2009
	Versión SMBIOS	2.5
	Répertoire Windows	C:\Windows
	Répertoire système	C:\Windows\system32
	Périphérique de démarrage	\Device\HarddiskVolume1
	Option régionale	France
	Couche d'abstraction matérielle	Versión = "6.1.7600.16385"
	Utilisateur	test-PC\Administrateur
	Fuseaux horaires	Paris, Madrid
	Mémoire physique (RAM) instal...	2,00 Go
	Mémoire physique totale	2,00 Go
	Mémoire physique disponible	1,41 Go
	Mémoire virtuelle totale	4,00 Go
	Mémoire virtuelle disponible	3,32 Go
	Espace pour le fichier d'échange	2,00 Go
	Fichier d'échange	C:\pagefile.sys

Outils shutdown:

En ligne de commande **shutdown**

Shutdown /s /t 30

arrêt dans 30 secondes

Shutdown /ls /t 0

fermeture de session immédiate

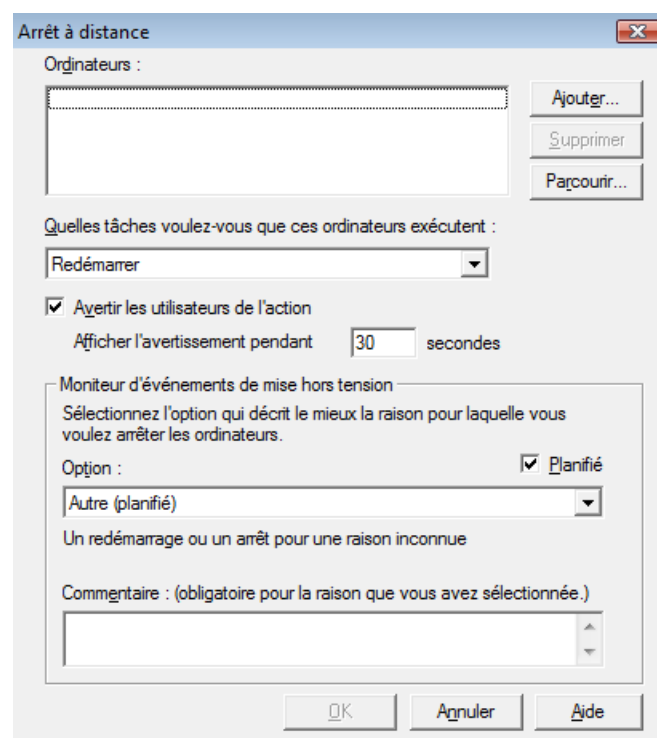
Shutdown /m \\\nomposte /t 0

arrêt du pc \\\nomposte « immédiat »

N.B : Les 2 options **-r -f** semblent obligatoires avec l'option **-m**

Une interface graphique est également disponible

Shutdown /i

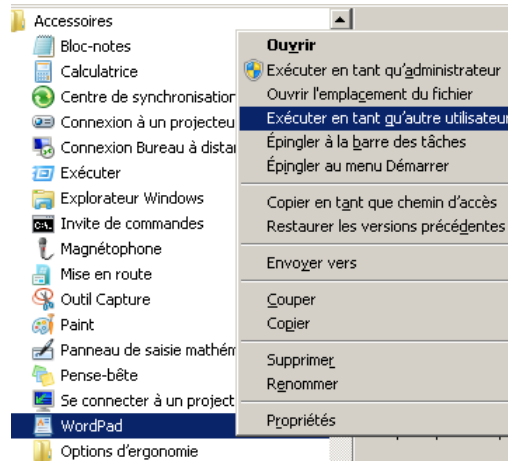


Whoami:

En ligne de commande **whoami** permet de connaître son login

```
C:\Users\Administrateur>whoami  
test-pc\administrateur
```

N.B: à ce propos on peut lancer une tâche avec un autre login (équivalent de RUNAS en ligne de commande) avec **Pointer + SHIFT + Clic DROIT**



CONSOLE MMC

Microsoft Management Console:

Dite plus couramment **MMC**, cette console d'administration n'est en fait qu'un coquille vide, ne faisant rien si ce n'est unifier et homogénéiser l'aspect des différents outils de gestion que l'on doit employer.

La MMC sert donc à fournir une interface commune pour tous les outils d'administrations sous Windows

Chaque MMC peut recevoir (ou on peut lui ôter) des outils d'administrations via ce que l'on appelle des « **snap-in** » ou encore des « **composant logiciels enfichables** ». Il existe un **snap-in** pour chaque outils de gestion.

Les consoles contiennent de manières générale un ou plusieurs snap-in et sont enregistrées dans des fichiers dotés de l'extension **.msc** stockés par défaut dans le dossier Outils d'Administration **Winnt\System32**

S'il est évident qu'il existe déjà un certain nombre de consoles prédéfinies, il est tout aussi évident que l'on peut se créer ses propres consoles personnalisées

Si on a besoin que d'une **partie** seulement d'une console (par exemple le gestionnaire de disques), Il peut donc être **avantageux** de lancer **uniquement** la partie intéressante, en exécutant le fichier d'extension **.msc** associé

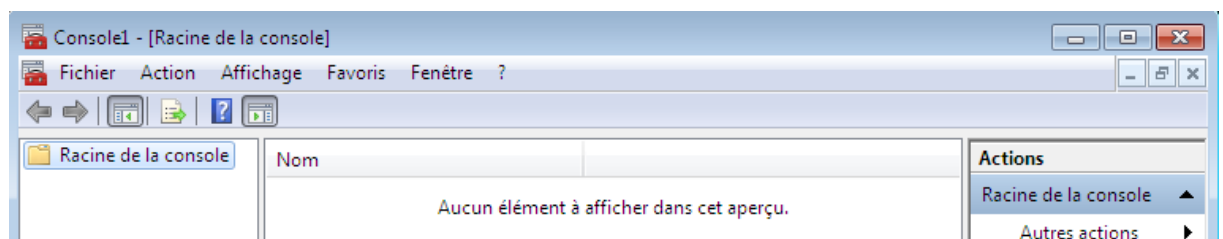
Fichier	Rôle
certmgr.msc	Certificats
ciadv.msc	Service d'indexation
devmgmt.msc	Gestionnaire de périphériques
dfrg.msc	Défragmenteur de disques
diskmgmt.msc	Gestion des disques
dnsmgmt.msc	Gestionnaire de DNS
eventvwr.msc	Observateur d'événements
faxserv.msc	Gestion du service de télécopie
fsmgmt.msc	Dossiers partagés
gpedit.msc	Stratégie de groupe
ias.msc	Service d'authentification Internet
lusrmgr.msc	Utilisateurs et groupes locaux
ntmsmgr.msc	Stockage amovible
ntmsoprq.msc	Demandes de l'opérateur de stockage amovible
perfmon.msc	Analyseur de performances
secpol.msc	Paramètres de sécurité locaux
services.msc	Services
wimgmt.msc	Infrastructure de gestion Windows (WMI)
comexp.msc	Service de composants
iis.msc	Services Internet
msinfo32.msc	Informations système

Créer une console personnalisée:

Il faut demander le menu **Démarrer / Exécuter**

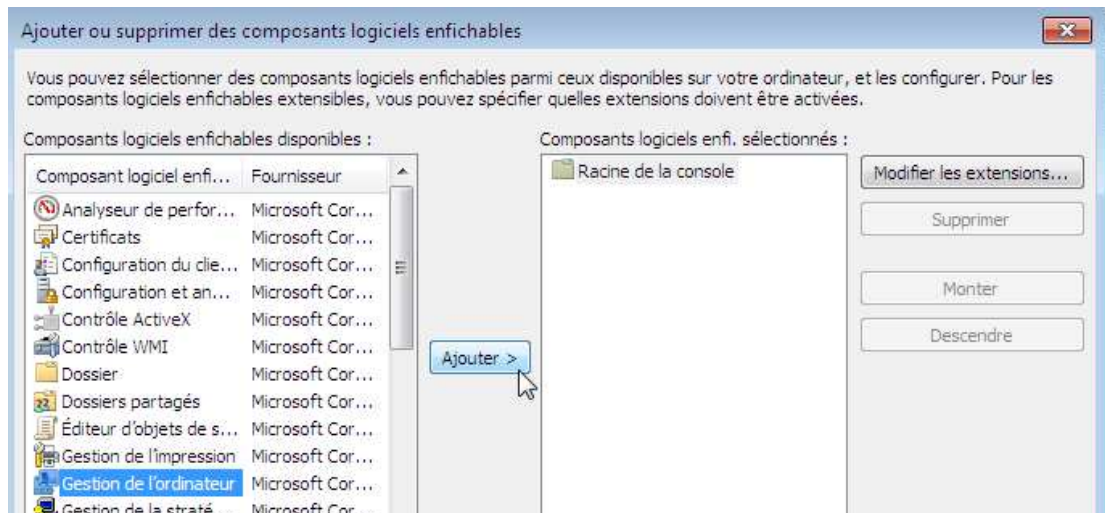
Et taper **mmc**

On obtient une console vide prête à être personnalisée

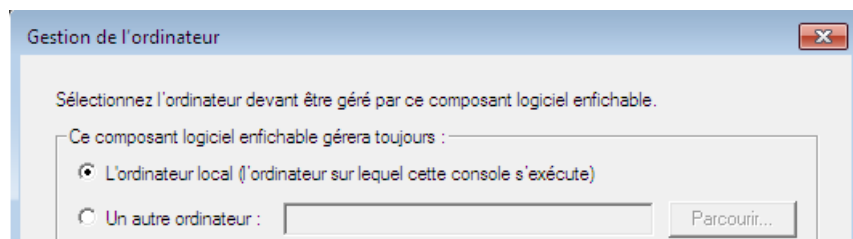


En étant placé à la racine de la console, demander dans le menu

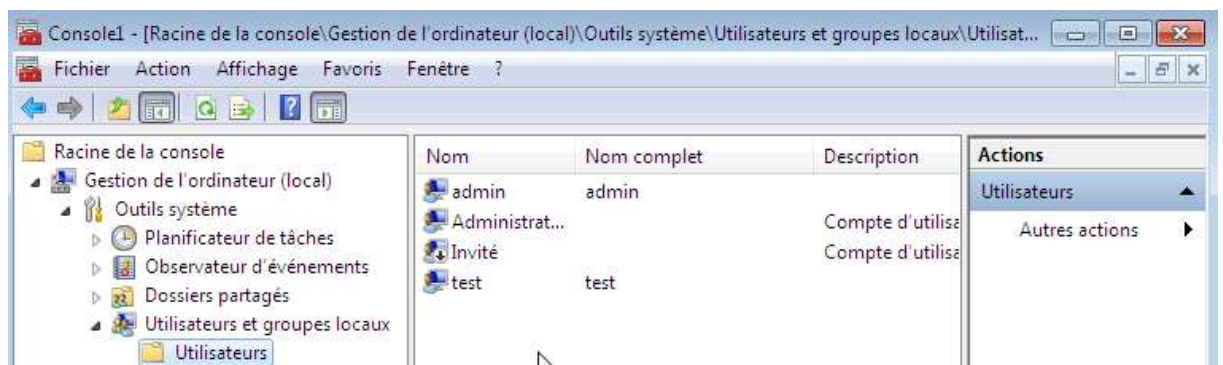
Fichier / Ajouter - Supprimer un composant logiciel enfichable



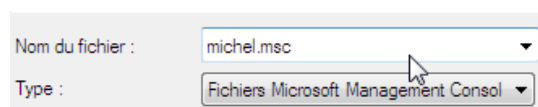
Dans la liste des snap-in choisir « **gestion de l'ordinateur** » (par exemple) et demander de gérer l'ordinateur local



Et l'on voit que notre console se personnalise !



Pour enregistrer cette console il faut demander le menu
Console / Enregistrer sous



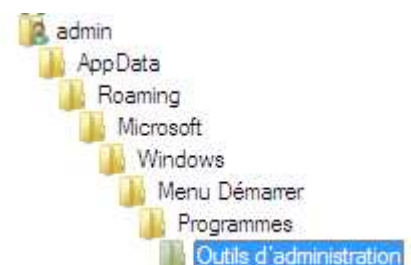
Et taper ici le nom de la console **mmc**, par exemple « **michel** »

Ce nom apparaîtra désormais dans le menu

Démarrer / Outils d'administration / michel...

Pour peu que l'on ait placé le fichier .msc dans le bon dossier...

N.B: on peut placer le fichier sur le bureau... ou ailleurs...



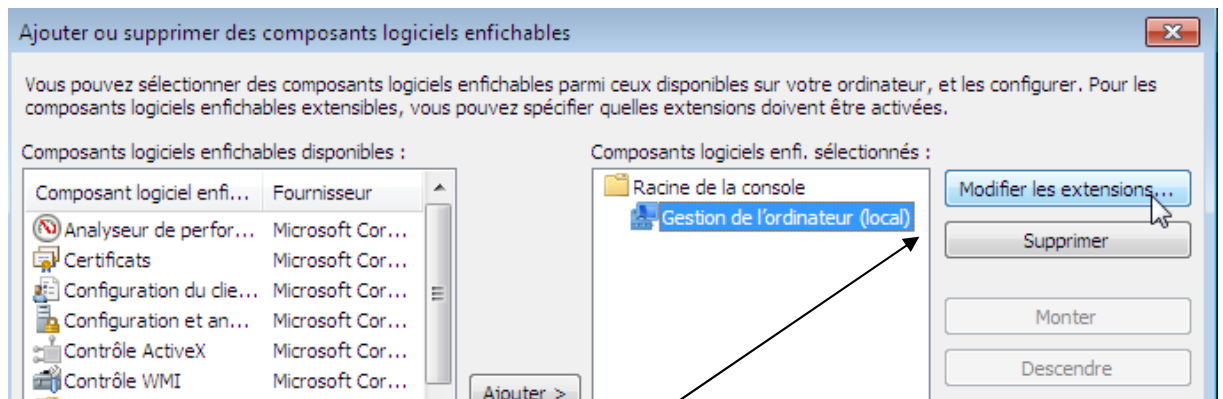
Limitier les fonctions d'un composant logiciel :

Lorsque l'on crée une console avec un composant, celui-ci peut donner accès à plein de fonctionnalités différentes. Si on veut ce composant, mais avec moins de fonctionnalités, (en quelque sorte on veut le « brider ») Il suffit alors de :

- désactiver certaines extensions de la console
- enregistrer la console en mode utilisateur...

Désactiver des extensions de la console :

Au moment d'inclure le composant **gestion de l'ordinateur**

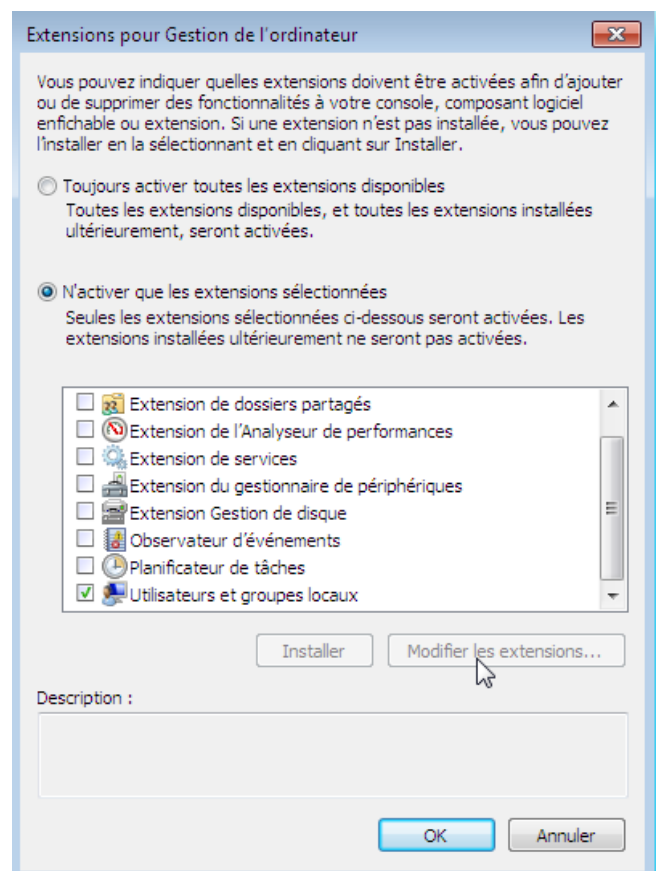


On demande **Modifier les extensions...**

pour obtenir alors

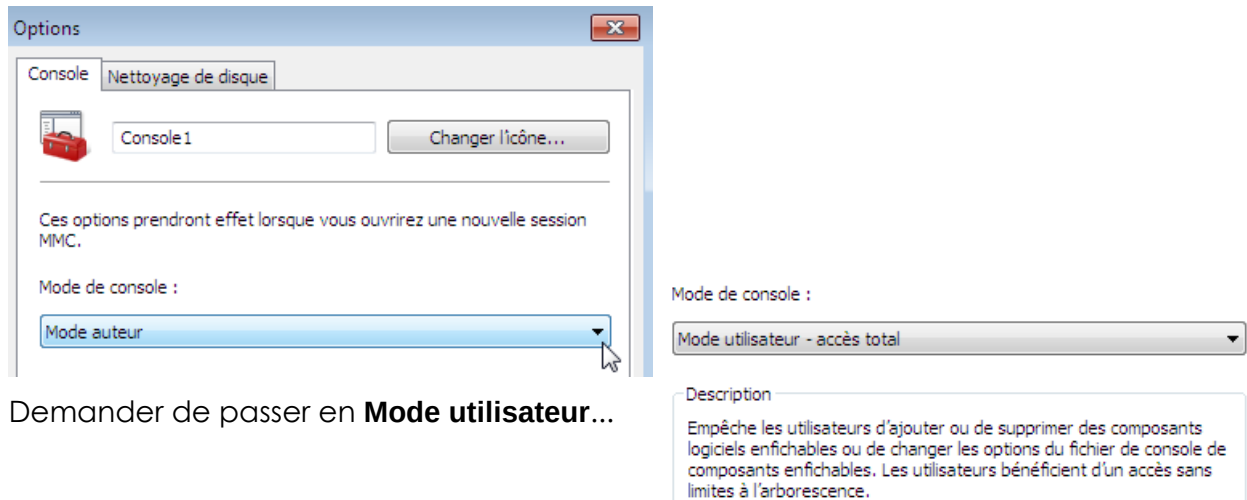
on demande de n'activer que les extensions sélectionnées

et ensuite on fait sa sélection...



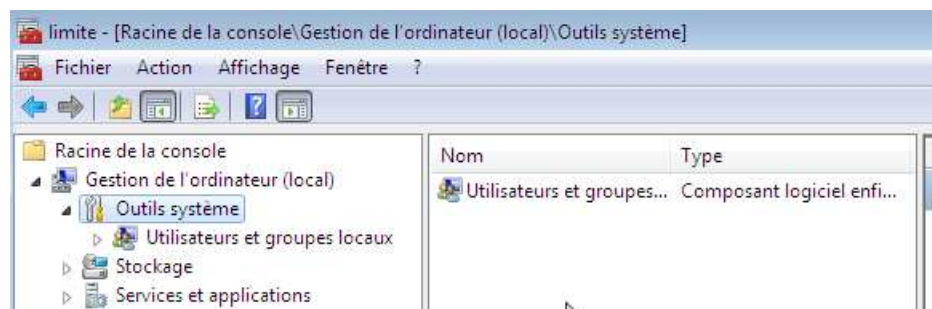
Enregistrer la console utilisateur :

Avant d'enregistrer la console, il faut dans le menu **Fichier / Option**



Demander de passer en **Mode utilisateur...**

Au prochain lancement, les composants enfichables de cette console ne sont plus modifiables...



ANNEXE : ECRAN BLEU

Les écrans bleu – erreur kernel de démarrage:

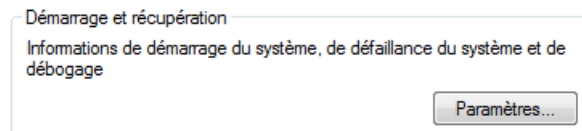
En général, ces écrans bleus ont deux causes principales, RAM et DD...

Il faut vérifier ces deux composants, (contact, perte et affaiblissement du signal, connectique mauvaise...)

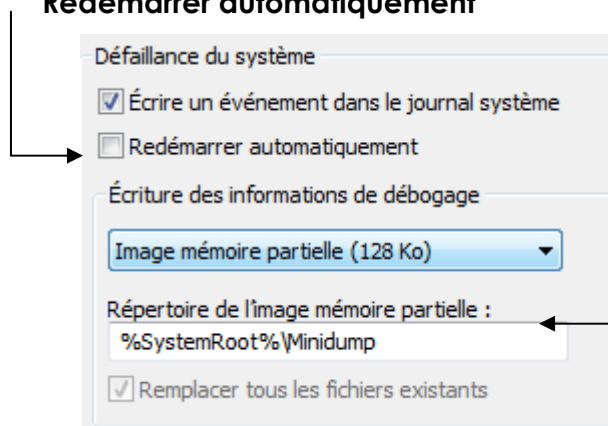
Les écrans bleu "aléatoires":

On peut aussi aller visualiser une information dans un fichier Mini-Dump...

Vérifier que dans les propriétés de **ordinateur**, on demande **Démarrage et récupération**



On peut pour se donner le temps de lire l'écran bleu en décochant **Redémarrer automatiquement**



Des fichiers **xxx.dmp** sont créés dans ce dossier...

Une fois paramétré, il ne reste plus qu'à attendre l'écran bleu.

Windbg" installation et paramétrage

System Requirements

The following are system requirements for the 32-bit version of Debugging Tools for Windows:

- 32-bit or 64-bit versions of Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, Windows XP, and Windows Server 2003; Windows 2000 and Windows NT 4.0.
- Microsoft Internet Explorer 5.0 or later.
- Approximately 25 MB of hard disk space.

See: [What's New for Debugging Tools for Windows](#)

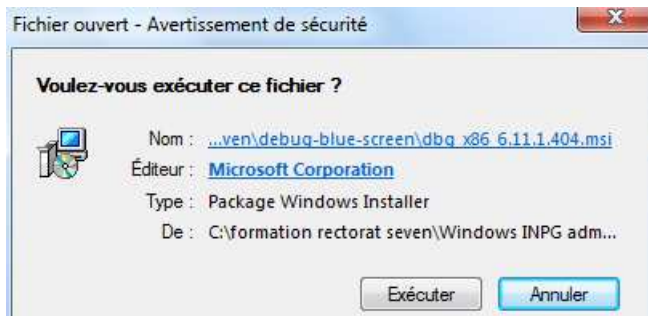
[↑ Top of page](#)

Download the Debugging Tools for Windows

Current Release version 6.11.1.404 - March 27, 2009

[Install 32-bit version 6.11.1.404 \[16.9 MB\]](#)

que l'on installe



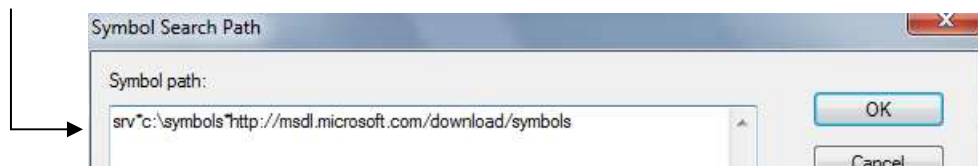
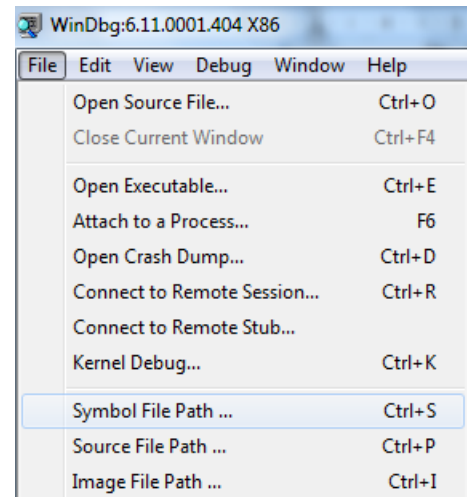
Une fois installé, il est nécessaire de paramétrer le chemin d'accès aux symboles qui permettent notamment de voir quelles sont les fonctions qui ont été appelée dans la pile, de voir les structures, etc avec leur nom d'origine. La plupart des fonctions du kernel commencent par **nt!**.

N.B: Les symboles sont disponibles en ligne...

Dans le menu **File / Symbol File Path...**

pour les télécharger en `c:\symbols`

srv*c:\symbols*http://msdl.microsoft.com/download/symbols



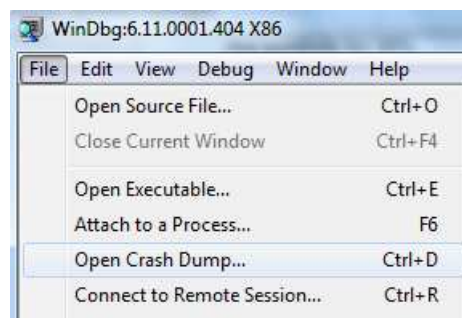
N.B: on peut aussi télécharger les symboles (puis les installer) voulus en



Fichier mini-dump

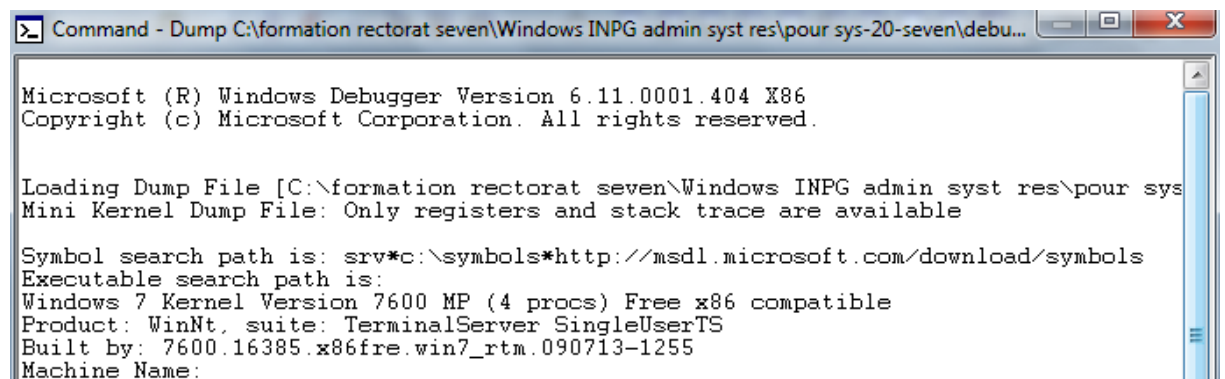
Un fichier xxxx.dmp se "lit" de la manière suivante...

File / Open Crash Dump...



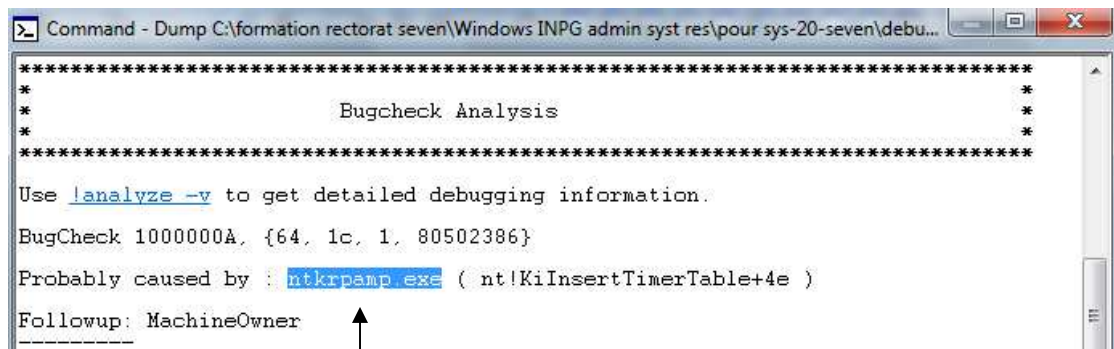
Et on indique le fichier xxx.dmp

On obtient sur un poste Seven



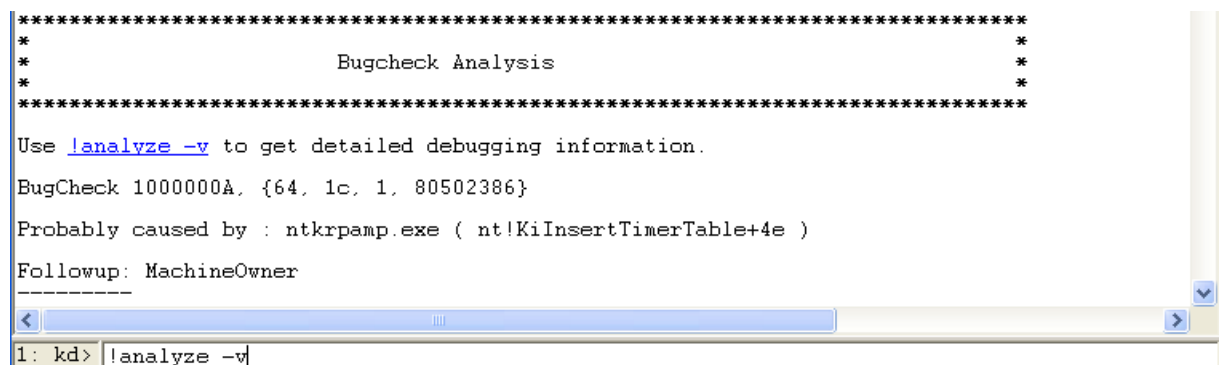
Rémonter une erreur

Première piste le nom du fichier qui cause l'erreur..

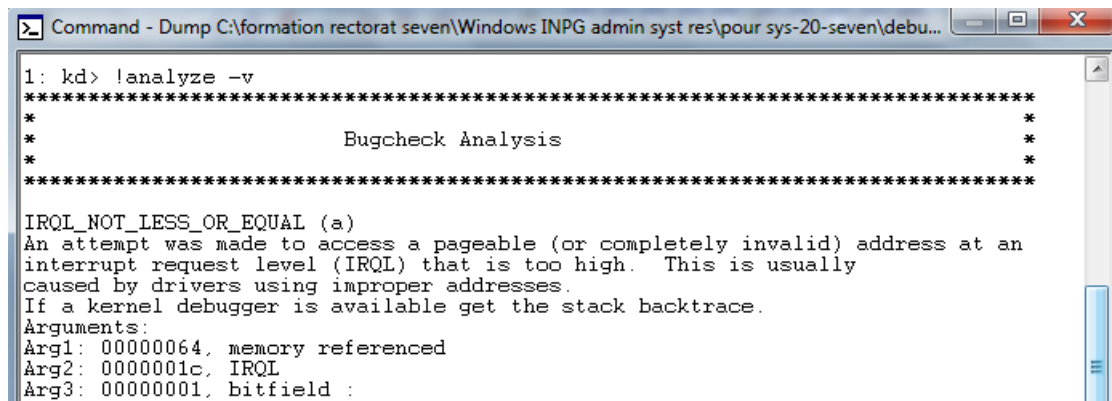


Si ce nom est trop générique, on peut alors avancer avec la commande

!analyze -v qui permet d'obtenir des informations complémentaires



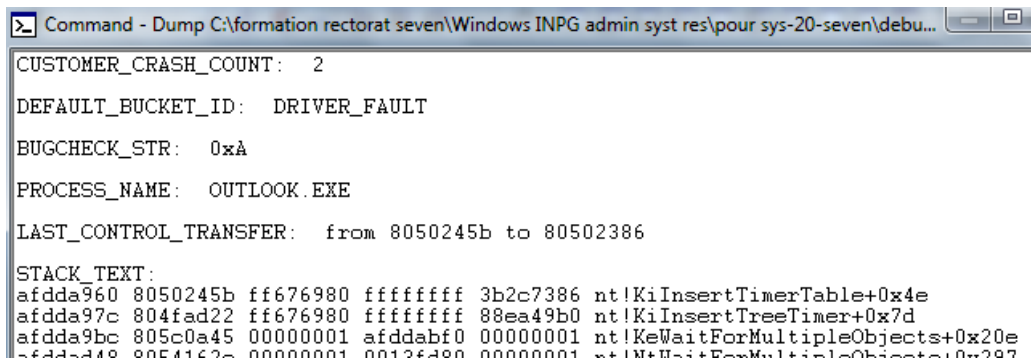
Donnant une indication...



```
1: kd> !analyze -v
*****
*                                     *
*                               Bugcheck Analysis                               *
*                                     *
*****

IRQL_NOT_LESS_OR_EQUAL (a)
An attempt was made to access a pageable (or completely invalid) address at an
interrupt request level (IRQL) that is too high. This is usually
caused by drivers using improper addresses.
If a kernel debugger is available get the stack backtrace.
Arguments:
Arg1: 00000064, memory referenced
Arg2: 0000001c, IRQL
Arg3: 00000001, bitfield :
```

Et plus loin



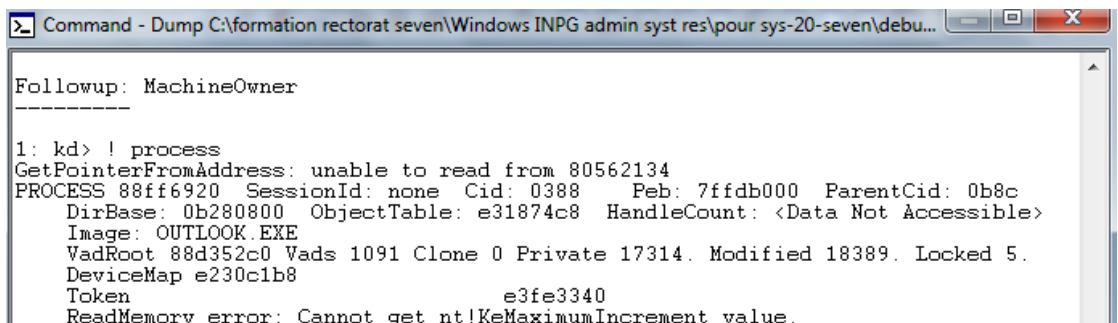
```
1: kd> !process 0 0
CUSTOMER_CRASH_COUNT: 2
DEFAULT_BUCKET_ID: DRIVER_FAULT
BUGCHECK_STR: 0xA
PROCESS_NAME: OUTLOOK.EXE
LAST_CONTROL_TRANSFER: from 8050245b to 80502386
STACK_TEXT:
afdda960 8050245b ff676980 ffffffff 3b2c7386 nt!KiInsertTimerTable+0x4e
afdda97c 804fad22 ff676980 ffffffff 88ea49b0 nt!KiInsertTreeTimer+0x7d
afdda9bc 805c0a45 00000001 afddabf0 00000001 nt!KeWaitForMultipleObjects+0x20e
afdda9d8 8054162a 00000001 00126d80 00000001 nt!KeWaitForMultipleObjects+0x297
```

La commande **!process**



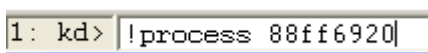
```
1: kd> !process 0 0
```

Liste les processus en cours lors du crash



```
1: kd> !process
Followup: MachineOwner
-----
GetPointerFromAddress: unable to read from 80562134
PROCESS 88ff6920 SessionId: none Cid: 0388 Peb: 7ffdb000 ParentCid: 0b8c
DirBase: 0b280800 ObjectTable: e31874c8 HandleCount: <Data Not Accessible>
Image: OUTLOOK.EXE
VadRoot 88d352c0 Vads 1091 Clone 0 Private 17314. Modified 18389. Locked 5.
DeviceMap e230c1b8
Token e3fe3340
ReadMemory error: Cannot get nt!KeMaximumIncrement value.
```

La commande **!process 88ff6920**

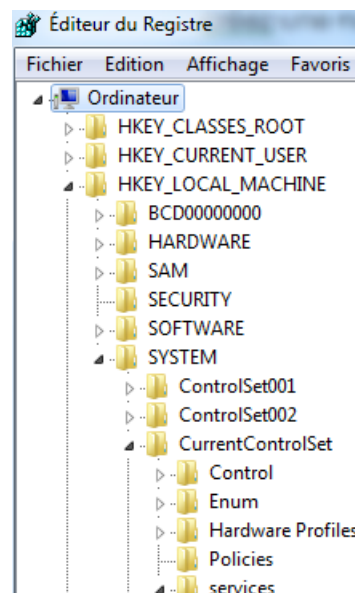


```
1: kd> !process 88ff6920
```

Détaillerait ce processus

Générer un BSOD

Via regedit trouver la clé



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters

	Nom	Type	Données
	(par défaut)	REG_SZ	(valeur non définie)
	LayerDriver JPN	REG_SZ	kbd101.dll
	LayerDriver KOR	REG_SZ	kbd101a.dll
	OverrideKeyboardIdentifier	REG_SZ	PCAT_101KEY
	OverrideKeyboardSubtype	REG_DWORD	0x00000000 (0)
	OverrideKeyboardType	REG_DWORD	0x00000007 (7)
	PollingIterations	REG_DWORD	0x00002ee0 (12000)
	PollingIterationsMaximum	REG_DWORD	0x00002ee0 (12000)
	ResendIterations	REG_DWORD	0x00000003 (3)

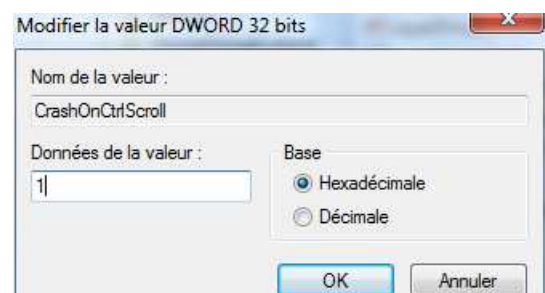
créez une nouvelle valeur de type DWORD et appelez-la **CrashOnCtrlScroll**

 **CrashOnCtrlScroll** REG_DWORD 0x00000000 (0)

faites un clic droit dessus et sélectionnez Modifier, mettez la valeur 1

fermez regedit

et redémarrez votre ordinateur



Vous pouvez provoquer un BSoD à la demande en

- maintenant enfoncée la touche CTRL de droite
- et en appuyant 2 fois sur la touche "Arrêt défil" ou "Scroll lock".

```
0: kd> !analyze -v
*****
*                                     *
*                               Bugcheck Analysis                               *
*                                     *
*****

MANUALLY_INITIATED_CRASH (e2)
The user manually initiated this crash dump.
Arguments:
Arg1: 00000000
Arg2: 00000000
Arg3: 00000000
```

SYSPREP

Versions de Sysprep:

L'outil **Sysprep (System Preparation)** prépare un ordinateur pour l'acquisition d'images ou la livraison à un client en configurant l'ordinateur de manière à créer un nouvel identificateur de sécurité (SID) d'ordinateur lors du redémarrage de ce dernier.

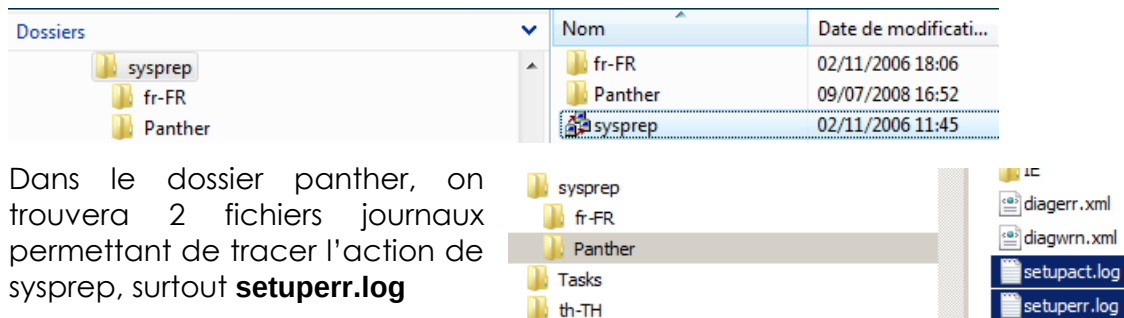
En outre, Sysprep nettoie les paramètres et les données spécifiques à l'utilisateur et à l'ordinateur qui ne doivent pas être copiés vers un ordinateur de destination.

La version de Sysprep installée avec l'image système Windows est la seule utilisable. Autrement dit, un Sysprep fourni avec Seven SP1 (ou Seven) ne peut travailler avec un XP, et vice-versa.

- Sysprep 3.14 Seven Sp1 –Seven ver 6.1.7601.17514
Se trouvant dans \Windows\system32\sysprep\...
- Sysprep 2.0 XP Sp3 – XP Sp2 ver 5.1.2600.5512
Se trouvant dans le MEDIA XP, ou en se téléchargeant...

Sysprep 3.14 pour Seven-2008:

A partir de seven, **Sysprep** est installé avec chaque version de Windows et doit toujours être exécuté à partir du dossier **%WINDIR%\system32\sysprep**



Dans le dossier panther, on trouvera 2 fichiers journaux permettant de tracer l'action de sysprep, surtout **setuperr.log**

Action de sysprep :

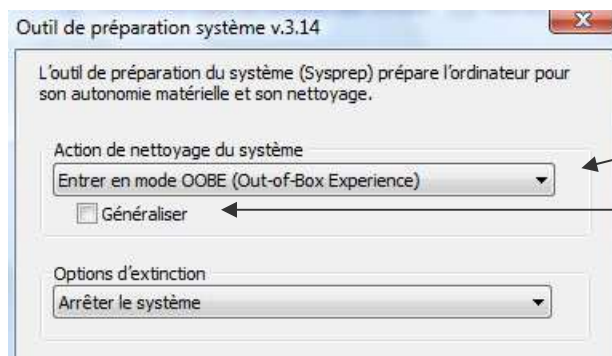
1. toutes les informations système uniques sont supprimées de Windows.
2. L'ID de sécurité (SID) est réinitialisée,
3. tous les points de restauration du système sont effacés
4. les journaux d'événements sont supprimés.

Lors du démarrage suivant de l'ordinateur,

5. un nouvel ID de sécurité (SID) est créé,
6. l'horloge d'activation de Windows est réinitialisée, (si cette horloge n'a pas déjà été réinitialisée à trois reprises)

Sysprep mode graphique:

Un double clic sur **sysprep** amène



Mode OOBE : re déclenche l'assistant de premier démarrage de Seven

Mode Audit : démarre le poste directement

Généraliser : Impérativement nécessaire, pour demander de régénérer les SID lors du re-démarrage

Mais dans laquelle il faut toujours demander

Sysprep /generalize:

Si vous avez l'intention de transférer une image système Windows vers un autre ordinateur, vous devez exécuter la commande **sysprep /generalize**

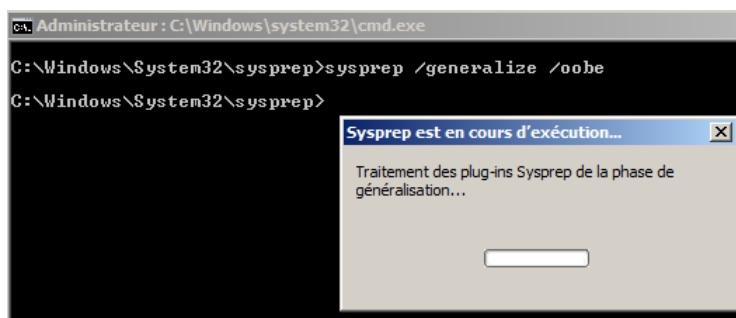
sysprep /generalize

- demande une confirmation de l'action generalize
- reboot immédiat après le sysprep.
- Puis lors la 1^{re} installation, à la fin un mini assistant se déroule demandant plusieurs paramètres

sysprep /generalize /oobe

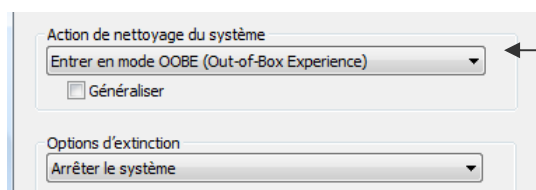
- Arrêt mais pas de reboot immédiat après le sysprep.
- Puis lors la 1^{re} installation, à la fin un mini assistant se déroule demandant plusieurs paramètres

c'est l'option courante avant une capture d'image



sysprep /audit

- Arrêt mais pas de reboot immédiat après le sysprep.
- Lorsque l'on demande /audit après re-démarrage du poste suite au sysprep, on se logue en tant que admin et on peut effectuer quelques manip sur le nouveau poste....



OOBE : à demander après le premier redémarrage suite au sysprep / audit sur la machine que l'on vient d'installer

N.B. Le mode audit permet d'effectuer des personnalisations et des configurations supplémentaires. Une fois ces opérations terminées, il faudra exécuter **sysprep /generalize /oobe**

Mini installation passe OOBE:

Suite à une demande via **sysprep** de terminer en installation **OOBE (Out Of Box Experience)**, lorsque le poste redémarre on a :

- Installation re-déTECTANT l'environnement matériel et les périphériques plug& play présent sur la nouvelle machine
- Reboot

Puis une mini installation se déclenche, demandant :

- Régionalisation
- nom utilisateur / nom machine
- mot de passe utilisateur
- (clé activation du produit)
- accepter la licence
- type de protection par défaut
- horodatage
- type connexion réseau (si carte réseau détectée)

Sysprep /unattend:c:\fichier.xml:

Si on veut automatiser la phase de mini installation consécutive à un sysprep, ou bien incorporer des réglages spécifiques, on peut lui indiquer au moment de la commande d'incorporer un fichier de réponses via l'option **/unattend** comme dans

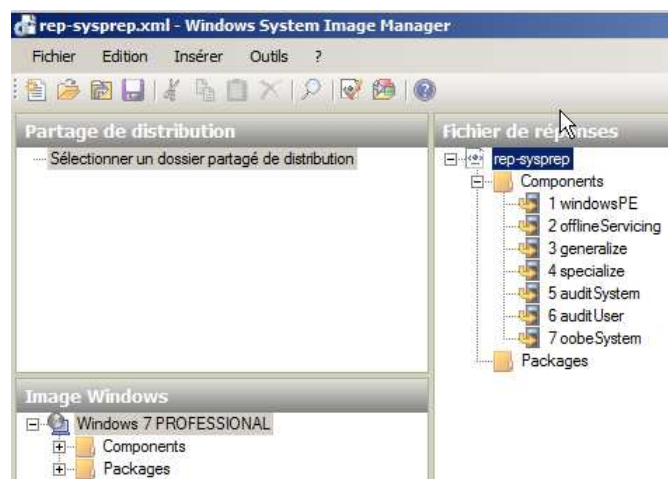
sysprep /generalize /oobe /unattend:c:\fichier.xml

Le fichier de réponse est créé de manière analogue aux autres fichiers de réponse, par l'outil WSIM

on peut le nommer comme on le souhaite

ici dans l'exemple

rep-sysprep.xml



N.B: Ce fichier (dans l'exemple `c:\rep-sysprep.xml`) est en fait automatiquement recopié dans le dossier **c:\windows\panther** sous le nom **unattend.xml**... Une fois la commande sysprep passée, ce fichier `rep-sysprepr.xml` peut être supprimé, car lors du reboot c'est sa copie en **%windir%\panther** qui est utilisée...

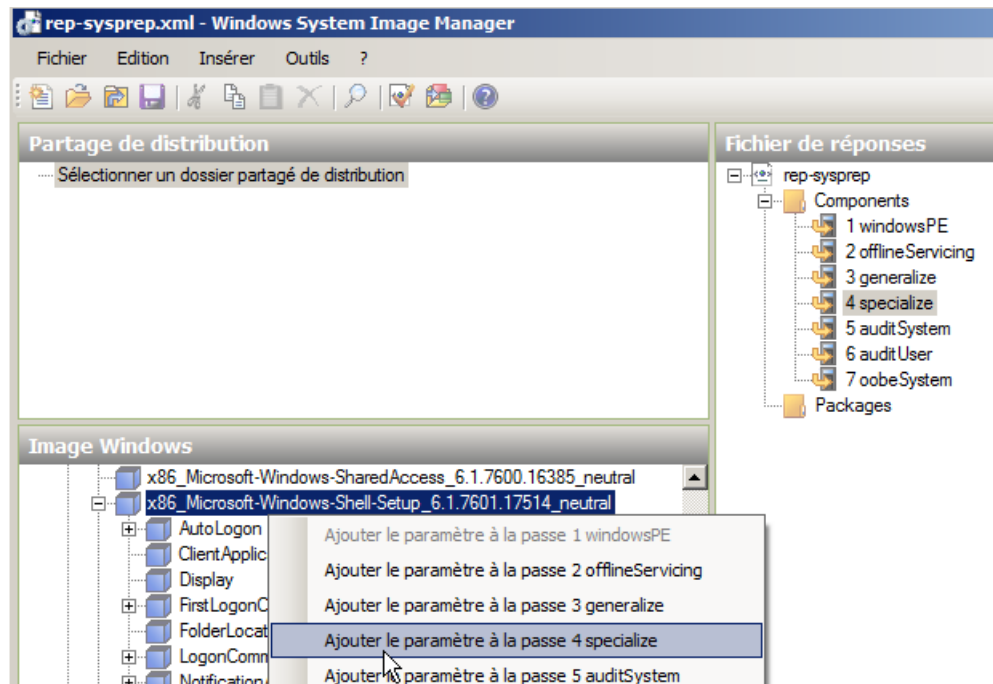
N.B: Dans la liste des emplacements possible pour le fichier de réponse, **%windir%\panther\rep-sysprep.xml** est en haut de la hiérarchie.

Sysprep /unattend copyprofile

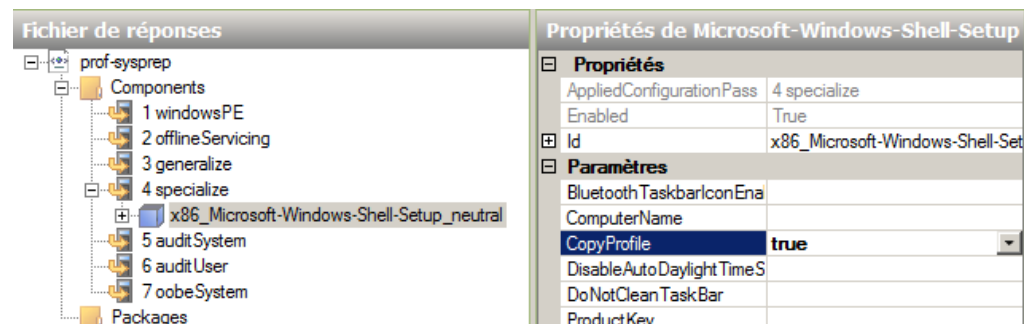
A partir de Seven, (et donc également pour 2008, 2008R2) la seule manière de se préparer un profil par défaut, est celle d'indiquer dans le fichier de réponse à exécuter au moment du sysprep une commande

Copyprofile à True

C'est un paramètre qui s'indique en **pas4 Specialize** dans le module **Microsoft-Windows-Shell-Setup_neutral**. Elle ne s'exécutera donc que lors du re-boot après que le sysprep se soit exécuté, de la phase mini oobe, passe specialize !



donnant



La procédure pour créer un profil par défaut est la suivante

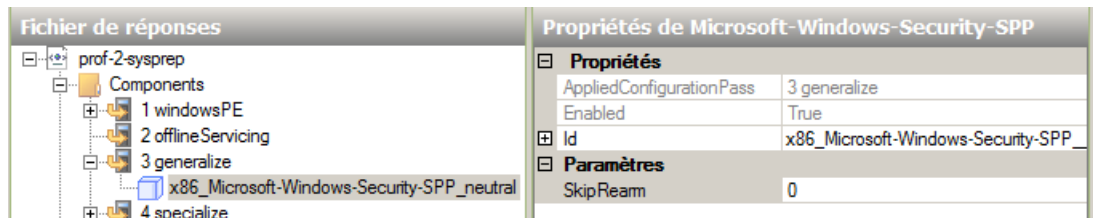
1. Créer un fichier de réponse nommé par exemple **prof-sysprep.xml**. contenant la commande **CopyProfile=True**
2. Ouvrir une session sur la machine "type" avec le compte **Administrateur** par défaut du poste (celui qui est dévalidé lors de l'installation...) et
 - a. Supprimer tous les comptes existants autres que l'administrateur.
 - b. Supprimer tous les profils existants éventuellement sur le poste.
 - c. Effectuer le paramétrage du profil en cours de l'administrateur.
3. Lancer la commande **sysprep** avec l'options **/unattend** comme dans:
/generalize /oobe /unattend:c:\prof-sysprep.xml

Activation et SkipRearm

Il n'existe aucune limite au nombre d'exécutions de Sysprep sur un ordinateur. Cependant, l'horloge de l'Activation de produit Windows commence son décompte la première fois que Windows est lancé.

La commande **sysprep /generalize** réinitialise l'activation du produit et donc elle ne peut le faire qu'à trois reprises maximum. Après trois exécutions de **sysprep /generalize**, l'horloge ne peut plus être réinitialisée...

On peut ignorer la réinitialisation de l'horloge d'activation à l'aide du paramètre **SkipRearm** dans le composant **Microsoft-Windows-Security-SPP** (anciennement vista **Microsoft-Windows-Security-Licensing-SLC**)



Microsoft recommande d'utiliser le paramètre SkipRearm avec la valeur du paramètre **SkipRearm** égale à **1** si on prévoit d'exécuter **Sysprep /generalize** à plusieurs reprises sur un ordinateur

Après avoir testé cette image, utilisez la commande **Sysprep /generalize** avec la valeur du paramètre **SkipRearm** égale à **0**.

Exemple de fichier de réponse

Avec les 2 commandes

Génération du profil par défaut et non - réarmement

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
  <settings pass="specialize">
    <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <CopyProfile>true</CopyProfile>
      <ComputerName></ComputerName>
    </component>
  </settings>
  <settings pass="generalize">
    <component name="Microsoft-Windows-Security-SPP"
processorArchitecture="x86" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SkipRearm>1</SkipRearm>
    </component>
  </settings>
  <component name="Microsoft-Windows-Deployment"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <task name="Install Windows 7 PROFESSIONAL"
cpi:source="wim:d:/win-seven/install.wim#Windows
7 PROFESSIONAL" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
  </component>
</unattend>
```