Système Windows 8.1 Pro – sys 20 – Cours -

Cours Système Windows 8.1 pro - Entreprise
Michel Cabaré – Ver 1.2 – Juin 2014-

http://WWW.CABARE.NET ©

Système Windows 8.1 Pro
Cours

Michel Cabaré – Ver 1.2 – Juin 2014

www.cabare.net ©

Ce Support à 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 81 SEVEN & XP

Positionnement dans la famille Microsoft :

Une fois mis de coté 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 worksgroup 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 1993extension 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…)

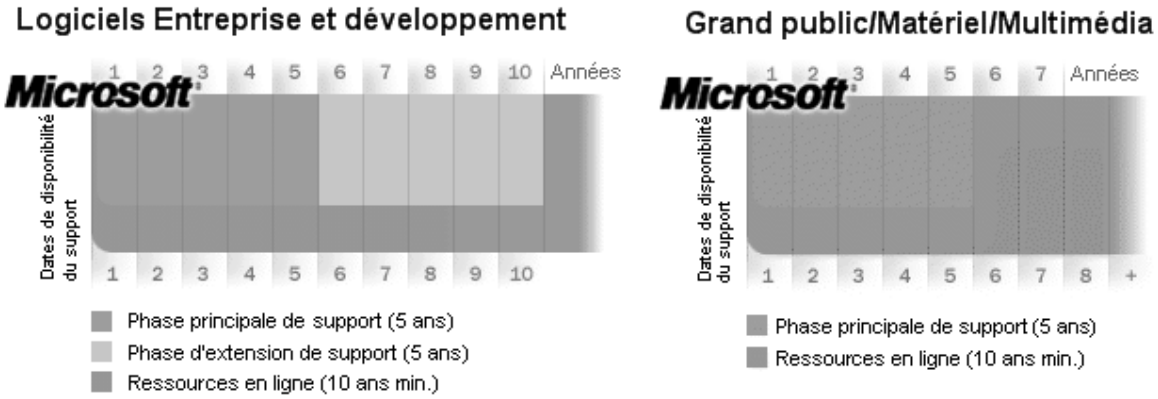
  Une mise à jour **7 - Seven**: starter, familiale, pro, intégrale
  - ✓ **6.1** en octobre 2009 **…**

  Une mise à jour **Windows - 8**: RT, 8, pro, entreprise
  - ✓ **6.2** en octobre 2012 **…**

  Une mise à jour **Windows – 8.1** : RT, 8, pro, entreprise
  - ✓ **6.3** en mai 2014

Durée du support chez Microsoft :

Grosso modo, 5 ans pour les Os Familiaux, et 10 ans pour les OS Professionnel



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 clients	Dernier Service Pack ou dernière mise à jour	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	13 janvier 2015	14 janvier 2020
Windows 8	Windows 8.1	9 janvier 2018	10 janvier 2023

Fonctionnalités Windows 8 :

Les éditions N de Windows 8 sont identiques aux éditions standard, à l'exception du Lecteur Windows Media et des technologies associées (Windows Media Center ou Lecture-Création de DVD)

Windows Hyper-V fonctionne uniquement sur les versions Professionnel et Intégrale de Windows 8

Les versions sont RT (processeur ARM tablettes)- Windows 8, Pro et Entreprise livrée uniquement avec un contrat corporate d'entreprise. (hors commerce détail)

Les principales différences entre les versions se résument ci-dessous :

	8 RT	**8**	**8 Pro**	**8 Entreprise**
Bureau à Distance	-	-	Oui	Oui
Chiffrement	-	-	Oui	Oui
Démarre depuis VHD	-	-	Oui	Oui
Hyper-V	-	-	Oui (64b)	Oui (64b)
Boot depuis USB	-	-	-	Oui
Intégration Domaine	-	-	Oui	Oui
Stratégies	-	-	Oui	Oui

CONFIGURATION MATERIELLE

Configuration requise :

Voilà les données pour une utilisation de **Windows 8**

- 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 Hyper-V (ex Windows XP Mode) requiert une RAM supplémentaire de 2 Go, un espace disque supplémentaire de 15 Go et un processeur avec une virtualisation du matériel avec Intel VT ou AMD-V activé dans le BIOS…

Et voilà un rappel les données pour une utilisation de **Windows 8**

8 Capable	8 Ready	En pratique
Proc type P4 minimum 1 Ghz + extension d'adresse physique (PAE) + bit de processeur (NX) + extensions Streaming SIMD 2 (SSE2)	Proc type P4 minimum 1 Ghz + extension d'adresse physique (PAE) + bit de processeur (NX) + extensions Streaming SIMD 2 (SSE2) z	
1 Giga de RAM	2 Giga de RAM (x64)	+ 2 Giga de RAM si Hyper-V(x64)
Vidéo DirectX 9.0 une définition d'écran XGA (1024 x 768 pixels)	Vidéo DirectX 9.0 - pilote WDDM Si affichage des applications Metro via la fonction Snap définition WXGA (1366 x 768 pixels)	Vidéo DirectX 10.0
16 Giga libres DD	20 Giga libres DD	40 Giga

Hardware Compatibility List :

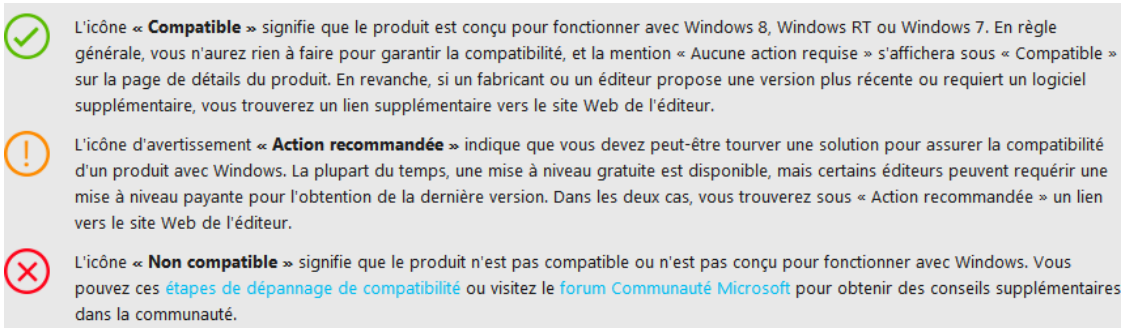
Dans Windows 8 (mais depuis NT) , les applications ne peuvent accéder directement au matériel car c'est lui qui contrôle directement l'intégralité du HARD, c'est pour cette raison que Windows 8 à priori ne supporte aucun driver non certifié, et qu'il peut être important de vérifier avant toute installation que

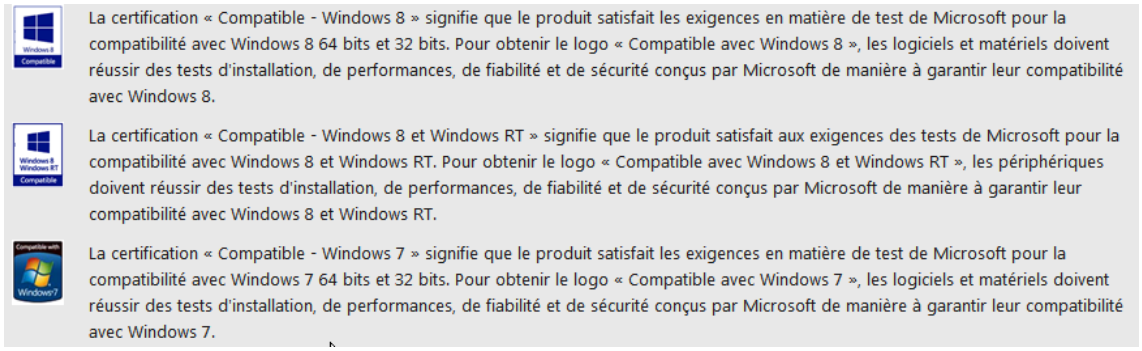
tout le matériel (y compris les cartes vidéo, cartes réseau, lecteur de CD-ROM, disques ...) soit référencé dans la HCL

Désormais les listes Windows 8 et Windows RT sont disponibles

http://www.microsoft.com/fr-fr/windows/compatibility/win8/CompatCenter/Home

Lorsque l'on fait une recherche, on peut obtenir





Beaucoup de matériels restent simplement « compatible » et non pas certifiés…

Qu' est-ce qu'un Service Pack :

Dans un premier temps on installe Windows puis 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'IMPERATIF FONCTIONNELS !

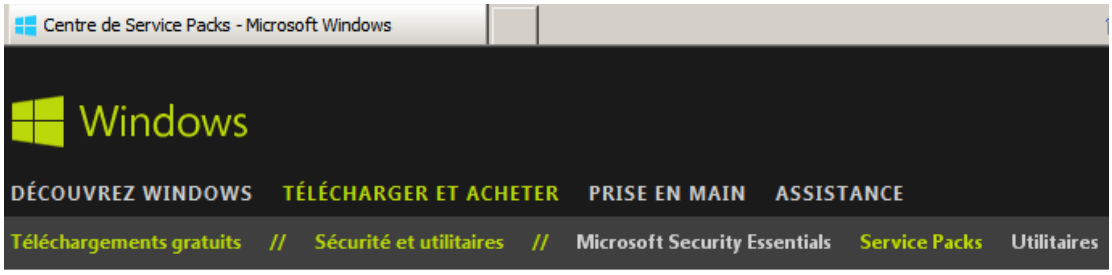
Sans rentrer dans le détail des listes d'erreurs corrigés par ces services packs, il reste à dire que normalement

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	pas de Sp à venir
8.1 livré 05/2014	6.30.build 9600	?

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 renf
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 minu
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** pou
Mises à jour automatiques pour Windows XP. Windows vous avertira lorsque les Service Packs dont vous avez besc
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 pourra télécharger

Aucun Service Pack disponible actuellement

Aucun Service Pack n'a encore été commercialisé pour Windows 8,

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

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

Un identifiant passeport microsoft peut être nécessaire…

Puis on gère ses inscriptions…2 lettres sont particulièrement intéressantes :

Technet

Alertes de Sécurité

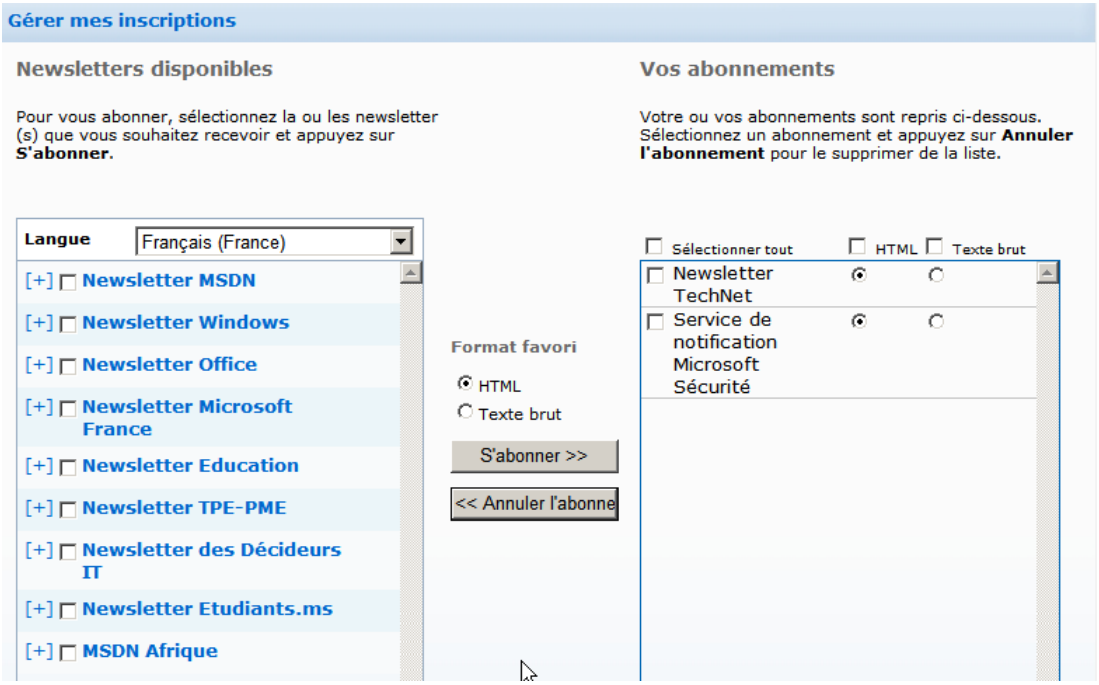
Donnant ensuite la possibilité de s'inscrire

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 newsletter.

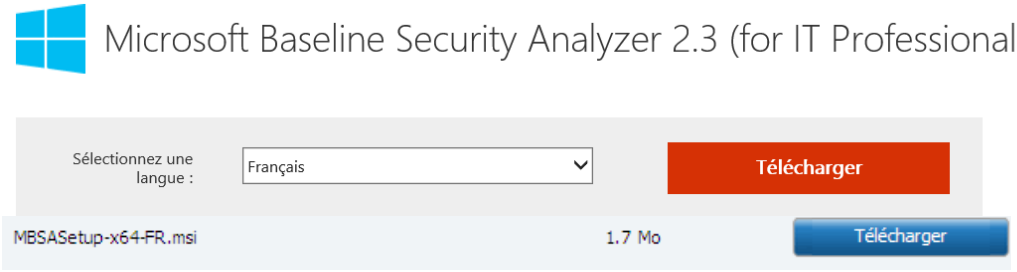
On fait une recherche avec « profil microsoft » et on peut se logguer avec un compte Passeport Microsoft – Microsoft Live

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



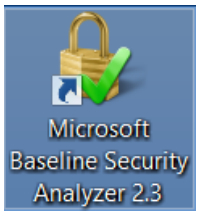
Outils MBSA 2.3:

Actuellement la version de MBSA (2.3 dernière release) supporte Windows 8.1 .

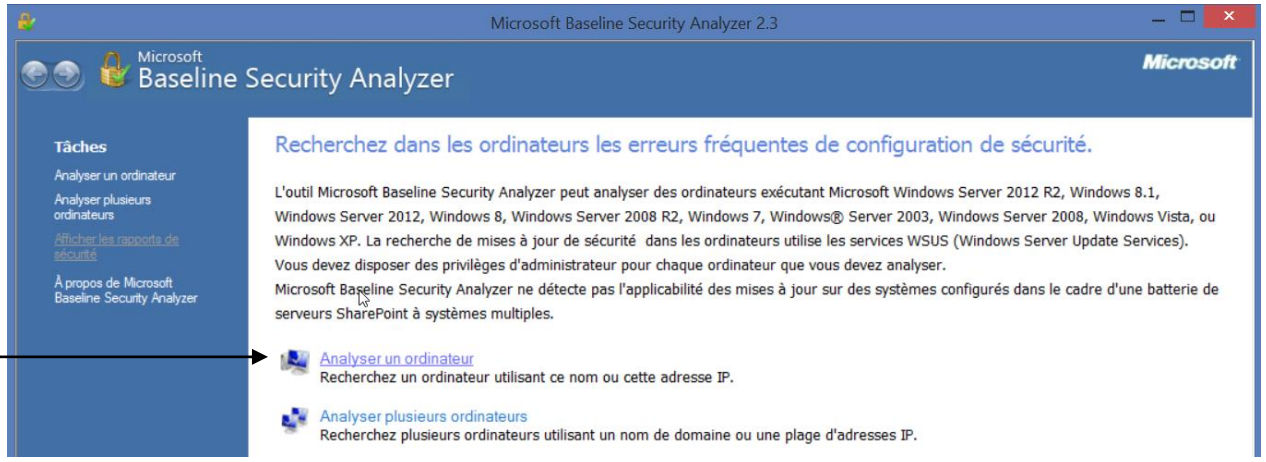


Il faut donc exécuter ce fichier…

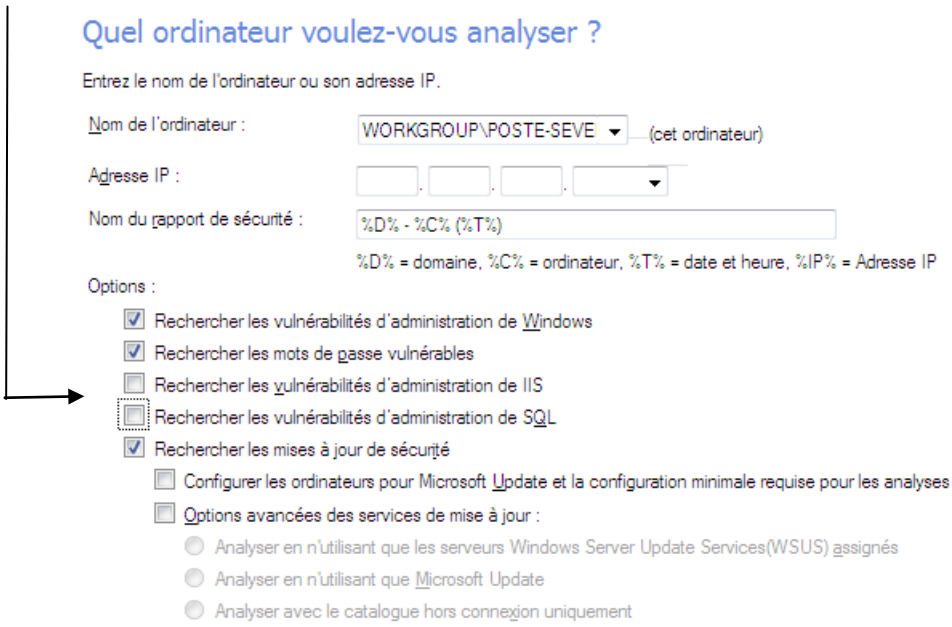
La version 2.3 de MBSA comprend une interface graphique



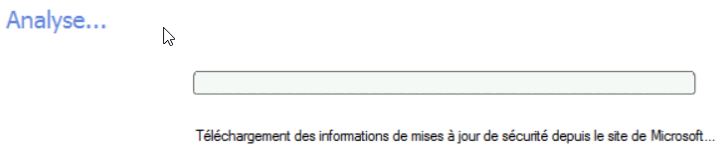
qui peut effectuer l'analyse locale de systèmes Windows 8



Peu de réglages sont indispensables à ce niveau, on décoche **IIS** et **SQL** et on demande de **Rechercher les mises à jour de Sécurité**…

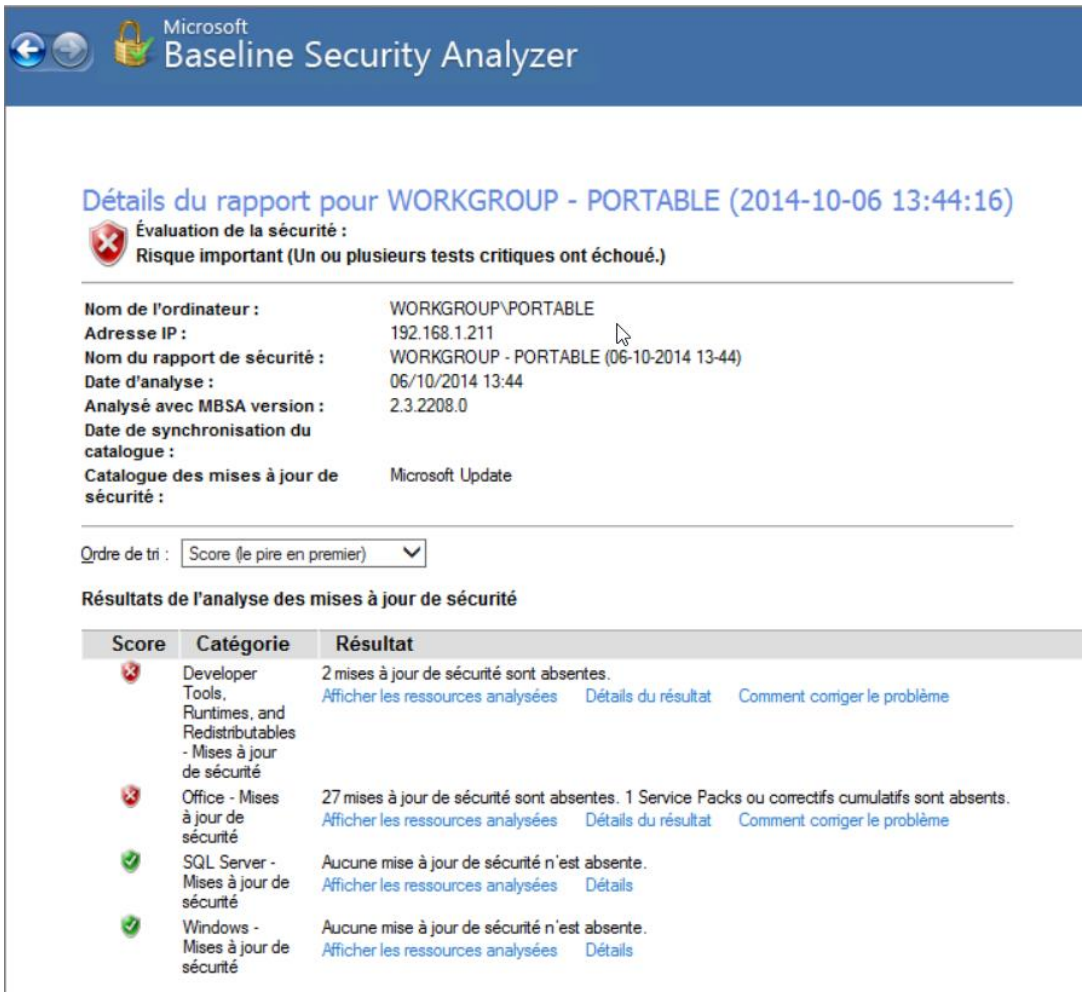


Après téléchargement (cela peut être long) d'une base de signature depuis le site de microsoft,



Une analyse est rendue

Un résultat est donné avec des indications sur les actions éventuelles



Résultats de l'analyse de Windows

Vulnérabilités d'administration

Score	Catégorie	Résultat
	Expiration des mots de passe	Certains comptes d'utilisateurs (3 sur 4) ont un mot de passe n'expirant pas. Afficher les ressources analysées Détails du résultat Comment corriger le problème
	Mises à jour incomplètes	Aucune installation de mise à jour logicielle incomplète n'a été détectée. Afficher les ressources analysées
	Pare-feu Windows	Le Pare-feu Windows est activé, et des exceptions sont configurées. Le Pare-feu Windows est activé sur toutes les connexions réseau. Afficher les ressources analysées Détails du résultat Comment corriger le problème
	Test des mots de passe des comptes locaux	Certains comptes d'utilisateurs (1 sur 4) ont un mot de passe vide ou simple, ou n'ont pas pu être analysés. Afficher les ressources analysées Détails
	Mises à jour automatiques	Les mises à jour sont automatiquement téléchargées et installées sur cet ordinateur. Afficher les ressources analysées
	Système de fichiers	Tous les disques durs (3) utilisent le système de fichiers NTFS. Afficher les ressources analysées Détails
	Autologon	L'ouverture de session automatique n'est pas configurée sur cet ordinateur. Afficher les ressources analysées
	Compte Invité	Le compte Invité est désactivé sur cet ordinateur. Afficher les ressources analysées
	Accès anonymes	Les accès anonymes sont restreints de façon adéquate sur cet ordinateur. Afficher les ressources analysées
	Administrateurs	Pas plus de 2 administrateurs ont été trouvés sur cet ordinateur. Afficher les ressources analysées Détails

Informations système supplémentaires

Score	Catégorie	Résultat
	Audit	L'audit des réussites ou des échecs d'ouvertures de session n'est pas activé. Autorisez l'audit et activez-le pour des événements spécifi fermeture de session. Consultez régulièrement votre journal d'événements pour détecter les éventuels accès non autorisés. Afficher les ressources analysées Comment corriger le problème
	Services	Aucun service potentiellement superflu n'a été détecté. Afficher les ressources analysées
	Partages	Nombre de partages disponibles sur votre ordinateur : 6.

NOTIONS POUR INSTALLER 8

Fichiers d'installation Image - WIM :

Comme Seven, Windows 8 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 64 bits et (éventuellement une 32 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 que une fois
- Démarrage de l'installation avec Windows PE 4.0, (boot.Wim) permettant de préparer (si besoin) disques et partition…

Il est possible d'installer Windows 8 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 Deploiement 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 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:

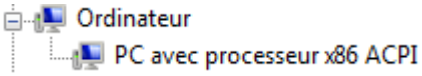
- hal.dll standard (Non-ACPI) PC
- halaacpi.dll ACPI Uniprocessor PC
- halmacpi.dll ACPI Multiprocessor PC

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

Sous Windows 8 (Seven)

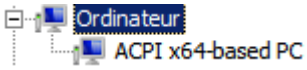
une seule HAL est désormais détectée, dénommée

PC avec processeur x86 ACPI



Ou

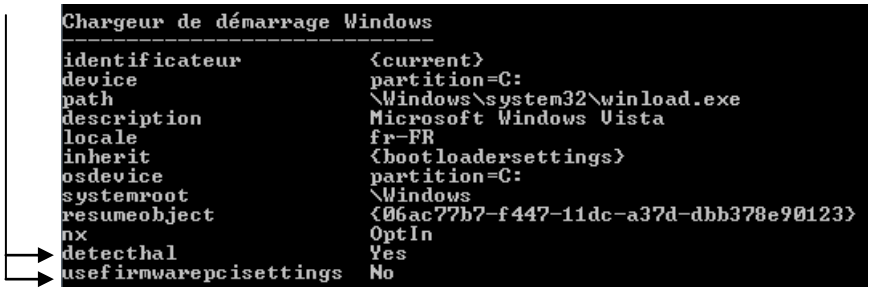
PC avec processeur x64 ACPI



Windows 8 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 :

detectehal **Yes**

usefirmwarepcisettings **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
usefirmwarepcisettings  No
```

Donc

Bcdedit /set {current} detecthal yes

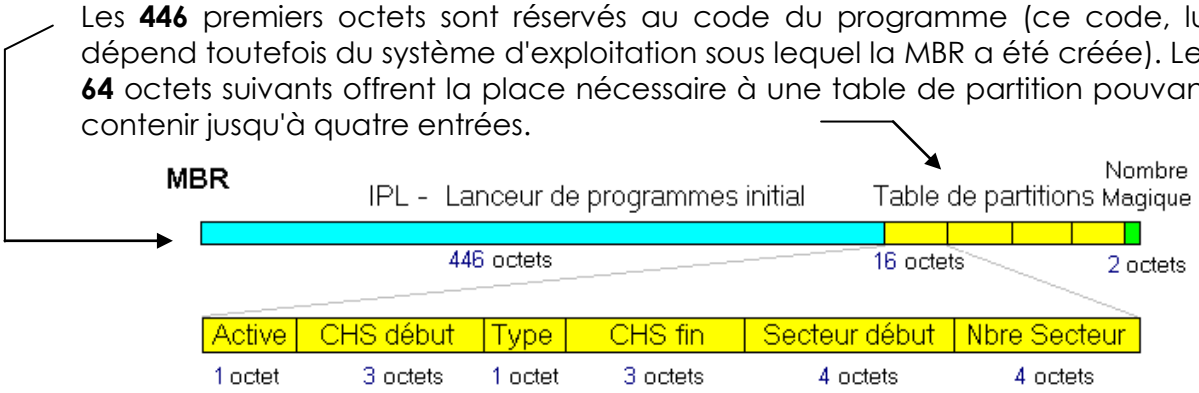
Et **Bcdedit /set {current} detecthal no**

Cette option fut gérable via msconfig un temps sous Seven RC… Depuis elle n'est accessible que via **Bcdedit**.

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 :
  - étendues (définissant une table de partition "hors MBR" dans ce que l'on nomme une EBR)
- Les partitions "*contenus*" = qui sont de deux types :
  - primaires (définies exclusivement dans une table de partition dite MBR Master Boot record) au nombre de **4 maximum** par disque physique
  - 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 :

DISQUE PHYSIQUE			
Partition primaire	Partition étendue		
	Partition logique	Partition étendue	
		Partition logique	Partition étendue
			Partition logique

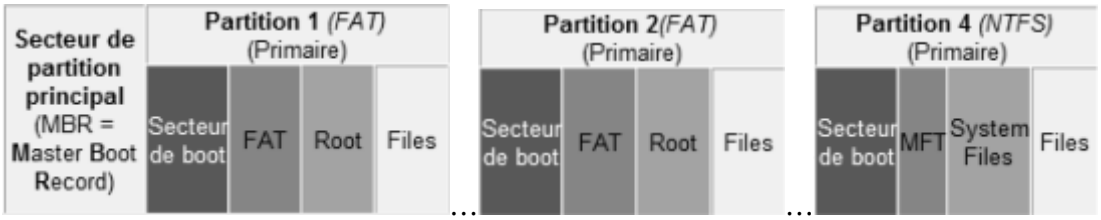
Ce disque possède 1 partition **PRIMAIRE** (celle où on va stocker le système d'exploitation généralement), et 3 partitions **LOGIQUES** (ici ce sont les seules qui nous intéressent : les "contenus", les partitions **ÉTENDUES** n'étant que des "contenants")

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 : 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, avec l'administrateur de disque NT4, seule est affichée la 1ère partition étendue, suivie de toutes les autres partitions logiques comme si elles étaient 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

	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. Taille maxi recommandée 2 Téraoctets	Volumes compris entre la taille d'une disquette et 2 Go	Volumes compris entre 512 Mo et 32 Go
Ne peut être utilisé sur floppy		formate jusqu'à 32 Go
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:

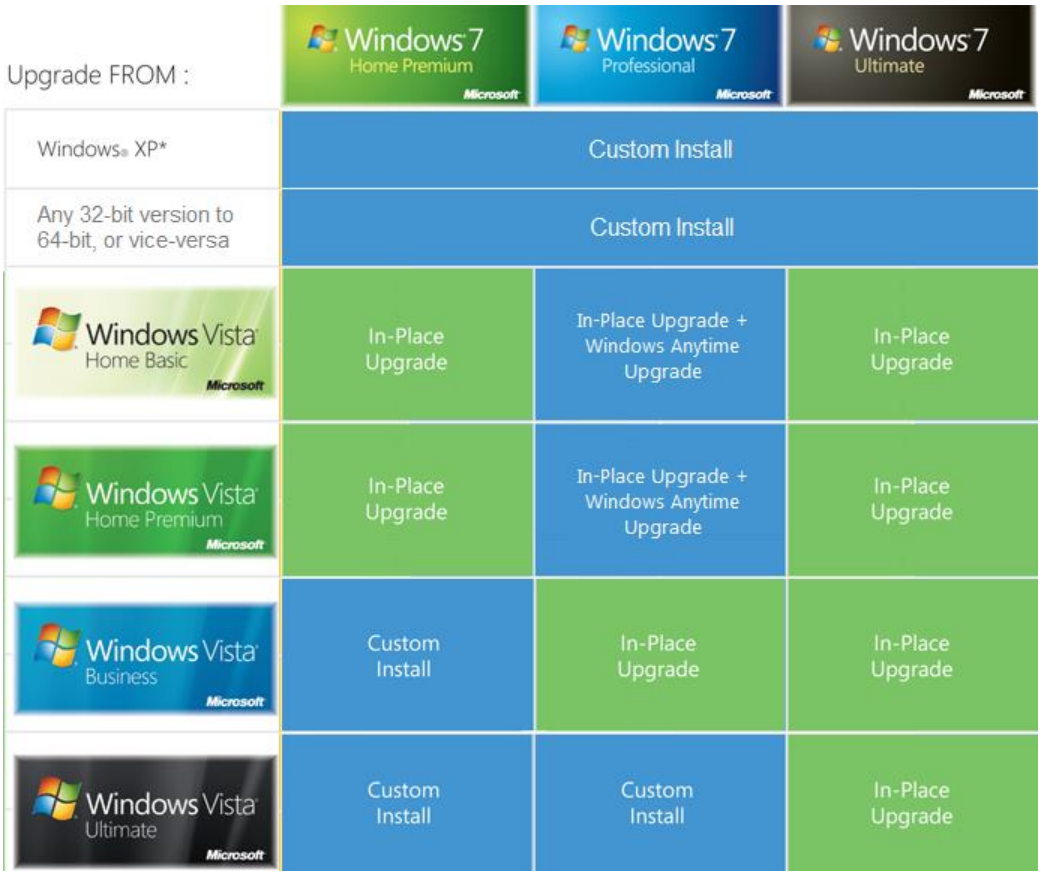
L'une des premières décisions que vous devez prendre est soit de mettre à niveau votre système d'exploitation actuel, soit de procéder à une installation entièrement nouvelle, soit encore de procéder à un multi-boot.

- 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 sur possible que certaines applications ne soient pas compatibles avec Windows 8

N.B: Après une mise à niveau, aucun moyen n'existe de revenir à la version antérieure !

On ne migre jamais d'une version 32 à 64 bits

On peut migrer uniquement dans les cas suivants pour Seven



- 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.

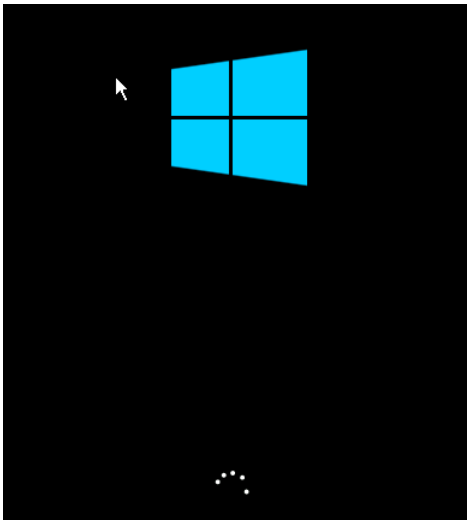
Evidemment, un seul credo opérationnel : « Pour passer de XP à Windows 8, il faudra sauvegarder les données puis réinstaller entièrement le système et les

fichiers » .Cependant pour passer de Seven 7 (voire Vista) à Windows 8 les risques sont bien moindres.

- Depuis **Windows XP** : compte tenu de la fin prochaine du support technique de cette version de Windows (avril 2014), la procédure de migration-reinstallation, «peut s'inscrire dans une démarche de co-déploiment de Windows 7 et Windows 8 »
- Depuis **Vista** : Microsoft recommande une migration sans attendre vers Windows 8 (le support technique de Vista s'achèvera en 2017).
- Si **Windows 7 en cours de déploiement**: « nous conseillons aux entreprises pour lesquelles le déploiement de Windows 7 est en cours d'aller au bout de cette procédure (...), et d'identifier en parallèle des employés ou groupes d'utilisateurs susceptibles de bénéficier de l'expérience offerte par Windows 8 pour un déploiement restreint à ces utilisateurs dans un premier temps ».
- Si **Windows 7 est déjà déployé** : On peut entamer la transition vers Windows 8, compte tenu de la grande compatibilité entre les deux OS.

Install complète Depuis CD :

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



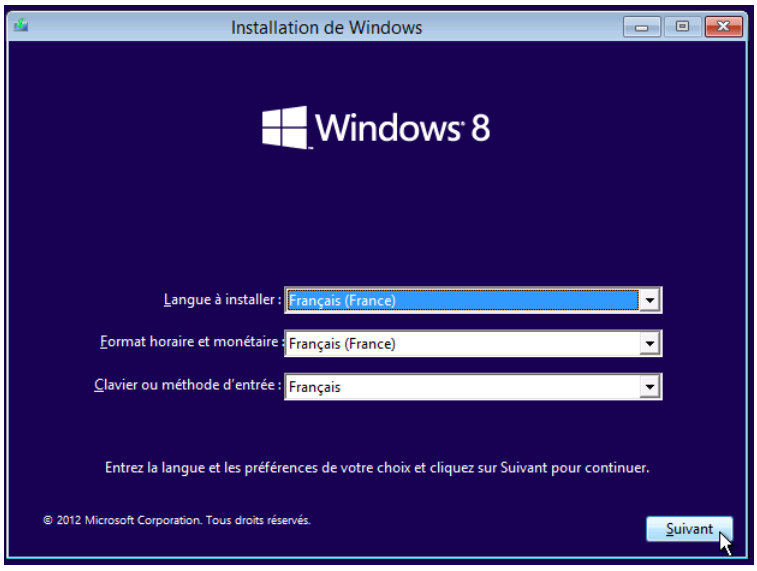
Il est conseillé de ne pas courir plusieurs lièvres à la fois, d'autant plus que faire une installation ne nécessite pas de connexion internet…

L'écran noir est déroutant, et peu « durer »..
seule une petite animation donne un signe de vie →

On passe avec une interface graphique de manière quasi immédiate…

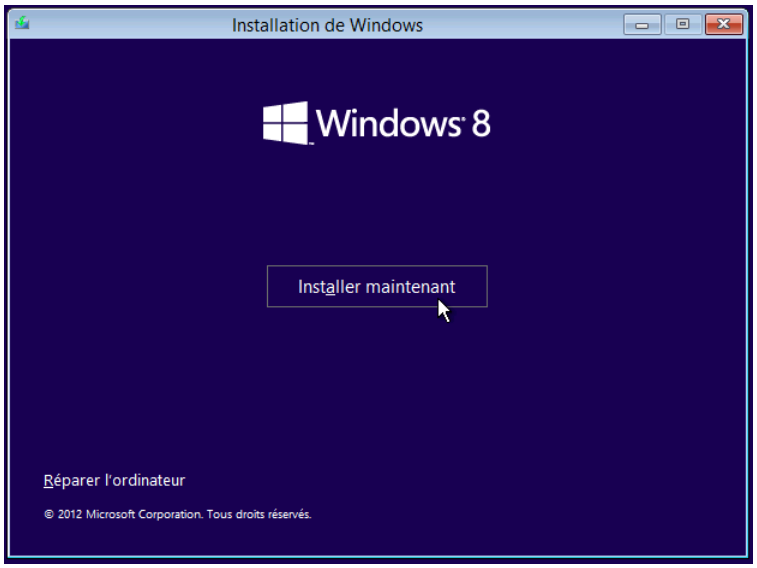
Paramètre régionaux :

Il suffit d'indiquer le pays, code clavier, formats numériques souhaite utiliser

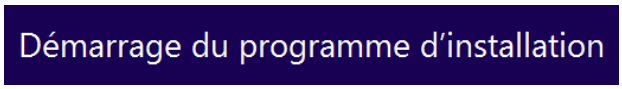


Installer / Réparer

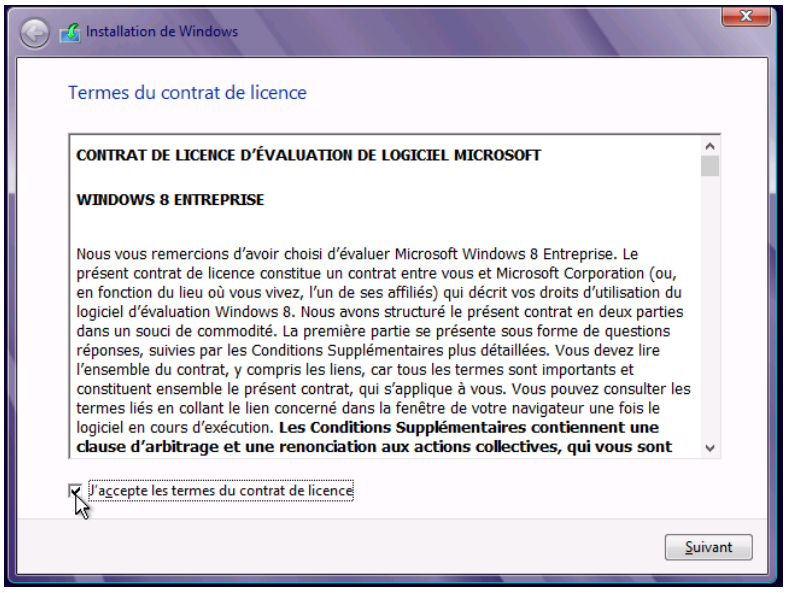
Il faut demander d'**Installer** Windows 8



Pour obtenir



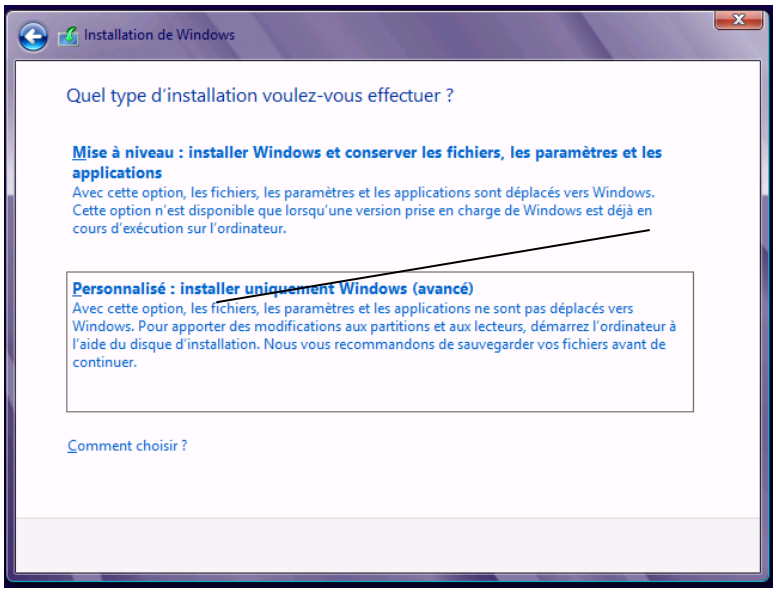
Licence



Il faut accepter la licence

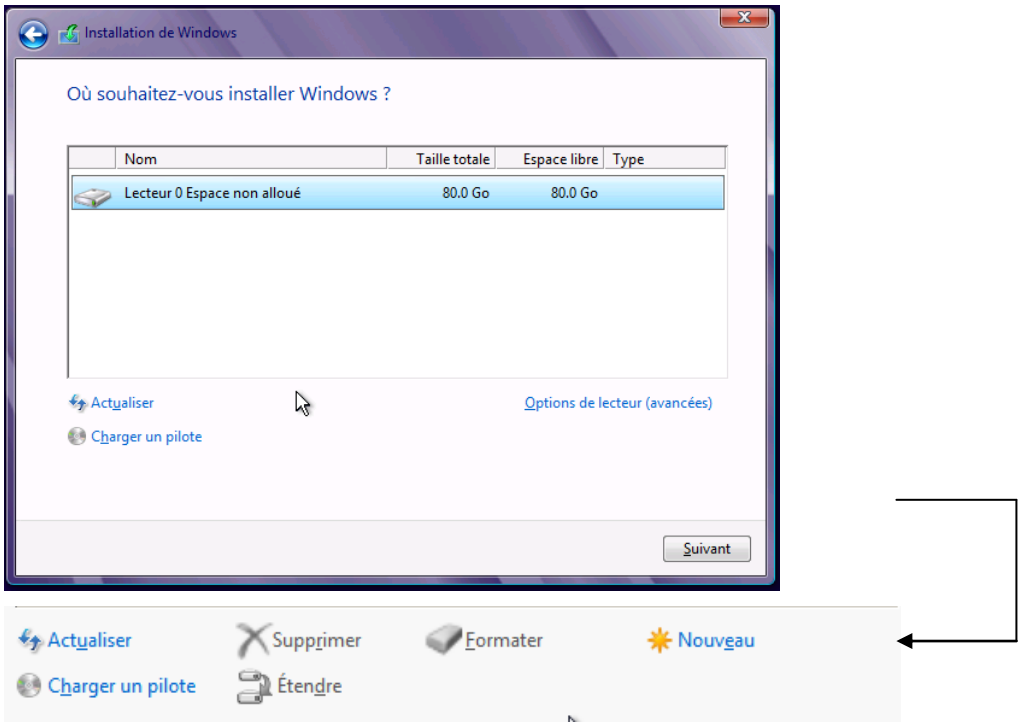
Mise à Jour / Installation Avancée

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 ou Seven…), et donc on demande Personnalisé : installer uniquement Windows (avancé).

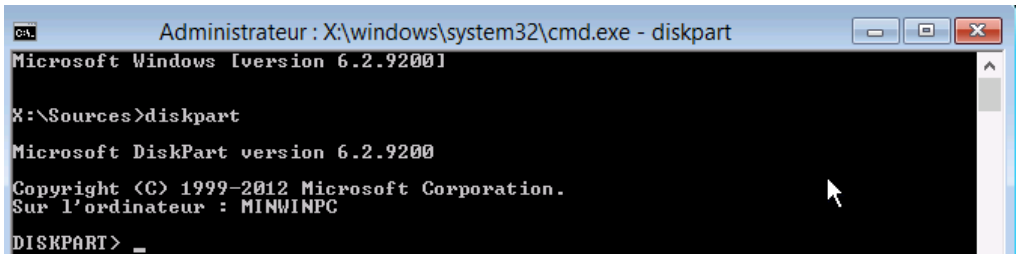


Création des Partitions

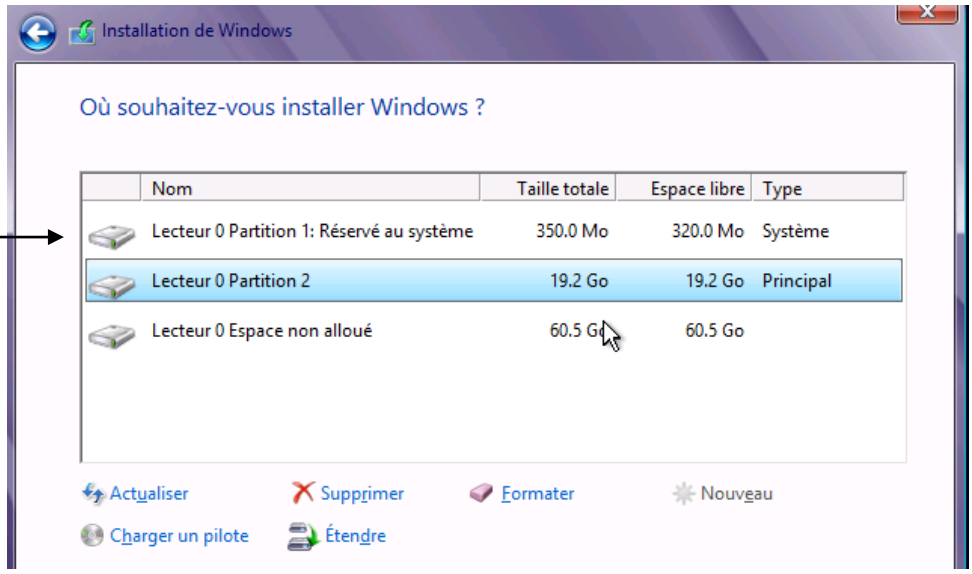
Lorsque l'on crée des partitions, ce sont des partitions Principales. Le formatage ne donne pas le choix du système de fichier, NTFS est utilisé (vu la taille disque).



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

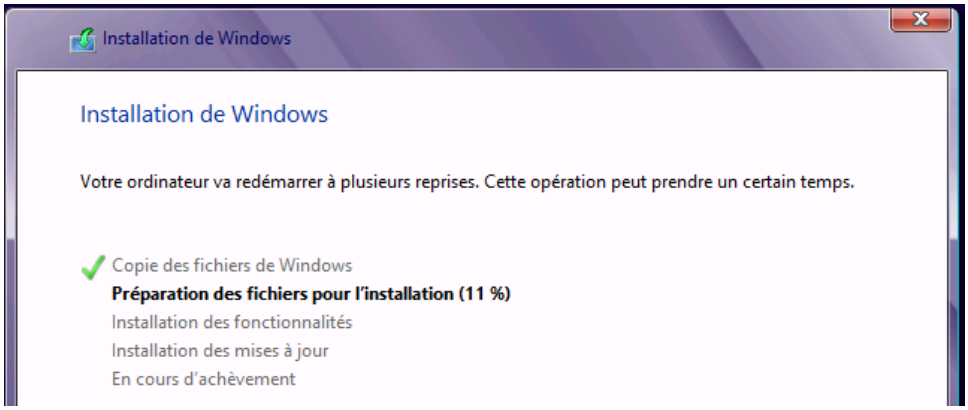


Une partition « cachée » système est crée pour stocker des outils de récupération en cas de crash

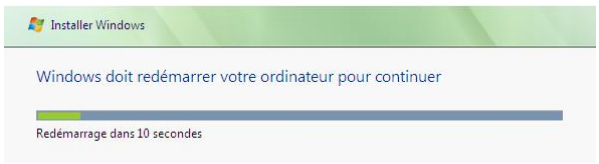


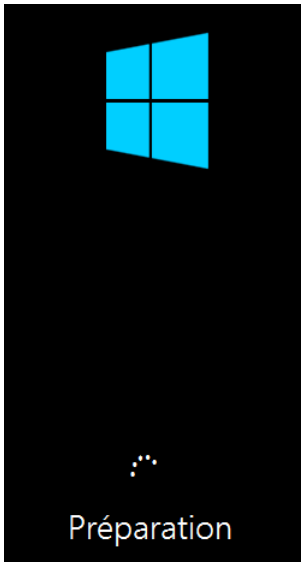
Copie des fichiers

Le programme d'installation poursuit,



Le programme d'installation décompresse les fichiers, génère un Re-Boot





Assistant premier démarrage (phase OOBE)

Il demande successivement :

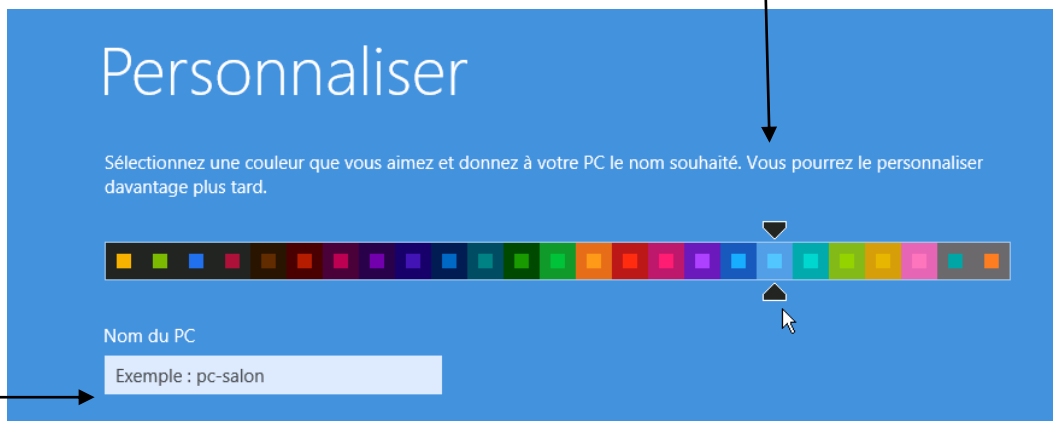
- Le nom machine

Entrez un nom différent des autres noms d'ordinateur sur votre réseau.

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

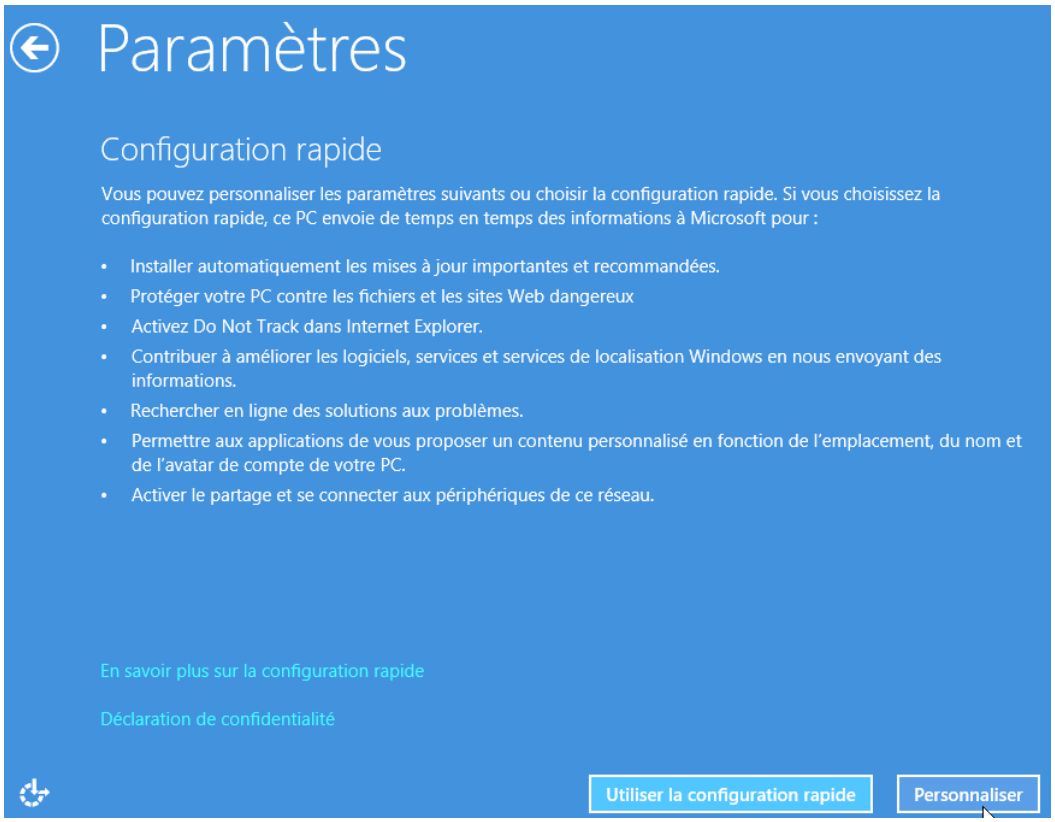
N.B : Utilisez uniquement les caractères suivant : les **chiffres de 0 à 9**, les **lettres majuscules et minuscules de A à Z** et le **trait d'union** (-).

- Un choix de couleur



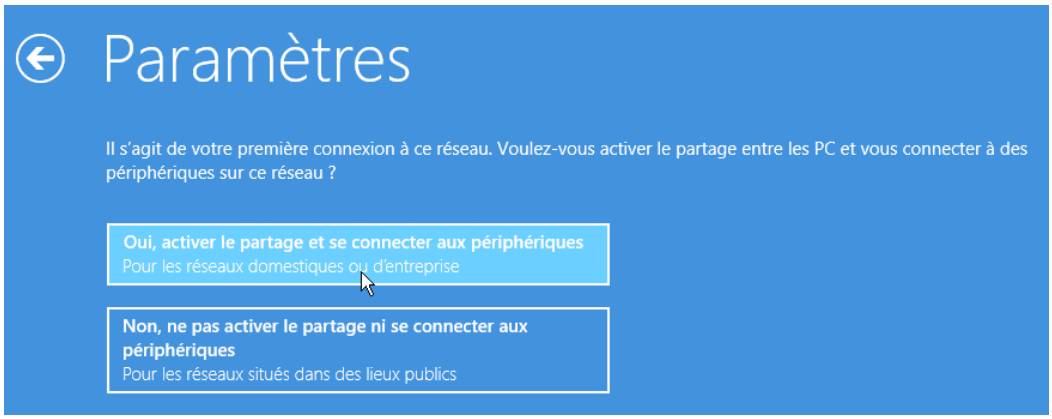
Configuration Rapide / Personnalisée

Fondamentalement les choix de la rapide sont équivalents aux choix de la personnalisée « par défaut » .Ces choix instaurent un dialogue assez soutenu entre le poste et Microsoft via le Web….

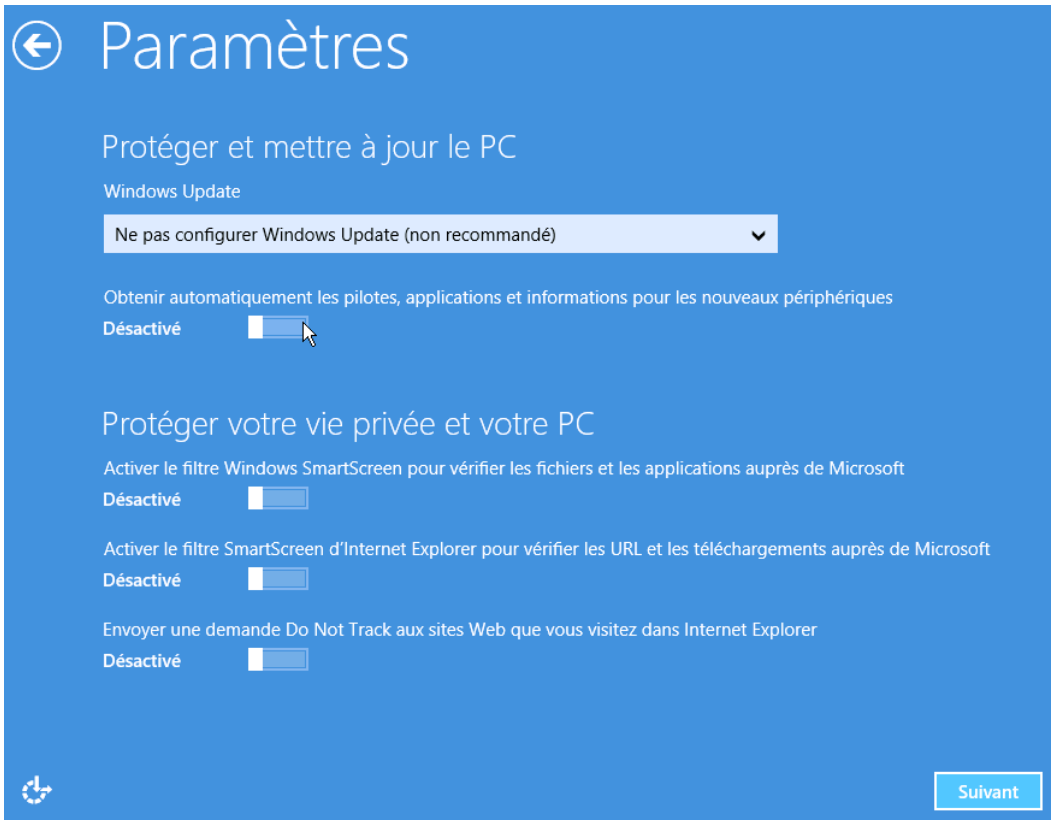


il vaut mieux demander Personnaliser

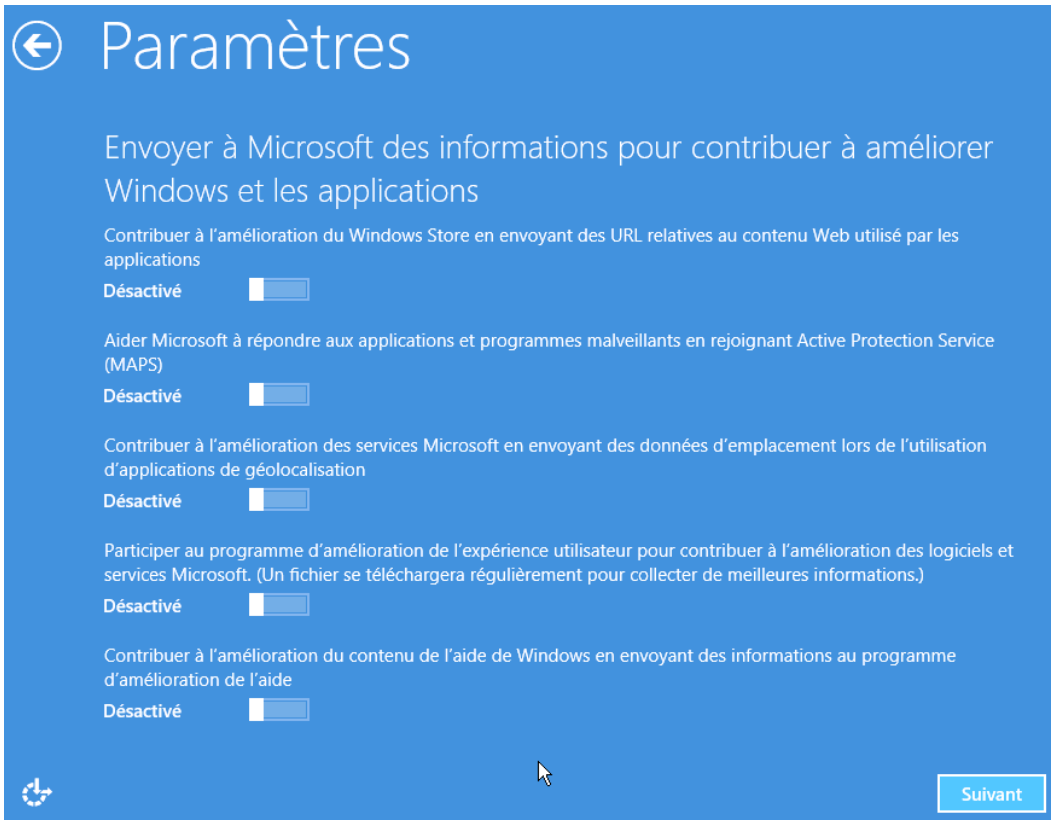
Profils Réseaux



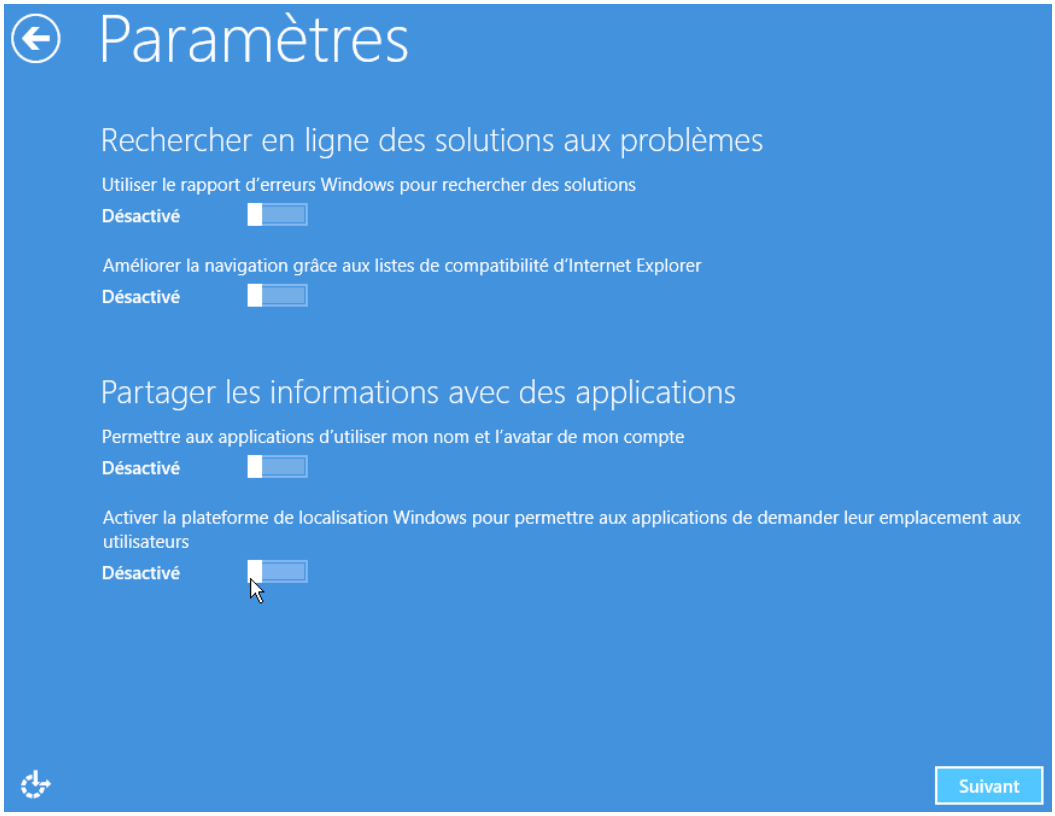
Mise à Jours Windows Update – Filtres IE



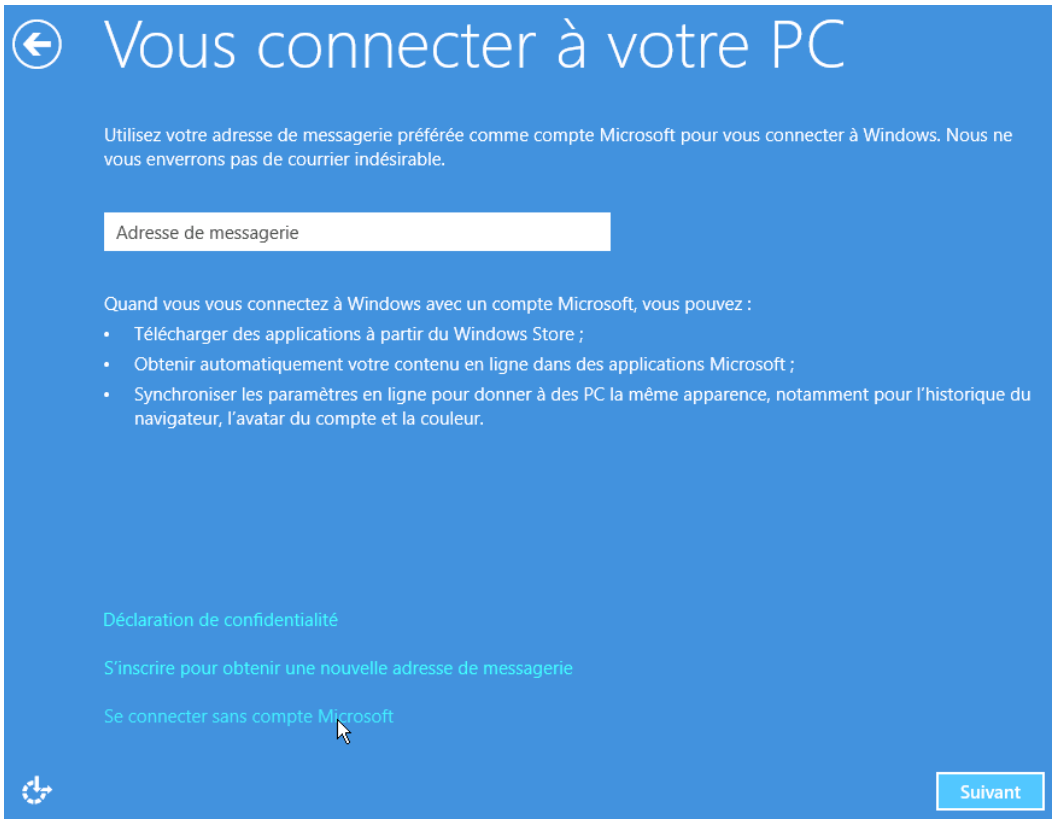
Aide Débugage Windows 8



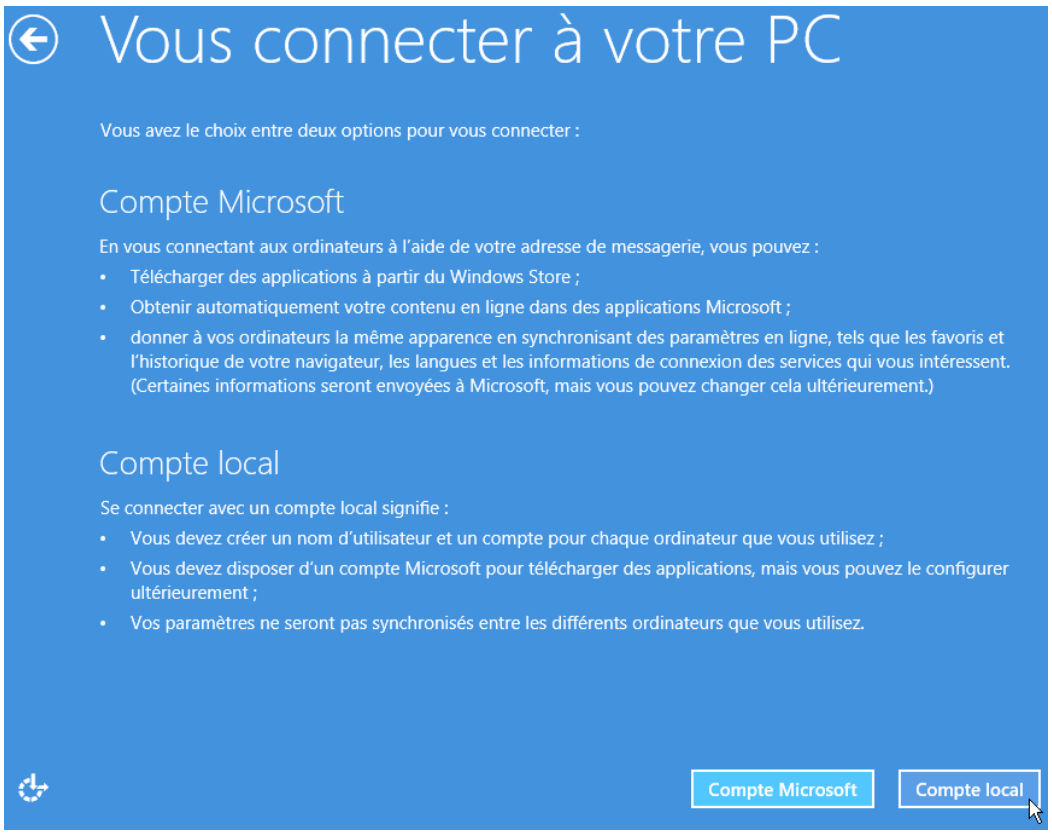
Compatibilité IE, Réseaux Sociaux, Géo-Localisation



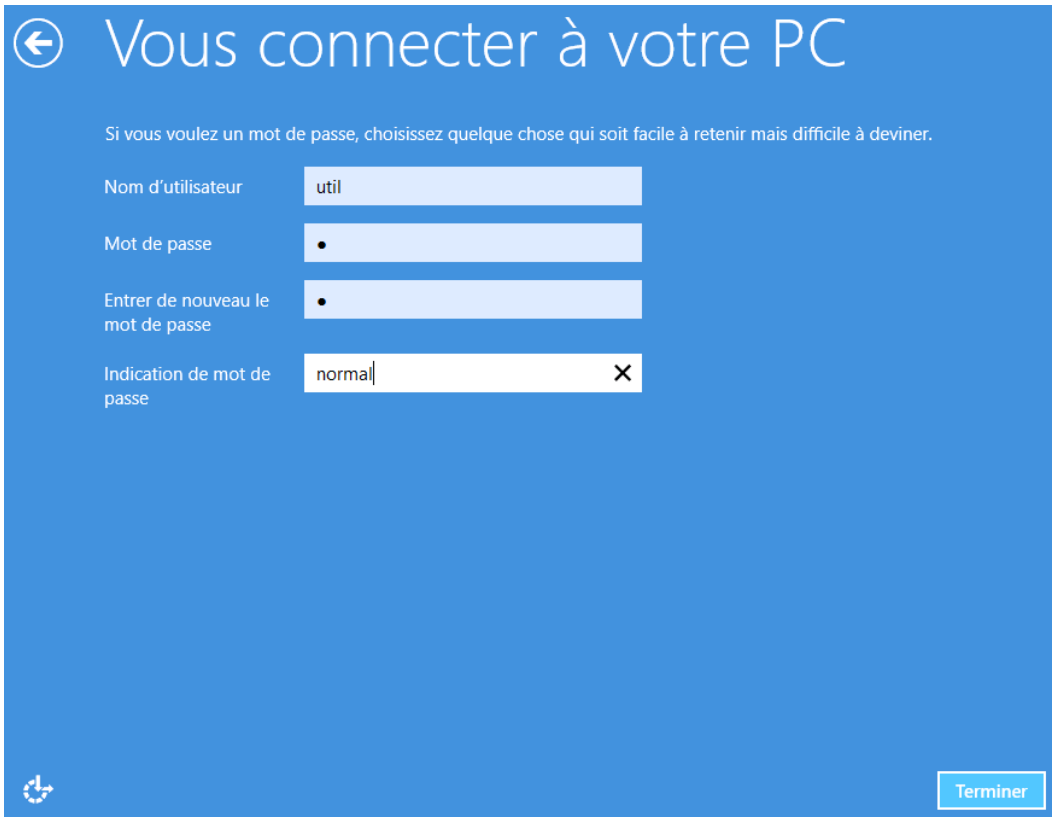
Email - Compte Local – Passeport Microsoft



On demande de se connecter sans compte microsoft



Création Compte Local



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

Et l'installation est terminée

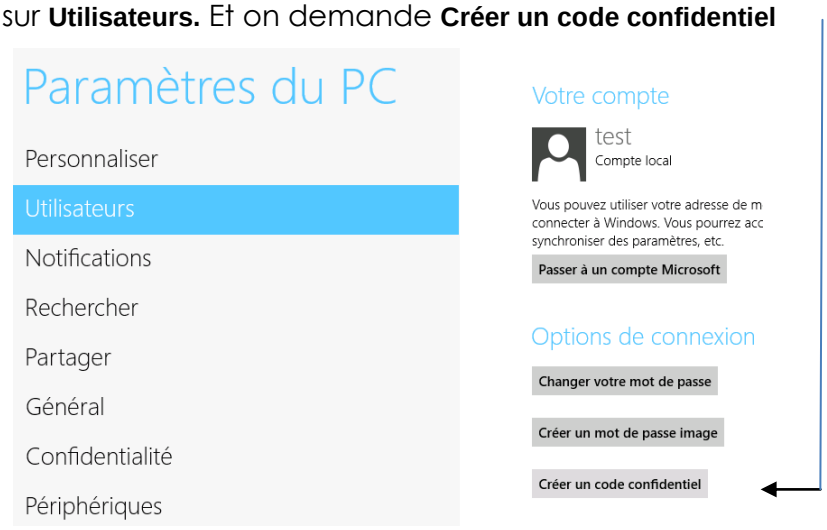
AUTHENTIFICATION WINDOWS 8

Par code confidentiel :

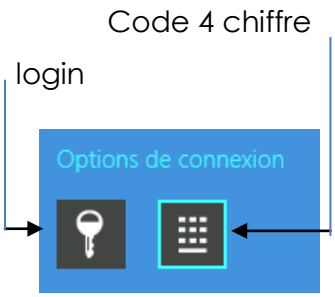
On saisit un mot de passe code à 4 chiffres ! C'est très peu sécurisé, à ne pas utiliser systématiquement !

Charm Bar / Paramètres, et **Modifier les paramètres du PC**

puis sur **Utilisateurs.** Et on demande **Créer un code confidentiel**



Lorsque Test va ouvrir une session, il verra des options de connexion disponibles

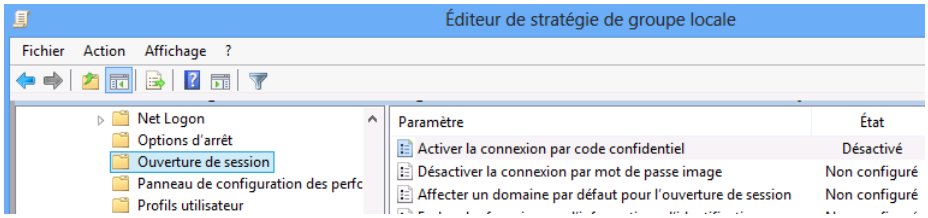


N.B : il est possible de désactiver cela dans pour les utilisateurs d'un domaine par une stratégie

C'est **Activer la connexion par code confidentiel** dans

Configuration Ordinateur\Modèles d'administration\ Système\Composants Windows

Ouverture de session

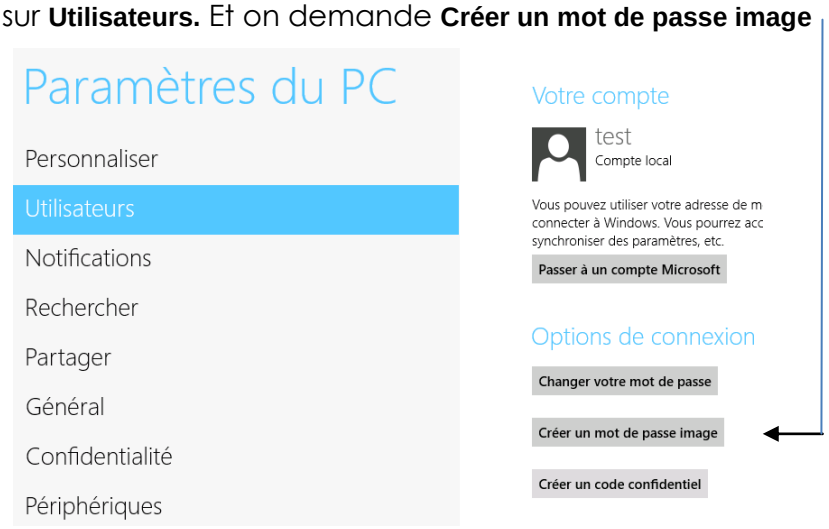


Par Tracé sur une image :

On mémorise une action à effectuer sur une image ! C'est peu sécurisé, à ne pas utiliser systématiquement !

Charm Bar / Paramètres, et **Modifier les paramètres du PC**

puis sur **Utilisateurs.** Et on demande **Créer un mot de passe image**



Il faut bien sûr choisir une image, puis effectuer les 3 gestes dessus…

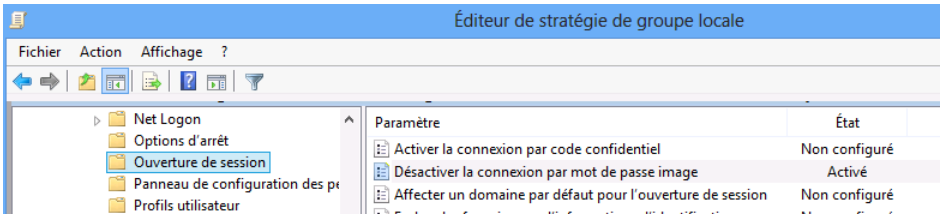
Lorsque Test va ouvrir une session, il verra des options de connexion disponibles

N.B : il est possible de désactiver cela dans pour les utilisateurs d'un domaine par une stratégie

C'est **Désactiver la connexion par mot de passe image** dans

Configuration Ordinateur\Modèles d'administration\ Système\Composants Windows

Ouverture de session



Login sur SAM ou AD :

Login Classique soit local (dans la Sam) soit sur l'AD.

Compte Microstore (non local) :

Grâce à son compte Microsoft, tel qu'un compte de messagerie Hotmail, l'utilisateur va ouvrir une session et retrouver ses propres paramètres et applications, ainsi que ses documents, depuis n'importe quel ordinateur pourvu de Windows 8. Ce service est basé sur le Cloud Computing …

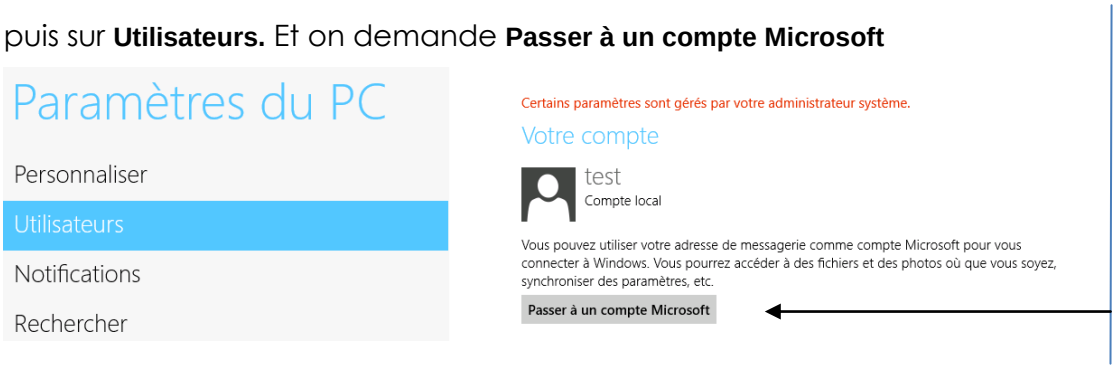
N.B : L'emplacement des données de l'utilisateur dans le nuage n'est pas connu de celui-ci.

L'authentification grâce à un compte Microsoft synchronise les éléments suivants :

- Applications téléchargées depuis Windows Store.
- Favoris, thèmes, préférences linguistiques.
- Mise à jour de votre réseau social Facebook, Hotmail, Twitter…Photos et autres fichiers stockés sur des services tels que SkyDrive, Flickr…

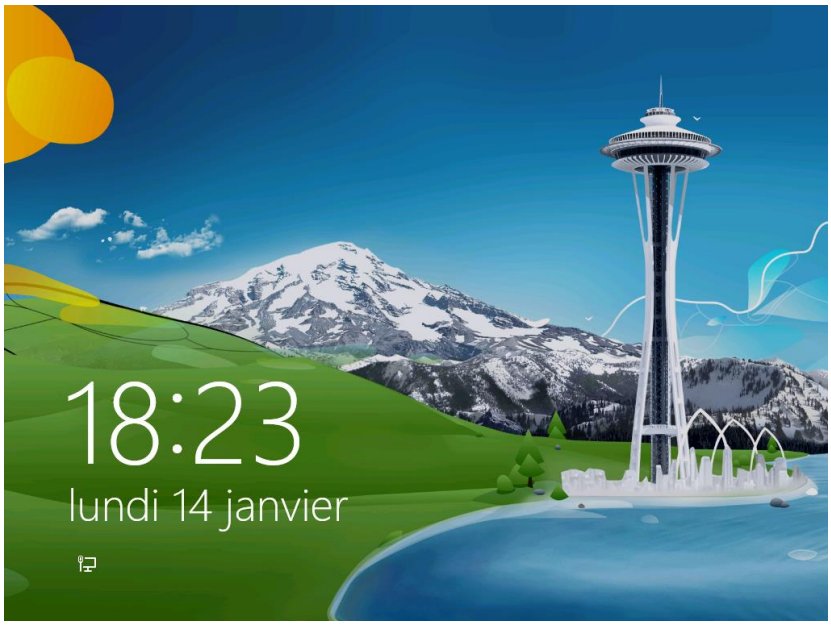
Charm Bar / Paramètres, et **Modifier les paramètres du PC**

puis sur **Utilisateurs.** Et on demande **Passer à un compte Microsoft**



Ecran de Verrouillage:

Il apparait lorsqu'aucune session inter-active n'est ouverte.



N.B : on peut choisir un autre fond, mais on ne peut rien « poser » dessus

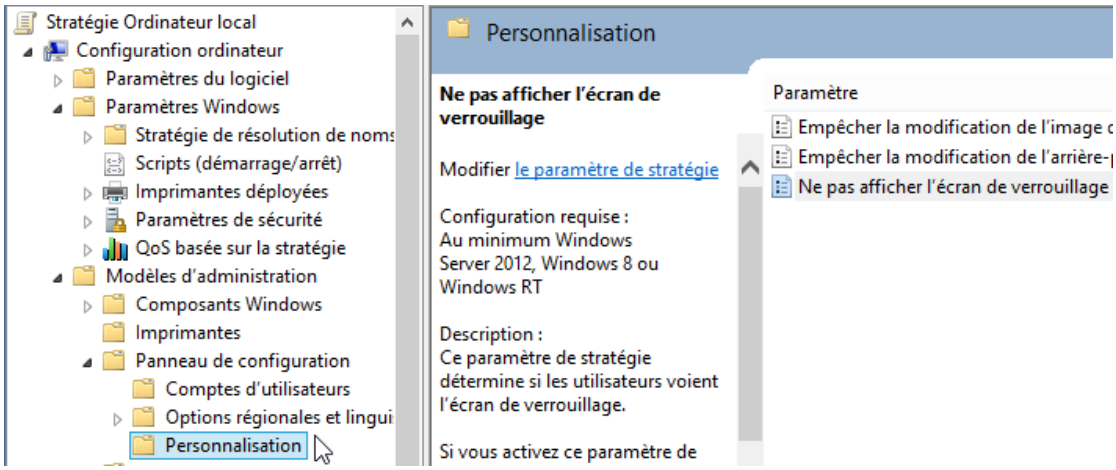
Via **Charm bar, paramètres, Modifier les Pamarètres du PC, Personnaliser**

Des que l'on s'est loggué On tombe sur l'écran d'accueil

N.B : si la désactivation de l'écran de verouillage est necessaire (car si on n'est pas ur une tablette, cela ne se justifie pas..) cel peut se gérer via les stratégies via **Gpedit.msc**

Configuration ordinateur / Modèles d'administration / Panneau de Configuration /Personnalisation

et on demande ne pas afficher l'écran de verrouillage…



Ecran d'accueil:

Il apparait lorsqu'une session inter-active est ouverte.

WINPE 4.0

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 basé sur le noyau de Vista, fut le précurseur

Windows PE 4.0 est basé sur le noyau de Windows 8 (Windows PE 3.0 était 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.

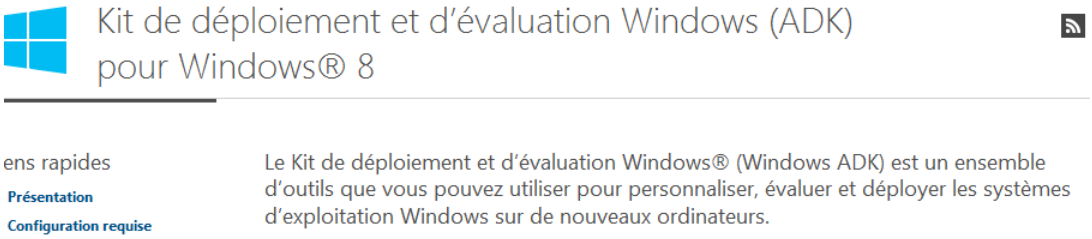
Windows PE 4.0 n'est pas uniquement destiné à l'installation de Windows, mais il peut être dissocié de ce dernier, et devenir à son tour un outil de dépannage et de diagnostic autonome !

Windows PE 4.0 intègre des drivers réseaux supplémentaires par rapport aux versions précedentes.

- Ce n'est pas une version Embedded de Windows (car il y a un reboot automatique toutes les 72h)

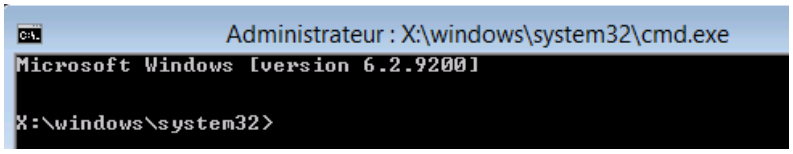
Il est possible de récupérer une copie de Windows PE soit :

- En l'extrayant d'un DVD d'installation de Windows 8
- En téléchargeant auprès de Microsoft un kit automatisé d'installation de Windows (**ADK**, pour **Assesment Deployement kit**)



Utiliser Windows PE lors de l'installation Seven:

Au démarrage apparaît l'écran qui vous accueille lorsque vous installez Windows 8, 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 Windows 8 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 Windows 8
2. Grâce à la très petite taille de l'environnement Windows PE 4.0, 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 de créer des partitions Fat ou 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
Ntdetect.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 »

Ntldr

Boot.ini

(fichier texte de choix options)

→ **Bootsect.dos (**Si autre OS que NT)

Ntdetect.com

Détection du matériel

Ntoskrnel

HAL

F8 + profils matériels

Chargement drivers (/SOS ds boot.ini)

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 hybernation 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 »

Bootmgr

décode le magasin en **\Boot\Bootstat.dat**

Winload.exe

(crée l'environnement d'execution pour SEVEN)

Détection hard HAL

F8+profils matériels

Appels drivers

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 »

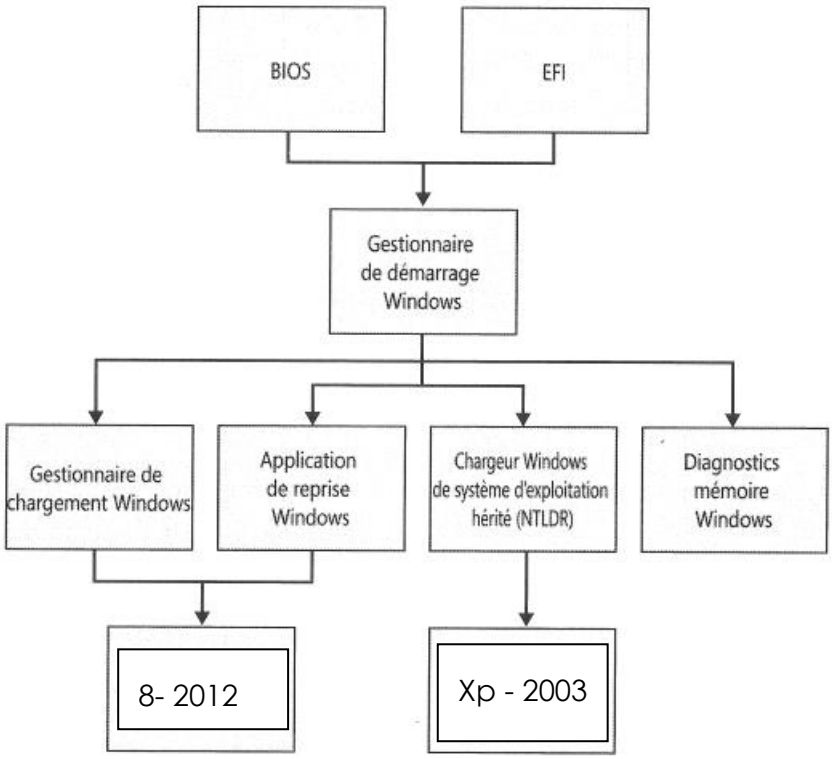
Bootmgr

décode les entrées du magasin en **\Boot\Bootstat.dat**

si Seven → si ancienne génération

Winload.exe	**Ntldr**
(crée l'environnement)	Boot.ini
(d'execution pour SEVEN)	(choix lignes ARC)
	Ntdetect.com
Détection hard	Détection hard
HAL	HAL
F8+profils matériels	**F8**+profils matériel
Appels drivers	Appels drivers

Ce qui au final, avec les outils de récupération 8/Seven et de diagnostic mémoire, pourrait donner le schéma suivant :



BOOT WINDOWS 8

Boot Windows 8 – abandon F8 :

Avec un processus de démarrage complet qui prend seulement quelques secondes, les différentes étapes composant la séquence de démarrage s'enchaînent trop rapidement pour que vous puissiez les remarquer (et a fortiori pour que vous puissiez les arrêter). La plupart des décisions influant sur le déroulement du démarrage sont prises au cours des deux ou trois premières secondes. Ensuite, le démarrage consiste simplement à accéder à Windows le plus rapidement possible. Ce délai de deux à trois secondes inclut le temps nécessaire à l'initialisation du microprogramme et à la phase POST (moins de deux secondes)

Les problèmes rencontrés avec la touche **F8** s'appliquent également aux autres touches pouvant s'avérer utiles au cours du démarrage

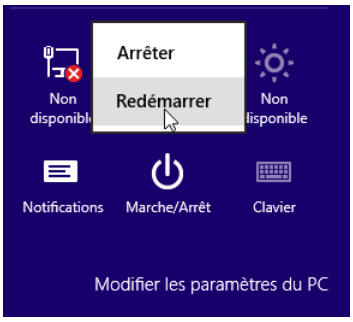
Pour résoudre ces problèmes, le **Menu Options de démarrage** rassemble toutes les possibilités, il contient tous les outils de dépannage, les méthodes d'accès à la configuration du BIOS, ainsi qu'une méthode simple permettant de démarrer sur d'autres dispositifs de stockage, par exemple des lecteurs USB.

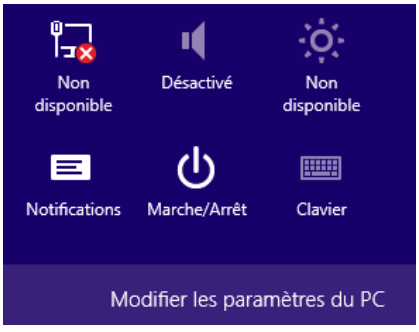
Méthodes accès au menu de démarrage:

1. Windows 8 à des comportements automatiques qui affichent automatiquement le menu des options de démarrage chaque fois qu'un problème susceptible d'empêcher le PC de démarrer correctement sous Windows se pose.

2. Appel via la **Charm bars / Paramètres**

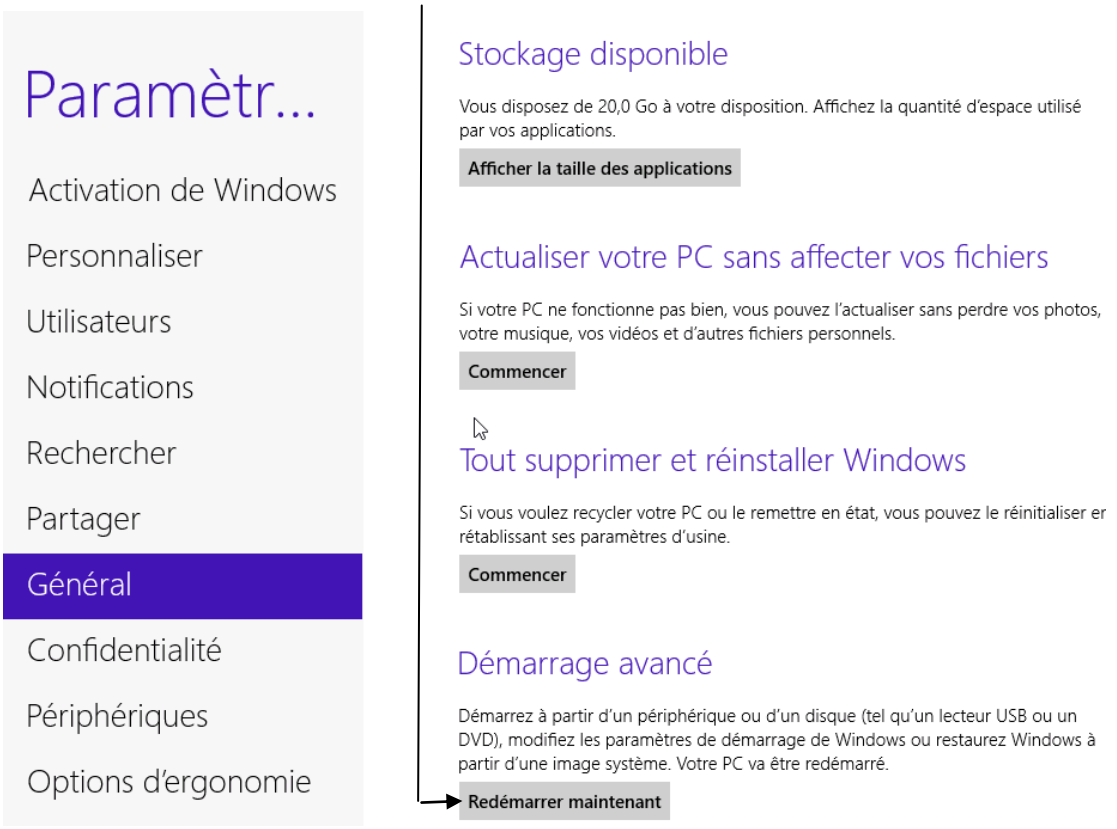
soit on redémarrer le poste en tenant la touche **MAJ** appuyée… + **Redémarrer**





Soit on demande **Modifier les paramètres du PC**

Puis dans **Général** on choisit **Redémarrer maintenant**



3. Appel en invite de commande **shutdown**

l'outils en invite de commande **shutdown avec l'option /r/o**

Shutdown /r /o arrêt immédiat

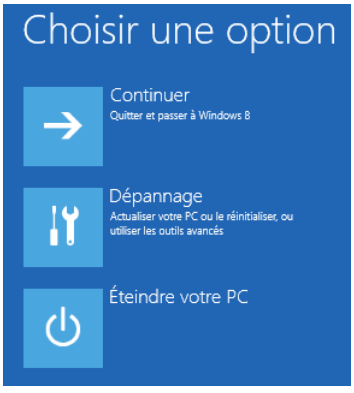
```
C:\Users\Administrateur>shutdown /r /o_
```

Ou encore mieux

Shutdown /r /o /f /t 0

Menu Options de démarrage:

Les 3 options de bases toujours présentes sont



Continuer : Si on est ici par inadvertance (ou que le comportement automatique de 8 nous y amène), mais que l'on ne souhaite rien faire,

Dépannage : C'est lui qui nous intéresse

Eteindre : Toujours la logique du démarrer / arrêter

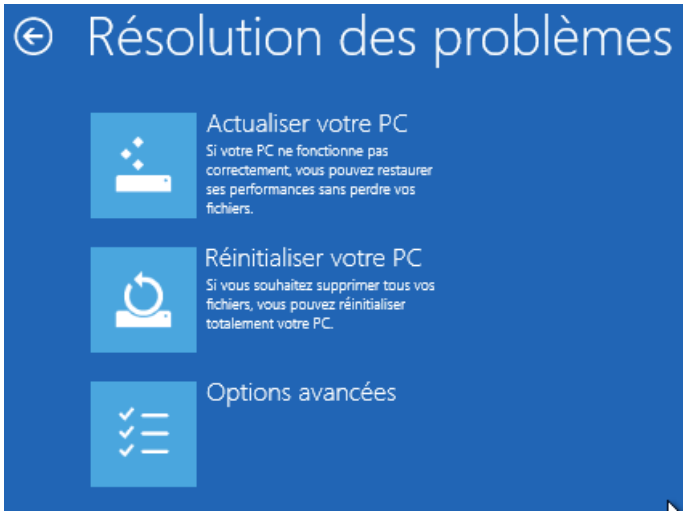
N.B : à noter que selon les cas, Multi-Boot, Boot sur UEFI, on peut avoir d'autres entrées présentes à ce niveau (notamment le choix du périphérique de boot)

Menu Options de démarrage - Dépannage:

C'est lui qui permet l'accès à toutes les manipulations

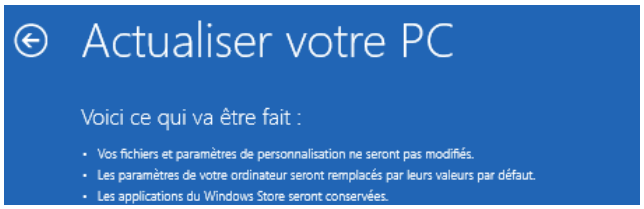
donne accès à la

Résolution des problèmes

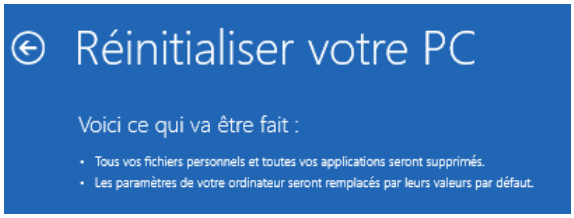


Si deux nouvelles fonctionnalitées « automatiques » apparaissent :

Actualiser votre PC et



Réinitialiser votre PC



On re-trouve avec les **Options Avancées** (déjà présentes sous Seven via WinRe)

Restauration du système

Ce sont les Point de Restauration

Récupération Image Système

Si on a fait 1 sauvegarde « image »

Réparation automatique comme seven l'algorithme de WinRe

Invite de Commande

C'est la Console de Récupération WinPe 4.0

Paramètres

Ex **F8** avec les options lors du re-démarrage

BCDEDIT

BCDEDIT et gestion du magasin :

La branche de la base de registre **BCD,** stockée dans **bootstat.dat**, contient un menu de démarrage et toutes les informations concernant les systèmes d'exploitation. L'ensemble des valeurs qui sont stockées dans cette branche prend le nom de "**magasin**", toujours stockée en **C:\BOOT\BCD**.

N.B: Si on a une partition cachée, le dossier **\BOOT** se trouvera dedans… il est possible de faire afficher la partition cachée en lui "assignant" une lettre", mais on ne pourra plus en standard la "re-cacher"…

Ce magasin ne peut se visualiser qu'avec la commande

bcdedit ou **bcdedit /enum** ou encore

bcdedit /enum all

Sauvegarde du magasin complet :

Une bonne précaution à prendre, consiste à faire une sauvegarde du magasin, avant de tenter des manipulations. Pour faire une sauvegarde du magasin (ici dans un dossier **c:\boot-back** crée au préalable) il faut faire

bcdedit /export <chemin> comme dans

```
C:\>bcdedit /export "c:\boot-back\testbcd"
Opération réussie.
```

et pour le récupérer il faut lancer

bcedit /import <chemin> comme dans

```
C:\>bcdedit /import "c:\boot-back\testbcd"
Opération réussie.
```

Reconstruction du Magasin :

En cas de gros problème on peut toujours tenter une reconstruction complète du magasin via la commande **bootrec /rebuildbcd** de la console de récupération

```
X:\windows\system32>bootrec /rebuildBcd
Recherche d'installations Windows sur tous les disques.

Veuillez patienter...
```

A éviter tout de même…

Structure du magasin:

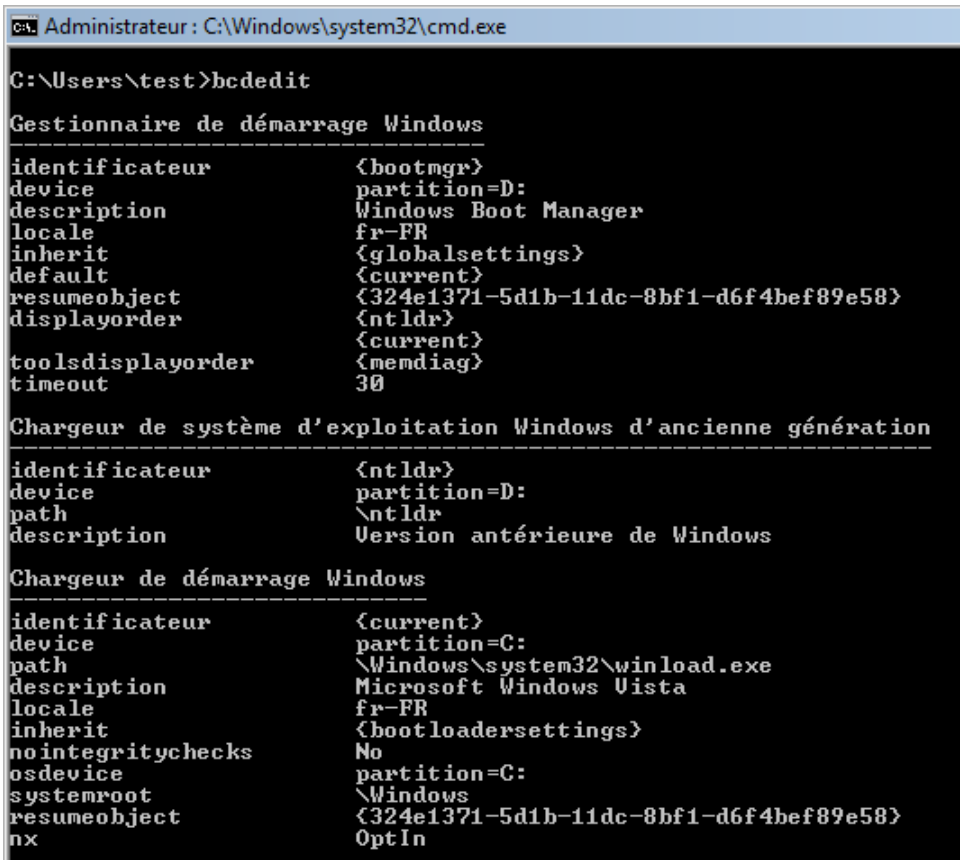
Section Gestionnaire de démarrage :

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 8-Seven-2012-2008 installée



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

- **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 8-Seven, stocké dans \Windows\system32)

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

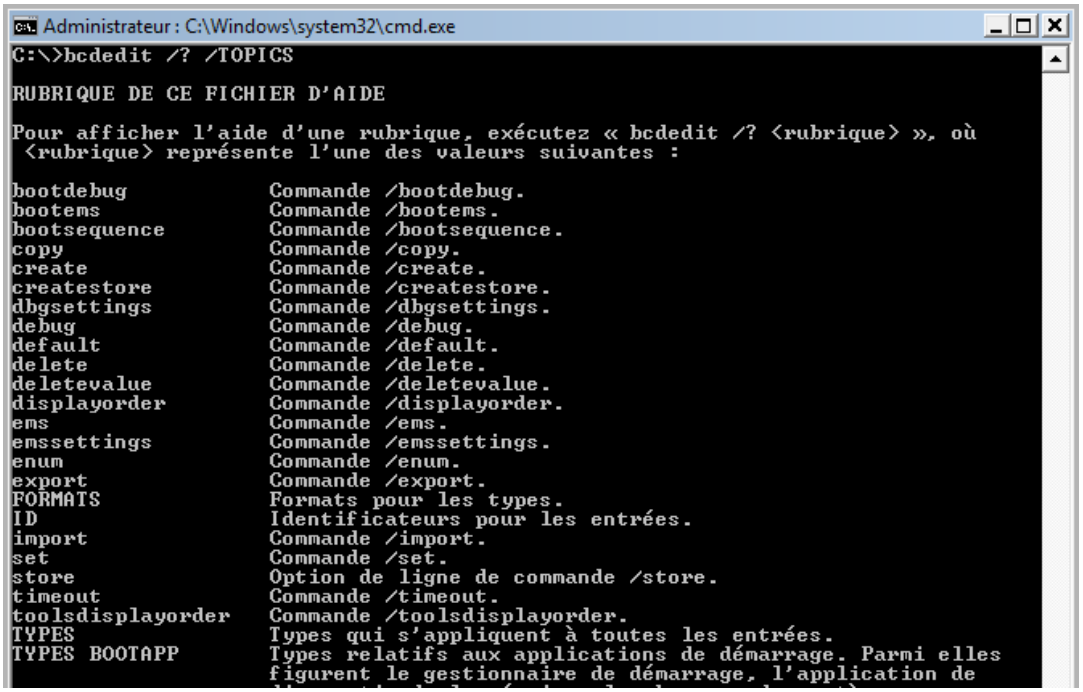
N.B: s'il y a plusieurs installations de 8-SEVEN alors on aurait plusieurs sections **Chargeur de démarrage Windows** avec comme identificateur des GUUID du genre `{cbd971bf-b7b8-4885-951a-fa03044f5d71}` contenant notamment les éléments : **Device – Path – Description – Osdevice - Systemroot**

BCDEDIT commande :

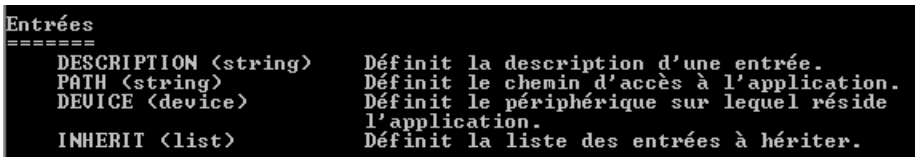
Une aide en ligne est disponible via

Bcdedit / ?

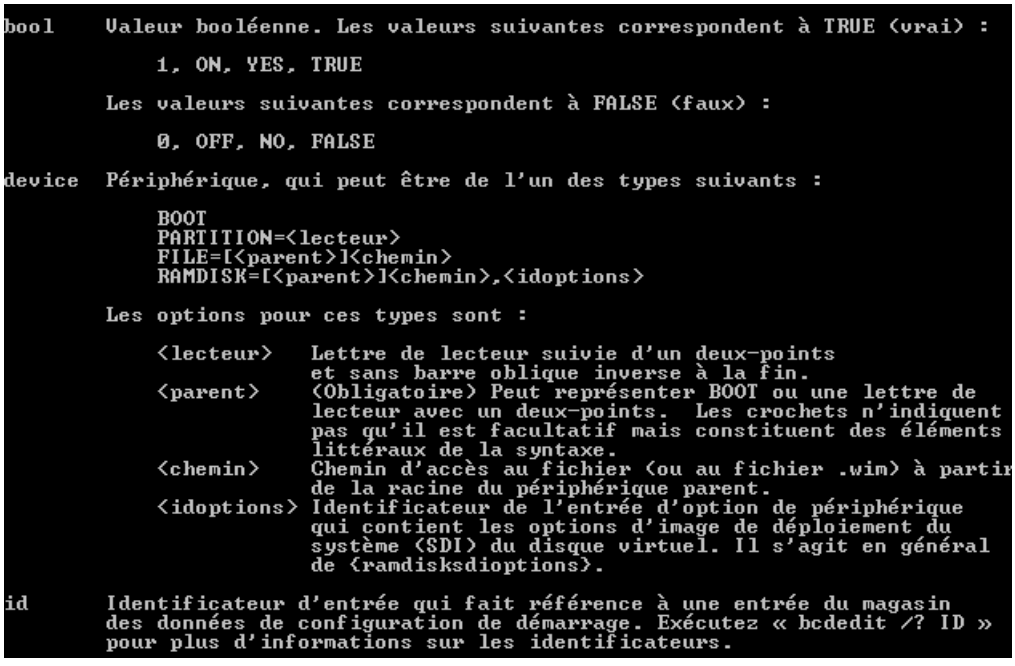
et les commandes sont nombreuses :



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



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



Copier-Dupliquer une entrée du magasin:

Dans notre magasin, avant de modifier l'entrée de Windows 8-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 généré

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 ou 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 qu'un GUUID. 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            {6900ba1b-1c65-11df-9c4e-9f716fb9c591}
displayorder            {current}
                        {6900ba1f-1c65-11df-9c4e-9f716fb9c591}
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

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

- cette entrée existe toujours,
- et elle est dupliquée pour chaque installation de 8 Seven ou Serveur 2008, dans ce cas elle n'est pas identifiée par **{current}** mais plutôt par un **{xxxguuidxxx}**

```
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.
```

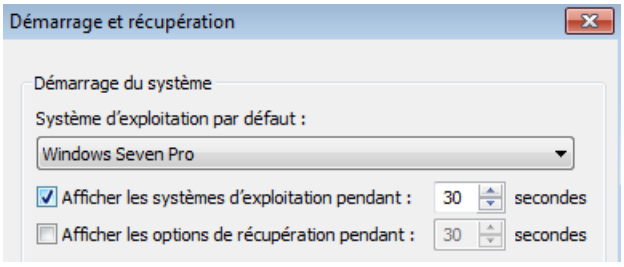
N.B : Pour nous ici, s'il s'agit de renommer l'entrée de notre Seven actuel (en cours), <id> pourra prendre la valeur absente, car cela vaudra **current** ! L'écriture simplifiée pourrait être

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 Boat 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
```

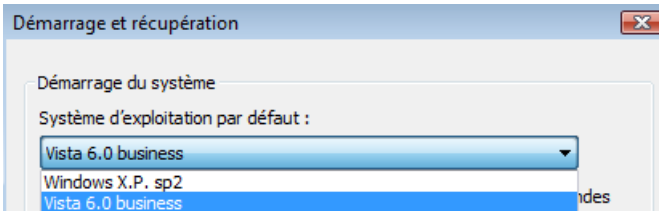
donc <id> devra prendre la valeur **{ntldr}**

```
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 **\boot.** Il est également disponible dans le kit **Adk** de microsoft

l'utilisation de cet utilitaire permet de faire face, soit depuis la **console RE** de 8-Seven, soit depuis la **console de récupération** XP… à une perte de l'amorçage selon le système voulut dans la MBR…

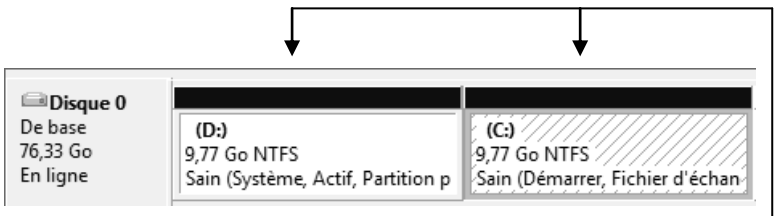
Installer Windows 8 à coté de XP (multi-boot)

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 Windows 8 dans une autre partition principale (voire un autre disque), ayant au mois 12 Giga de libre
  Il n'est plus possible de faire cohabiter Windows 8 et Xp dans une même partition.
- Il faut booter sur le CD de Windows 8 (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 Windows 8 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 :



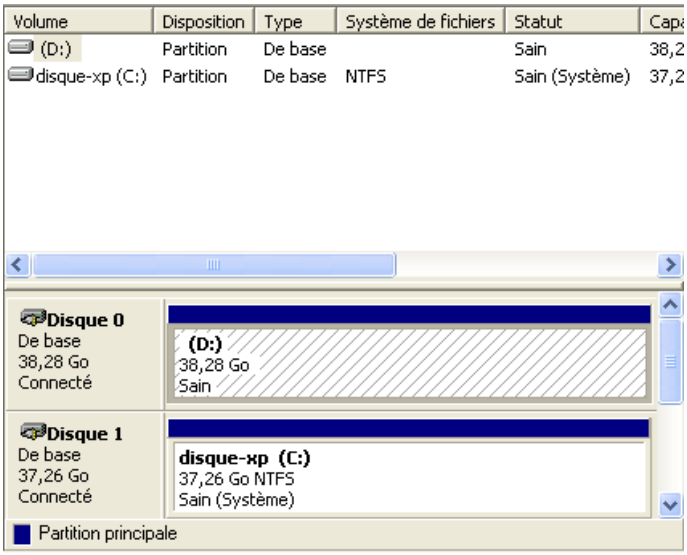
Le résultat fonctionne, la partition active est inchangée ! (mais le lettrage est modifié dans Windows 8 qui se trouve en C : et la partition principale active passe en D :…)

- ✓ Ce qui amènera aussi également la présence sur D : du dossier **\boot** et du fichier **bootmgr** (qui se stockent sur la partition active…)
- ✓ le lecteur de Windows 8 est déclaré en C :

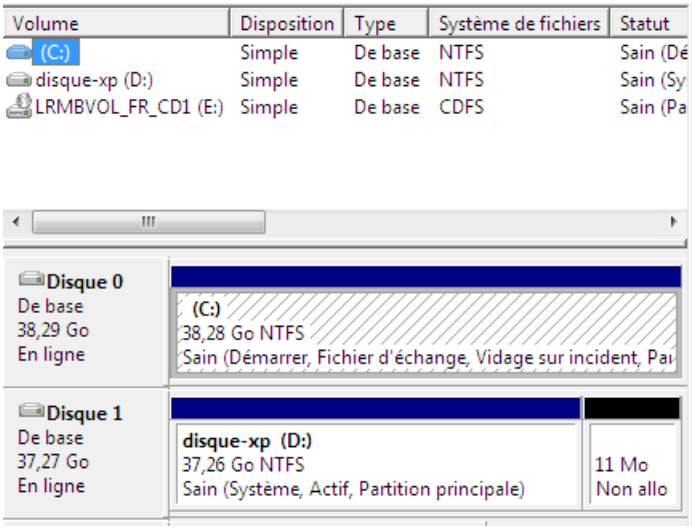
autre disque :

Ce sera sans doute le cas le plus fréquent.

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



Le résultat fonctionne, la partition **active** est inchangée ! (mais le lettrage est surprenant dans Windows 8 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 **\boot** et du fichier **bootmgr** (qui se stockent sur la partition active…)
- ✓ Le lecteur de Windows 8 est déclaré en C :

Installer XP à coté de Windows 8

Si vous voulez installer une version antérieure du système d'exploitation Windows sur un ordinateur Windows 8, c'est beaucoup plus complexe, et non garantit 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 8.

Supprimer un boot Seven (retour boot Xp):

Sur une machine Multi-Boot XP – Windows 8 comme crée précédemment, on souhaite ne pas garder Windows 8 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 Windows 8

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 8.
   (Le dossier **\Boot** figure sur le Média Windows 8.)

2. Redémarrez l'ordinateur
   et donc uniquement Xp apparaît au boot.

3. Supprimer la partition sur laquelle Windows 8 était installé

4. Faire le ménage des fichiers amenés par Windows 8 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 boite 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 :

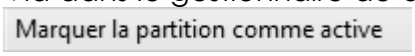
xcopy D:\Boot C:\Boot /c /h /o /s /e **(copie de tout le dossier)**

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

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 WINDOWS

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 nommé **Bootmgr**.

Séquence démarrage Bootmgr

3 étapes

« Séquence POST »

Bootmgr avec le magasin **\Boot\Bootstat.dat**

si Windows 8 / 7

Winload.exe

(crée l'environnement)

(d'execution pour SEVEN)

si XP – 2000 - NT

Ntldr

Boot.ini

(choix lignes ARC)

Ntdetect.com → **Bootsect.dos**

(autres)

(Win 9x et DOS)

Ntoskrnel Détection hard **HAL**

F8+profils matériels (si présent)

Appels drivers (/SOS ds boot.ini)

Smss.exe (gestionnaire de session)

Lance Win32 (affiche la barre de progression)

Lance les services en Boot-execute

Winlogon.exe

Gestion LSA

Lsass.exe (gestion CTRL-ALT-SUPPR)

Screg.exe

Derniers services à démarrer

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

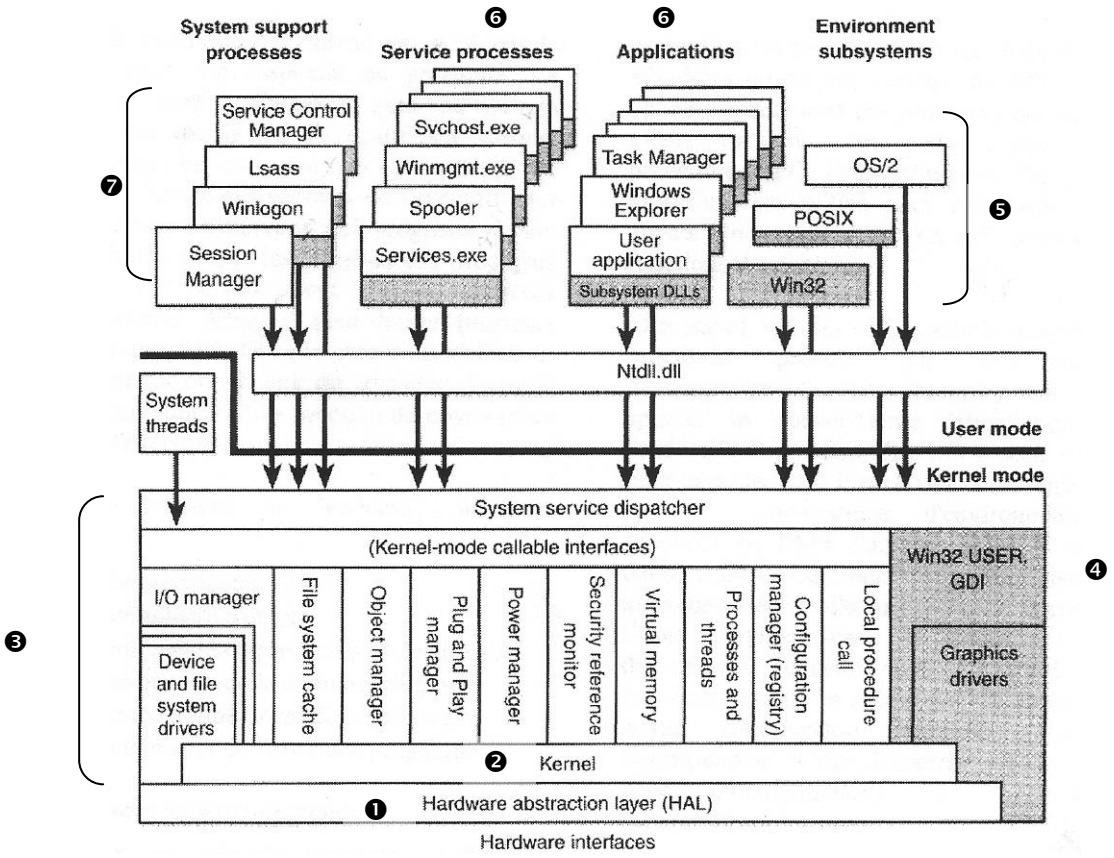
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

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

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

Vocabulaire système sous 8-SEVEN :

Schématiquement on peut distinguer :

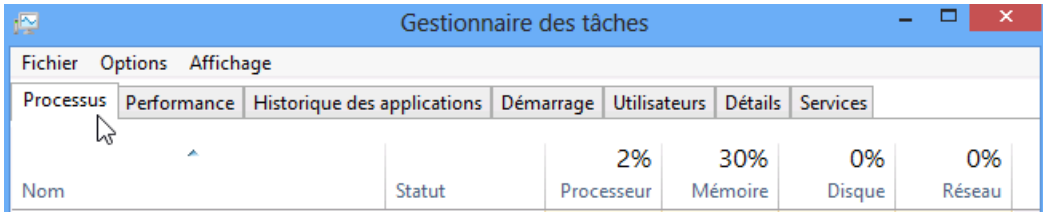


- LA **HAL** ❶ou couche d'abstraction matérielle : fournie des fonctions pour contrôler le bus système, canaux DMA, déclenchement des interruptions, horloge système… toutes ces fonctions sont utilisées dans les autres parties du noyau
- Le **Kernel** ❷ (micro kernel) : c'est le noyau toujours en mémoire,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

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

Lister les Processus - graphique:

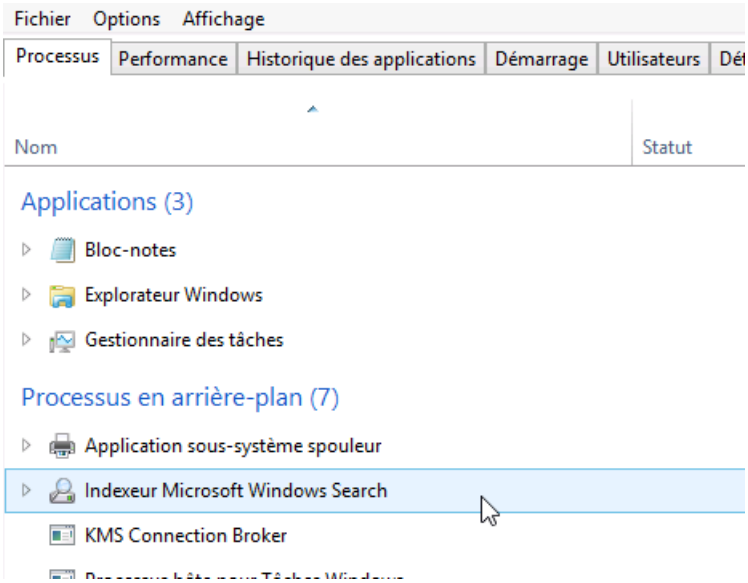
Appelable via **CTRL+ALT+SUPPR** ou via les propriétés de la barre des tâches, le **Gestionnaire des tâches** donne une vision plus complète de la chose !



Plusieurs onglets sont disponibles, l'onglet **Processus** regroupe

Des Application :

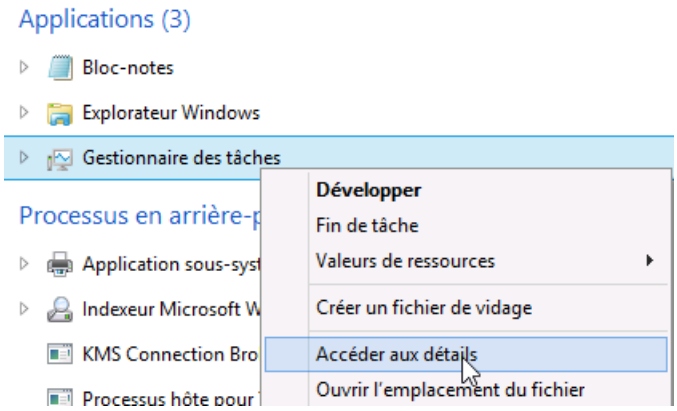
Programme lancé par l'utilisateur, ou lancé automatiquement au démarrage de Windows. Tourne dans une interface fenêtre, normalement sans incidence sur le fonctionnement de Windows 8



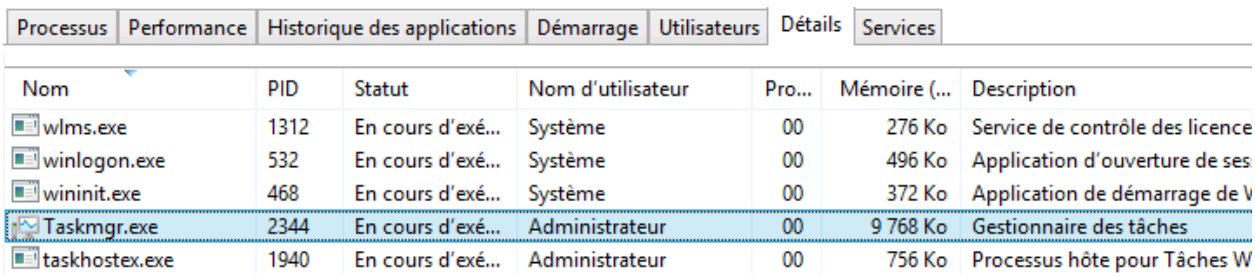
Des Processus :

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

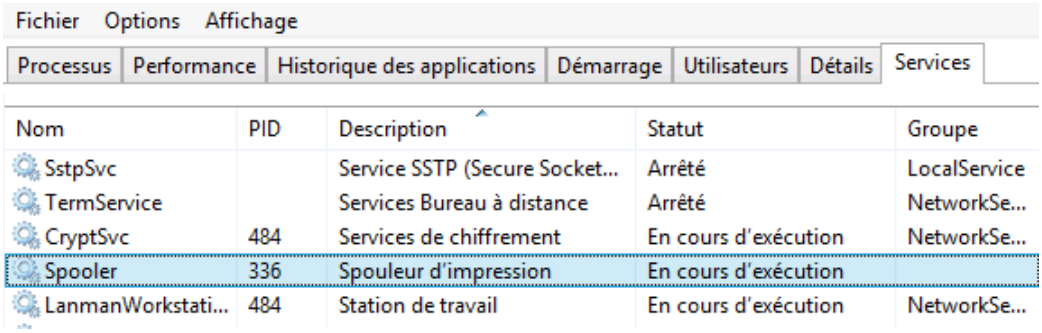
Depuis un processus on peut demander vie le menu contextuel **Accéder aux Détails** pour voir si un executable précis correspond



Donnant dans l'onglet **Détails** le positionnement sur le Processus en Cours avec son **PID**

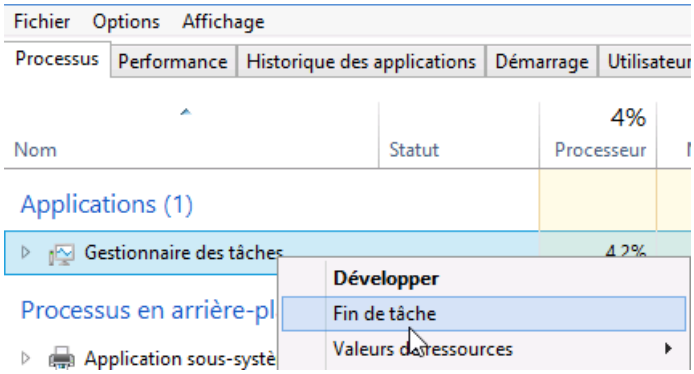


l'onglet **Services :** regroupe les Programmes géré par le système d'exploitation comme "partie intégrante du système". Un service est caractérisé par le fait qu'il peut se gérer via le gestionnaire de service Windows, et est lancé dans un processus, souvent associé avec d'autres services.

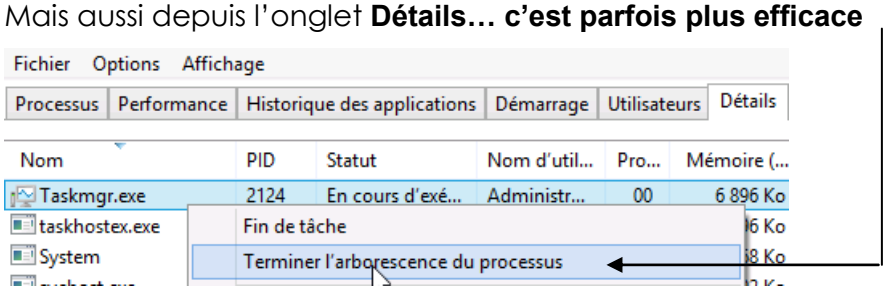


Arrêter un Processus, un service :

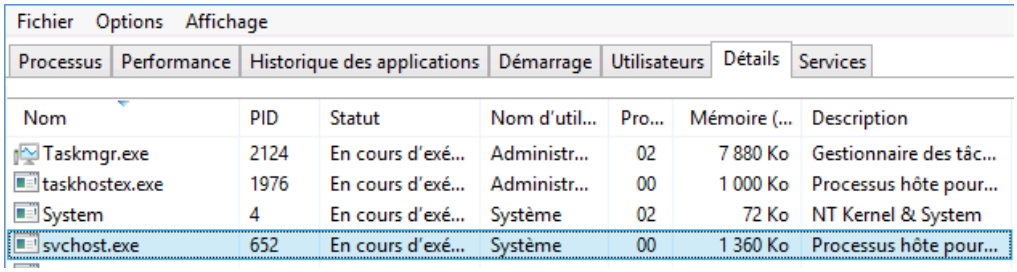
Cela peut se faire soit depuis l'onglet **Processus**…



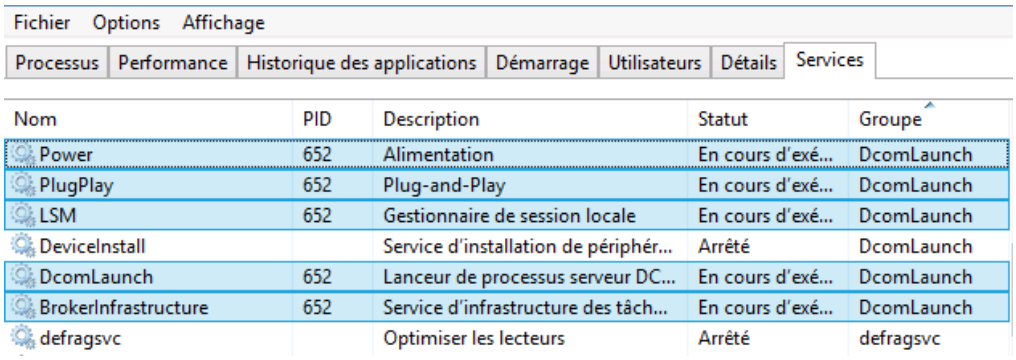
Mais aussi depuis l'onglet **Détails… c'est parfois plus efficace**



depuis l'onglet **Détails**… on peut accéder aux services



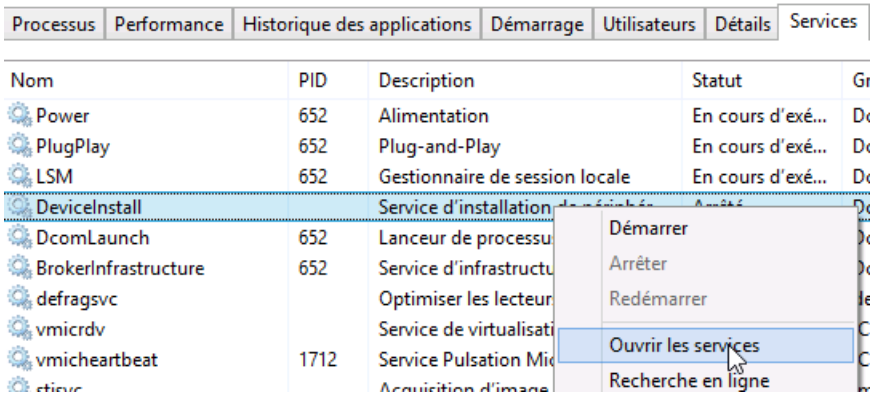
Ainsi souvent un processus générique **svchost** intègre comme son nom le laisse supposer plusieurs services



Dans l'onglet **Services** on peut

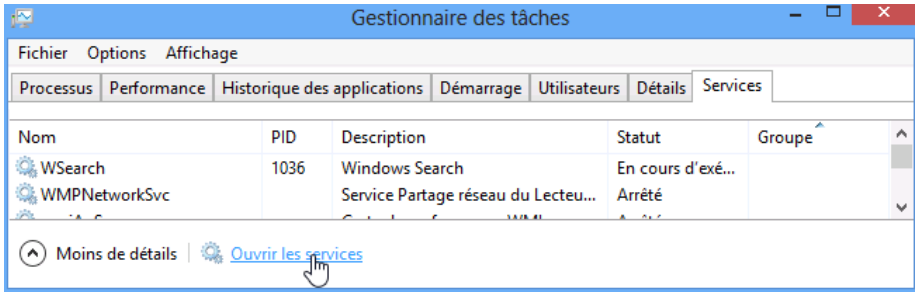
Arrêter/Démarrer un service: selon son état

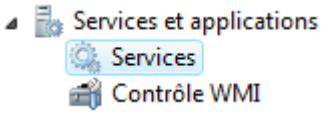
Et accéder à la gestion des services **via Ouvrir les services…**



Gestionnaire de Services

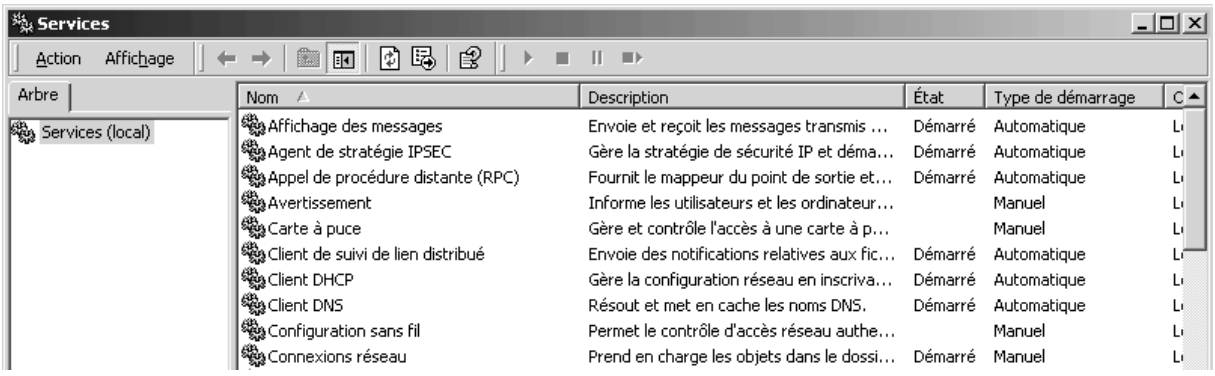
Accessible via le **gestionnaire des tâches**, bien sûr **Ouvrir les services**



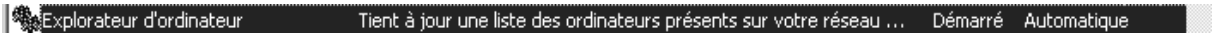


mais aussi Clic droit - **Ordinateur / Gérer / Services**

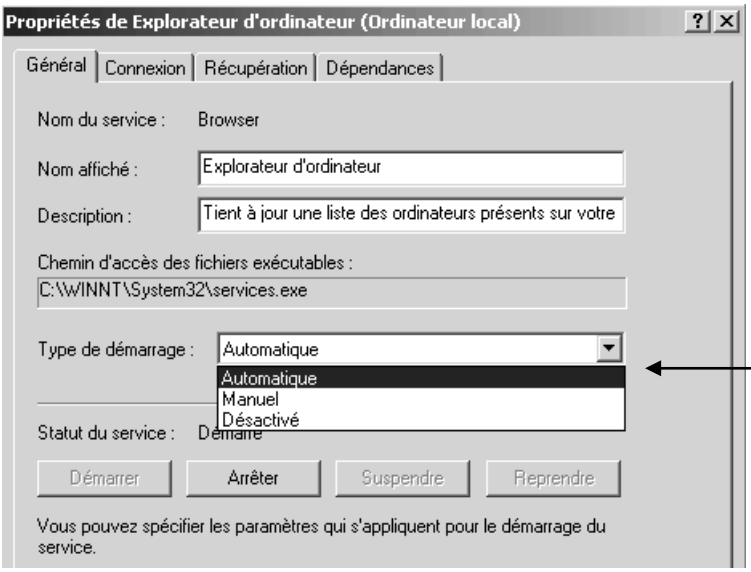
Ou **Panneau de configuration / Outils d'administration /**



Pour un service particulier

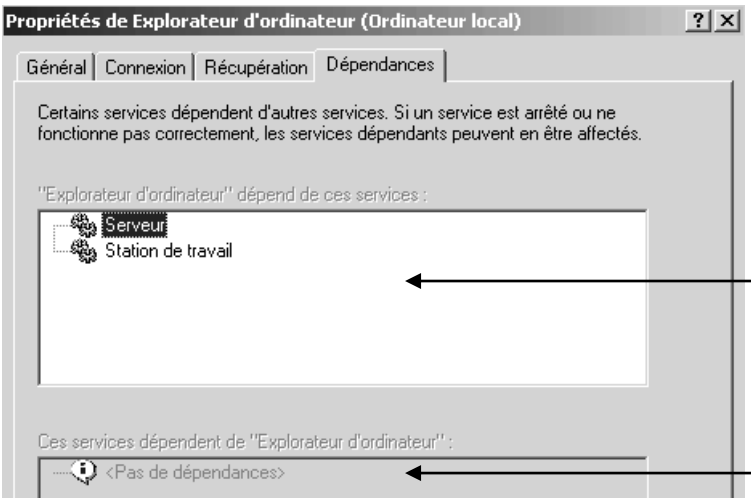


on peut demander via les propriétés



Essentiellement pour le prochain démarrage du poste

et on peut avoir une idée des dépendances…



De qui ce service dépend…

Qui dépends de ce service…

Lister les Processus – invite de commande:

Tasklist (SEVEN - XP):

Cette commande porte pas mal de zone d'ombre…

Tasklist

```
C:\Documents and Settings\Administrateur>tasklist /?

TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]
         [/M [module] | /SVC | /V] [/FI filtre] [/FO format] [/NH]
```

Si ces options fonctionnent, les autres options ont l'air plus délicates à utiliser…

Tasklist /SVC Tasklist /M

Taskkill (depuis SEVEN - XP):

Cette commande aussi porte pas mal de zone d'ombre…

Taskkill

Si ces options fonctionnent, les autres options ont l'air plus délicates à utiliser…

Taskkill /PID x

Et

Taskkill /PID x /F

Et

Taskkill /PID x /F /T

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 a son tour **Crss.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** a 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

anciens types 2000 - wdm :

Windows 2000 – wdm

Introduit le nouveau modèle de contrôleurs de Windows fondés sur Windows Driver Model (**WDM**)

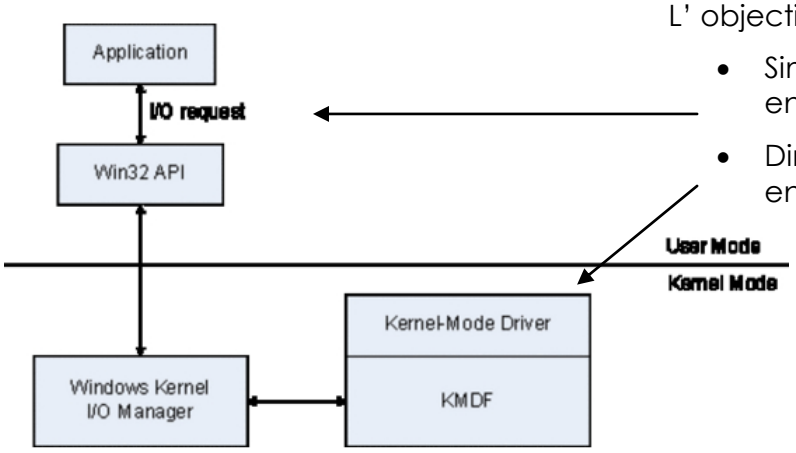
Pour communiquer avec le système, le pilote passe par une interface que l'on appelle communément **device-driver interface** ou **DDI**. De même, ces DDI sont très proches du noyau et leur modification implique souvent une recompilation des pilotes les utilisant. Ces DDI sont critiquées par les développeurs 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 WDF :

Depuis Vista, à 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



L' objectif est double :

- Simplifier l'écriture des drivers en **User Mode**
- Diminuer le nombre de drivers en **Kernel-Mode**,

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 User Mode, ils se retrouvent un peu dans le cas d'un programme et n'ont accès qu'à l'espace mémoire qui a été alloué à leur processus. Un plantage du pilote ne corromp plus l'ensemble du système, qui pourra redémarrer le pilote comme un programme utilisateur.

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

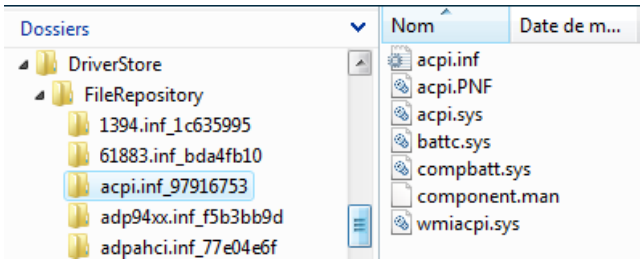
Depuis SEVEN, il existe deux étapes distinctes

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 Windows 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 Windows 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**,
- En modifiant l'image via l'utilitaire **DISM** des outils de déploiement **WAIK-ADK**
- En les déployant avec **WSUS**
- 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 Windows 8

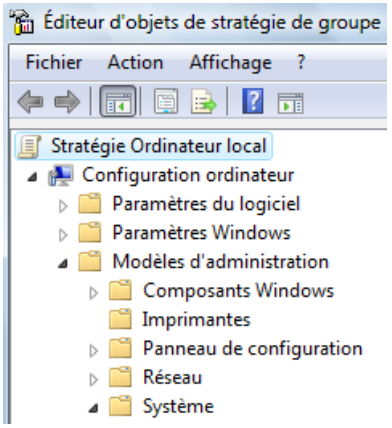
1. on connecte le périphérique
2. le service Plug and Play le détecte
3. Windows 8 cherche le pilote dans le magasin, si un pilote est présent, il installe le périphérique sans autres formes de procédure.
4. Si un pilote n'est pas présent, Windows cherche dans les chemins fournis MAIS vérifie que l'utilisateur 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 :

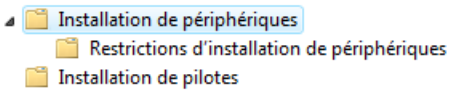
Comme désormais il est possible d'installer potentiellement un périphérique sans avoir de Droits élevé, de nouvelles **Stratégies** sont disponibles dans

gpedit.msc… Puis

Configuration ordinateur \Modèles d'administration\Système



Deux entrées nouvelles



Drivers certifiés :

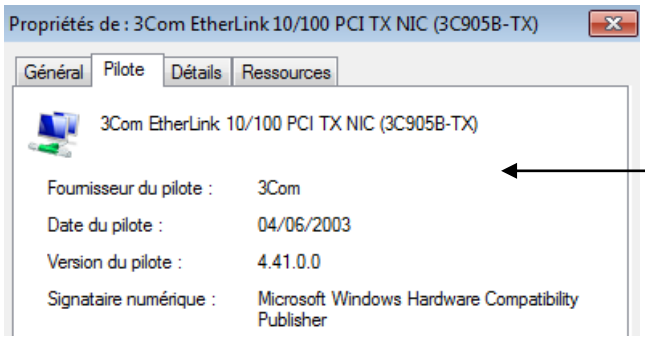
La signature numérique indique qu'un pilote ou fichier précis a atteint un certain niveau de test et qu'il n'a pas été modifié - endommagé - ou remplacé par le processus d'installation d'un autre programme.

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

Les fichiers des pilotes de périphériques et du système d'exploitation fournis nativement avec Windows 8 ont une signature numérique Microsoft.

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

Windows accepte par défaut uniquement des pilotes certifiés, mais pas forcément conçus pour lui ! (Certifié ne veut pas dire développé pour…)



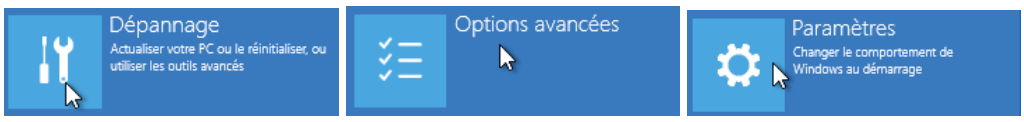
Voici un driver accepté par Windows datant de 2003 !

Il est signé …

Installation de pilotes non certifiés :

Soit une machine Windows 8 sur laquelle on ouvre une session en **mode sans Echec**, donc via le Menu des Options de démarrage , **MAJ+Redémarrer**

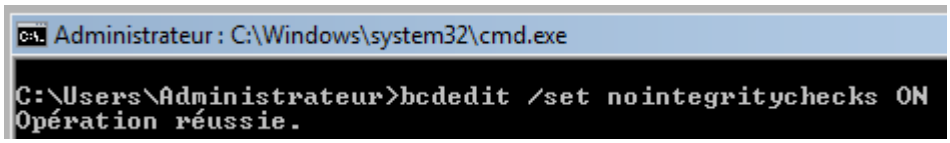
/ Dépannage / Options Avancées / paramètres / F7



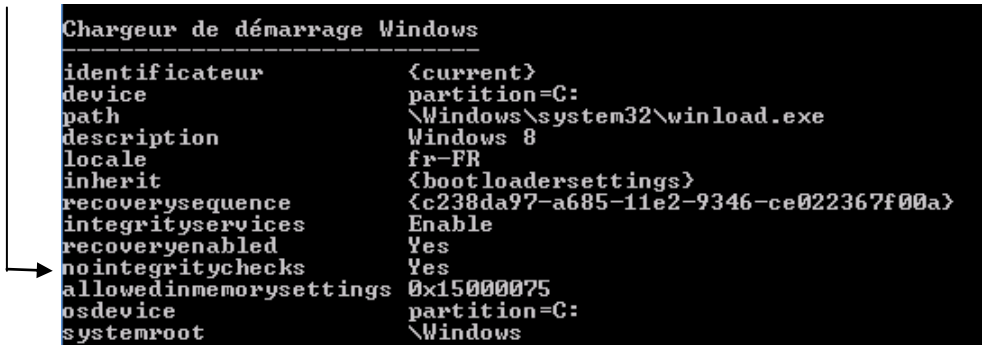
Puis **F7 - Désactiver le contrôle obligatoire de signature des pilotes**

Soit en invite de commande

Bcdedit /set nointegritychecks ON



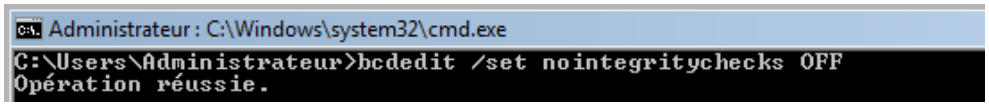
Ce qui aura pour effet de modifier le magasin de manière à avoir



Puis redémarrage, et installation du driver non signé…

Pour re-protéger ensuite le système il faut

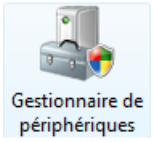
Bcdedit /set nointegritychecks OFF



et redémarrage

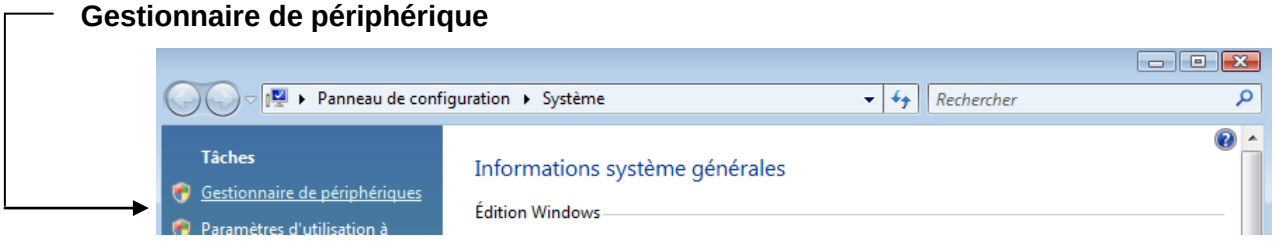
Gestionnaire de périphérique:

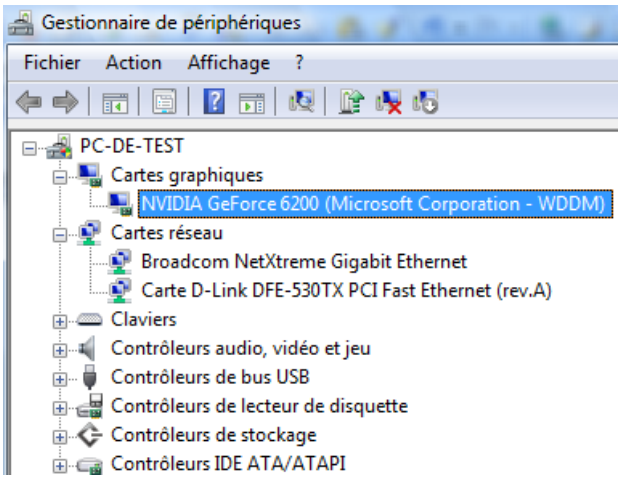
Cela peut se faire de différentes manières, la manière « préconisée » par microsoft étant de faire apparaître via le



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

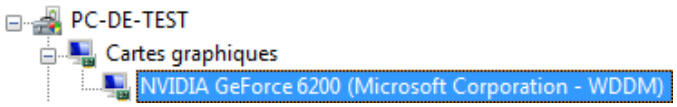
(par exemple Cartes graphiques)

Ainsi que leurs composants

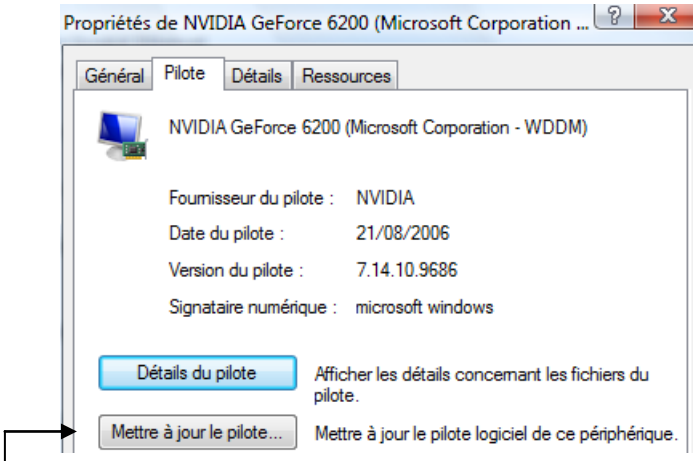
(par exemple NVIDIA GeForce 6200)

Versions - Installation de pilotes :

On demande les propriétés du composant sélectionné

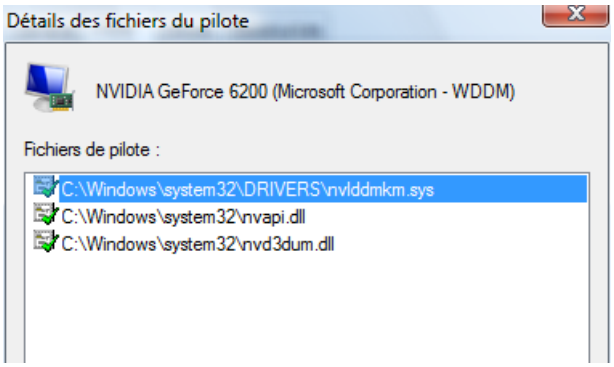


pour obtenir



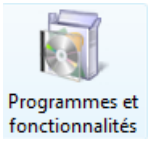
On peut facilement **Mettre à jours le pilote**

On peut aussi avoir des renseignements sur le driver installé actuellement, et savoirs les fichiers utilisés via **Détails du pilote**



Installation driver via Update :

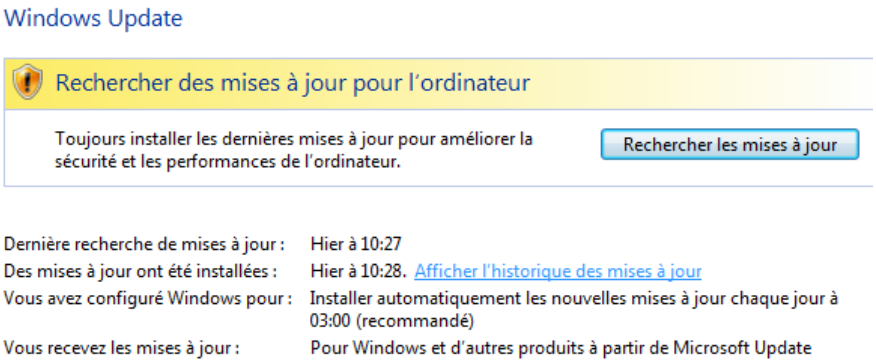
On demande les propriétés du composant sélectionné



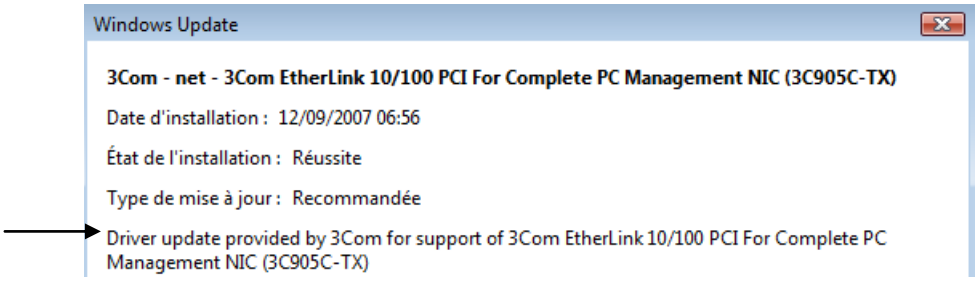
On peut avoir une idée de la provenance du pilote. Dans le panneau de configuration on demande **Programmes et fonctionnalités**

Puis **Afficher les mises à jour installées**

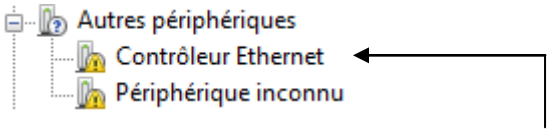
Windows Update / Afficher l'historique des mises à jour



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

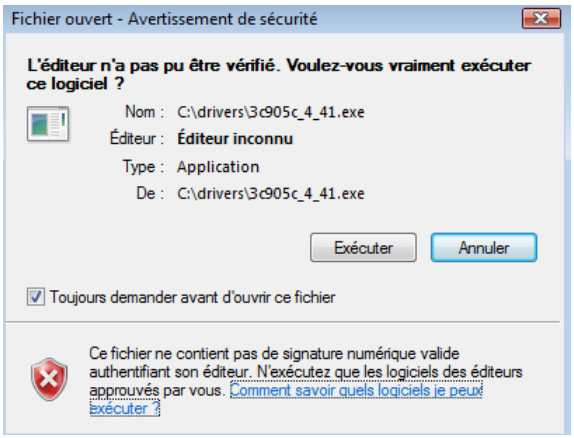


Installation driver via Fichiers locaux :

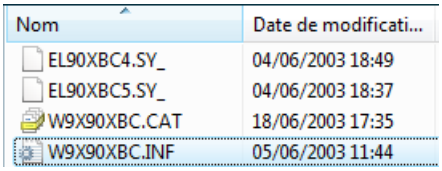


On veut récupérer un driver pour notre carte **3Com 3C905**…

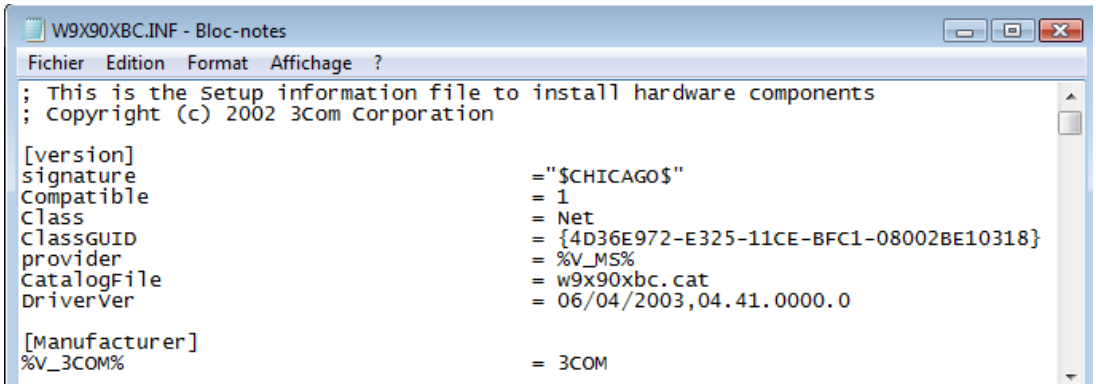
Il faut déjà obtenir un package du driver correct, et l'installer quelque part sur notre poste… Cela peut faire apparaître des mises en gardes du au format auto-extractible de ces packages !



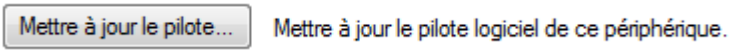
Si le constructeur travaille bien, il fournit un fichier **xxx.inf**



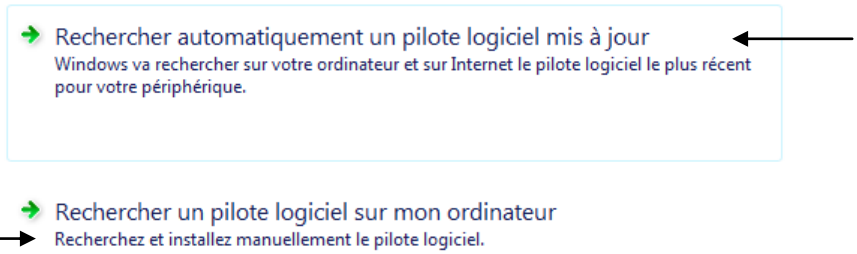
Contenant la définition du driver et son installation



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

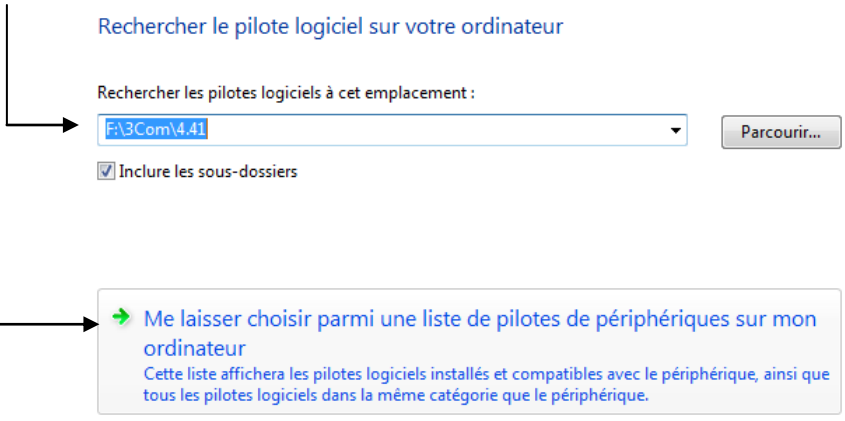


Windows 8 nous demande de choisir, il faut lui indiquer que l'on dispose du package localement

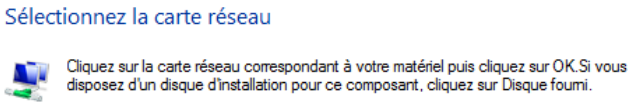


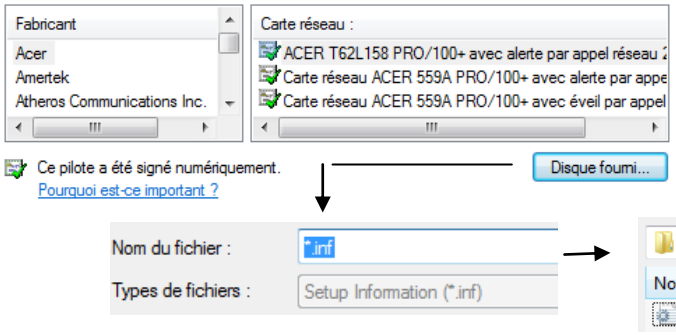
Ne pas demander **Rechercher auto**… car cela revient à **Windows Update**

S'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



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

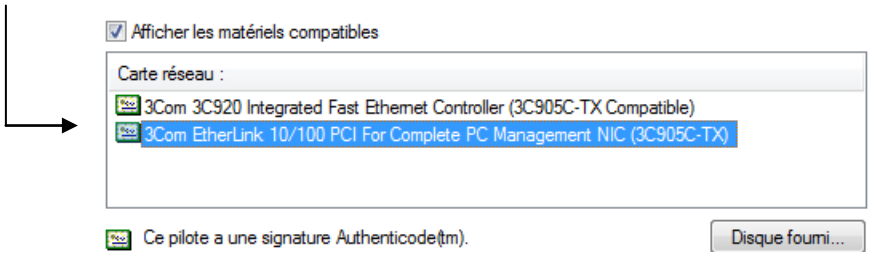




En demandant **Disque fourni** il faut repérer notre fichier **xxx.inf**

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

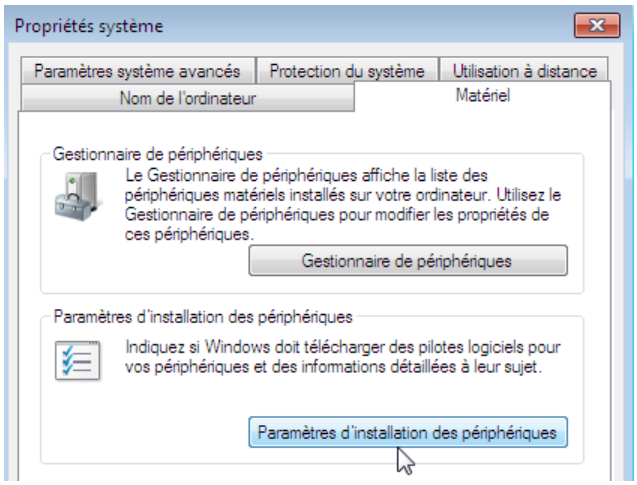
Et si nécessaire nous propose un choix

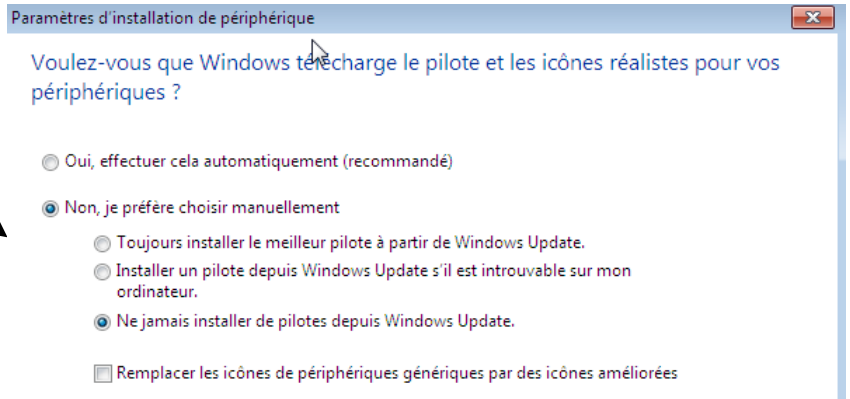


Méthode par défaut installation de drivers :

Dans les propriétés du poste de travail, **paramètres systèmes avancé**

puis onglet **Matériel** **Paramètres d'installation des périphériques**



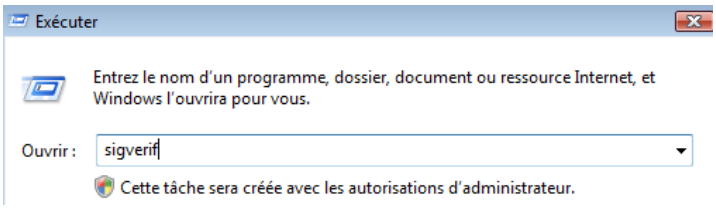


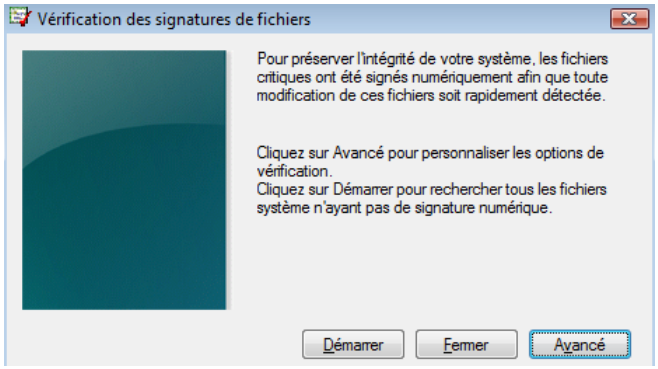
Sigverif vérification drivers signés:

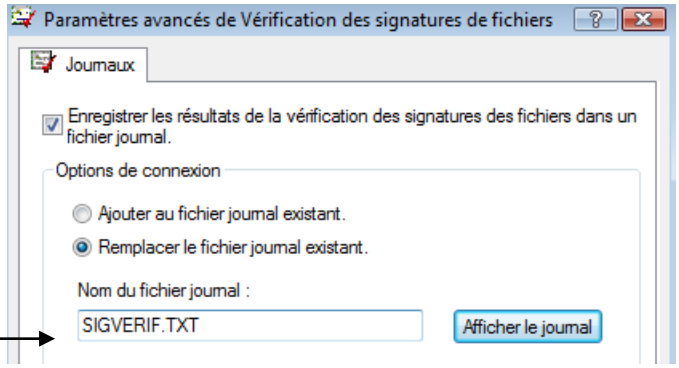
On peut aussi a tout moment demander d'effectuer une vérification sur une machine installée, et sur laquelle on aurait laissé un certain nombre d'installation se faire...

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

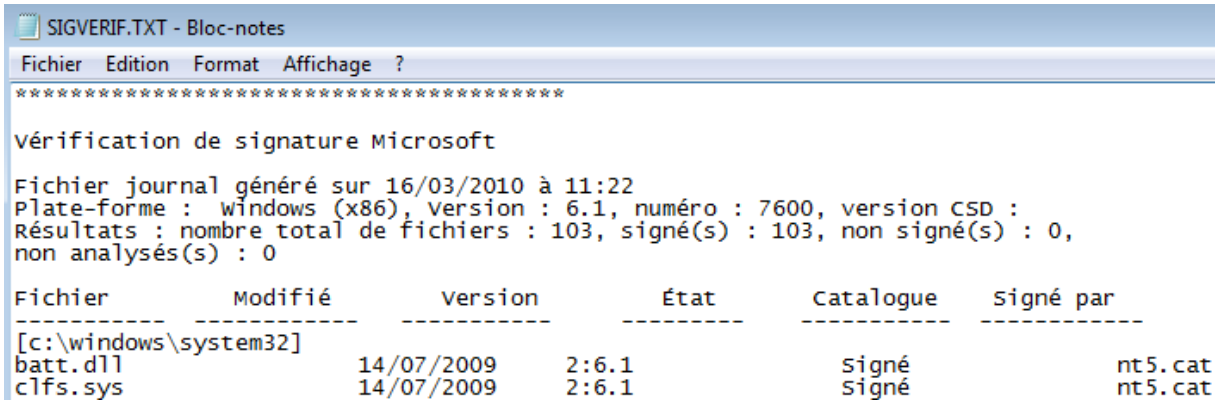
sigverif



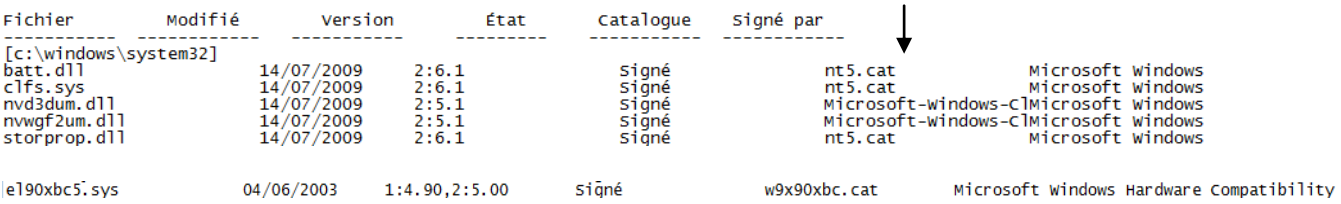




on à le résultat dans un fichier journal



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



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
asyncmac.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 *l'utilisateur* ou le *domaine\utilisateur*. 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.

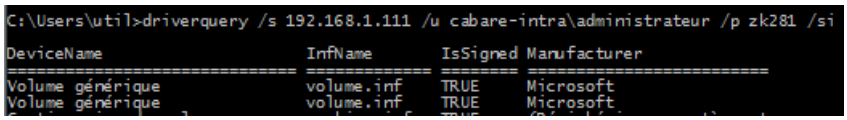
Ainsi **Driverquery /SI** donnerait pour tous les drivers du poste courant l'information s'ils sont signés ou non

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

DeviceName                  InfName         IsSigned Manufacturer
=========================== =============== ======== ========================
Volume générique            volume.inf      TRUE     Microsoft
Gestionnaire de volume      machine.inf     TRUE     (Périphériques système st
Pilote d'énumérateur de lecteu machine.inf  TRUE     (Périphériques système st
```

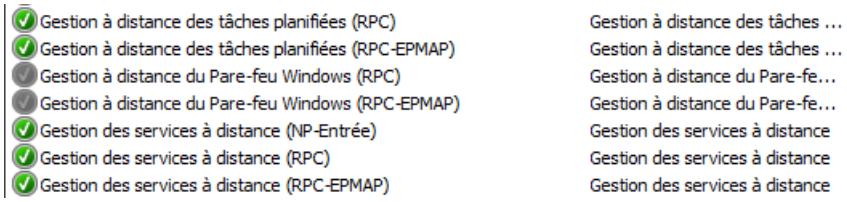
Dans l'exemple ci-dessous, on teste les drivers d'une machine en ***192.168.1.10*** avec un login ***administrateur*** et un mot de passe ***local***.

```
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
```

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***.



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**...et la **gestion à distance des tâches planifiées**...



INTÉGRITÉ WINDOWS 8

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 forcement 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 fichiers existe en

%systemroot%Winsxs

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

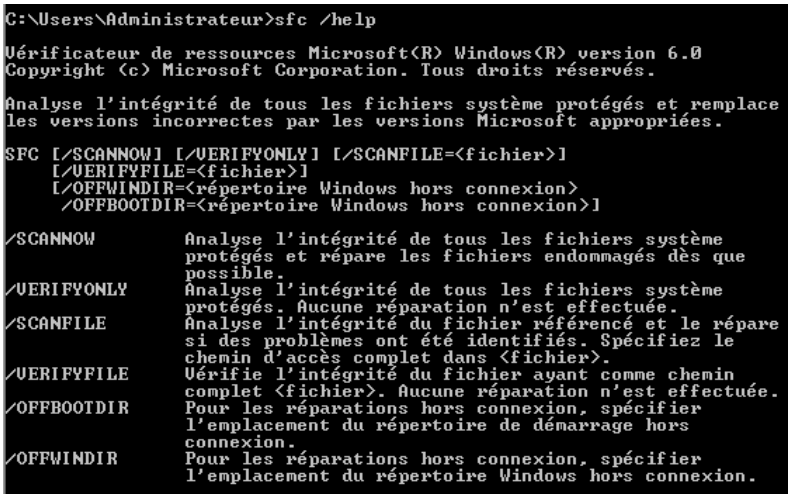
1. le dossier **Winsxs**,
2. le Média d'origine,
3. le point d'installation réseau…

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 Windows (sans attendre la vérification en tache de fond)



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 !

- ✓ Lorsqu'une opération requière des droits élevés, une boite 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 boite de dialogue lui demande alors un compte et un mot de passe ayant des droits d'administration…

N.B : en réglage standard, 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.

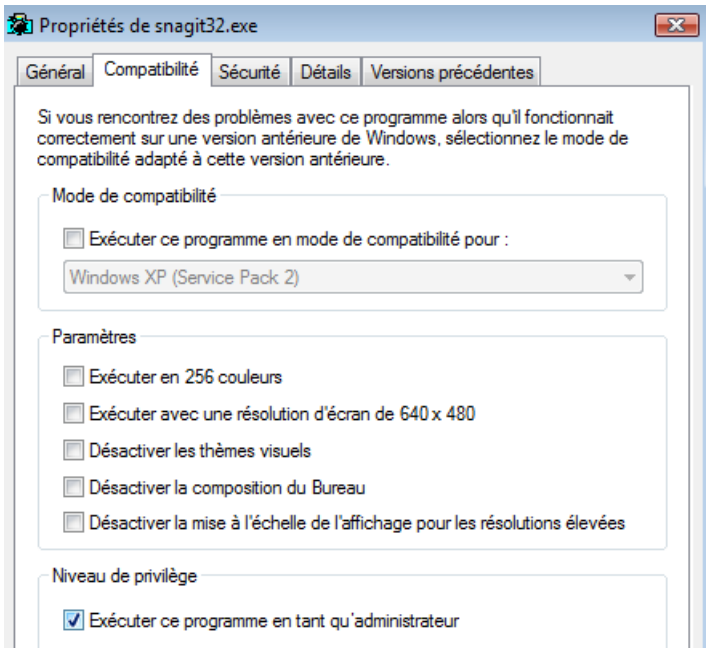
Avec Windows 8, lorsque vous ouvrez une session, **LSASS** va créer deux jetons. Un qui va contenir toutes les informations comme dans Windows XP et un autre jeton "restreint" qui ne contiendra que les privilèges d'un utilisateur standard.

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

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

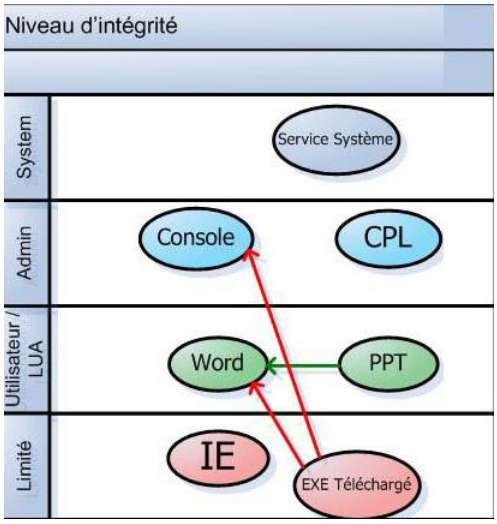
C'est donc ce deuxième jeton qui sera utilisé pour lancer les différentes applications. Pour utiliser le premier jeton, celui avec tous les privilèges, vous devrez passer par une élévation de privilège

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**

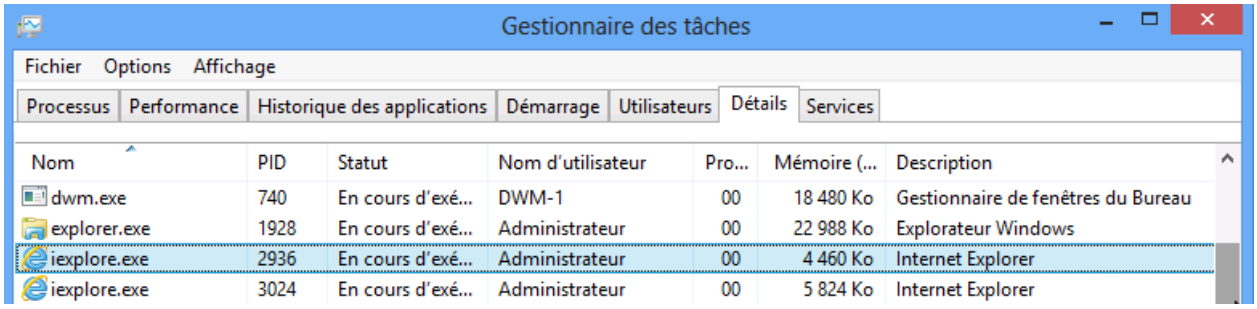


- Il faut savoir que les processus Utilisateur / LUA ne peuvent pas modifier les processus s'exécutant dans un niveau d'intégrité supérieur. (mais ils peuvent les lire pour obtenir des infos…)
- Le groupe des administrateurs à un **IL** élevé
- Pour un utilisateur, les processus qu'il lance et ses fichiers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

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

Iexplorer : avec un **Il** d'utilisateur (pour stocker ses favoris…)

Iexplorer : avec un **Il** bas pour executer les activex et autres…



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…

Gestion de l'UAC (panneau de configuration):

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

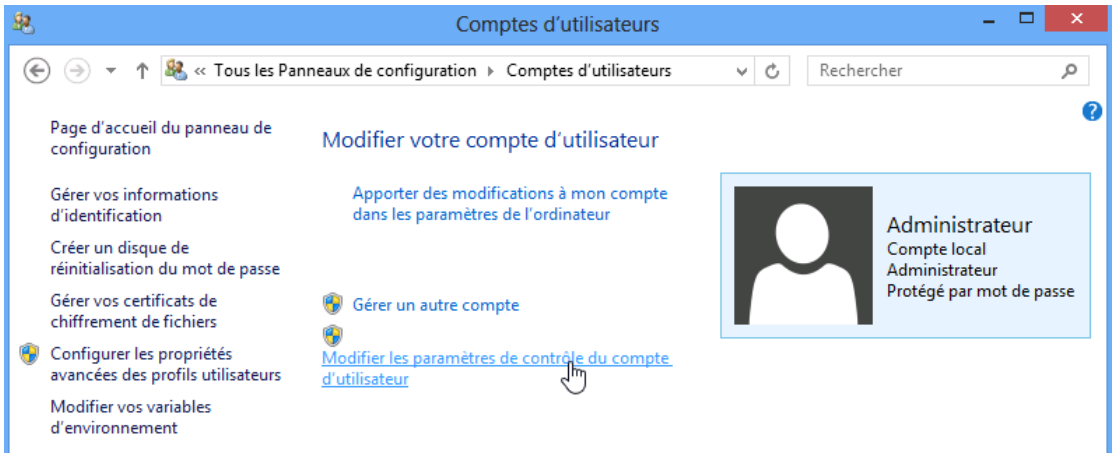
Il est recommandé de ne pas désactiver les invites du contrôle de compte d'utilisateur dans les paramètres de stratégie de groupe ou en agissant sur le curseur.

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 :

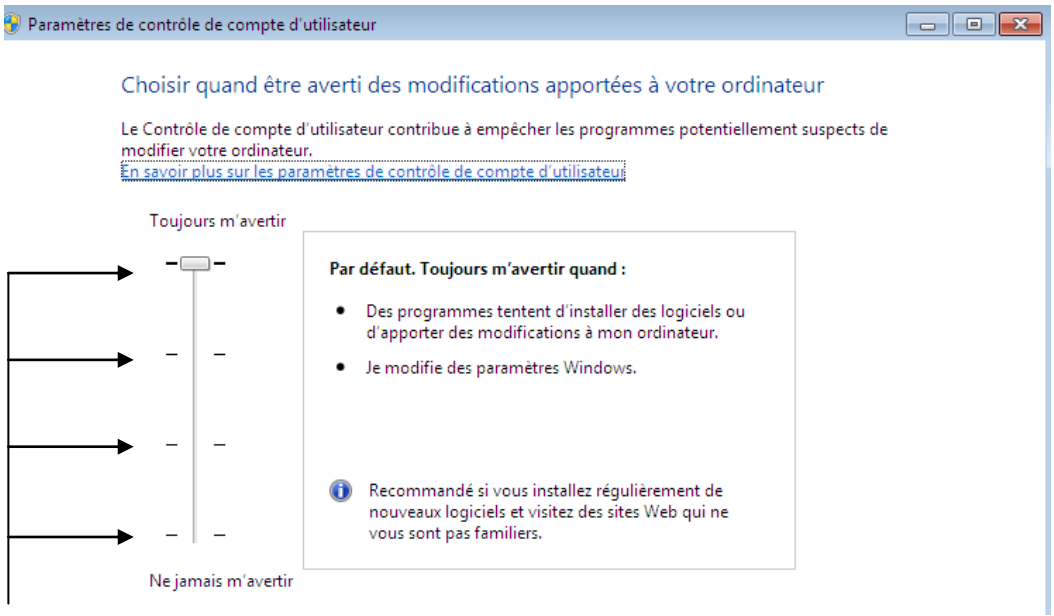
- Mode protégé d'Internet Explorer
- Virtualisation de fichiers système et du Registre

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

Panneau de configuration / Comptes d'utilisateurs



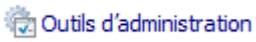
la commande **Modifier les paramètres de contrôle de compte d'utilisateur**

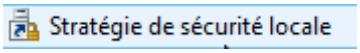


la prise en compte de cette commande peut demander un redémarrage.

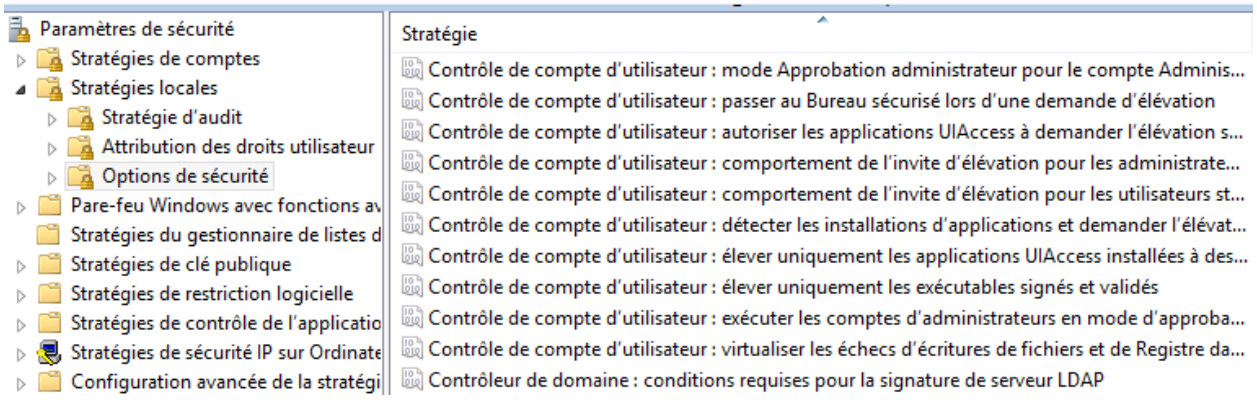
Gestion de l'UAC (stratégies locales):

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

Dans le **Panneau de Configuration / Outils d'administration /** 

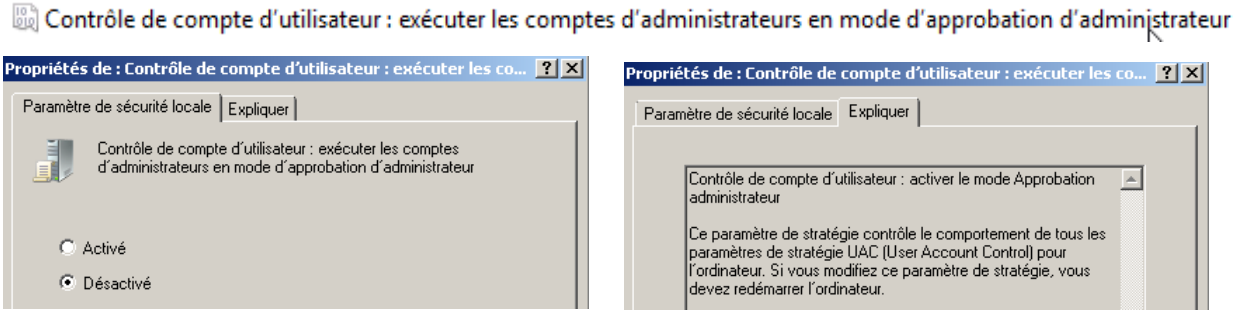
Puis **Stratégies de sécurité locales** 

Puis dans les **Stratégies locales / Options de sécurité** les stratégies repérées par la mention : Contrôle de compte d'utilisateur



Désactivation de l'UAC :

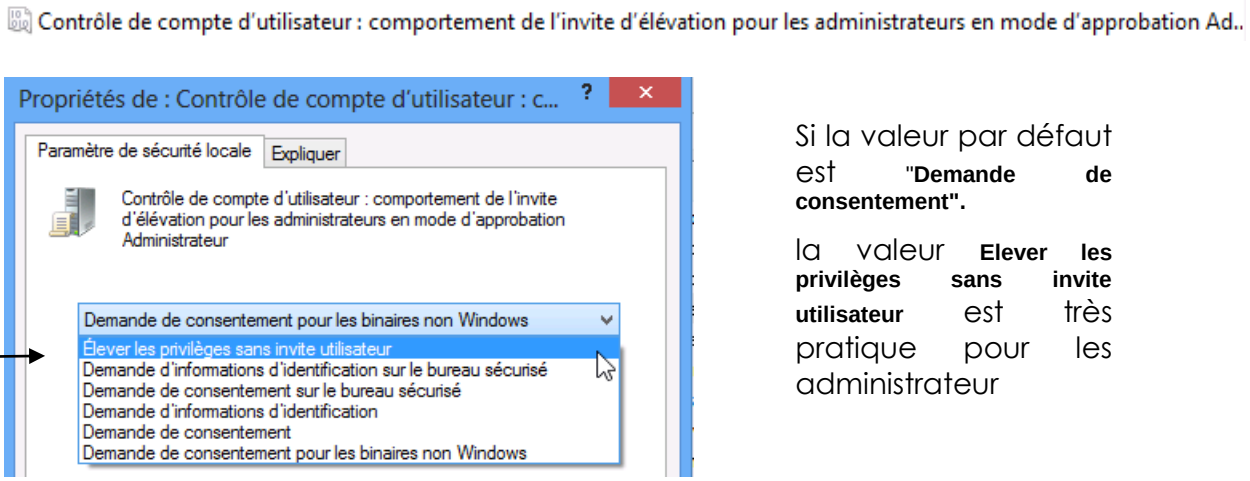
Sans doute le plus ... radical



N.B : re-démarrage du PC obligatoire

Désactivation de l'UAC pour les Administrateur :

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



Si la valeur par défaut est **"Demande de consentement".**

la valeur **Elever les privilèges sans invite utilisateur** est très pratique pour les administrateur

Désactivation l'UAC pour les Utilisateurs :

Lorsque les logiciels anciens deviennent incompatibles

Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard

Activation l'UAC aussi pour le compte Administrateur Root :

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

Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrateur intégré

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 Windows 8, puisque un compte administrateur "autre" bénéficiera de l'effet protecteur de l'UAC sans occasionner de gêne (il suffit de demander une élévation de privilège silencieuse).

On peut demander une invite d'élévation automatique, mais on peut 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 8.

- 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
- Windows 8 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 Windows 8 allant écrire dans **Program Files** ou dans des dossiers systèmes fonctionnent. On parle de « **programmes hérités** »

Windows 8 traite un processus comme « virtualisable » si :

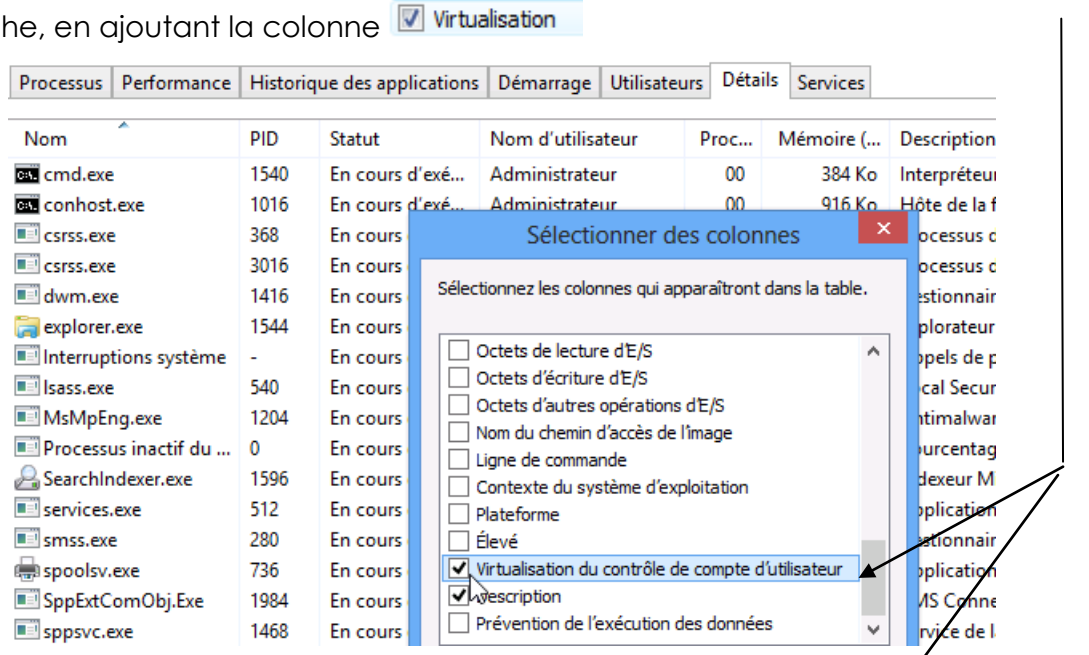
- il fait 32 bits (et non 64 bits),
- il ne s'exécute pas avec les droits administratifs,
- il n'a pas un fichier de signature spécifique pour Windows Seven

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

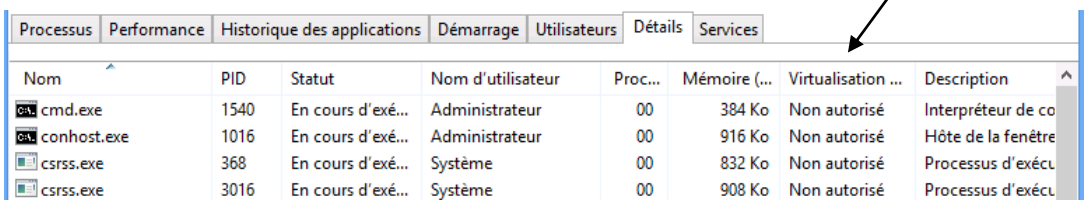
- %ProgramFiles%
- %ProgramData%
- %SystemRoot%

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



donnant

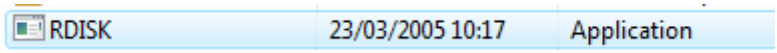


N.B : Comme les informations sont stockées dans le répertoire utilisateur, cela peut être gênant. Par exemple, pour une application qui stocke les meilleurs scores : l'utilisateur fera toujours le meilleur score !

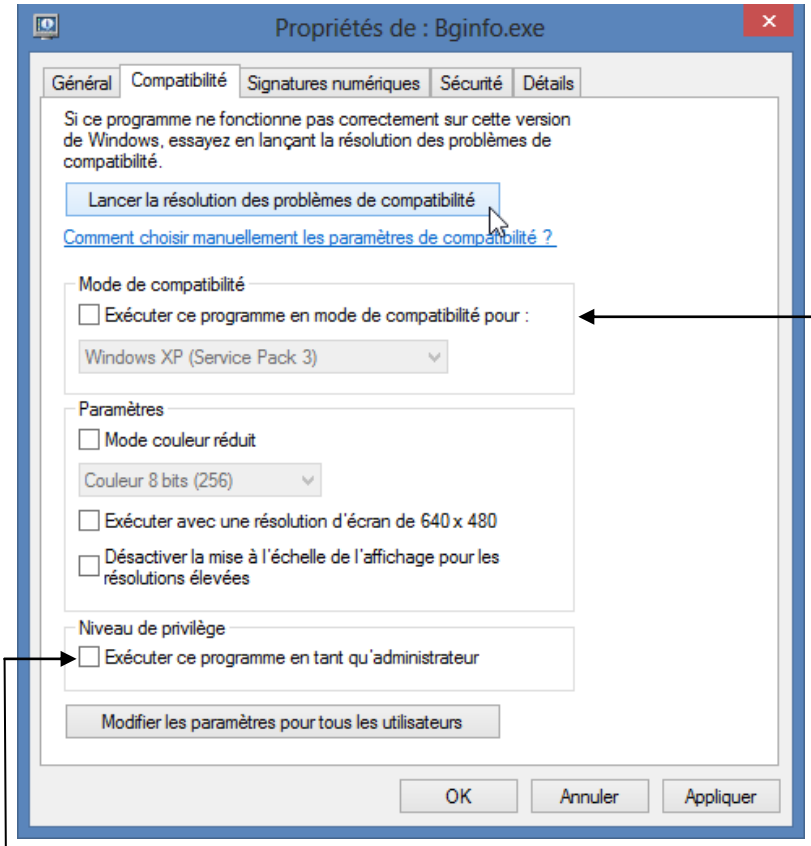
COMPATIBILITE AVANT WINDOWS 8

Exécuter en mode compatibilité:

Si un programme fonctionnait correctement sur une version antérieure à Windows 8, et que vous ne disposez pas de la version spécifique, on peut tenter de demander de l'exécuter en mode compatibilité. Par exemple

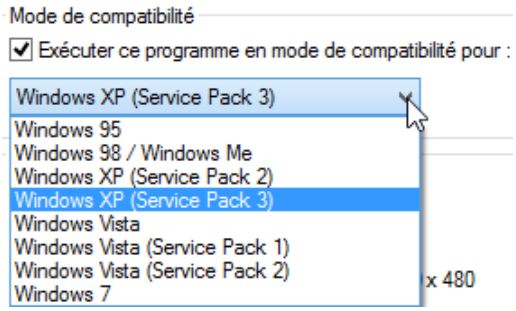


On demande clic-droit sur l'exécutable, **propriétés** onglet **Compatibilité**



On peut spécifier

- si il y a besoin d'exécuter avec un privilège d'administrateur
- On peut choisir un mode de compatibilité



Séquence possible:

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

Il se peut qu'il faille désactiver l'UAC

Il se peut qu'il faille installer un autre OS avec Hyper-V pour pouvoir installer l'application

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 Windows 8 contre les virus, peut être responsable de crashs intempestifs sur votre système

bcdedit.exe /set {current} nx AlwaysOff

Puis re démarrage

La réactivation de la protection se fait par

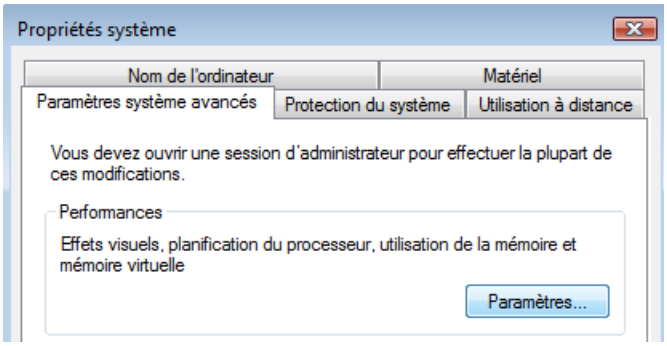
bcdedit.exe /set {current} nx Optin

(et re démarrage)

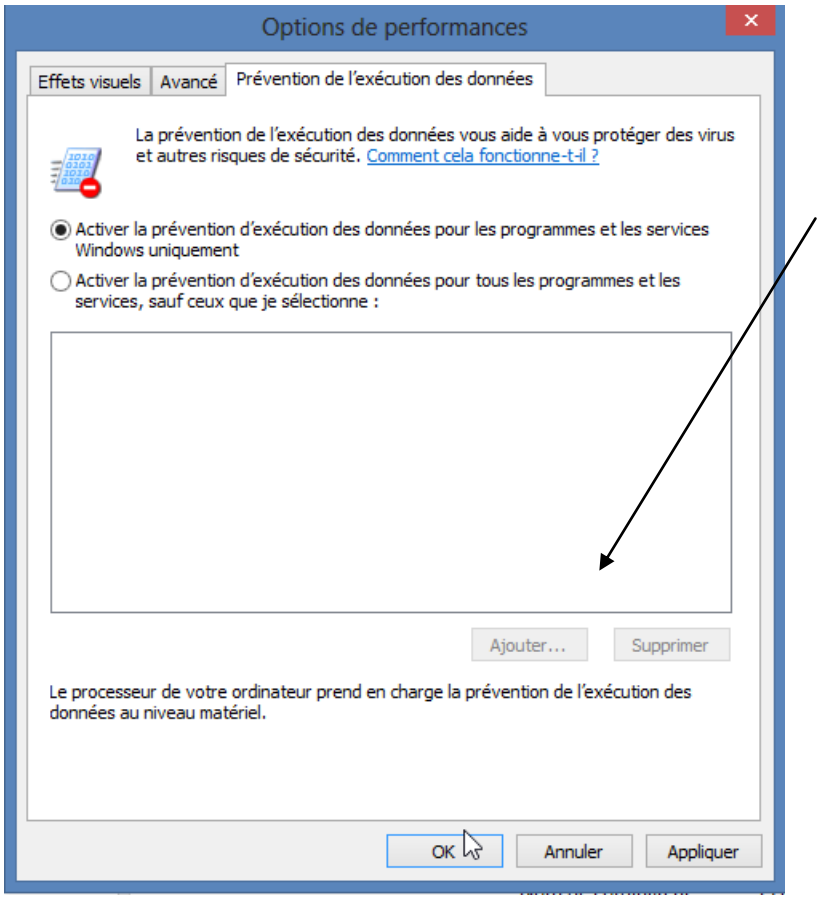
Désactivation pour une application de DEP :

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.

WINRE

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** (**P**réinstallation **E**nvironnement) cet environnement remplace la console qui existait sous XP

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

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 regitre 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

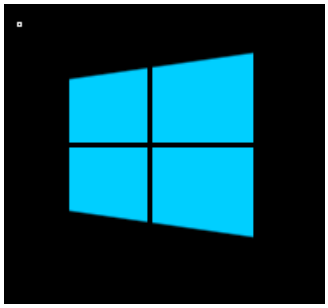
1. renforcement du système EFS
2. Algorithme de chiffrement plus robustes
3. Apparition de BitLocker associant chip TPM et clé USB

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:

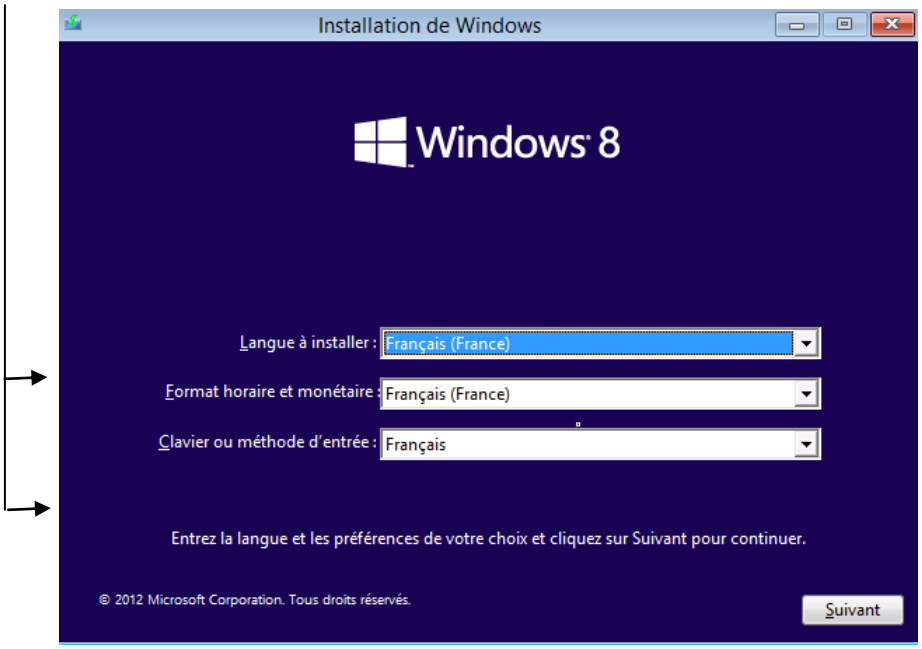
Si l'environnement de Récuperation n'est pas pré-installée sur la machine (machine livrée ainsi, avec une pré-installation de secours), alors on peut toujours à partir du DVD relancer une pseudo-installation

La fenêre Windows 8 apparaît



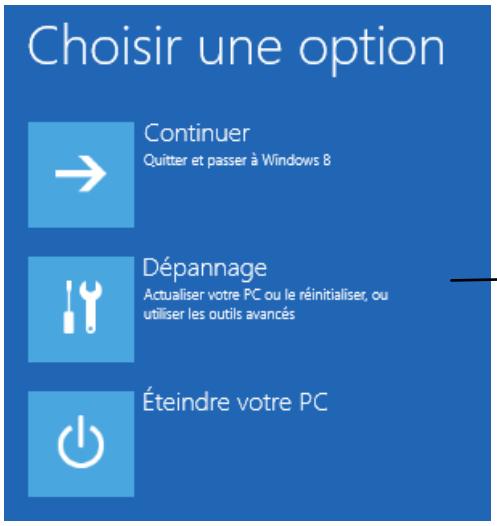
N.B : Le temps de chargement peut être assez long

il faut choisir une régionalisation



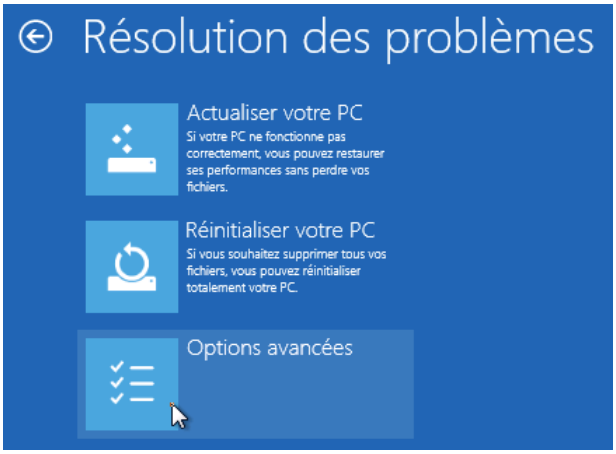
Puis on demande **Réparer l'ordinateur**

et on tombe sur le **menu options de démarrage**



C'est lui qui permet l'accès à toutes les manipulations. On choisit **Dépannage**

Qui donne accès à la **Résolution des problèmes**



On demande **Options Avancées** (déjà présentes sous Seven via WinRe)

Restauration du système

Ce sont les Point de Restauration

Récupération Image Système

Si on a fait 1 sauvegarde « image »

Réparation automatique comme seven l'algorithme de WinRe

Invite de Commande

C'est la Console de Récupération WinPe 4.0

Paramètres

Ex **F8** avec les options lors du re-démarrage

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

1. **ETAPE 1** : séquence POST jusqu'à l'affichage du « rond ».

   à ce niveau on peut avoir des :

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

2. **ETAPE 2** : « rond » 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

Les problèmes à ce niveau peuvent être matériels ou logiciels:

Problèmes hardware

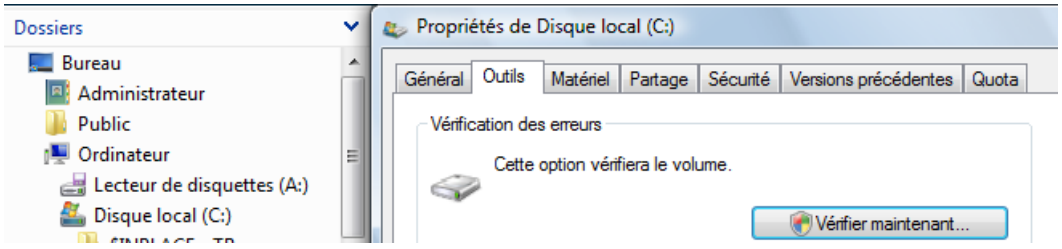
Les causes fréquentes peuvent être

- des problèmes mémoire:
- des problèmes de disque dur

On peut essayer de "prévenir" une panne de disque dur… Windows 8 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 rapports consigné par cette technologie.

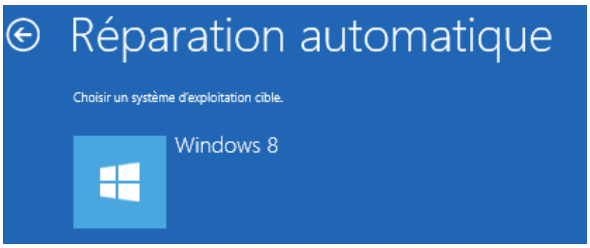
On peut aussi préventivement réaliser des commandes en invite de commande **chkdsk c: /f /r**, (et éventuellement les planifier via un petit batch), moduler le comportement par défaut via **chkntfs**…

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 a 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

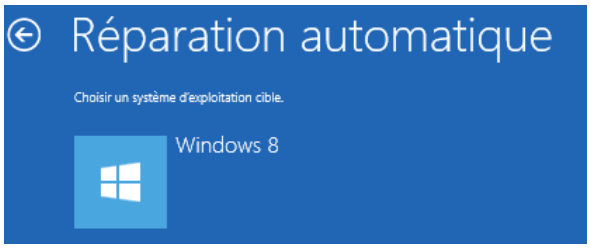
/FIXMBR, **/FIXBOOT** et deux nouvelles **/SCANOS** et **/REBUILDBCD**

Cf chapitre suivant " WinRE console de récupération"

Etape 2 affichage du « rond » avant session

A ce niveau, le noyau Windows 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 surtout tenter de passer par les "**options de démarrage**" **/ options avancées /- paramètres ex F8** (Cf chapitre suivant "Options de démarrage F8")

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\RoamingMenu\Microsoft\Windows\ Start Menu \ Programmes\Démarrage

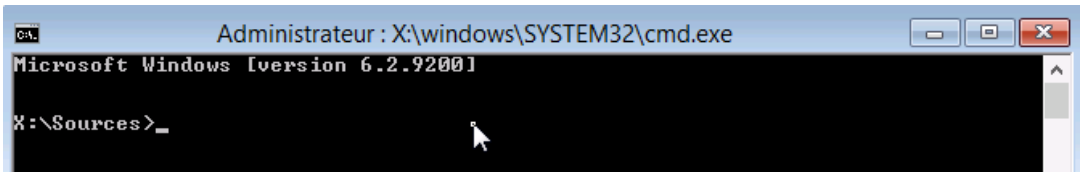
SHIFT + "**Ouverture de session**" : ne pas exécuter ces programmes

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

WINRE - CONSOLE DE RECUPERATION

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	
LISTSVC	Plus disponible
LOGON	Plus disponible
MAP	**Diskpart**
MD	

MKDIR	
MORE	
RD	
REN	
RENAME	
RMDIR	
SYSTEMROOT	
TYPE	

En cas de gros problème on peut toujours tenter une reconstruction complète du magasin via la commande **bootrec /rebuildbcd** de la console de récupération

```
X:\windows\system32>bootrec /rebuildBcd
Recherche d'installations Windows sur tous les disques.

Veuillez patienter...
```

Modifier les partitions - Utilitaire Diskpart

Depuis Vista, il est possible de modifier la taille des partitions sans perdre leur contenu. Cela peut par exemple faire de la place pour une installation de Windows 8 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

  Nº 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

  Nº volume    Ltr  Nom          Fs     Type        Taille   Statut      Info
  ----------   ---  -----------  -----  ----------  -------  ----------  --------
* Volume 0     C                 NTFS   Partition     37 G   Sain        Système
  Volume 1     D                        DVD-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

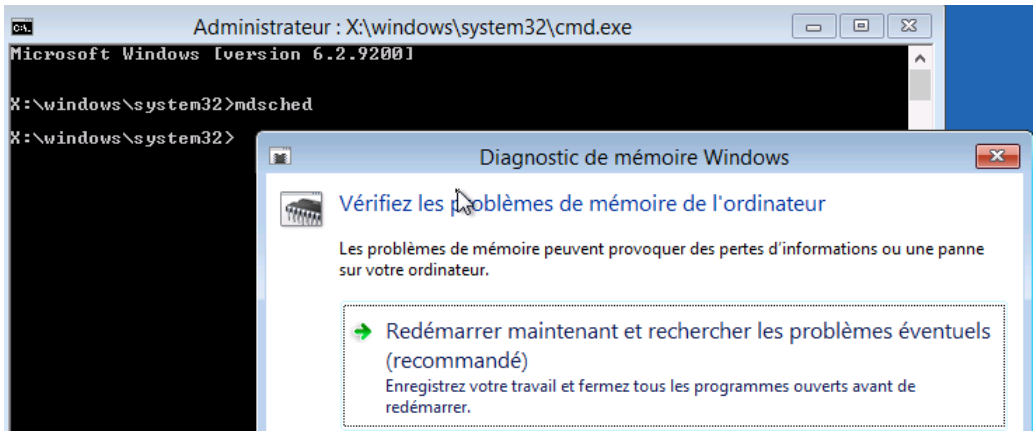
```
DISKPART> shrink desired=10000

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
```

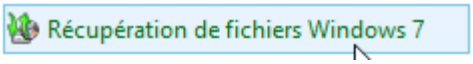
Outil mdsched



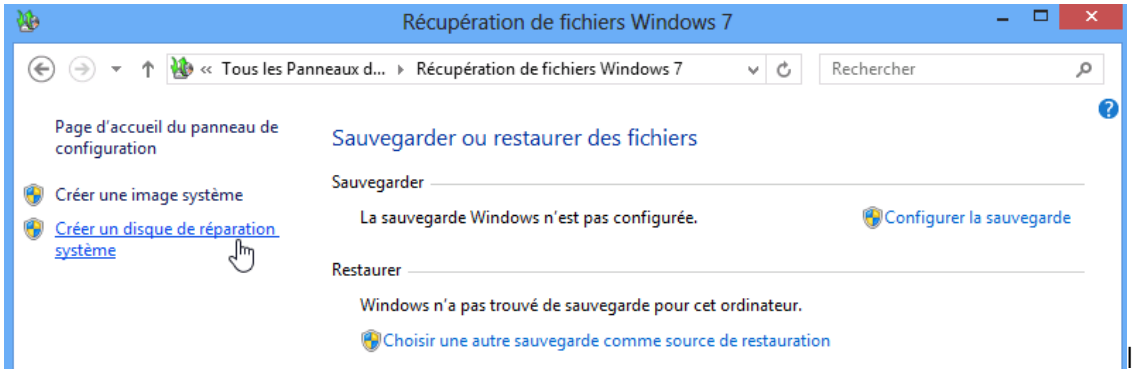
CREATION DE WINRE SUR CD - USB

Création CD WinRe

Via le menu **panneau de Configuration / Récupération de fichiers Windows 7**

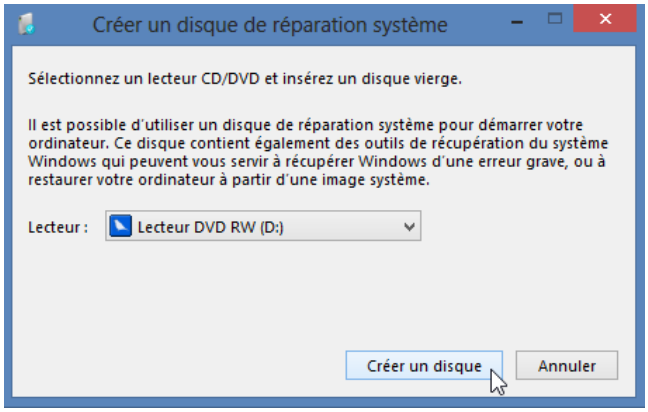


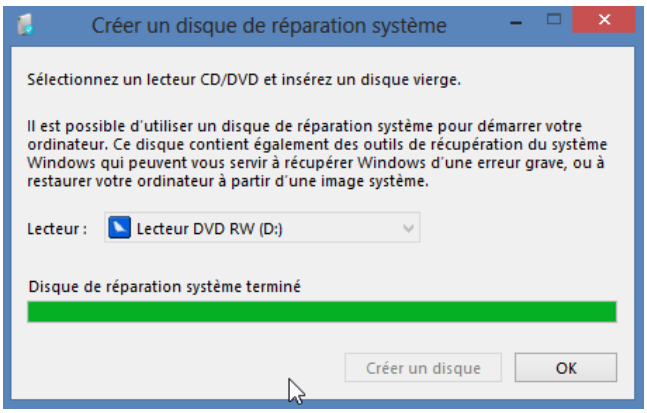
On demande **Créer un disque de réparation Système**



Il

il faut avoir bien sur un graveur DVD…

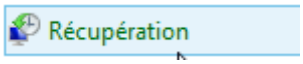




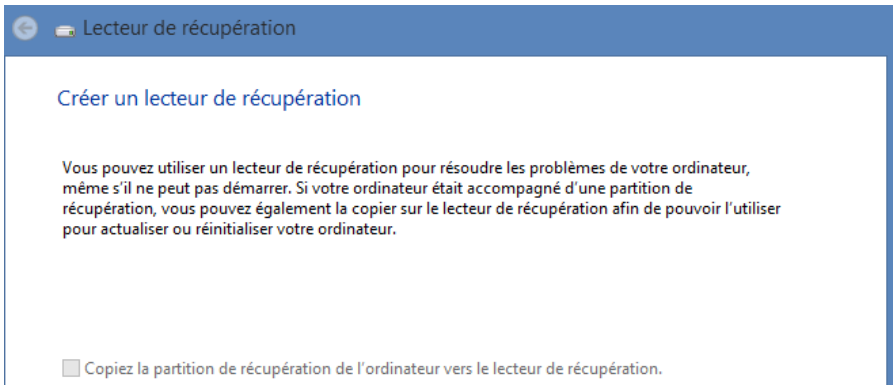
C'est un CD-DVD contenant un Win RE et les outils de réparation présents sur le DVD de Windows 8…

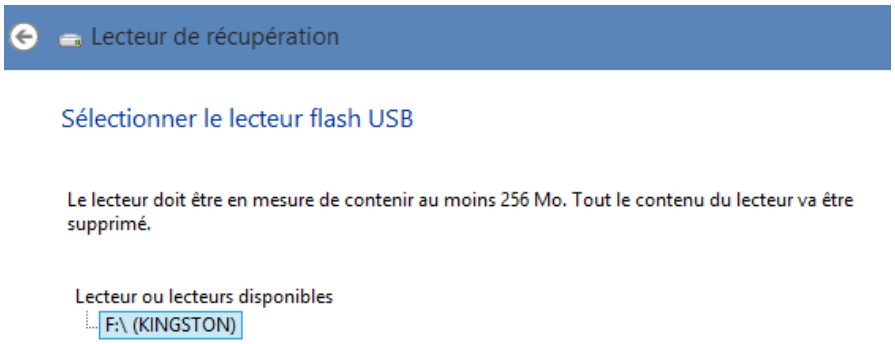
Création Lecteur USB

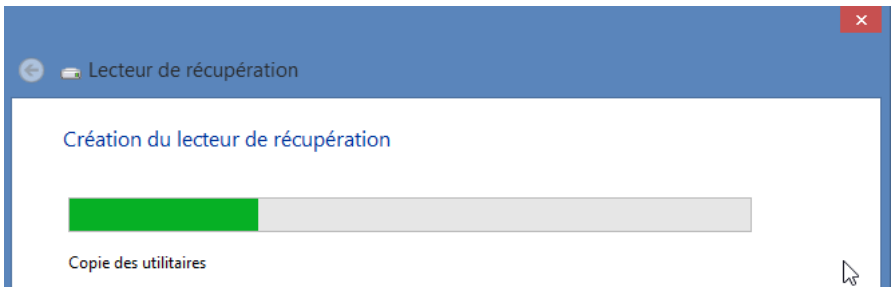
Via le menu **panneau de Configuration / Récupération**



On demande **Créer un lecteur de récupération**





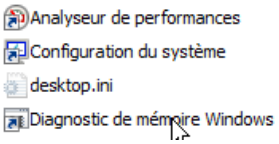


Si le Bios le permet, on peut désormais booter sur notre clé…

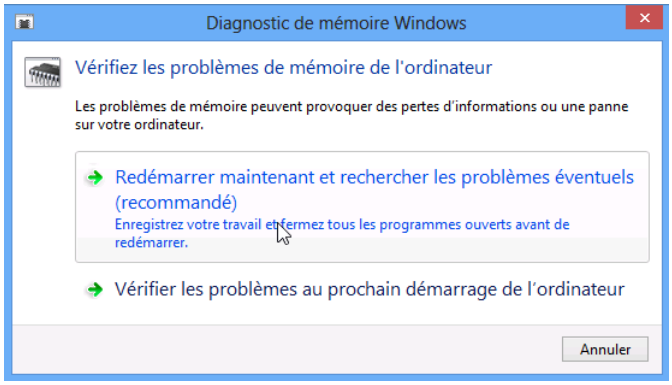
TEST MEMOIRE

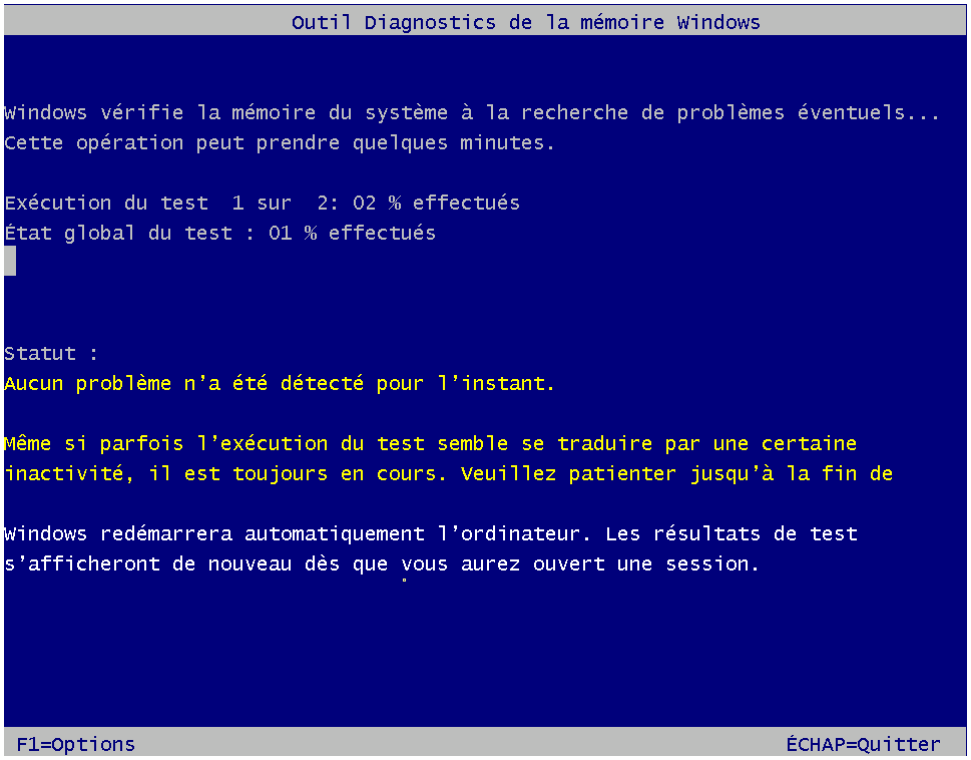
Depuis Windows 8

Via le menu **panneau de Configuration / Outils d'administration**



On demande **Diagnostic de mémoire Windows**





F1 permet d'executer des tests plus complets…

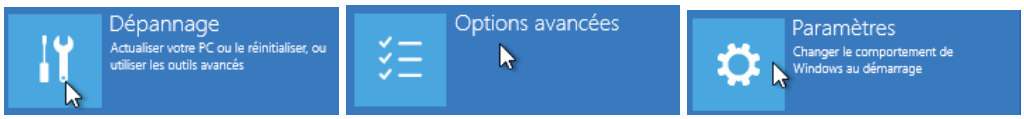
Correspondant à l'outil **mdsched.exe**

PARAMETRES DE DEMARRAGE – EX F8

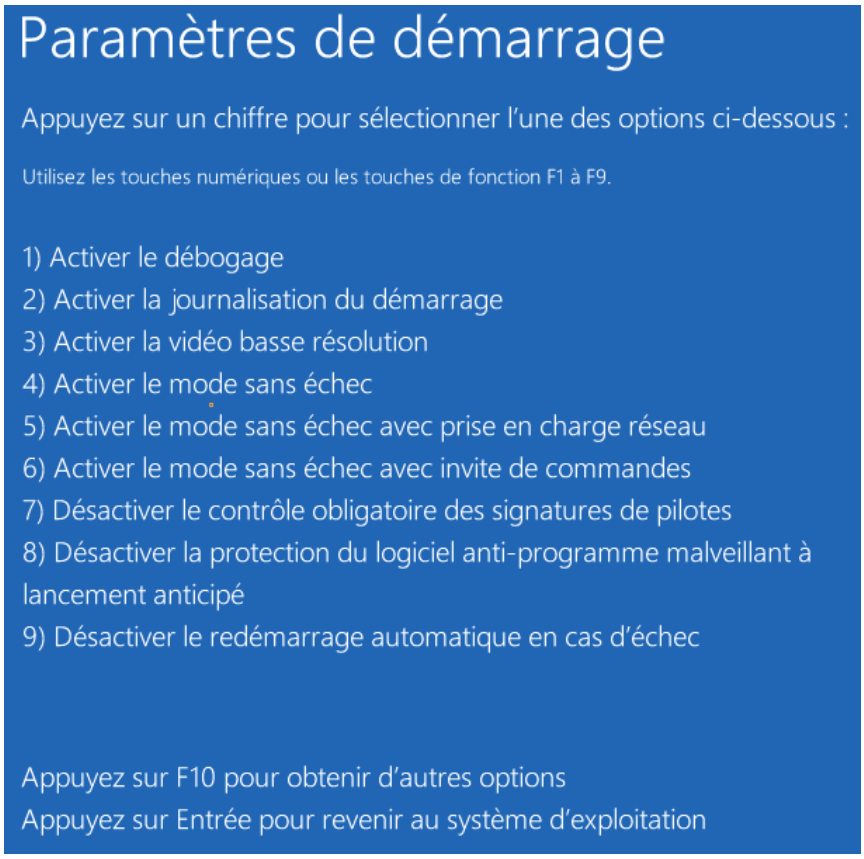
Accès aux options avancées :

Soit une machine Windows 8 sur laquelle on ouvre une session en **mode sans Echec**, donc via le Menu des Options de démarrage , **MAJ+Redémarrer**

/ Dépannage / Options Avancées / paramètres / F4



On dispose de :



Options principales :

Dans l'ordre d'intêret

F4 - 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 « a minima »

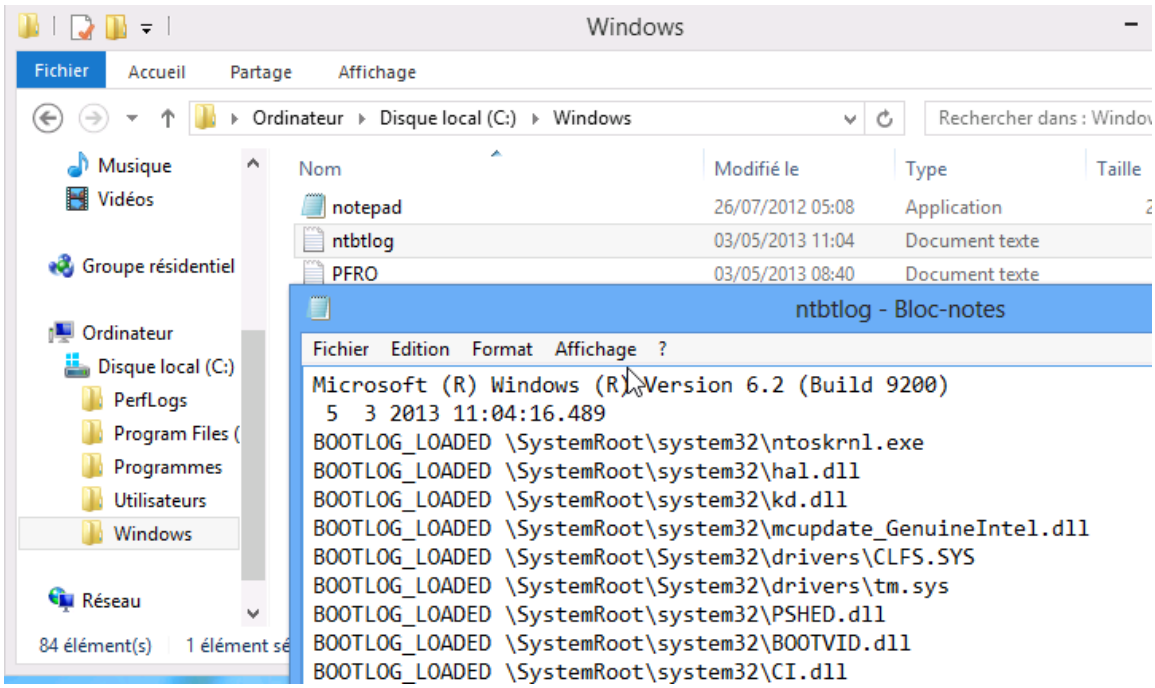
F6 - Invite de commande en mode sans Echec :

idem ci-dessus mais en dévalidant l'interface graphique…

F2 Activer la journalisation au demarrage :

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 Windows 8



F3 Activer la video en basse résolution :

pilote VGA en 640x480

F7 Désactiver le contrôle obligatoire de la signature des pilotes :

permet d'installer des drivers non signés

F8 Désactiver la protection du logiciel anti-programmes malveillants:

permet de ne pas langer ***windows defender*** et autres

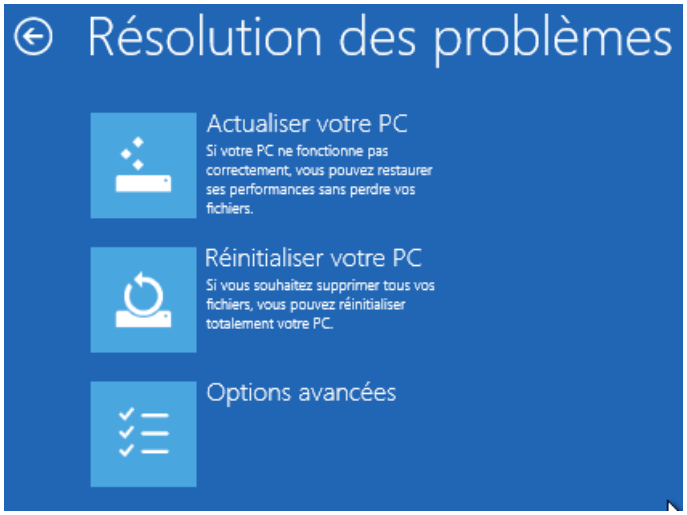
ACTUALISER – REINITIALISER LE PC

Menu Options de démarrage - Dépannage:

C'est lui qui permet l'accès à toutes les manipulations

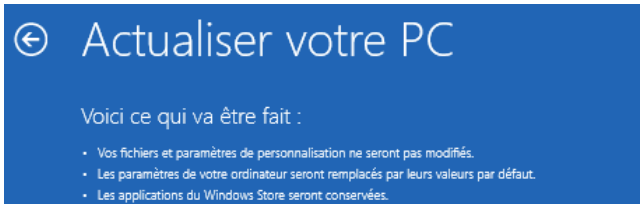
donne accès à la

Résolution des problèmes

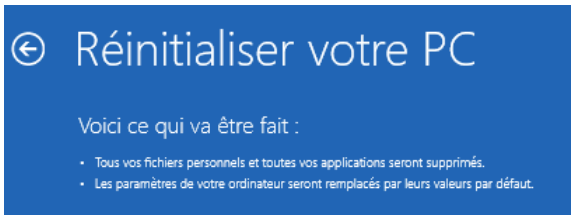


Si deux nouvelles fonctionnalitées « automatiques » apparaissent :

Actualiser votre PC



Réinitialiser votre PC



Actualiser votre PC:

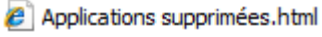
Sont sauvegardés

- Les données (dans mes documents)
- Les paramètres des Windows (bureau, interface, réglages)
- Les applications Windows Store
-

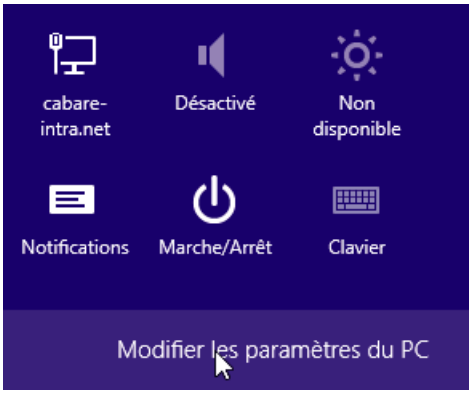
Ne sont pas sauvegardés

- Paramètres Pare-Feu

Une liste des applications supprimées (si elles avaient été installée depuis des Sources ou le Web) est crée dans un fichier sur le Bureau



Cela peut aussi se lancer depuis la **Charm bar** / **Paramètre**



onglet **Général** / **Actualiser votre PC**

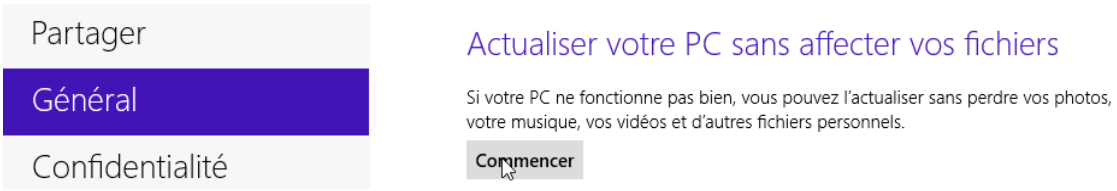
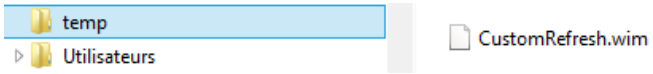


Image personalisée Recimg:

Par défaut, les applications de bureau sont donc supprimées lorsque vous actualisez un ordinateur fonctionnant sous Windows 8, sauf si vous créez une image personnalisée. Lorsque on demander de rafraîchir notre poste windows 8, il utilise comme image « système » source soit le DVD d'origine, soit une image personnalisée avec la commande recimg. Donc **recimg** va permettre de définir une image de restauration personnalisée nommée **customrefresh.wim**



On peut voir s'il existe une image personnalisée par **recimg /showcurrent**

```
C:\Users\Administrateur>recimg /showcurrent

Aucune image de récupération personnalisée active.
Code d'erreur : 0x80070490
```

On crée une image via la commande

recimg /createimage c:\temp

```
C:\Users\Administrateur>recimg /createimage c:\temp
Emplacement du système d'exploitation source :  C:
Chemin d'accès de l'image de récupération : c:\temp\CustomRefresh.wim
Création de l'image de récupération. Appuyez sur [Échap] pour annuler.
Initialisation en cours
100%
Création d'une capture instantanée
100%
Écriture de l'image (cela peut prendre un certain temps)
1%
```

N.B : cette image n'intègre aucun fichiers ou données utilisateurs, qui sont elles toujours sauvegardés au moment de l'opération **Actualiser votre PC**… Cela n'a pour effet que d'inclure les programmes et applications que l'on aurait installé sur le poste, qui eux ne sont pas, forcément, dans le DVD d'origine.

N.B : cette image ne fonctionne que pour les applicatifs installés en C : (cela ne permet pas la gestion de disques durs multiples…

Une fois la commande terminée

```
La création et l'inscription de l'image de récupération sont terminées.
```

on peut vérifier de nouveau par **recimg /showcurrent**

```
C:\Users\Administrateur>recimg /showcurrent

\\?\GLOBALROOT\device\harddisk0\partition1\temp
RecImg : opération terminée
```

Si on perd le dossier ***\temp*** contenant notre image actualisée, la réactualisation se fera de nouveau depuis le DVD, sans aucune application…

Si on récupère une image (qui doit toujours être nommée **customrefresh.wim)** que l'on stocke dans un nouveau dossier ***\temp-new*** on peut refaire pointer Windows 8 dessus par la commande

recimg /setcurrent c:\temp-new

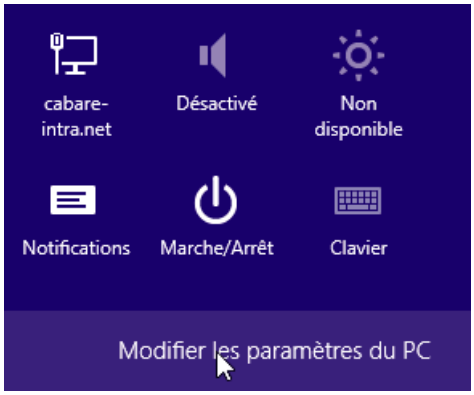
Réinitialiser votre PC:

Rien n'est sauvegardé

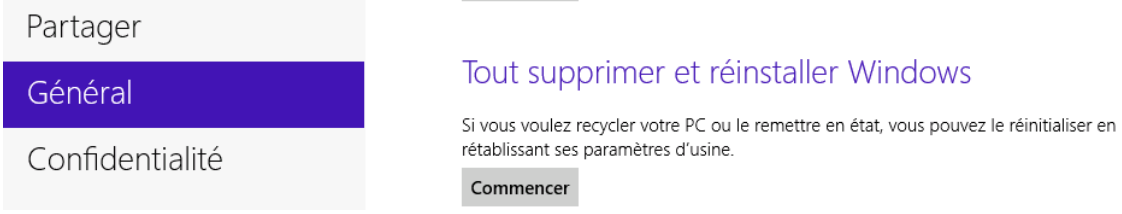
- Ni les données
- Ni aucune application

Les partitions sont formatées et Windows 8 sera réinstallé de base…

Cela peut aussi se lancer depuis la **Charm bar** / **Paramètre**



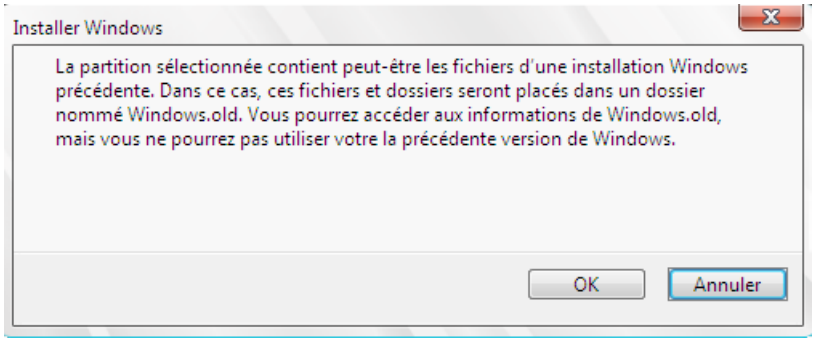
onglet **Général / Tout supprimer reinstaller**



REINSTALLER COMPLETEMENT

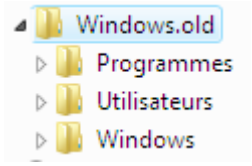
Réinstaller le système :

Il est possible de réinstaller complètement Windows 8 (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

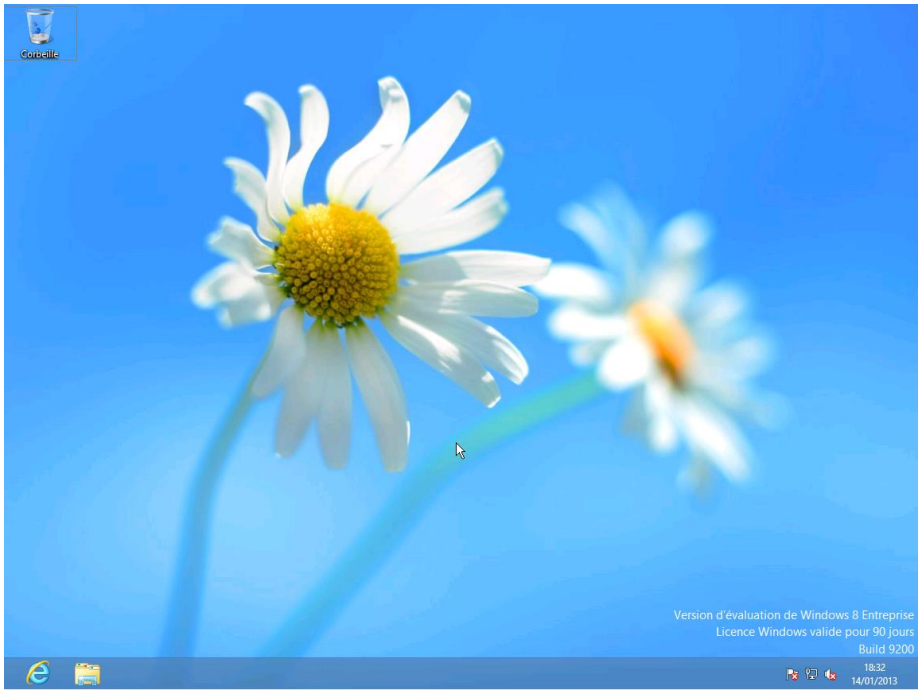
Il est donc possible d'aller récupérer manuellement des données dans ces structures préservées.

N.B: Après une **installation complète**, Si vous avez installé Window 8 dans la même partition que votre ancien SEVEN, ou XP, il n'est pas possible de désinstaller le nouveau système.

LES TUILES DE L'ACCUEIL

Ecran Accueil par défaut

Alors que le bureau se contente d'une résolution 1027 x 768 px



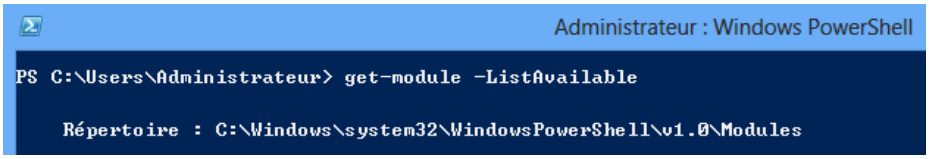
l'écran d'accueil windows 8demande une résolution de 1366 x 768 px

Les tuiles suivantes peuvent apparaître :

Courrier IE Windows Store Bing Calendrier Cartes Skydrive

Gestion des tuiles pré-définies en Powershell

On passe en powershell. La commande **Get-Module –ListAvailable** permet de recenser 2 modules importants pour la gestion des tuiles : **Appx** et **Dism**



On importe le module

```
PS C:\Users\Administrateur> Import-Module appx
PS C:\Users\Administrateur> _
```

On peut vérifier les les commandes importées par un

(Get-Module appx).exportcommands

```
PS C:\Users\Administrateur> (Get-Module appx).exportedcommands

Key                                                    Value
---                                                    -----
Add-AppxPackage                                        Add-AppxPackage
Get-AppxPackage                                        Get-AppxPackage
Get-AppxPackageManifest                                Get-AppxPackageManifest
Remove-AppxPackage                                     Remove-AppxPackage
Get-AppxLastError                                      Get-AppxLastError
Get-AppxLog                                            Get-AppxLog
```

la liste des packages installés sur le poste 8 est disponible via

Get-AppxPackage (respectivement **Get-appxprovisionedPackage –online)**

```
PS C:\Users\Administrateur> Get-AppxPackage

Name                   : windows.immersivecontrolpanel
Publisher              : CN=Microsoft Windows, O=Microsoft Corporation,
Architecture           : Neutral
ResourceId             : neutral
Version                : 6.2.0.0
PackageFullName        : windows.immersivecontrolpanel_6.2.0.0_neutral_
InstallLocation        : C:\Windows\ImmersiveControlPanel
IsFramework            : False
PackageFamilyName      : windows.immersivecontrolpanel_cw5n1h2txyewy
PublisherId            : cw5n1h2txyewy

Name                   : WinStore
Publisher              : CN=Microsoft Windows, O=Microsoft Corporation,
Architecture           : Neutral
ResourceId             : neutral
Version                : 1.0.0.0
PackageFullName        : WinStore_1.0.0.0_neutral_neutral_cw5n1h2txyewy
InstallLocation        : C:\Windows\WinStore
IsFramework            : False
PackageFamilyName      : WinStore_cw5n1h2txyewy
PublisherId            : cw5n1h2txyewy

Name                   : Microsoft.BingFinance
Publisher              : CN=Microsoft Corporation, O=Microsoft Corporat
Architecture           : X64
ResourceId             :
Version                : 1.2.0.135
```

Si on veut supprimer un package, on le supprime d'abords pour l'utilisateur Administrateur Build-In courant, avec son fullname

Remove-AppxPackage fullname

```
PS C:\Users\Administrateur> Remove-AppxPackage Microsoft.BingFinance_1.2.0.135_x64__8wekyb3d8bbwe
```

puis pour les autres users (a venir…)

Remove-AppxProvisionedPackage –online –PackageName:fullname

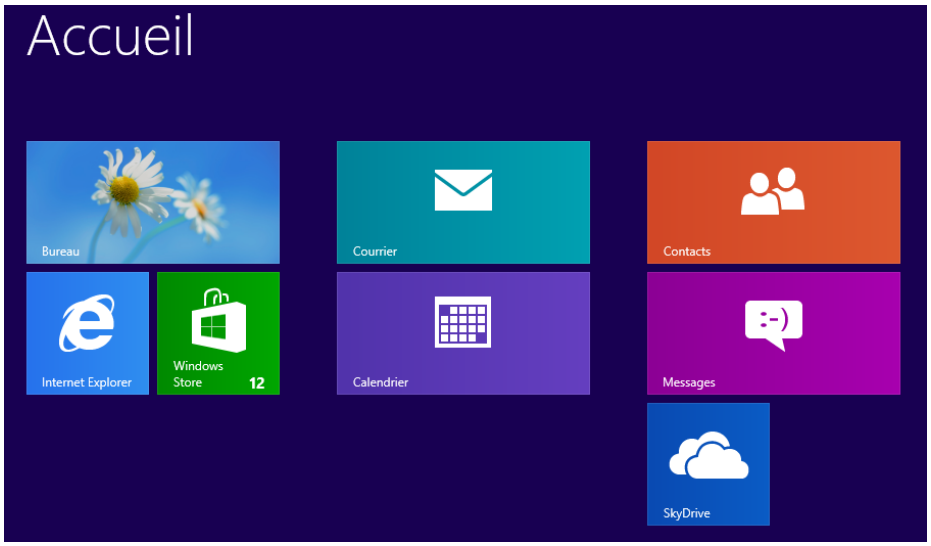
```
PS C:\Users\Administrateur> Remove-AppxProvisionedPackage -online  -PackageName Microsoft.BingFinance_1.2.0.135_x64__8w
kyb3d8bbwe

Path          :
Online        : True
Restart Needed : False
```

N.B : si on ne fait pas les deux, lors d'un eventuel sysprep il peut y avoir erreur

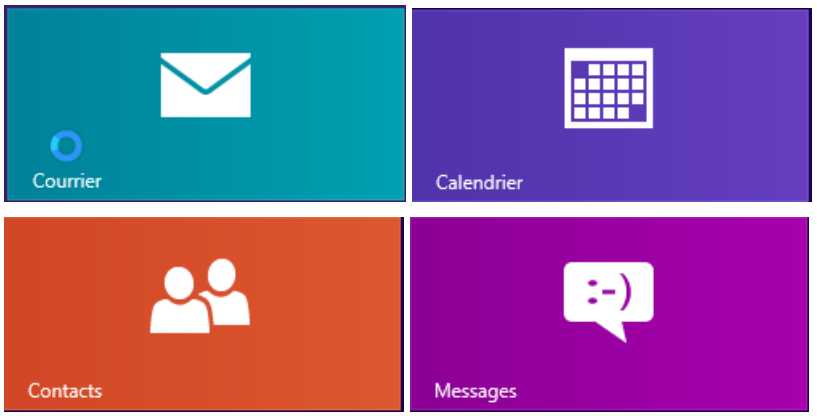
On peut supprimer sans état d'ames les packages suivants

```
Microsoft.BingNews_1.2.0.135_x64__8wekyb3d8bbwe
Microsoft.BingSports_1.2.0.135_x64__8wekyb3d8bbwe
Microsoft.BingTravel_1.2.0.145_x64__8wekyb3d8bbwe
Microsoft.BingMaps_1.2.0.136_x64__8wekyb3d8bbwe
Microsoft.BingWeather_1.2.0.135_x64__8wekyb3d8bbwe
microsoft.windowsphotos_16.4.4204.712_x64__8wekyb3d8bbwe
Microsoft.BingFinance_1.2.0.135_x64__8wekyb3d8bbwe
Microsoft.Camera_6.2.8514.0_x64__8wekyb3d8bbwe
Microsoft.Bing_1.2.0.137_x64__8wekyb3d8bbwe
Microsoft.ZuneMusic_1.0.927.0_x64__8wekyb3d8bbwe
Microsoft.ZuneVideo_1.0.927.0_x64__8wekyb3d8bbwe
Microsoft.XboxLIVEGames_1.0.927.0_x64__8wekyb3d8bbwe
```

Pour obtenir un écran plus épuré



Voire si on supprime en plus



les 4 sont supprimables via

```
microsoft.windowscommunicationsapps_16.4.4206.722_x64__8wekyb3d8bbwe
```

Alors que 

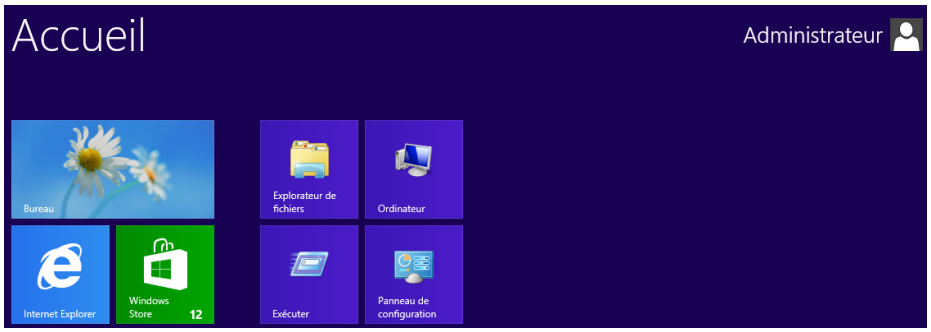
est gérable par

```
microsoft.microsoftskydrive_16.4.4204.712_x64__8wekyb3d8bbwe
```

ce qui devient assez radical...

Epingler des tuiles sur l'accueil

On peut facilement ajouter des tuiles sur l'écran Accueil en demandant lorsque l'on est sur une application de l'épingler sur l'Accueil…



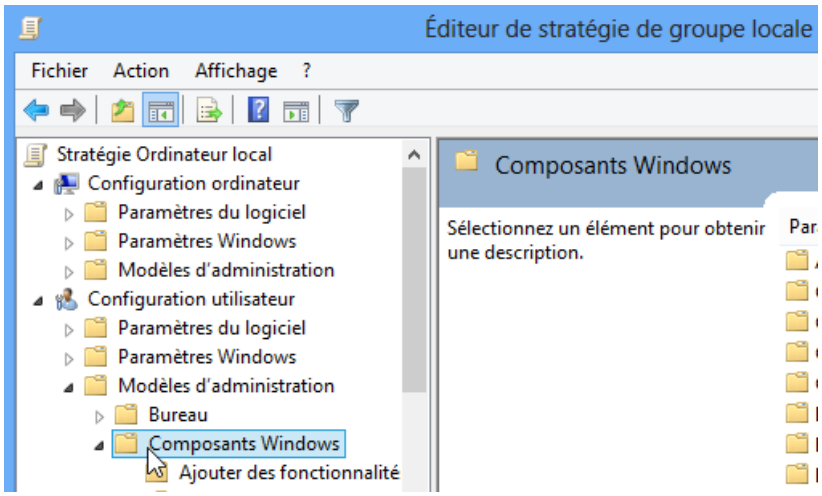
Gestion Windows Store

l'icone Windows Store ne peut être supprimée, mais elle peut être désactivée de manière a ce que les utilisateurs ne puissent ajouter n'importe qu'elle tuile sur leur poste

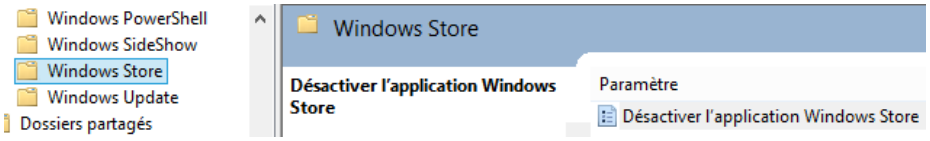
on pourra par stratégie

gpedit.msc

Configuration Utilisateur / Modèles d'administration / Composants Windows

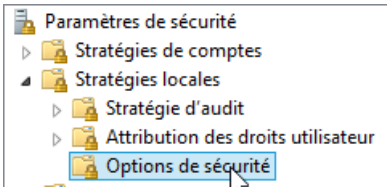


chercher l'entrée **Windows Store**

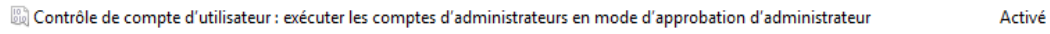


Si on décide de laisser **Windows Store** actif, alors il faut que l'**UAC** soit en place…y compris donc pour les comptes Administrateurs, donc dans les

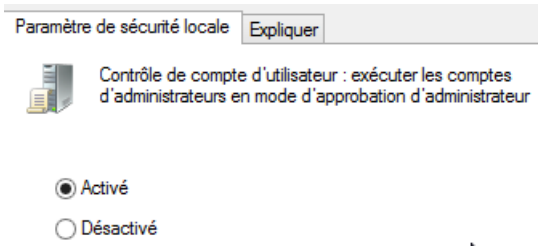
stratégies de sécurité locale /



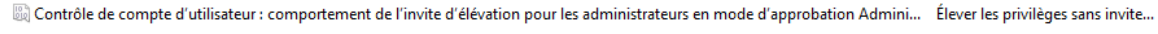
UAC actif, y compris pour les administrateur (sauf l'admin intégré)



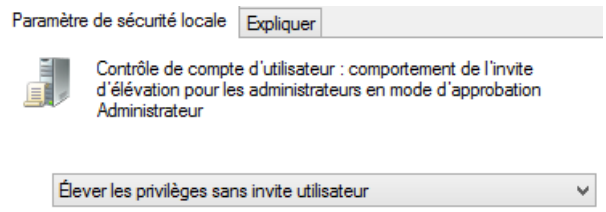
donc



même si on peut demander une élévation automatique, donc



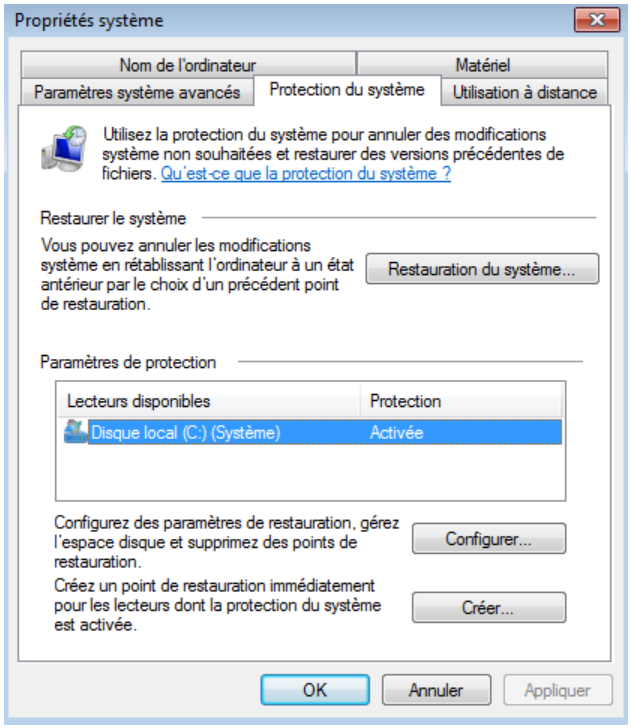
donc



POINTS DE RESTAURATION

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 est 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.

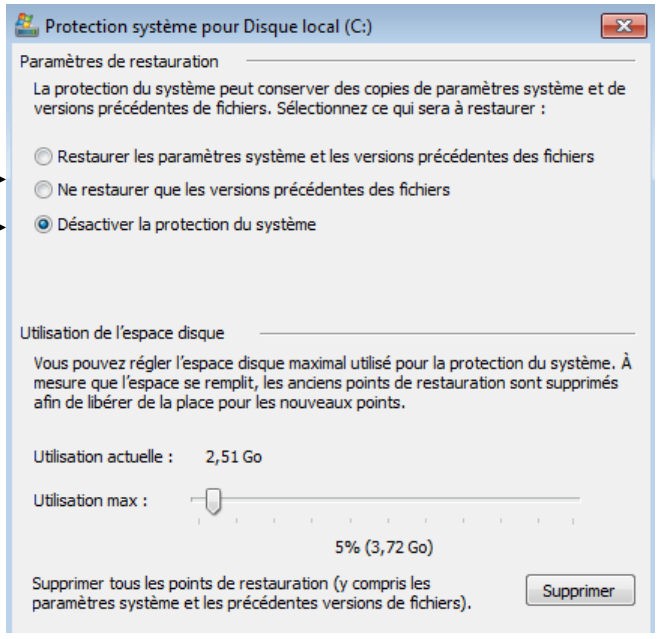
N.B : on peut dissocier le lecteur système des lecteurs de données.

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

Désactivation de la Restauration

Il faut demander **Configurer…**

Puis au choix

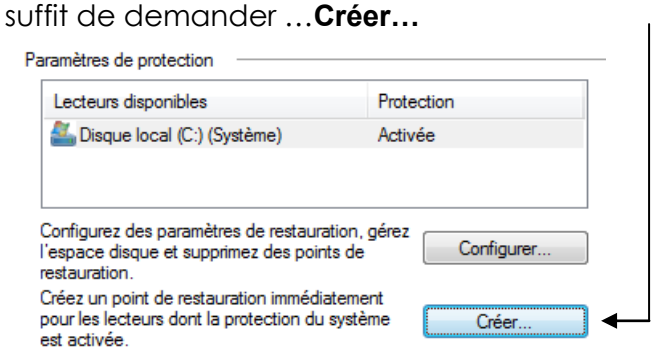


N.B: L'espace disque disponible pour la restauration est ajustable, et détermine le nombre de point de restauration qui peuvent être crées. (la config par défaut peut stocker plusieurs semaines de points de restauration.)

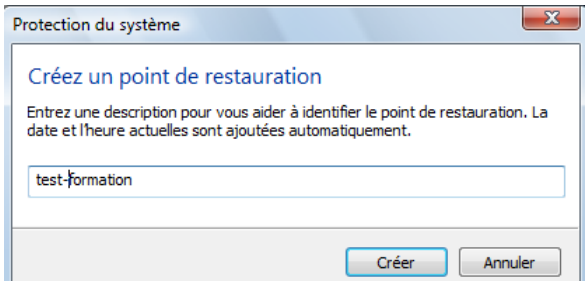
Création d'un point de restauration

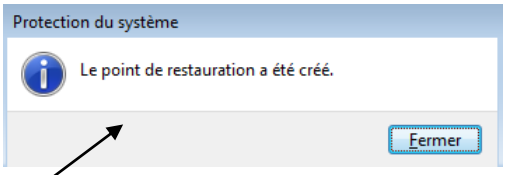
Les points de restauration sont créés par le système (lors de l'installation de programme, drivers, mise à jours système…) ou par l'utilisateur

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

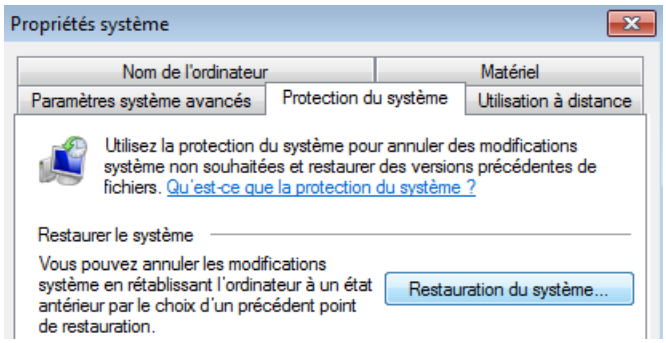




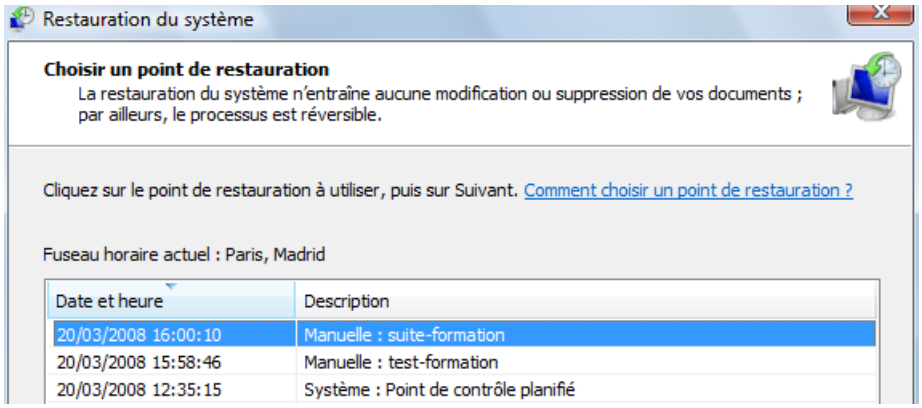
puis on demande **Créer** et on devrait obtenir

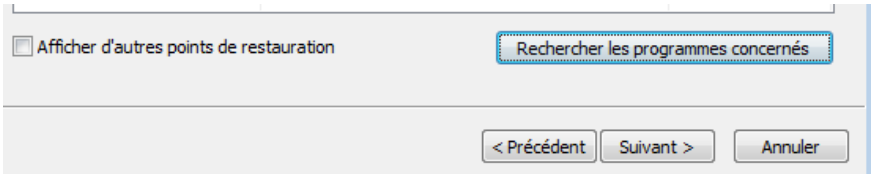
Utiliser Annuler un point de restauration

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

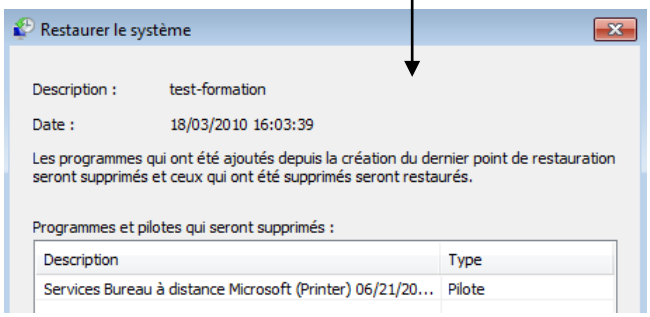


C'est un assistant La liste des points de restauration apparaît …

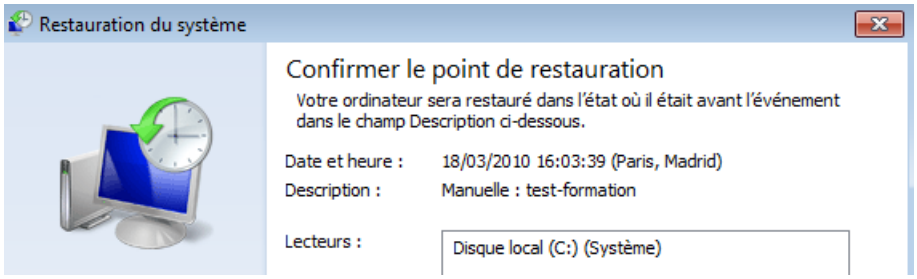




A titre d'information, pour aider dans le choix du point de Restauration, le bouton **Rechercher les programmes concernés** est assez utile…



après avoir choisit, 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** : crées toutes les 24 heures, et après 10 heures de fonctionnement à la suite.
2. **Points de restauration d'installation de programmes / pilotes**: crées 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, I 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-a
f8a-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-8
173-0080c8e6c311}\
   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 :

Windows 8 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 Windows (si elle est effectuée ou programmée)

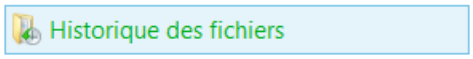
N.B: Ne pas confondre effectuer des sauvegardes de fichier , la technique des points de restauration et la création d'image disque système de Windows 8…

Image système - vhd :

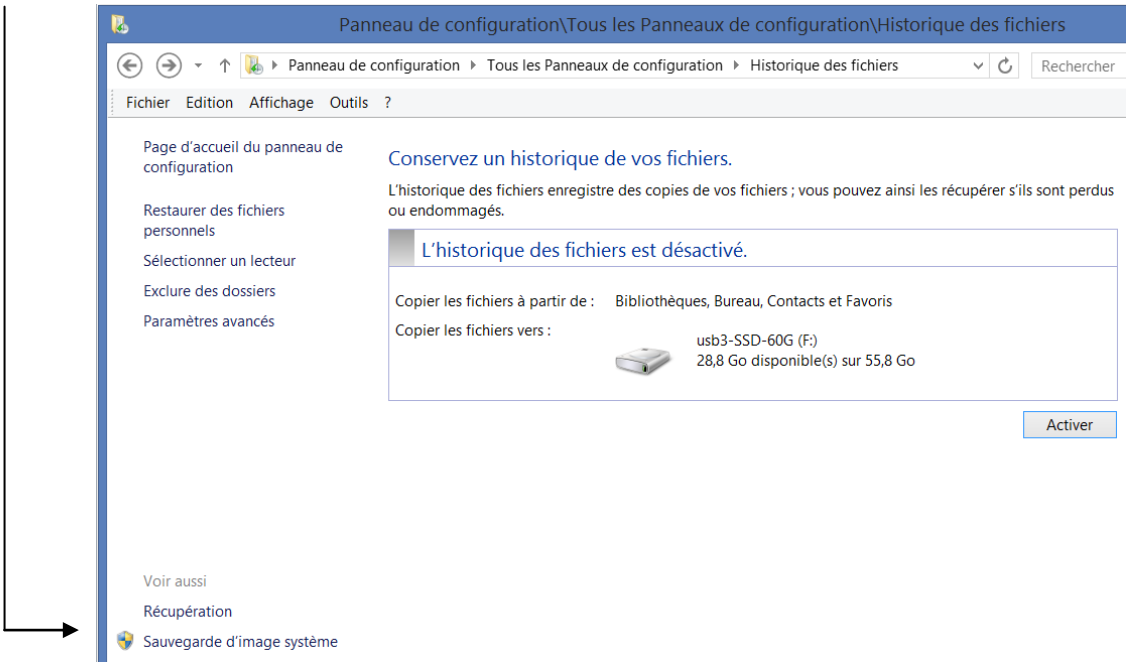
Il est donc possible de sauvegarder un volume entier au format **.vhd**

- Avantage : permet de restaurer un ordinateur complet
- Avantage : peut être stocké que sur un lecteur local (CD, DVD, disque amovible…) ou Réseau
- Inconvénient : occupe plus de place, de temps

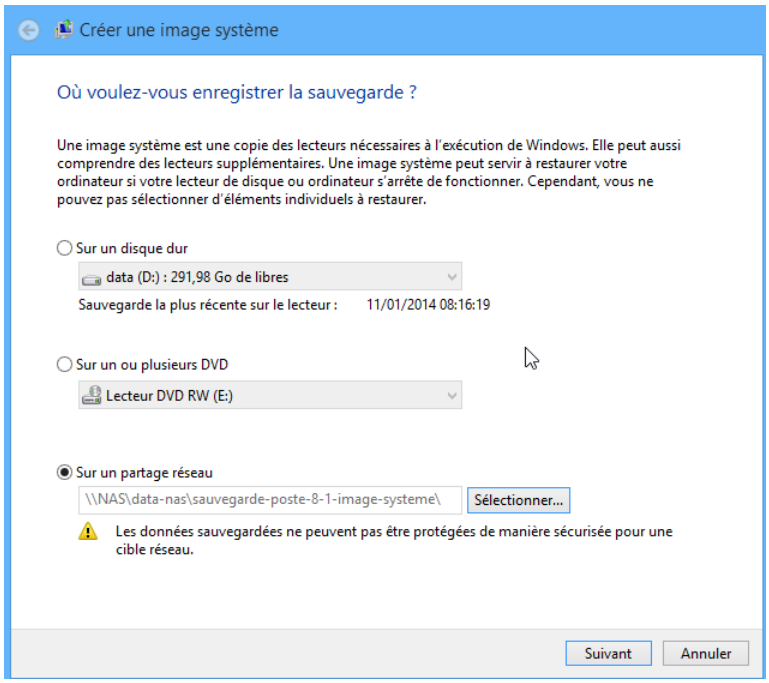
Via le menu **panneau de Configuration / Historique des fichiers**

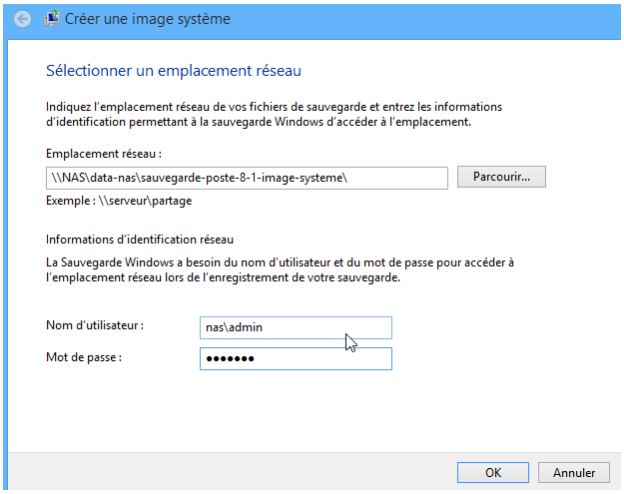


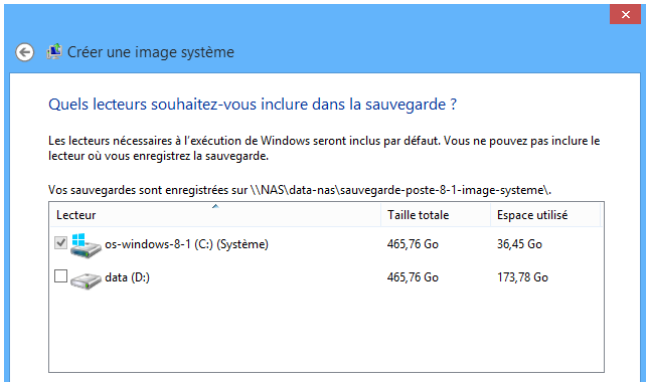
On demande **Créer une image système**

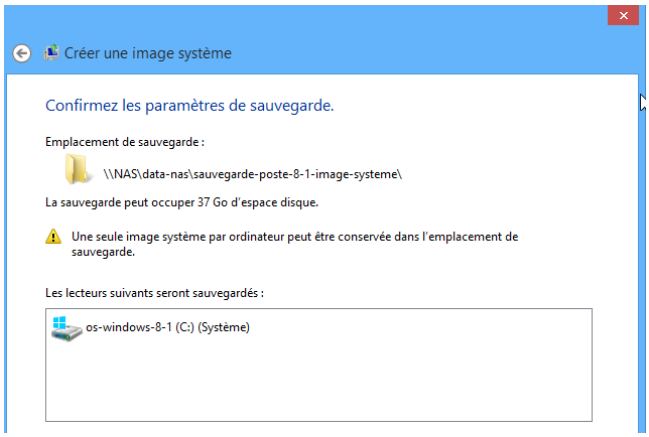


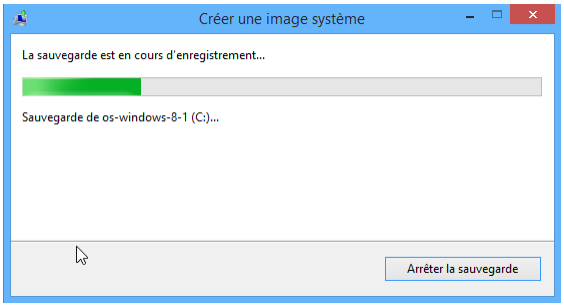
Ici avec **Sauvegarde d'image système** un assistant se déclenche



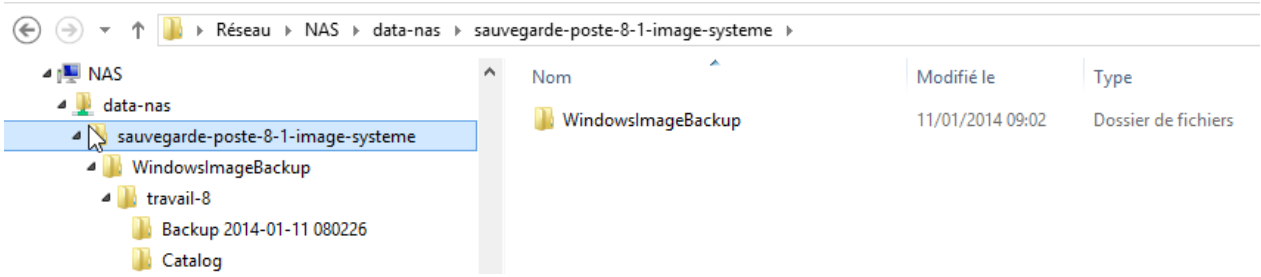




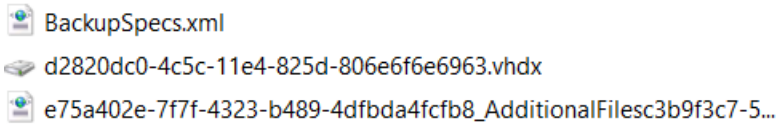




Cela crée



Avec une nature de fichier .VHDX



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

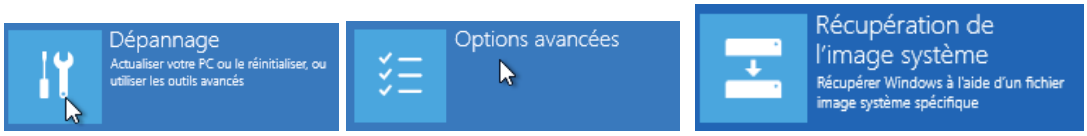
```
C:\Users\Administrateur>wbadmin get status
wbadmin 1.0 - Outil de ligne de commande de sauvegarde
(C) Copyright 2004 Microsoft Corp.

La sauvegarde du volume Réservé 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

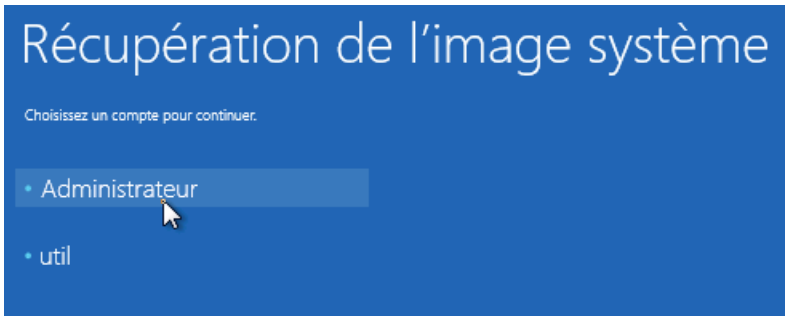
Cela peut se faire en bootant sur le CD démarrant Windows RE

Ou via le Menu des Options de démarrage , **MAJ+Redémarrer**

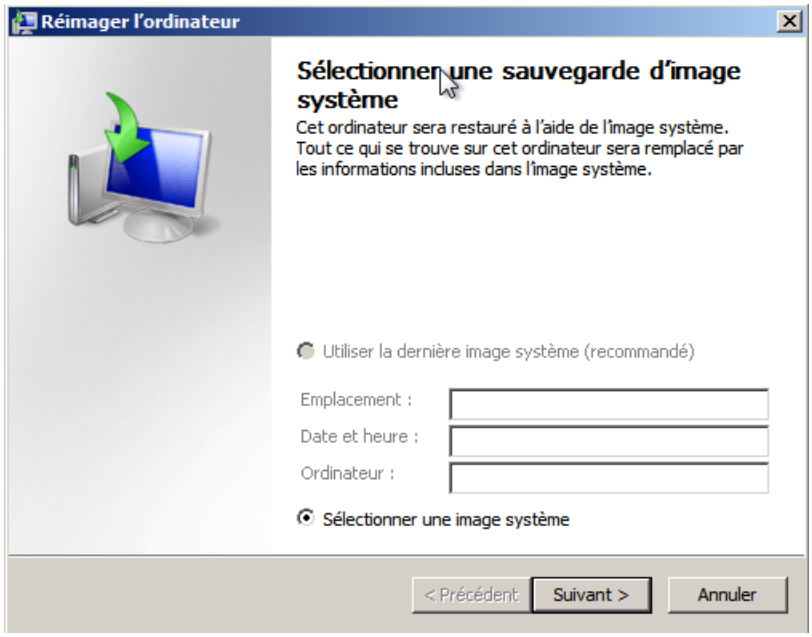
et **Dépannage / Options Avancées / Récupération de l'image système**



Il faut s'authentifier, puis

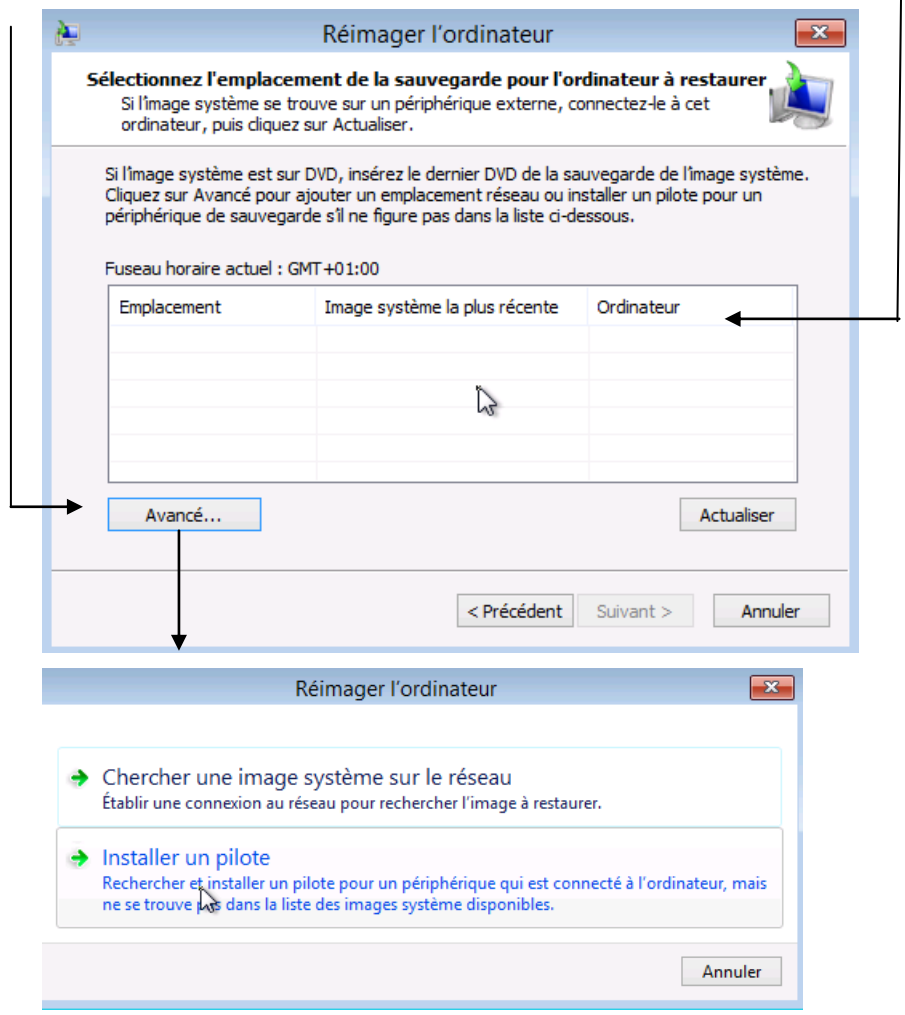


Cela déclenche un assistant

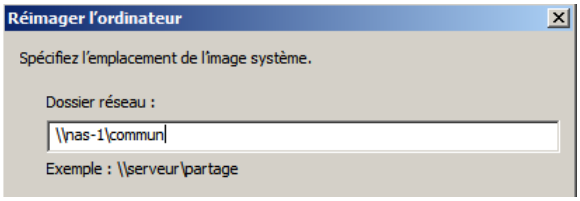


N.B: La dernière image système apparaît si elle est stockée localement…

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



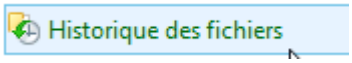
N.B: à ce stade on utilise les drivers réseau connus du Media utilisé ! Attention donc au périphériques non reconnus en standard par Windows 8



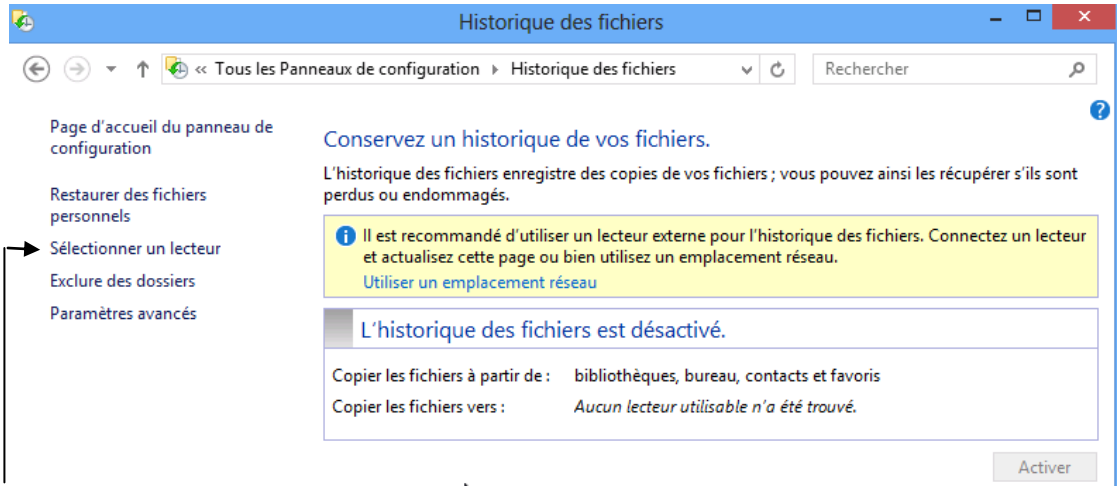
HISTORIQUE DES FICHIERS

Mise en place

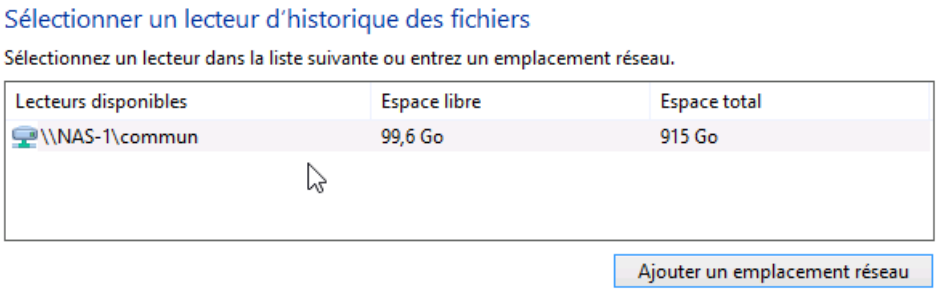
Via le menu **panneau de Configuration / Historique des fichiers**



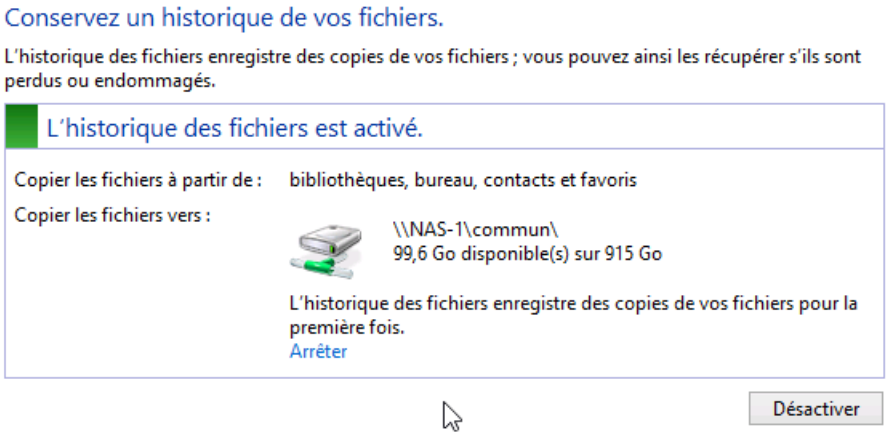
Il faut mettre en place un lecteur de stockage …



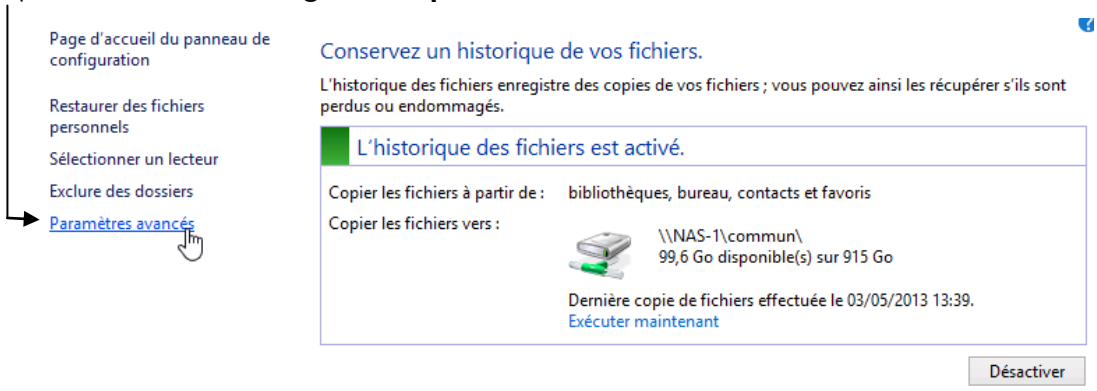
On demande de **Sélectionner un lecteur**



Et on active

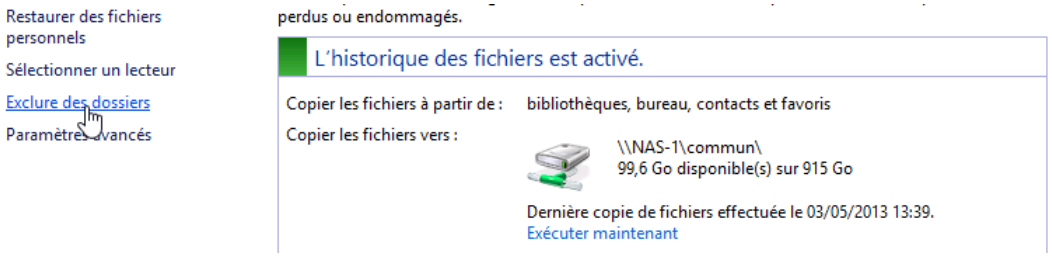


On peut demander de gérer les **paramètres avancés**

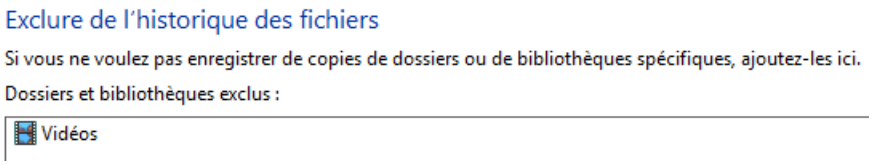


Pour définir la fréquence des synchronisations

On peut demander d' **Exclure des dossiers**

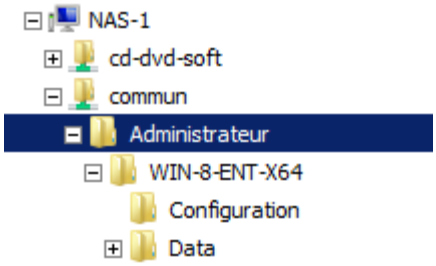


Par rapport aux emplacements pré-définis, c'est-à-dire **Bibliothèque, Bureau, contacts et favoris**…

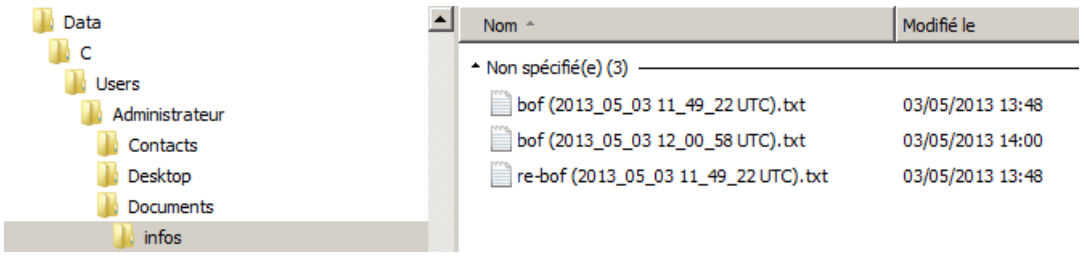


Stockage

Physiquement une arborescence est créée, avec le nom de login utilisateur , (ici dans l'exemple ***administrateu***r) et le nom du poste windows 8 (ici dans l'exemple ***win-8-ent-x64***)

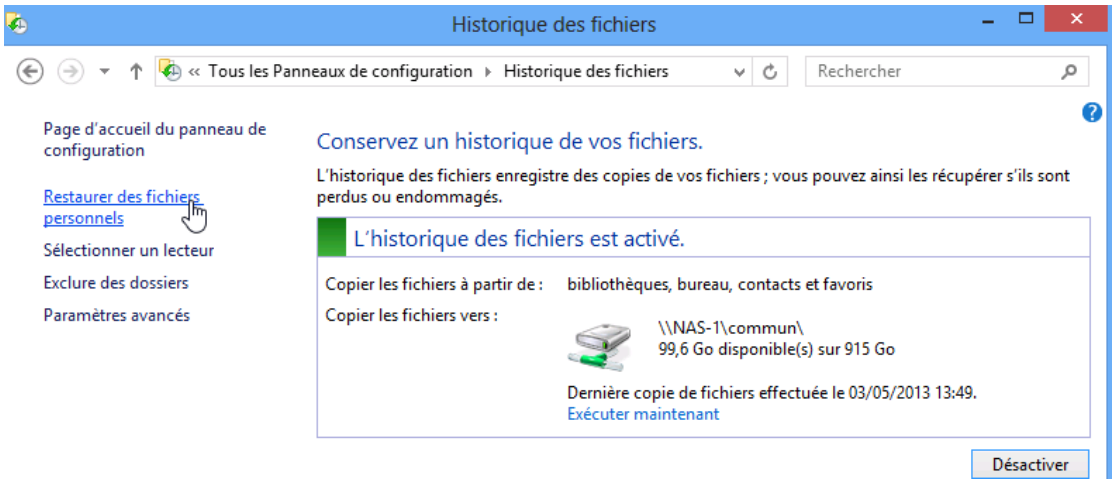


Que l'on peut retrouver donc

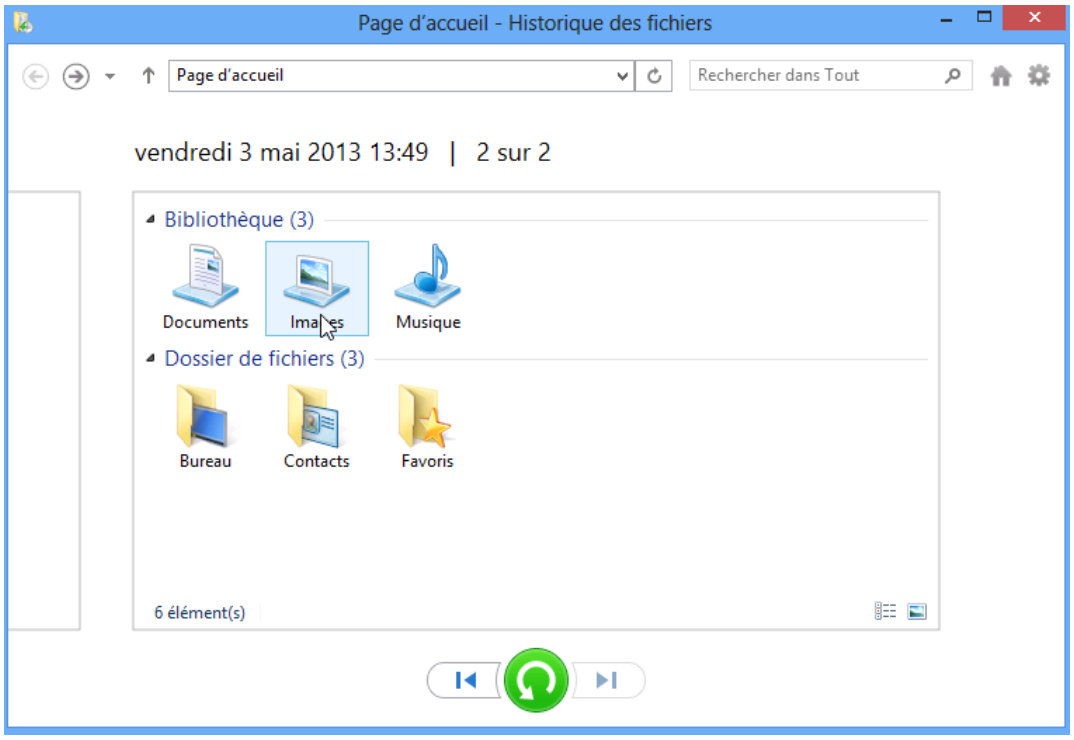


Restaurer des fichiers

Via le menu **panneau de Configuration / Historique des fichiers**



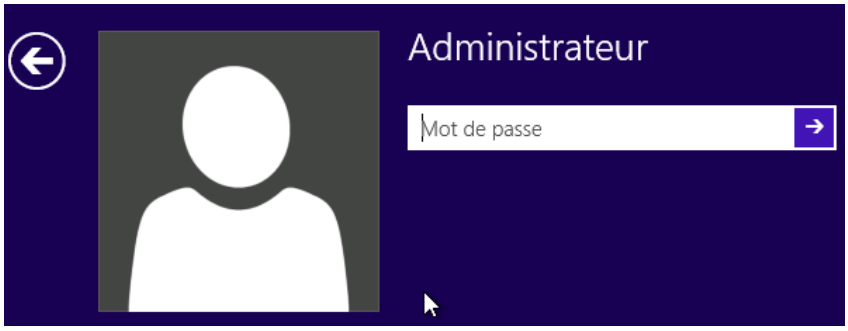
On a une interface qui se suffit à elle – même



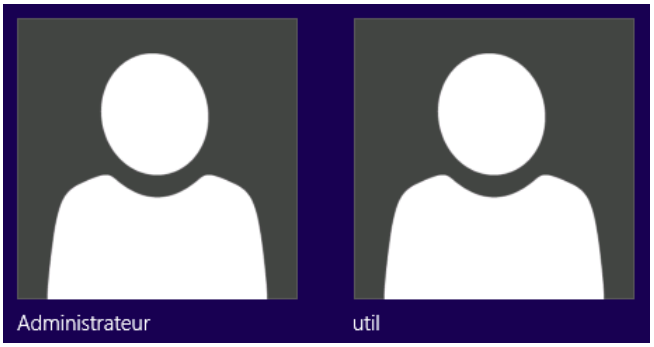
COMPTES UTILISATEURS

Compte d'utilisateurs – session:

On parle de **compte utilisateur** lorsque l'on définit un individu nommément 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



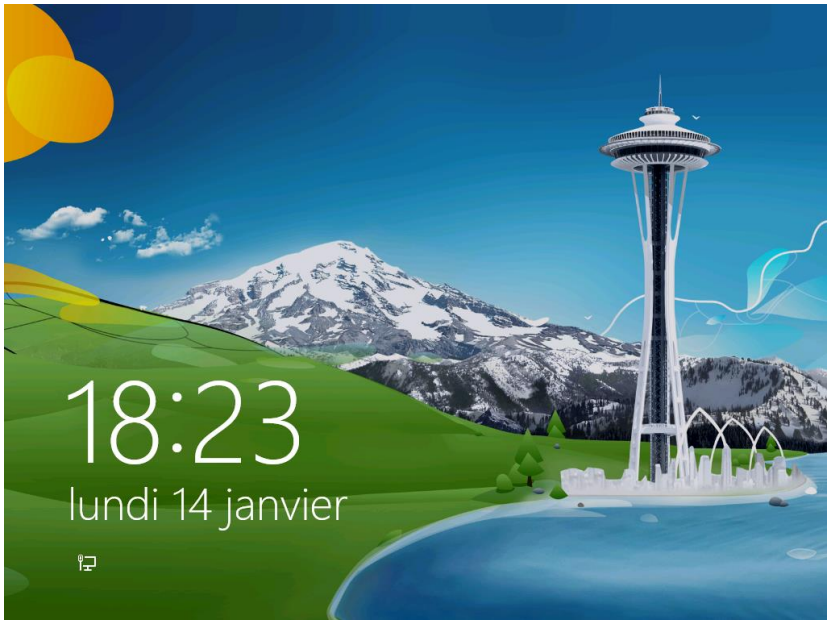
Le mot de passe peut contenir jusqu'à **127 caractères**

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

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

L'écran de Verrouillage qui apparait lorsqu'aucune session inter-active n'est ouverte.

Des que l'on s'est loggué On tombe sur l'écran d'accueil



N.B : si la désactivation de l'écran de verouillage est demandée cela peut se gérer via les stratégies via **Gpedit.msc**

Configuration ordinateur / Modèles d'administration / Panneau de Configuration /Personnalisation

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

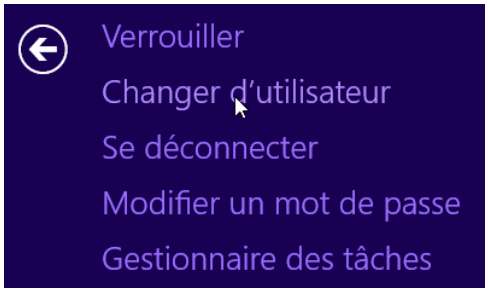
Séquence authentifiée 2 ↓

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 Windows 8 (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 plus nécessaire de fermer la session d'un autre 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

Ouverture de session

Séquence authentifiée 1 ↓

Changer d'utilisateur (entrée stand-by)

Ouverture de session

Séquence authentifiée 2 ↓

Fermeture de session

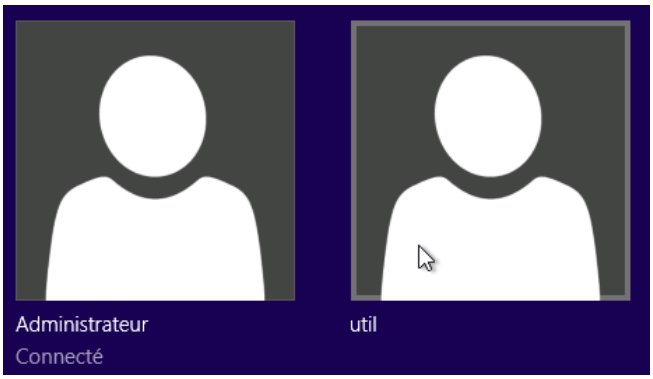
(sortie stand-by)

Séquence authentifiée 1 ↓

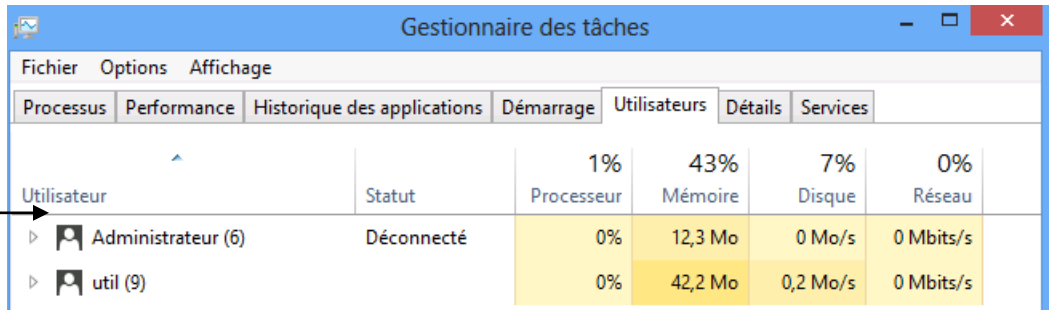
Fermeture de session

Arrêt Poste

Pour chaque connexion de chaque session, par exemple Util 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

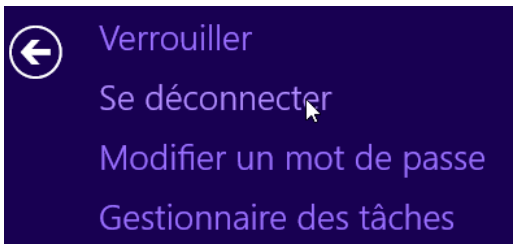


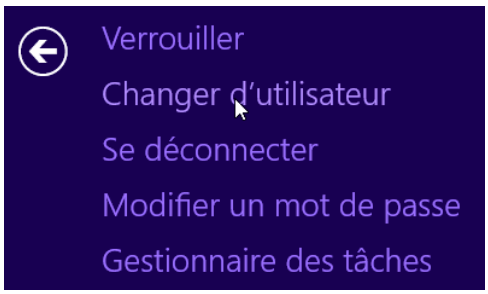
N.B: Cette fonctionnalité, extrêmement gourmande en ressource, pose certains problèmes avec des applications non spécifiquement dessinée pour **Windows 8**, et entraîne parfois des pertes de donnée …

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

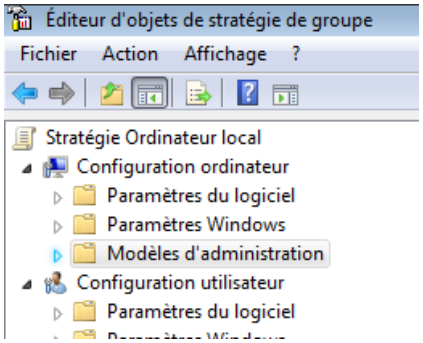
Désactiver la bascule rapide Utilisateur

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





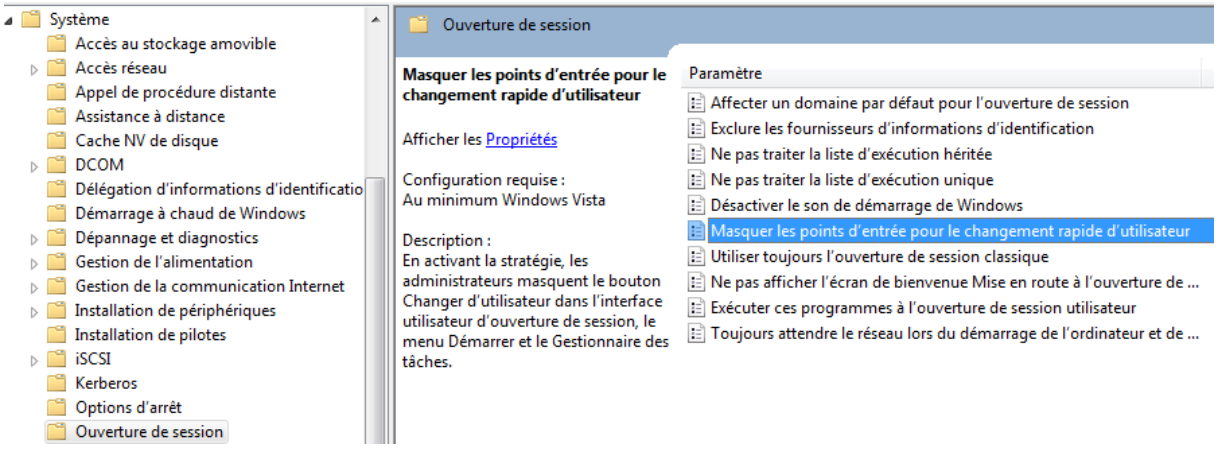
Soit on utilise **gpedit.msc**



Configuration ordinateur / Modèles d'administration

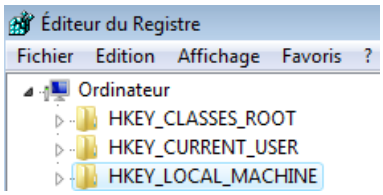
puis

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

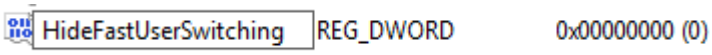
Regedt32.exe



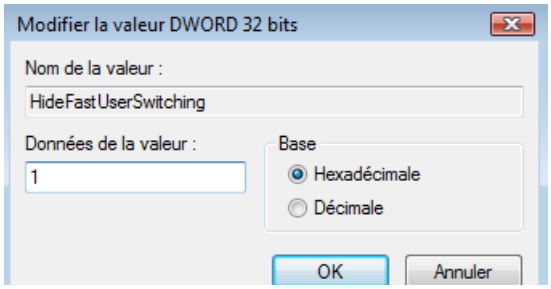
Et dans la clé

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.



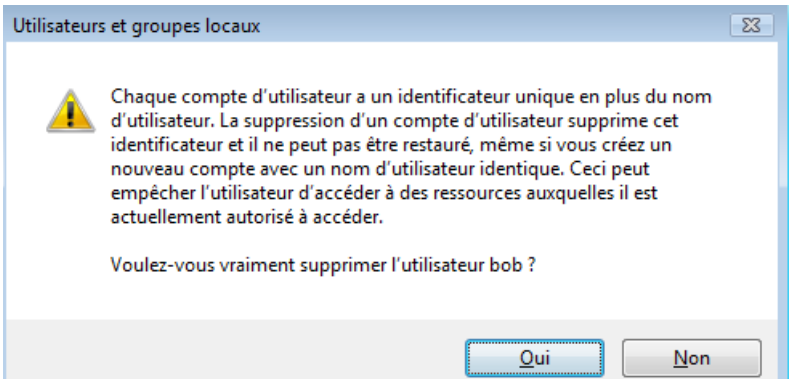
N.B : cette option est automatiquement activée si le poste fait partie d'un domaine. (par défaut la bascule entre utilisateurs locaux est activé sur un poste en workgroup)

SID Sécurity identifier :

Le **SID** est un numéro d'identification unique sur un poste Windows 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° création, et par conséquent on ne pourra réutiliser les ressources droits et permissions allouées lors de la première utilisation

Windows 8 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
============================== ============================================
win-8-ent-x64\administrateur S-1-5-21-3539324183-3274001343-3598065848-500
```

Comptes pré-définis :

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

Sous **Windows 8** 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 s

- Ce compte par défaut est inactivé

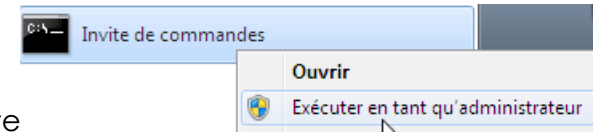
N.B: dans la pratique, lors de l'installation d'un poste Windows 8 hors domaine, un assistant se déroule lors du premier démarrage, demandant les noms des "futurs" utilisateur du poste…. Cela a pour effet de créer des comptes utilisateur – administrateurs !

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

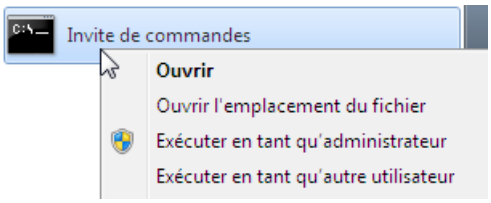
Exécuter en tant que:

On peut lancer une application avec un login autre que celui en cours… ou en tant qu'administrateur, pour éviter les problèmes liés à l'UAC

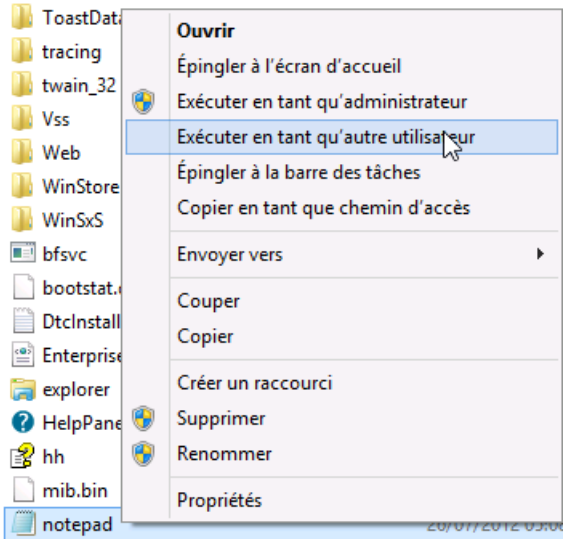
Soit **clic droit** / sur l'invite

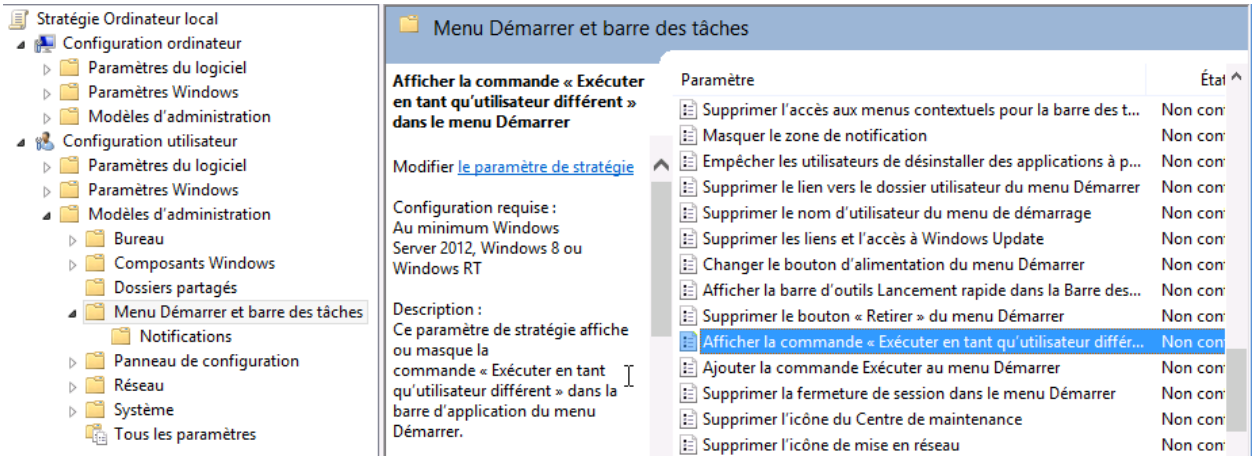


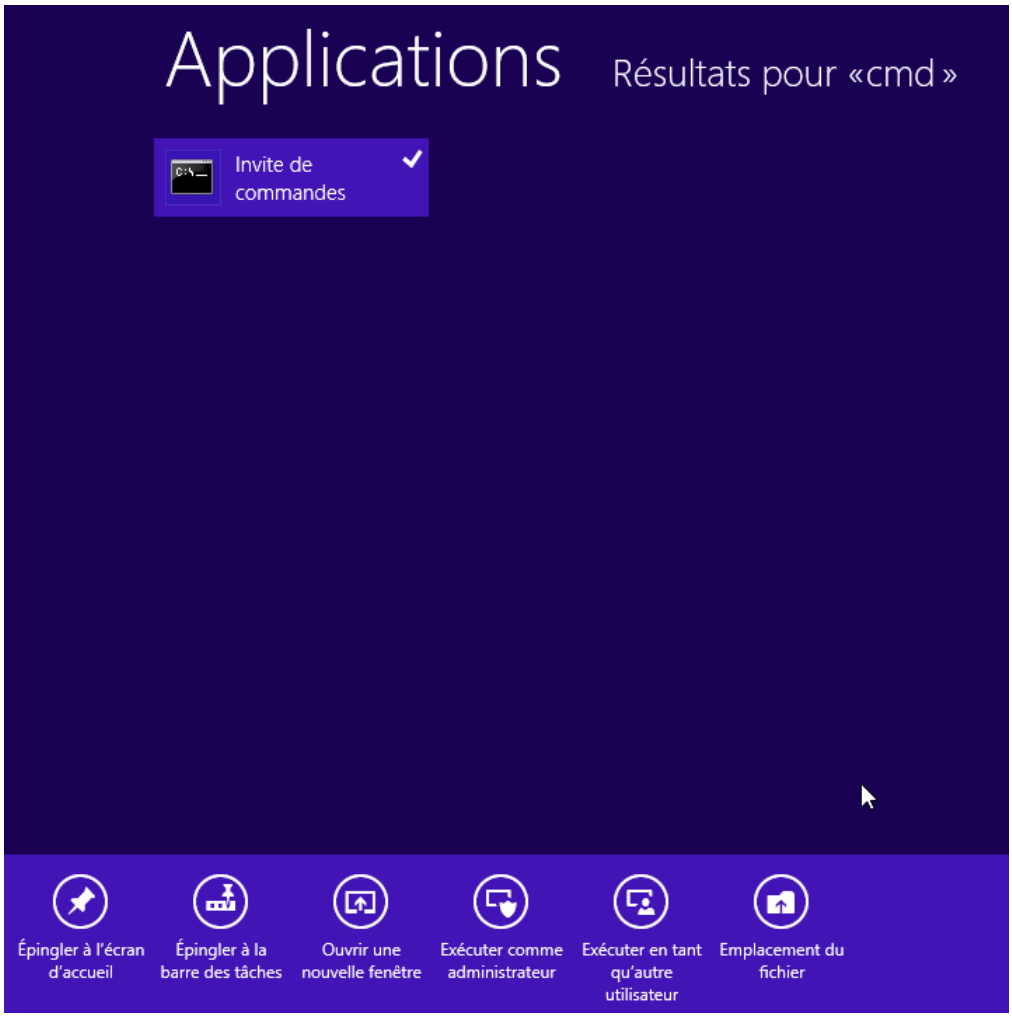
Soit **MAJ + clic droit** / sur l'invite



Soit **MAJ + clic droit** / sur l'executable







Utilisateurs locaux:

Il est possible de créer des comptes utilisateurs sur un poste **Windows 8** on parle alors de comptes locaux, qui n'ont de portée que la machine sur laquelle ils sont créés.

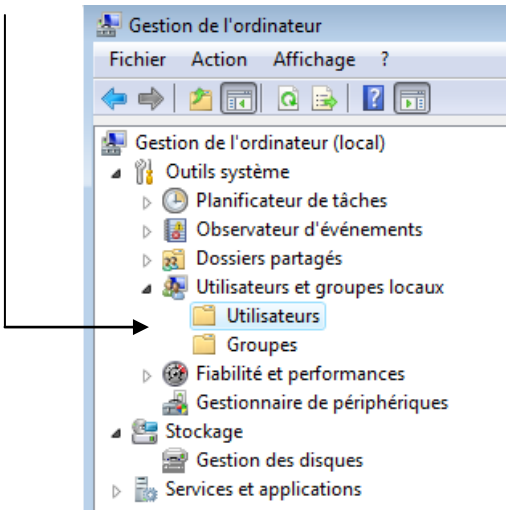
La meilleure façon pour faire cela se trouve dans le menu

Démarrer / Panneau de configuration (affichage classique)

/ Outils d'Administration/ Gestion de l'ordinateur

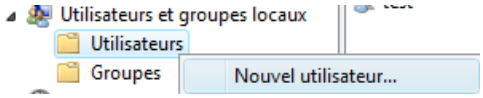
Ou plus rapidement par clic droit sur l'icône **Ordinateur** du bureau

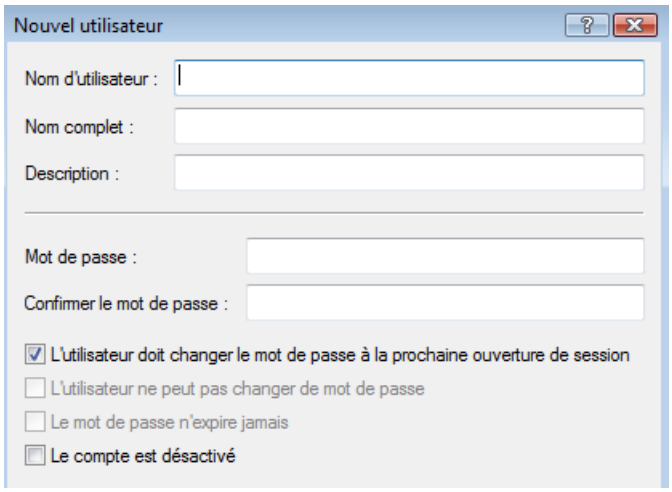
Sur l'icône **Ordinateur** du bureau on demande clic droit **gérer**



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

Puis **Nouvel utilisateur…**

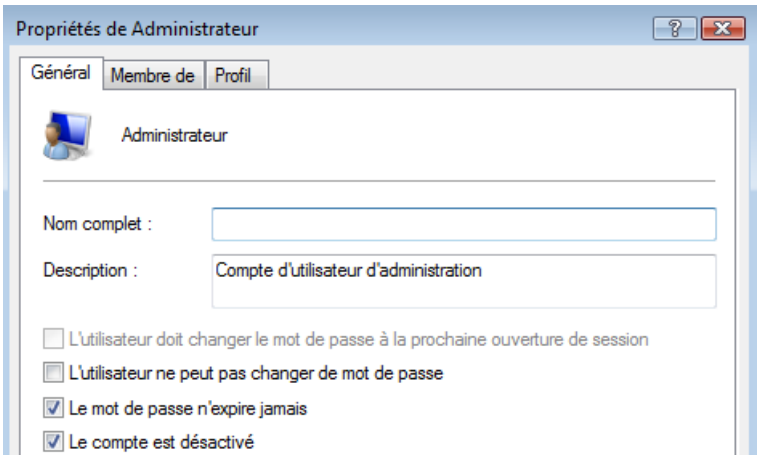




Gestion des Comptes:

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

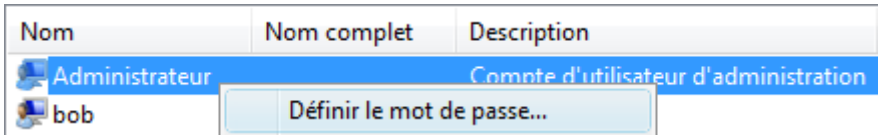
Comme on ne peut pas lui donner un mot de passe lors de l'installation, il faut impérativement lui en donner un lors de son activation !



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

Re-définition de mot de passe

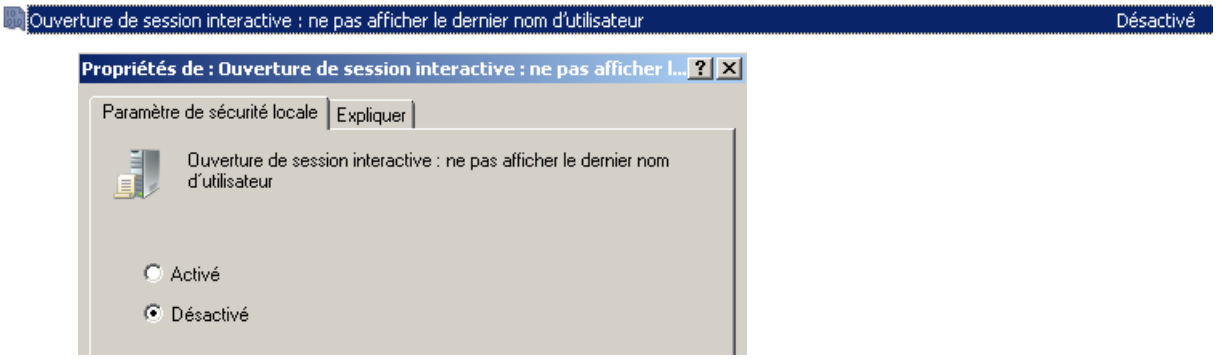
Si on en a les privilèges, on réinitialise le mot de passer d'un compte utilisateur en faisant clic-droit sur le compte à changer, puis on demande **Définir le mot de passe…**



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

GROUPES 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 biens définis, 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 définis, 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 groupe 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 lnk. 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 **lnk** de 800 octets ?, alors qu'avec un lien symbolique, nous pourrons savoir combien pèse le dossier cible, géré 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 l bureau, il vous suffira de créer des liens symboliques sur le bureau avec ces dossiers.

N.B: Les jonctions de répertoire font "double emplois" 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 crée 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 Windows 8) ou **Default User** (sous XP)

Emplacement Profils Locaux Seven:

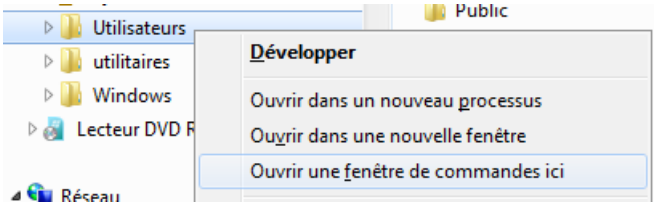
Les Profils Windows 8 ne sont pas stockés comme les profils XP:

XP (**Document and Settings**)	Windows 8 -7 (**Users** ou "***Utilisateurs***")

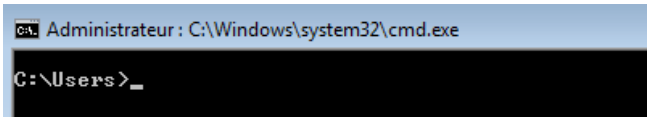
- Le dossier Racine des profils devient « visuellement » le dossier **\Utilisateurs** (selon la régionalisation française) mais se trouve être le dossier **\Users** (anciennement **\Document and Settings)**

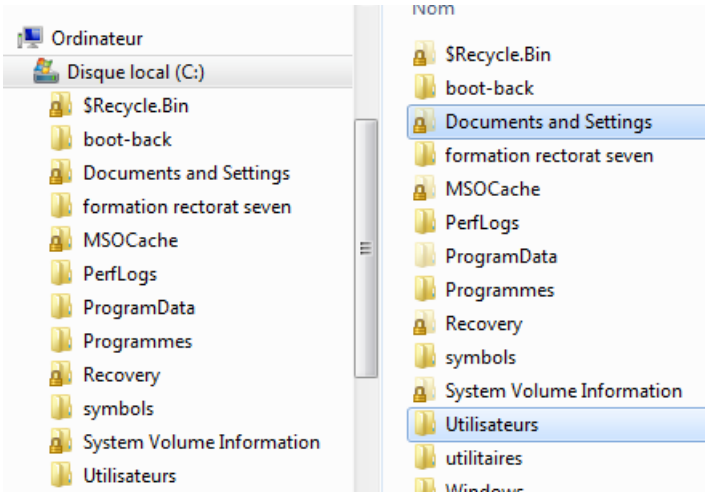
N.B : Avec la régionalisation Windows 8, le dossier **Users** apparaît dans l'explorateur comme **Utilisateurs.** Mais on le retrouve en demandant

Clic-Droit / Ouvrir une fenêtre de commandes ici

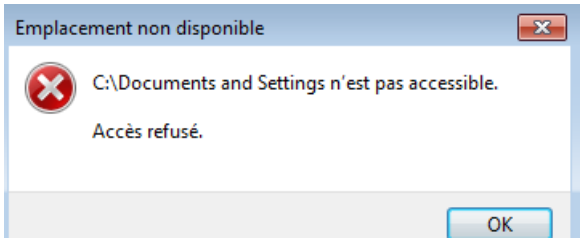


On obtiendra



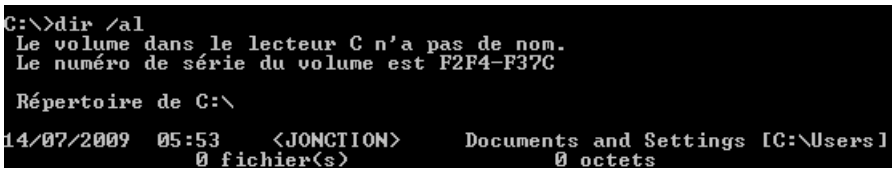


N.B : on ne peut plus « accéder » à **Documents and Settings**… ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **user**…



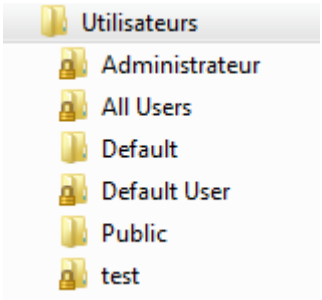
La commande en invite

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



Structure des Profils Windows 8:

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



2 nouveaux dossiers système :

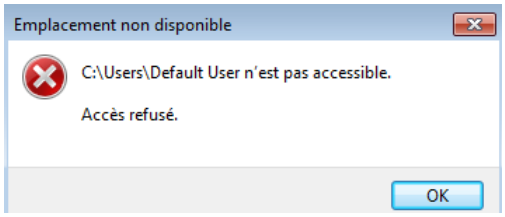
Default et **Public**

2 jonctions pour compatibilité XP-2000 :

Default User et **All Users**

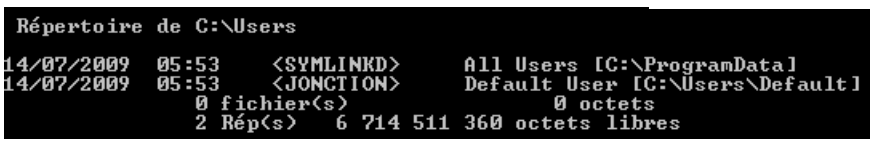
Et les dossier profils des utilisateur crées : Administrateur , test, xxxxx

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…

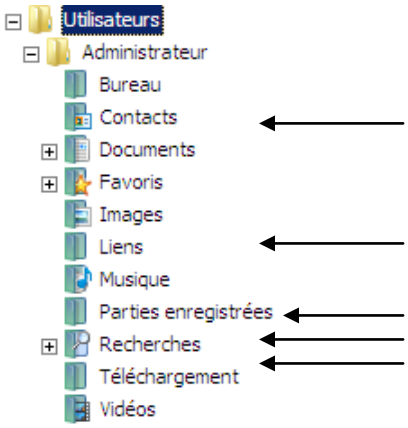


Structure d'un profil Utilisateur

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

XP (**Document and Settings**)	Windows 8 -7 (**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**

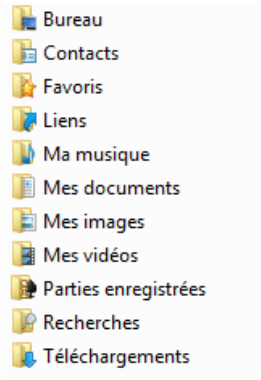
- Les préfixes **mes** et **ma** sont supprimés des dossiers **document** ou **musique** (à la place de **mes document** ou **ma musique**
- Les dossiers **document** ou **musique…** ne sont plus des sous-dossiers du dossier mes documents, mais sont directement crées à la racine du dossier profils (en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



5 Nouveaux dossier dans un profil sous Seven

Contacts
Liens
Parties enregistrées
Téléchargement
Recherches

- 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 Windows 8 dans un sous dossier du profil utilisateur **\AppData\Roaming\Microsoft\Windows…** comme par exemple

Menu Démarrer	**Appdata\Roaming\Microsoft\Windows\Start Menu**
Modèles	**Appdata\Roaming\Microsoft\Windows\Templates**

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

Profil par Défault

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    <JONCTION>     Default User [C:\Users\Default]
```

Méthode Certifiée pour modifier le profil par défaut

Il n'est plus possible dans Windows 8 selon Microsoft de modifier le profil par défaut comme on le faisait dans XP

Ceci car certains petits bug apparaissaient 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 !!

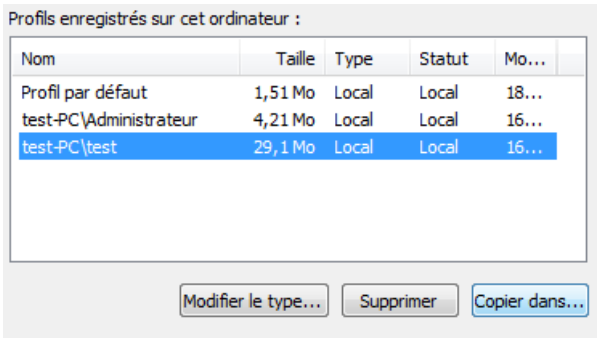
1. Créer un utilisateur "test" (ou mieux "*test*-xyz") ayant des droits d'administration sur le poste

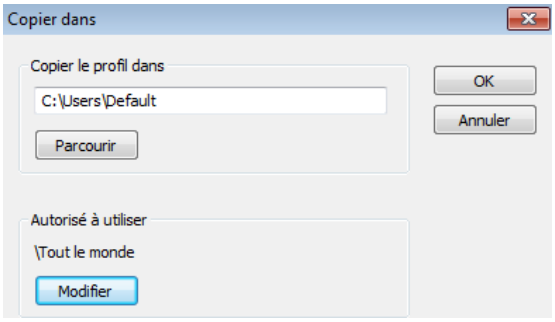
2. Ouvrir une session avec, et faire tous ses réglages…

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

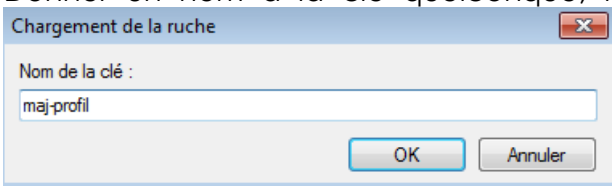
4. Installer l'utilitaire "**windows enabler**"  et l'activer 

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





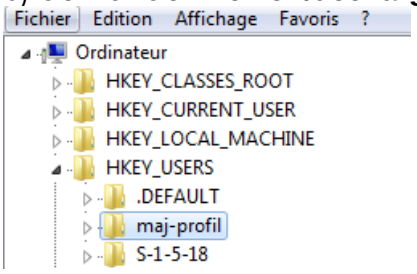
6. Sélectionner la branche **HKLM** et lancer **regedit,** demander **Fichier / Charger la ruche** et aller chercher la ruche **ntuser.dat** du profil par défaut (donc depuis **c:\user\default**).
Donner un nom à la clé quelconque, mais unique, comme "*maj-profil*"

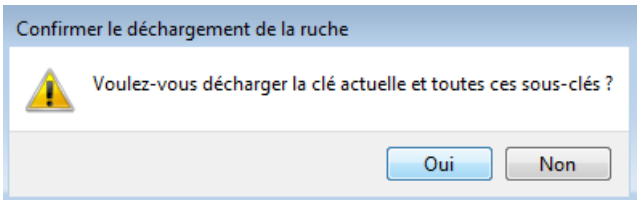


7. dans cette clé, rechercher le nom du profil d'origine du modèle, (donc pour nous "test" (ou mieux *test-xyz*)

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

XP (**Document & Settings**)	Windows 8 (**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    <JONCTION>     Application Data [C:\ProgramData]
18/02/2010  09:25    <JONCTION>     Bureau [C:\Users\Public\Desktop]
14/07/2009  05:53    <JONCTION>     Desktop [C:\Users\Public\Desktop]
14/07/2009  05:53    <JONCTION>     Documents [C:\Users\Public\Documents]
18/02/2010  09:25    <JONCTION>     Favoris [C:\Users\Public\Favorites]
14/07/2009  05:53    <JONCTION>     Favorites [C:\Users\Public\Favorites]
18/02/2010  09:25    <JONCTION>     Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010  09:25    <JONCTION>     Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009  05:53    <JONCTION>     Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009  05:53    <JONCTION>     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    <JONCTION>     Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010  09:25    <JONCTION>     Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009  05:53    <JONCTION>     Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009  05:53    <JONCTION>     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**
- pour exécuter un programme à l'ouverture de session **c:\ProgramData\Microsoft\Windows\Start Menu\Programs\startup**

(ProgramData ▸ Microsoft ▸ Windows ▸ Menu Démarrer ▸ Programmes ▸ Démarrage)

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

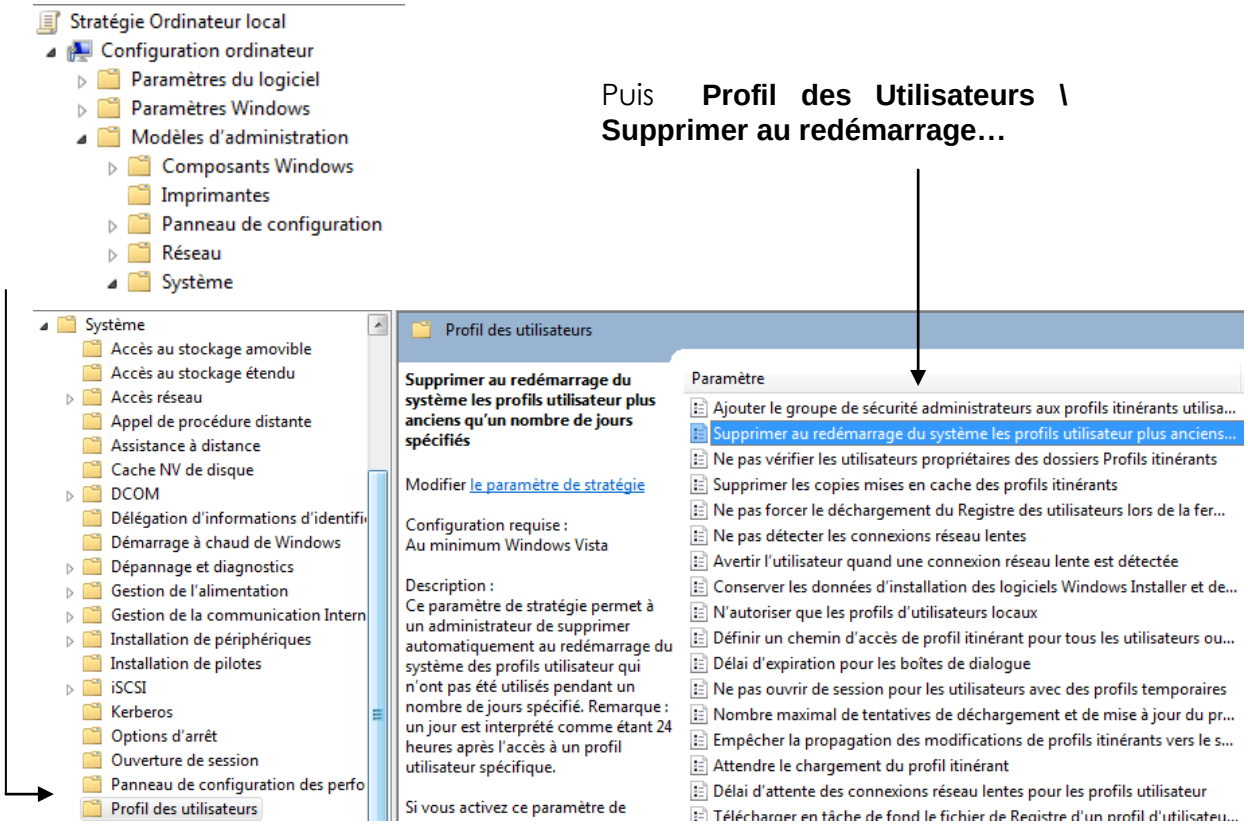
```
18/02/2010  09:25    <JONCTION>     Bureau [C:\Users\Public\Desktop]
14/07/2009  05:53    <JONCTION>     Desktop [C:\Users\Public\Desktop]
14/07/2009  05:53    <JONCTION>     Documents [C:\Users\Public\Documents]
18/02/2010  09:25    <JONCTION>     Favoris [C:\Users\Public\Favorites]
14/07/2009  05:53    <JONCTION>     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 Windows 8:

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

Configuration ordinateur \ modèles d'administration\ Système



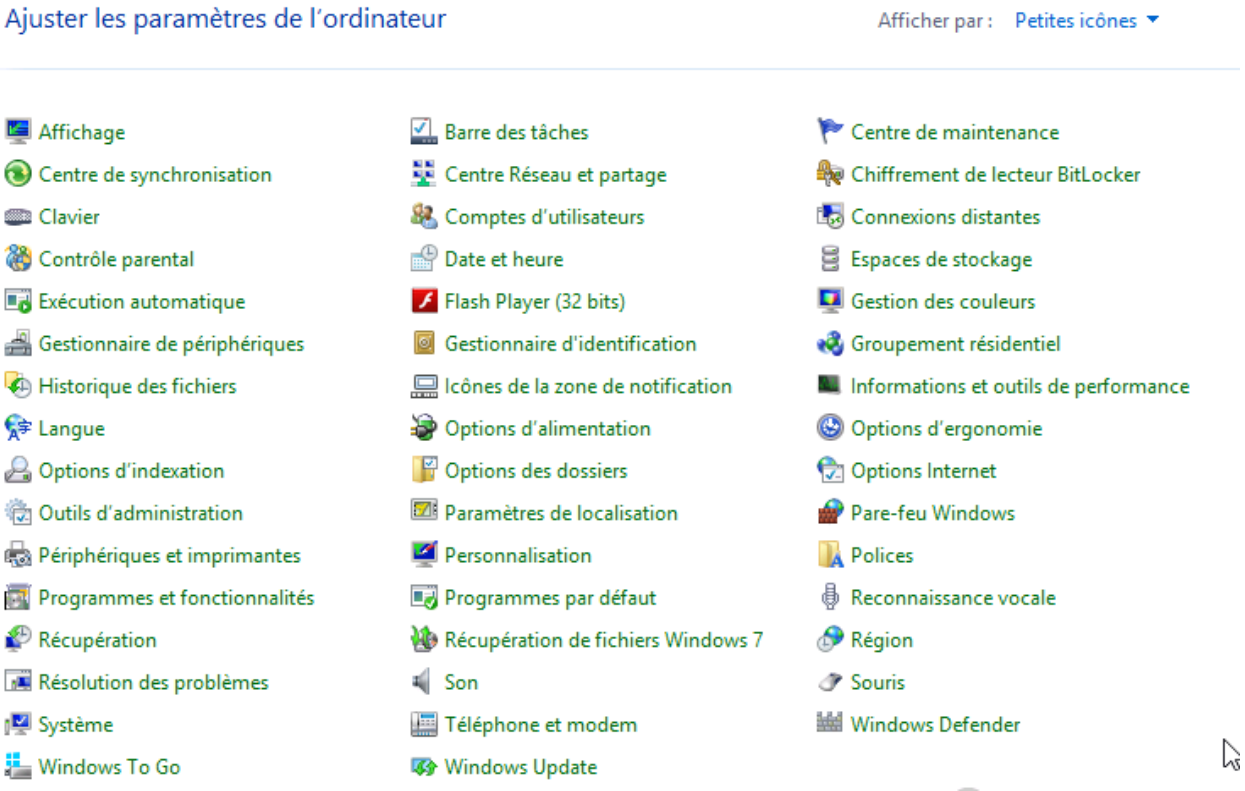
Puis **Profil des Utilisateurs \ Supprimer au redémarrage…**

INTERFACE WINDOWS 8 - 7

Panneau de Configuration:

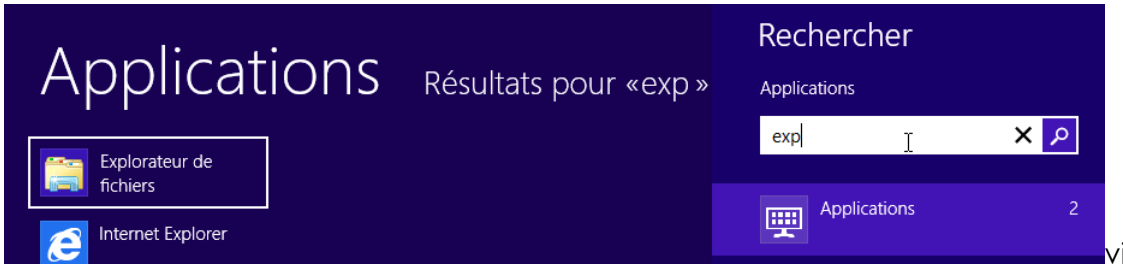
Affichage **WIndows 8** par catégories

Affichage **Windows 8** par petites icones



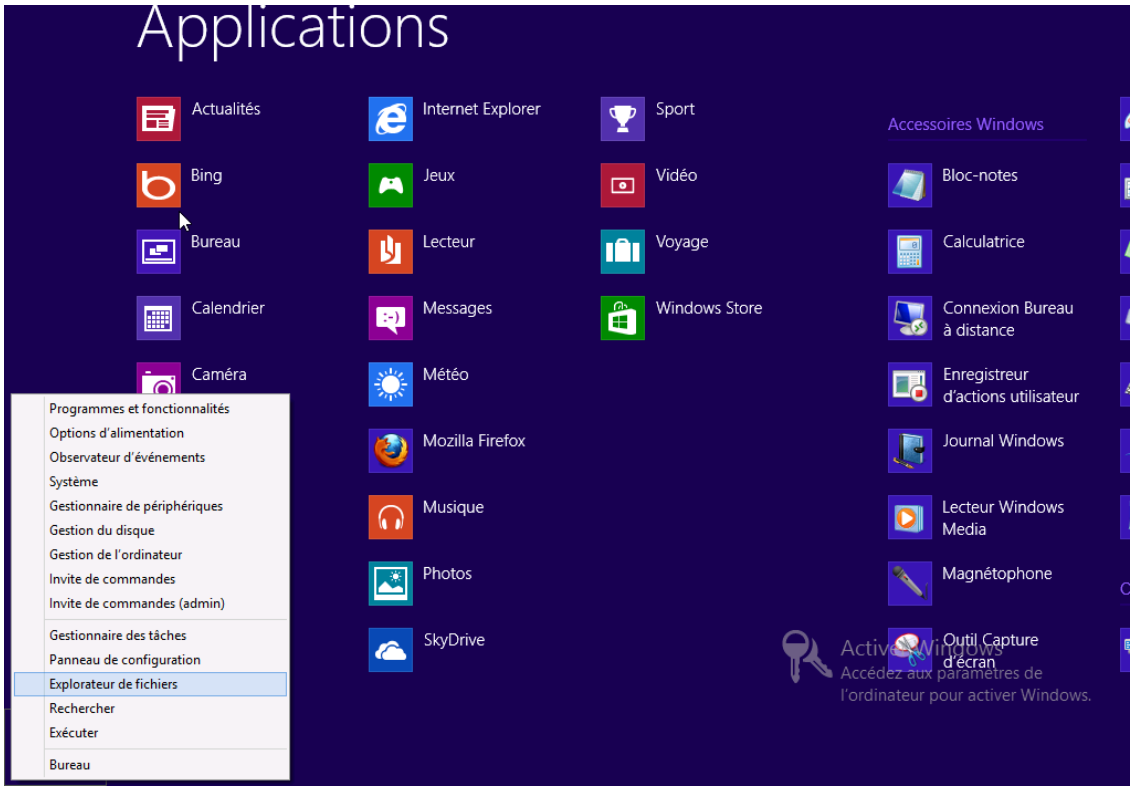
L'explorateur Windows:

On lance l'explorateur soit via la recherche de la Charms Bar

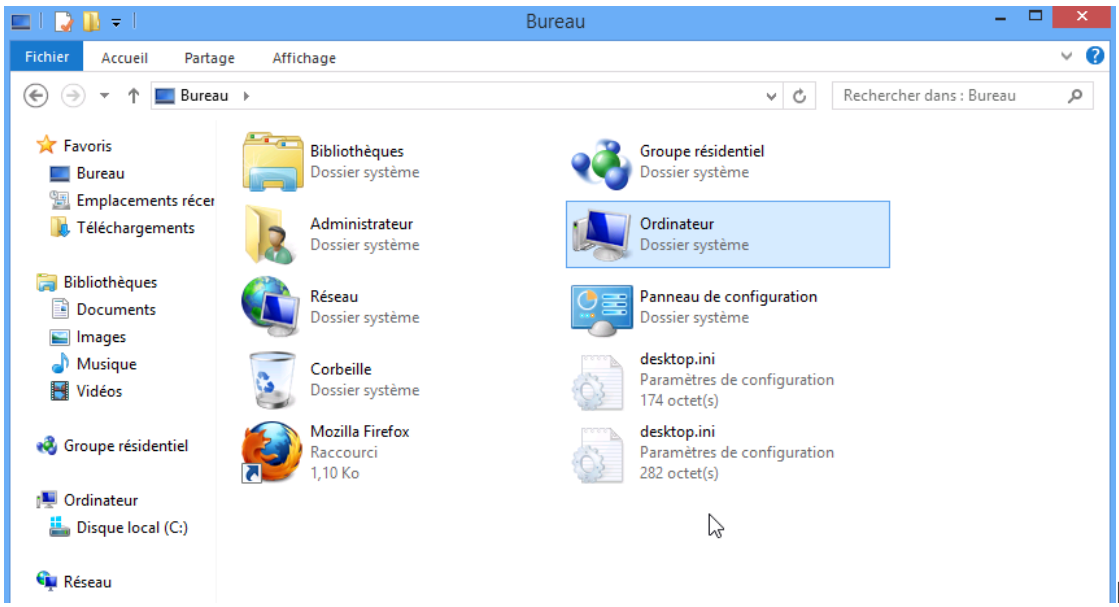


vi

Soit clic / droit **Explorer** dans la barre des tâches en bas à gauche sur l'icône Accueil

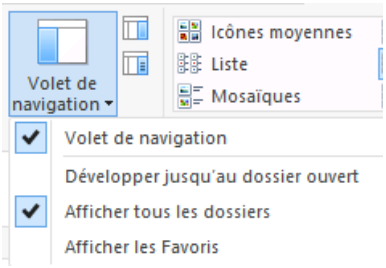


Ce qui donne



P

par rapport à l'aspect par défaut de l'explorateur windows on peut modifier notamment dans **Affichage / le Volet de navigation**



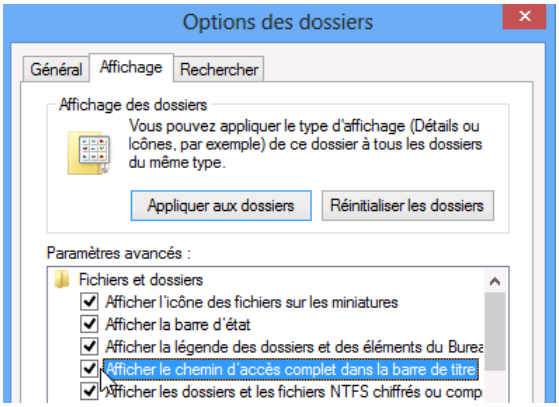
Volets de Navigation

Afficher tous les dossiers

Pas de Favoris

Toujours dans **Affichage / Option on demande Modifier les options des dossiers**

onglet **Affichage**



Afficher le chemin d'accès complet

Ne pas masquer les extensions

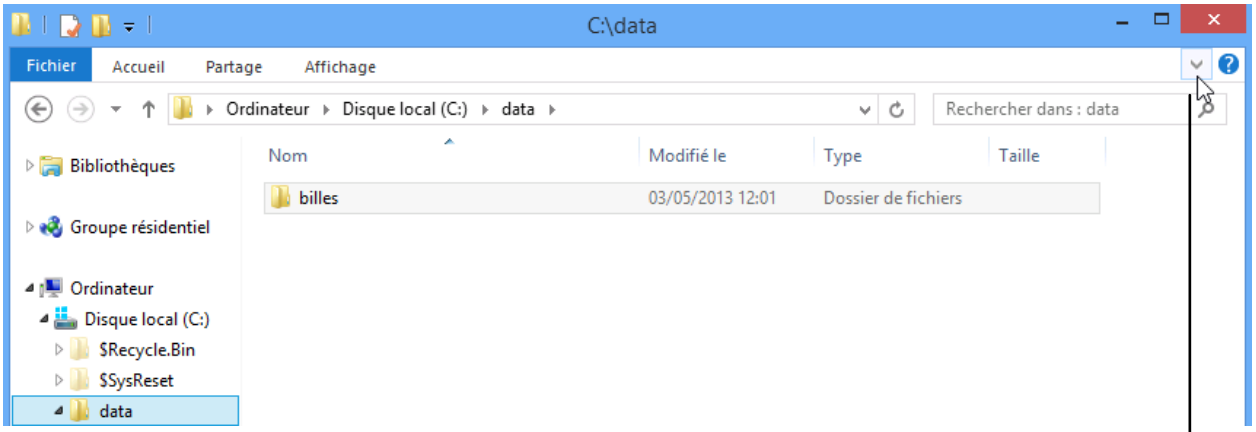
Ne pas masquer les fichiers cachés

Ne pas masquer les lecteurs vides

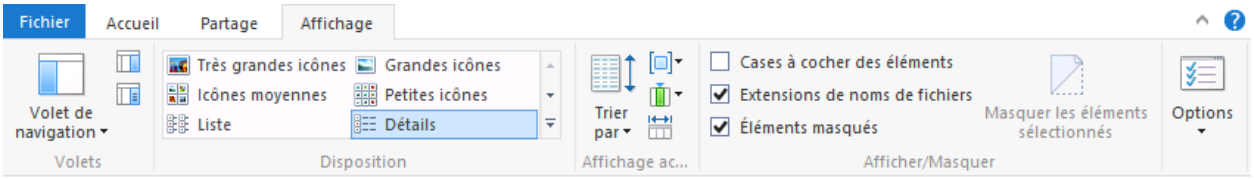
Ne pas masquer les fichiers systèmes

Ne pas utiliser l'assistant partage

Ensuite pour le **Ruban** c'est une affaire de choix …

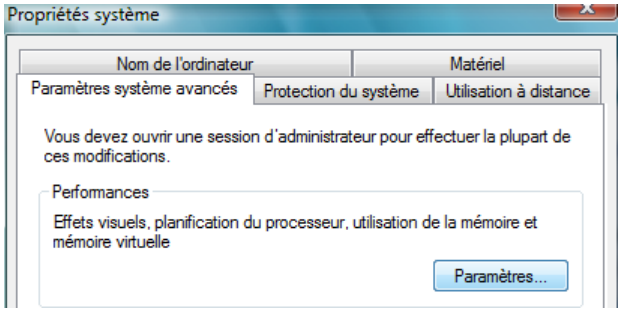


Se développe en

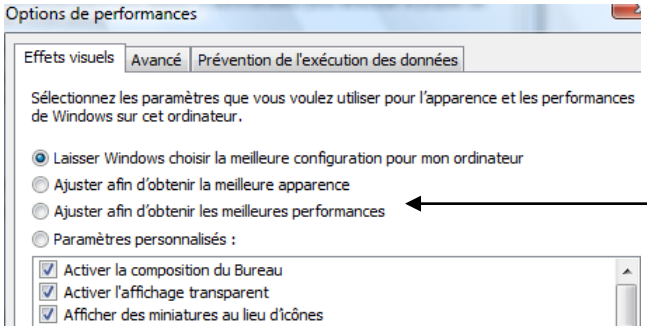


Interface Aero:

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



donnant



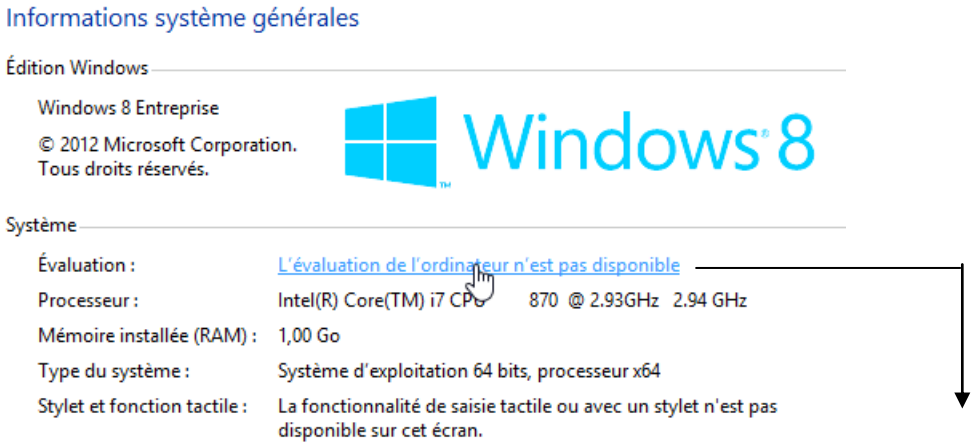
Pour Désactiver AERO on demande d'obtenir les meilleures performances

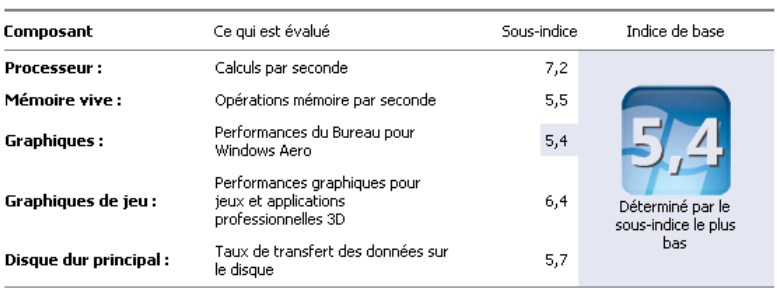
(Sans effet 3D à gogo…)

NB : **ALT+TAB** pour passer d'une application à l'autre gère désormais le **bureau**

Note Windows 8:

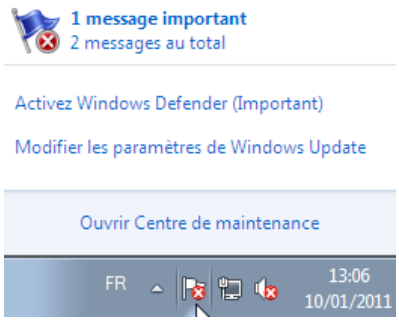
Dans les **propriétés** de **Ordinateur**





Messages du Centre de Maintenance :

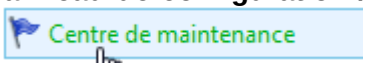
Le "centre de maintenance" de Windows peut s'avérer parfois un peu… verbeux



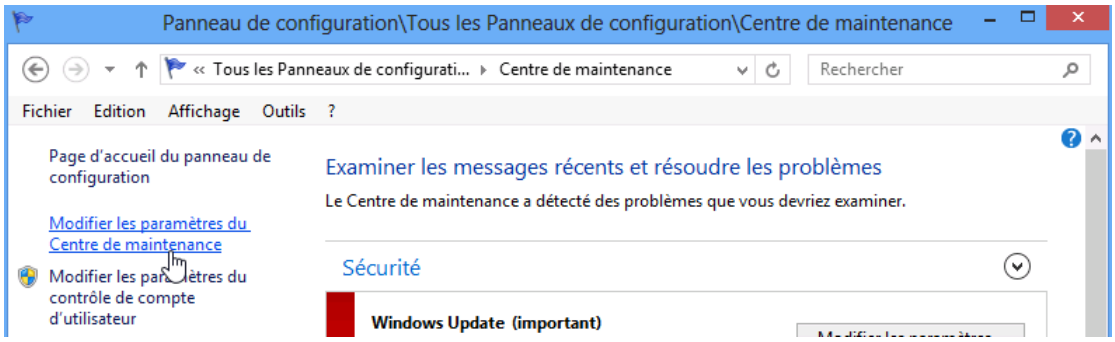
On peut gérer les messages via clic/droit

ou

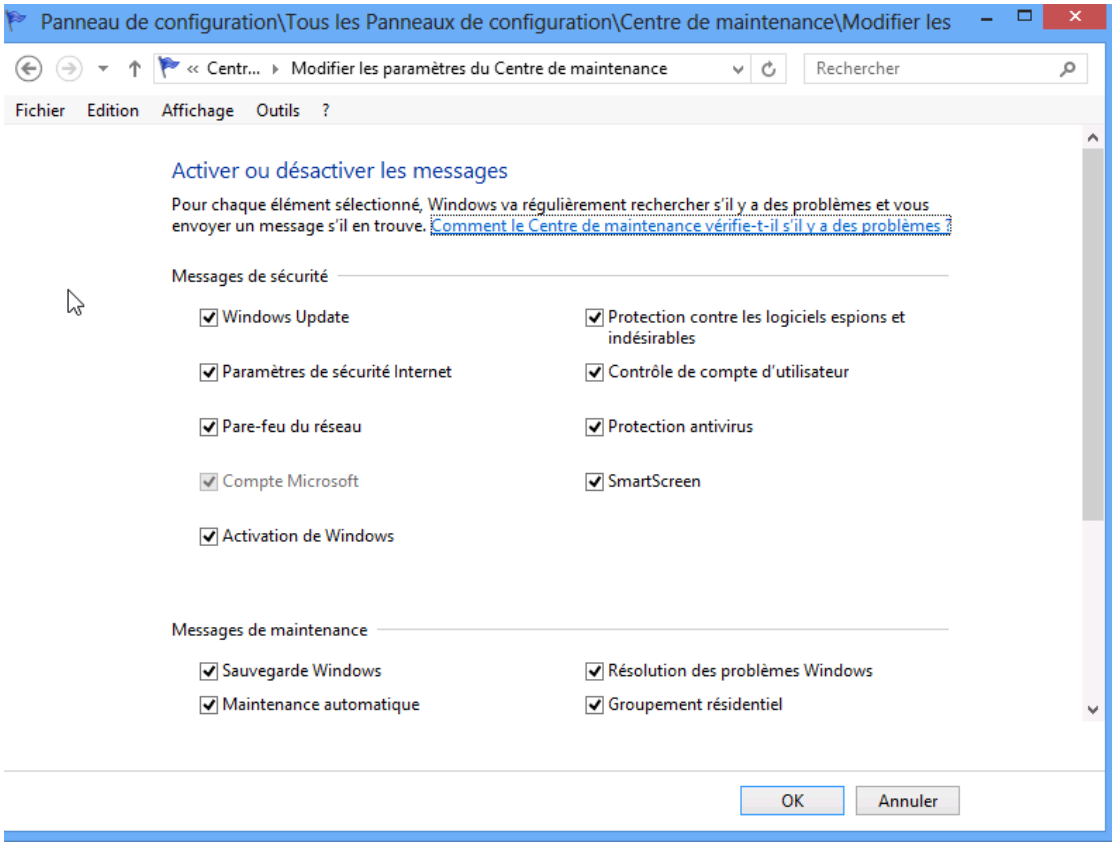
Panneau de configuration / Centre de Maintenance

/ 

Modifier les paramètres du centre de maintenance…

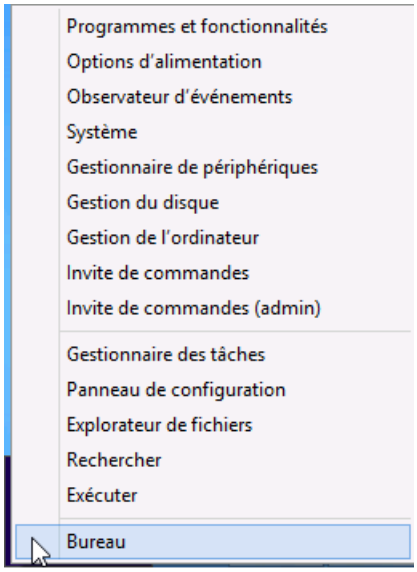


Et on choisit



Menu Contextuel / Accueil

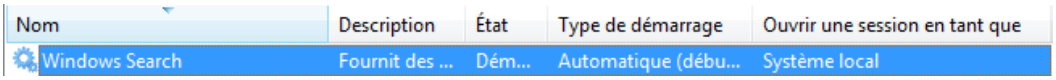
En bas à gauche, sur l'icône Accueil (lorsqu'elle apparaît) on retrouve quasiment à l'identique le menu Contextuel du Menu Démarrer…

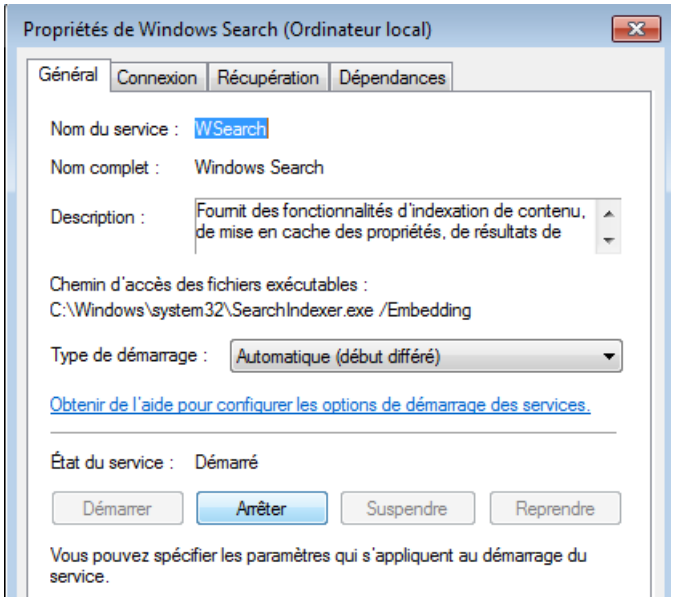


Compromis Performances – arrêt services:

Certaines fonctionnalités de Windows 8 sont « gourmandes », et par conséquent peuvent être désactivées si besoin, comme l'indexation automatique :

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



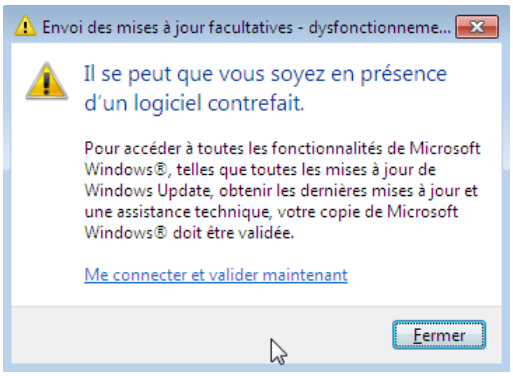


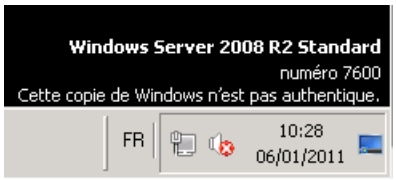
SLMGR – ACTIVATION LICENCE

Installer Windows 8 sans Clé:

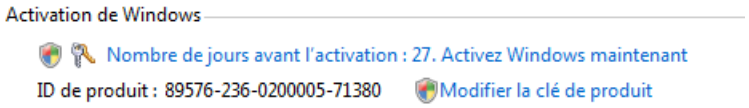
Pour des raisons diverses (habitudes, économie et surtout organisation) on peut vouloir installer **Windows 8** sans saisir de clé

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 Windows 8 - slmgr:

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

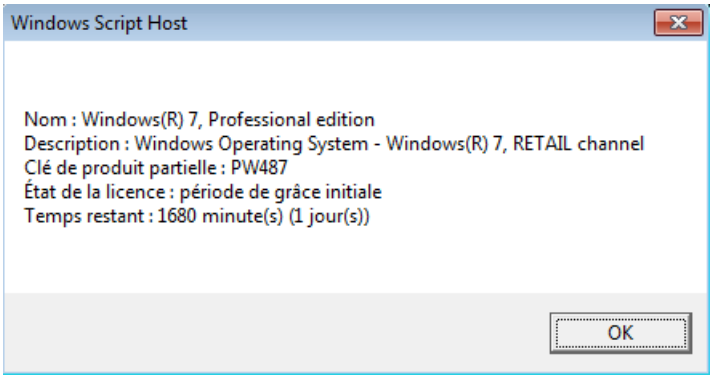
On peut demander **Slmgr / ?**

```
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
```

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

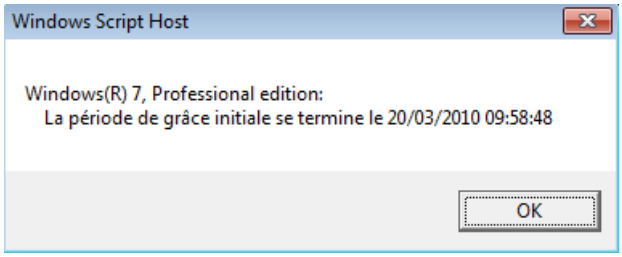
slmgr –dli

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

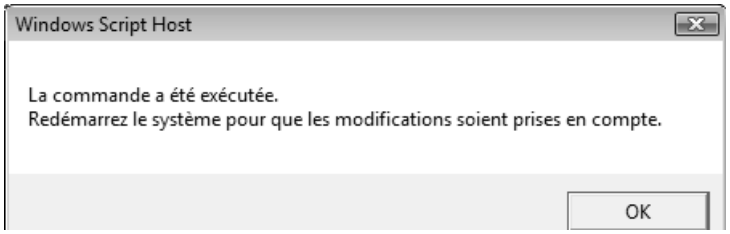


Réactivation période de grâce

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_
```

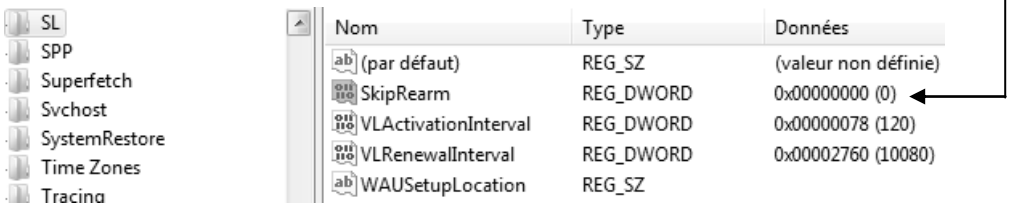
après un petit délais on obtient



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



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:

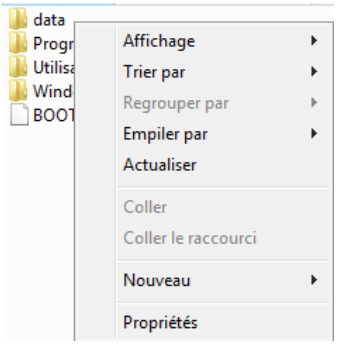
Slui 3 en ligne de commande permet juste de saisir une licence

INCLASSABLES WINDOWS 8

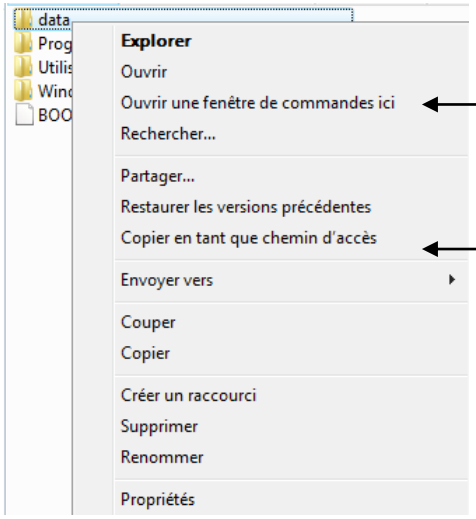
Menu étendus (invite de commande):

On peut avoir des menus "contextuels" complets à l'aide de la touche MAJ

Menu contextuel



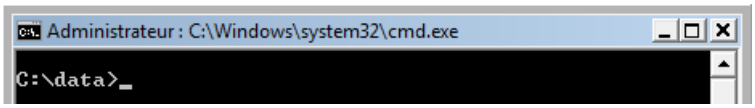
MAJ + Menu contextuel



2 commandes pratiques apparaissent

Ouvrir une fenêtre de commande ici

Positionne le path local d'une invite de commande directement dans le dossier



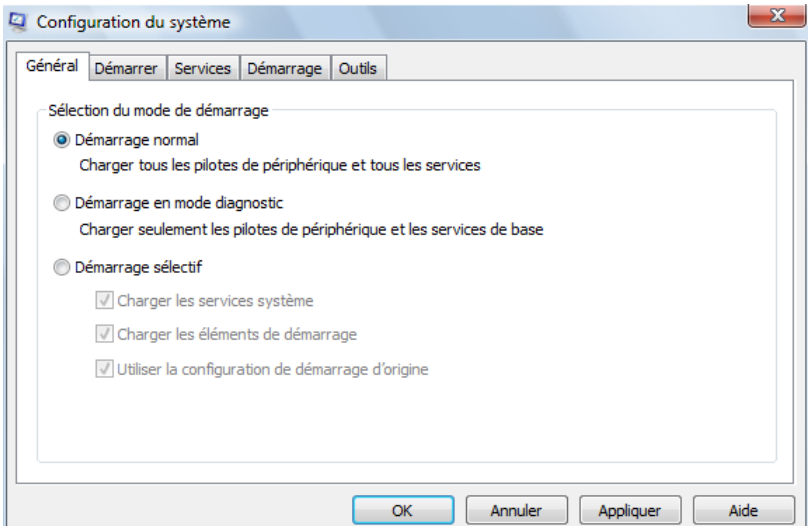
Copier en tant que chemin d'accès

Permettant de récupérer la chaîne entre guillemet du chemin

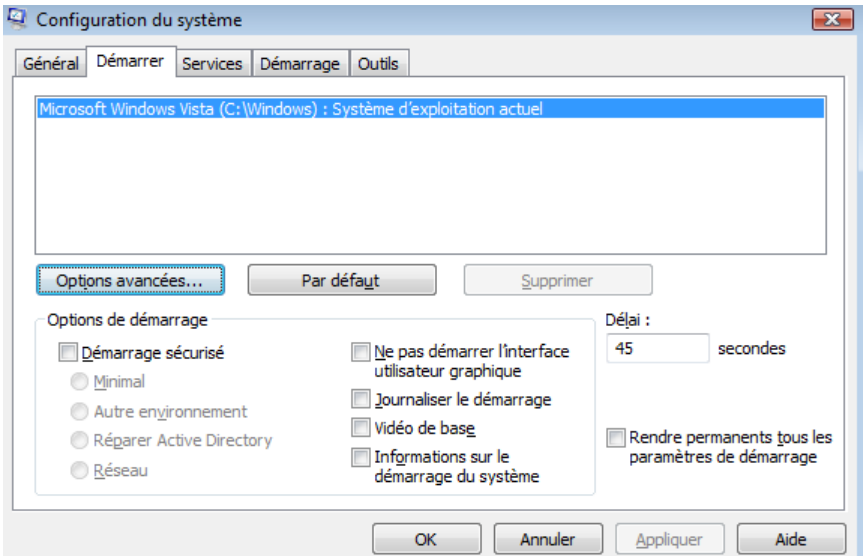
"C:\data"

Options démarrage msconfig.exe :

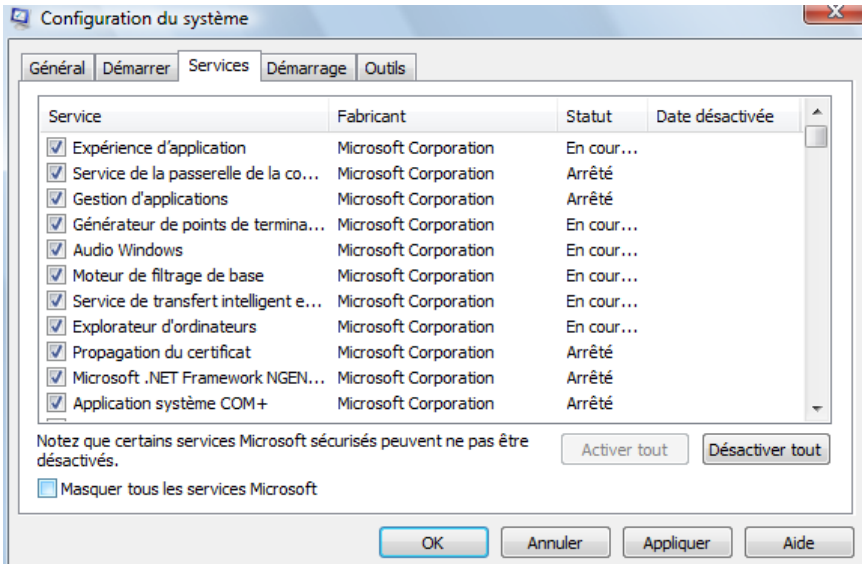
Disposant de 5 onglets fort pratiques **Général**



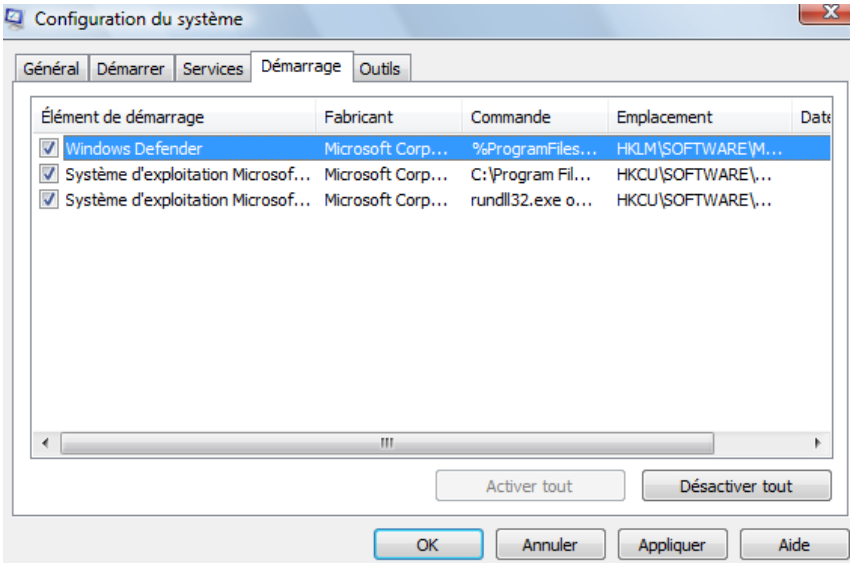
Démarrer



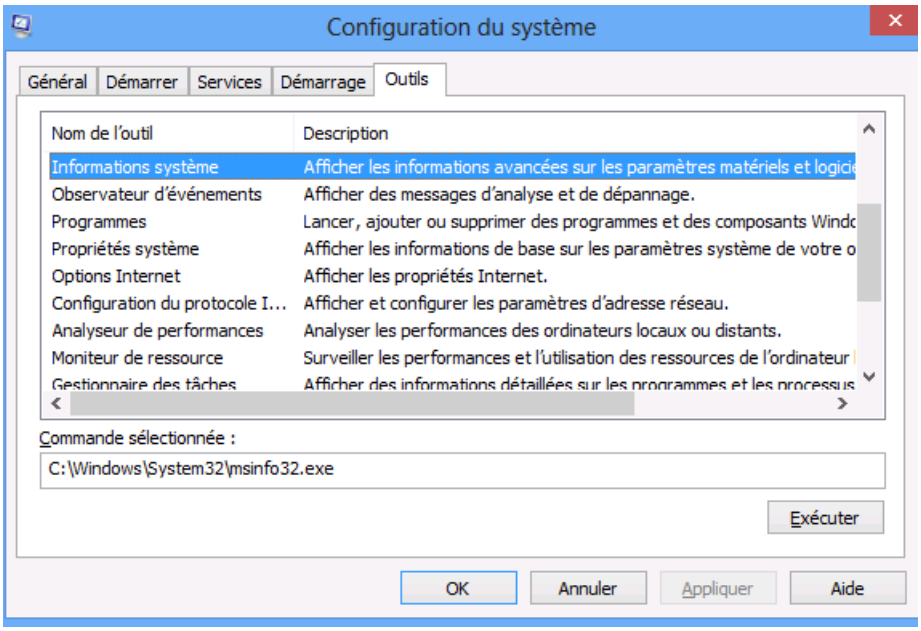
Services



Démarrage



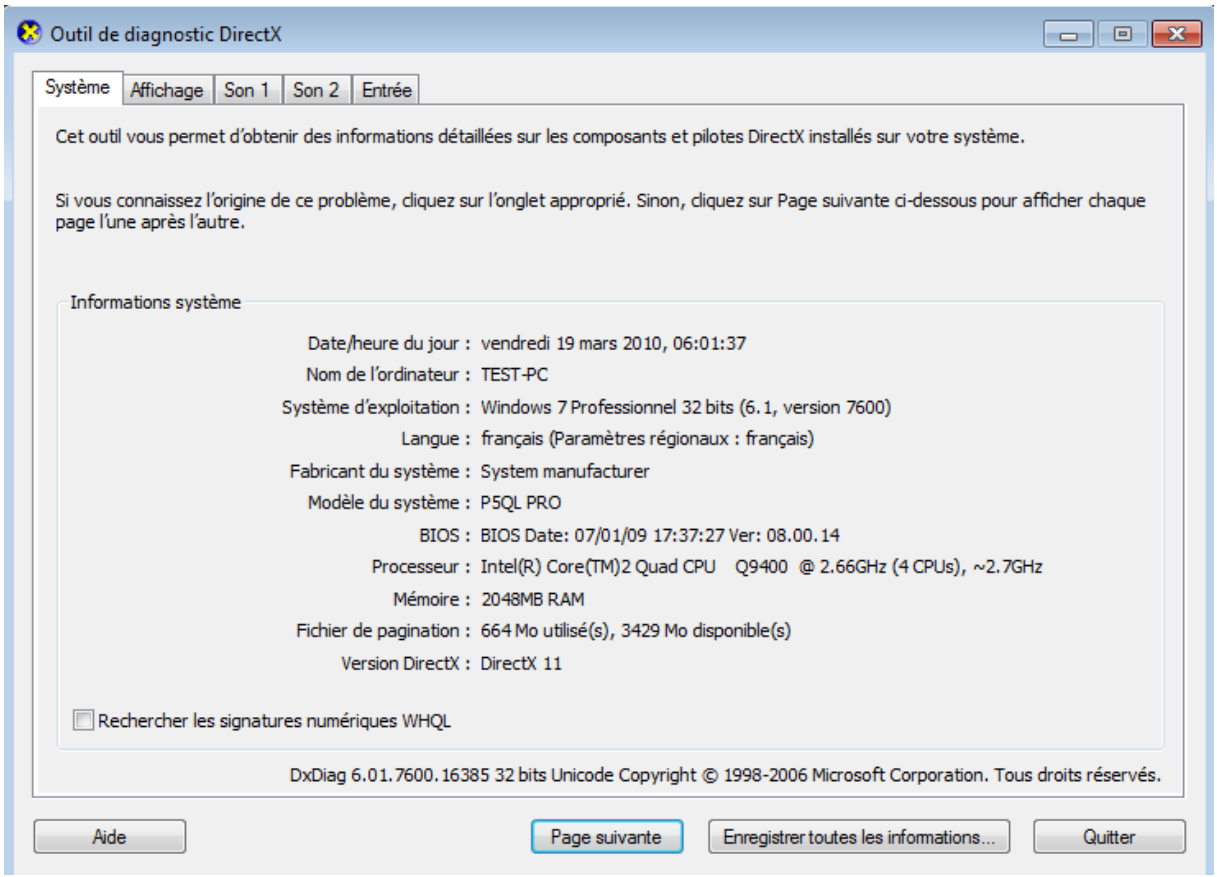
Outils



Dont **msinfo32.exe**

Outils dxdiag:

Pour tester les pb directx, en ligne de commande **dxdiag**



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**

Pour accéder au menu options de démarrage **shutdown avec l'option /r/o**

Shutdown /r /o arrêt immédiat

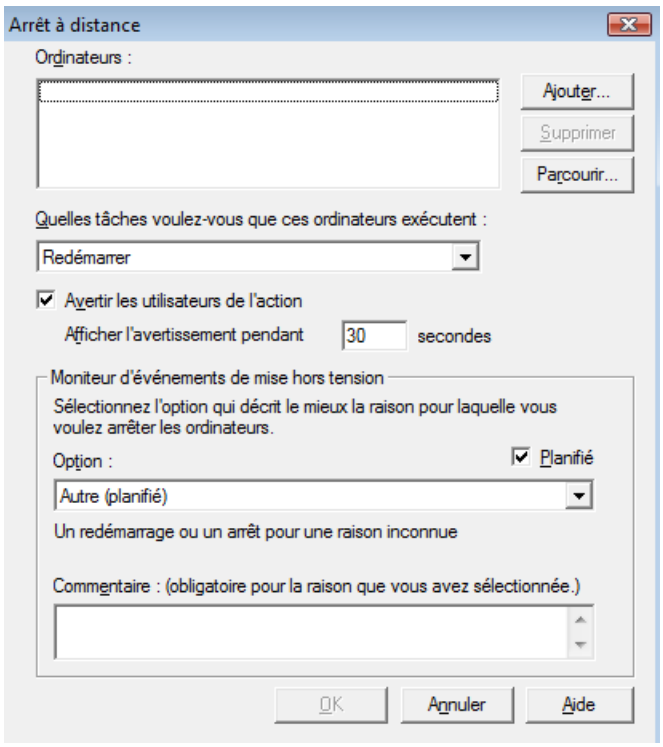
```
C:\Users\Administrateur>shutdown /r /o_
```

Ou encore mieux

Shutdown /r /o /f /t 0

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 tache 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 pré-définies, 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

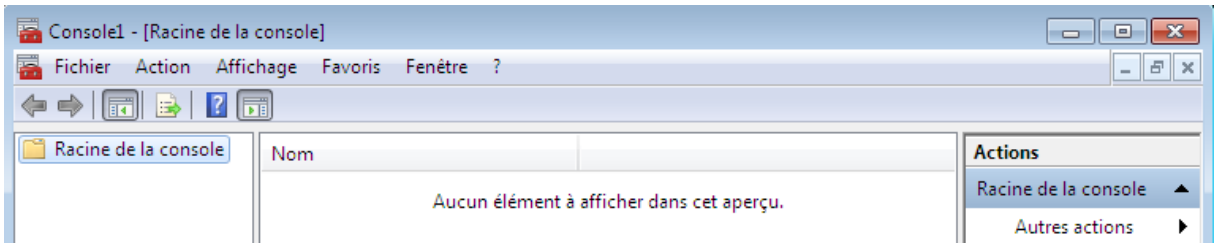
Fichier	*Rôle*
certmgr.msc	Certificats
ciadv.msc	Service d'indexation
devmgmt.msc	Gestionnaire de périphériques
dfrg.msc	Défragmenteur de disques
diskmgmt.msc	Gestion des disques
dnsmgmt.msc	Gestionnaire de DNS
eventvwr.msc	Observateur d'événements
faxserv.msc	Gestion du service de télécopie
fsmgmt.msc	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
wmimgmt.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 **Executer /** Et taper **mmc**

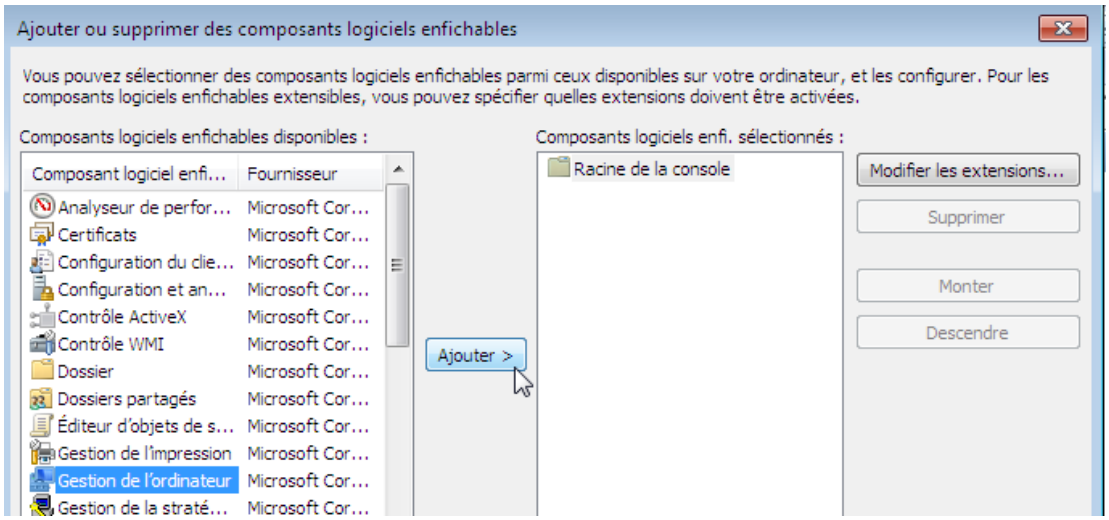
Ou rechercher MMC

On obtient une ***console1*** vide prête à être personnalisée

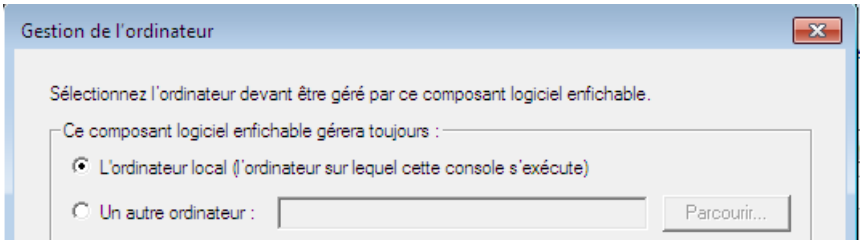


En étant placé à la racine de la console, demander dans le menu

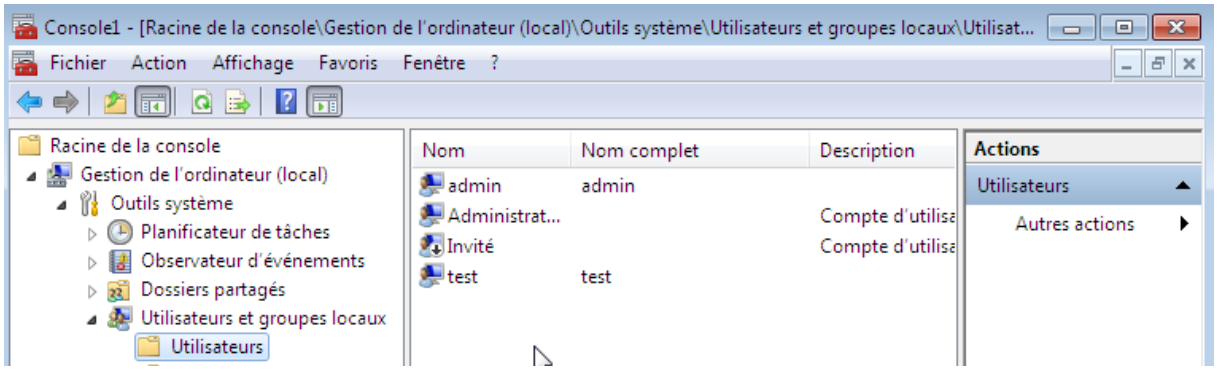
Fichier / Ajouter - Supprimer un composant logiciel enfichable



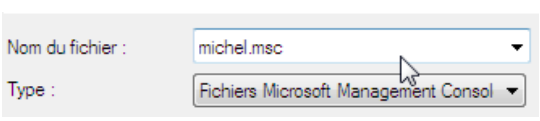
Dans la liste des snap-in choisir « **gestion de l'ordinateur** » (par exemple) et demander de gérer l'ordinateur local



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*** »

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…

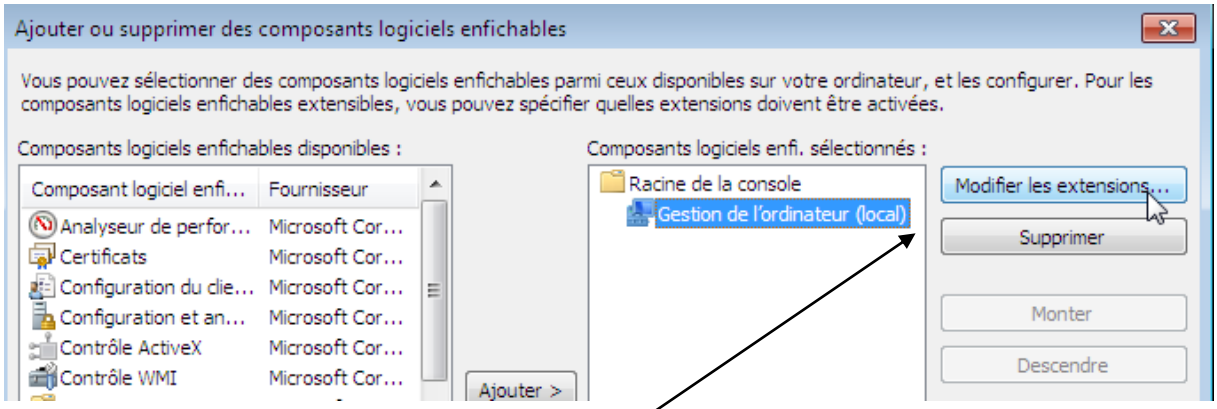
Limiter les fonctions d'un composant logiciel :

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 de :

- désactiver certaines extensions de la console
- enregistrer la console en mode utilisateur...

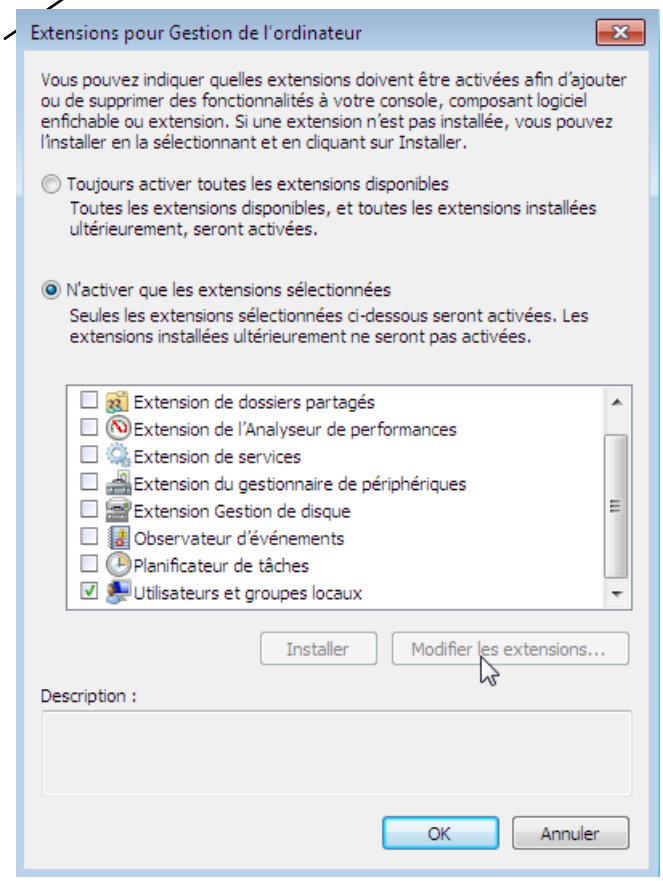
Désactiver des extensions de la console :

Au moment d'inclure le composant **gestion de l'ordinateur**



On demande **Modifier les extensions…**

pour obtenir alors

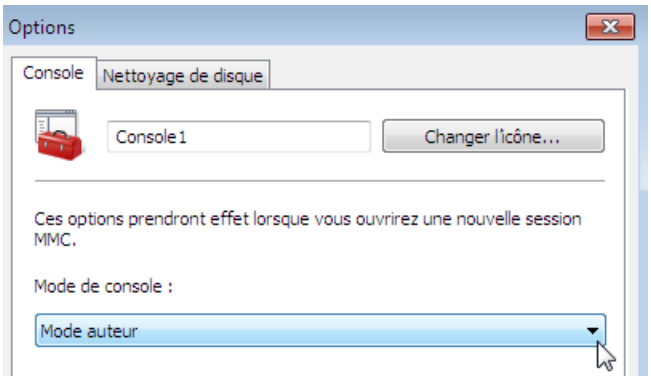


on demande de n'activer que les extensions sélectionnées

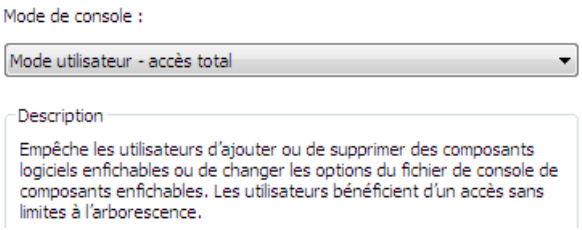
et ensuite on faite sa sélection...

Enregistrer la console utilisateur :

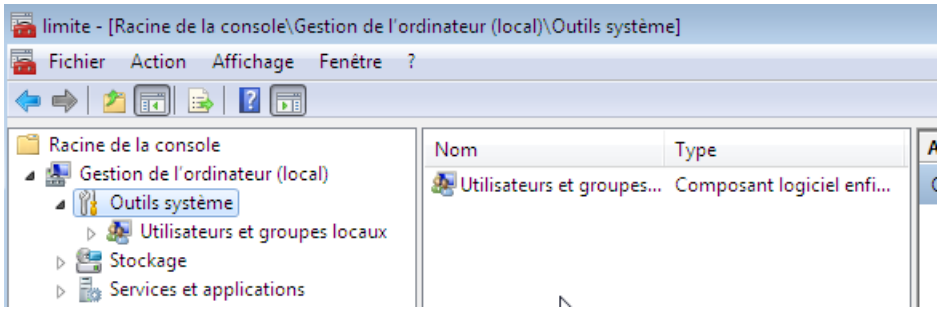
Avant d'enregistrer la console, il faut dans le menu **FIchier / Option**



Demander de passer en **Mode utilisateur**...



Au prochain lancement, les composants enfichables de cette console ne sont plus modifiables... et son réduit à la gestion utilisateur



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 fournit avec Seven SP1 (ou Seven) ne peut travailler avec un XP, et vice-versa.

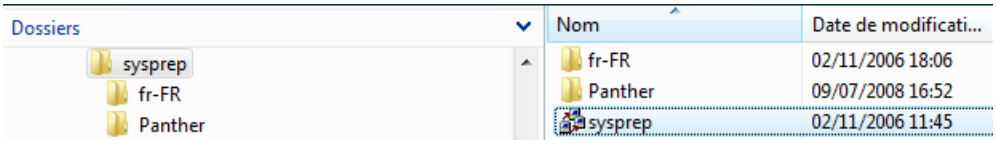
- **Sysprep 3.14** Windows 8 - Seven Sp1 – Seven (voire 2012 – 2008)

  Se trouvant dans \Windows\system32\sysprep\...
- **Sysprep 2.0** XP Sp3 – XP Sp2

  Se trouvant dans le MEDIA XP, ou en se téléchargeant…

Sysprep 3.14 pour 8 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 :

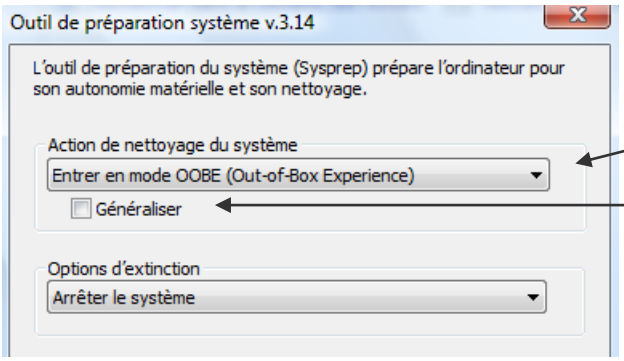
1. toutes les informations système uniques sont supprimées de Windows.
2. L'ID de sécurité (SID) est réinitialisée,
3. tous les points de restauration du système sont effacés
4. les journaux d'événements sont supprimés.

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 Windows

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**

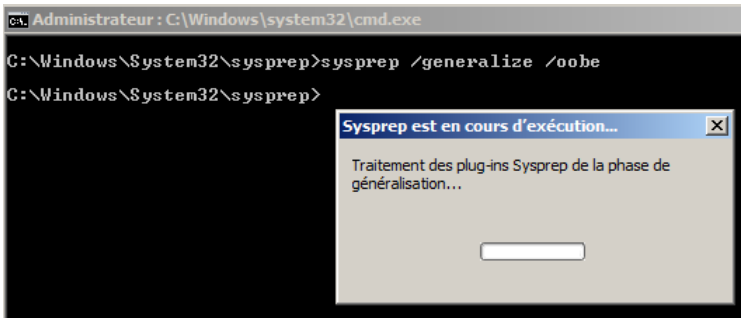
sysprep /generalize

- demande une confirmation de l'action generalize
- rebbot immédiat après le sysprep.
- Puis lors la 1° installation, à la fin un mini assistant se déroule demandant plusieurs paramètres

sysprep /generalize /oobe

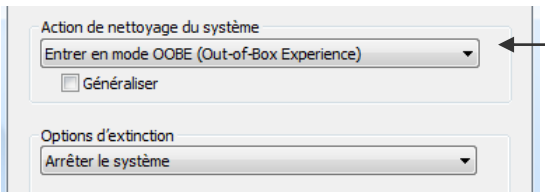
c'est l'option courante avant une capture d'image

- Arrêt mais pas de re-boot immédiat après le sysprep.
- Puis lors la 1° installation, à la fin un mini assistant se déroule demandant plusieurs paramètres



sysprep /audit

- Arrêt mais pas de rebbot immédiat après le sysprep.
- Lorsque l'on demande /audit après re-démarrage du postye 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

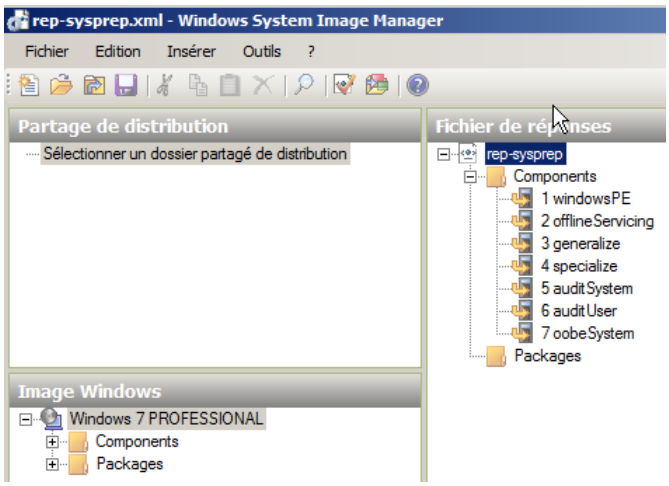
sysprep /generalize /oobe /unattend:c:\fichier.xml

Le fichier de réponse est crée 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…

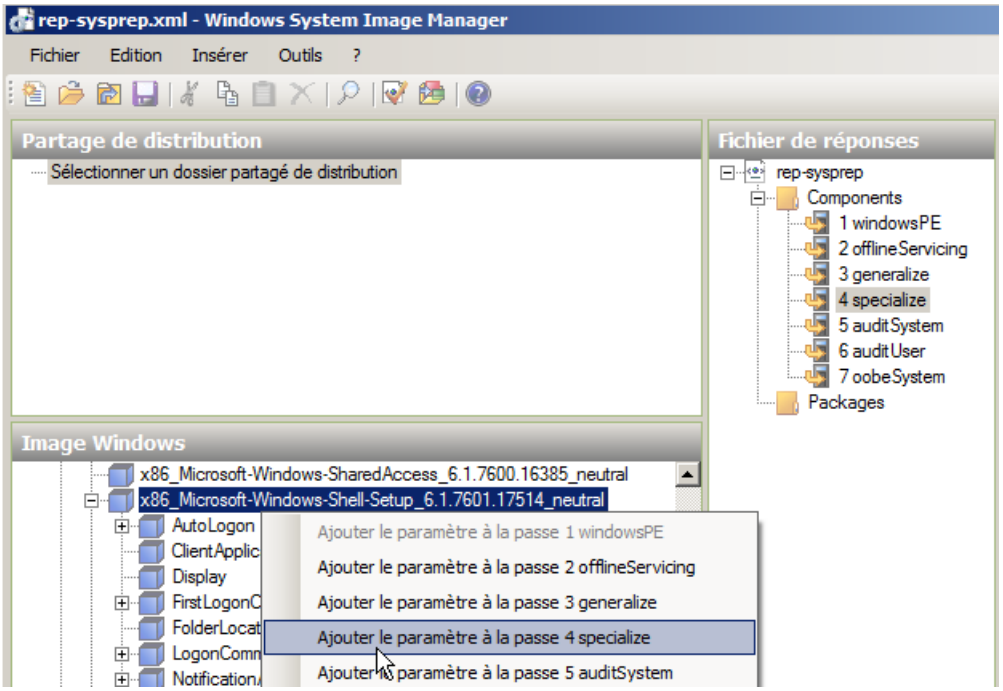
N.B: Dans la liste des emplacements possible pour le fichier de réponse, **%windir%\panther** *rep-sysprep***.xml** est en haut de la hiérarchie.

Sysprep /unattend copyprofile

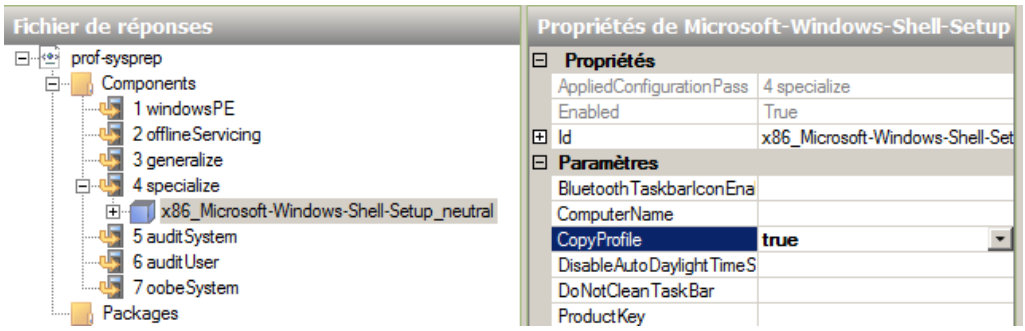
A partir de Seven, (et donc également pour Windows 8, 2008, 2008R2) la seule manière de se préparer un profil par défaut, est celle d'indiquer dans le fichier de réponse à exécuter au moment du sysprep une commande

Copyprofile à **True**

C'est un paramètre qui s'indique en **passe4 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 executé, 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:

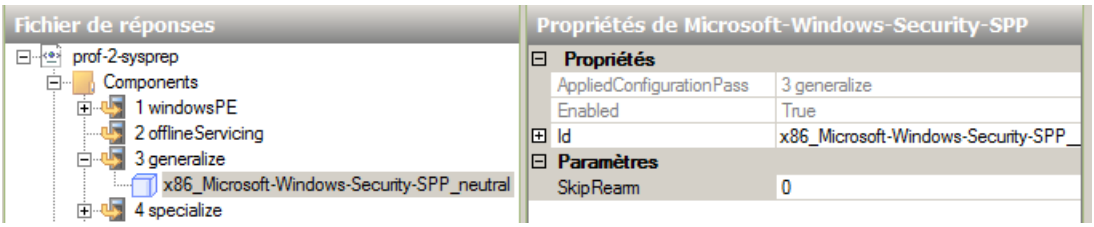
   /generalize /oobe /unattend:c:\prof-sysprep.xml

Activation et SkipRearm

Il existe des limites au nombre d'exécutions de Sysprep sur un ordinateur, 3 sur seven, 7 sous windows 8. 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 elle ne peut le faire qua 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 **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>
    <cpi:offlineImage cpi:source="wim:d:/win-seven/install.wim#Windows
7 PROFESSIONAL" xmlns:cpi="urn:schemas-microsoft-com:cpi" />
</unattend>
```

N.B : rappel le fichier log se trouve en **C:\Windows\System32\Sysprep\Panther**