http://WWW.CABARE.NET ©

# Système Windows 7 Seven Sp1 – sys 20 – Travaux Pratiques -

## Installation Administration Windows 7 Sp1

**Michel Cabaré – Ver 2.3 – Juin 2011-**

**Système Windows 7 Seven Sp1**
**Travaux Pratiques**

**Michel Cabaré – Ver 2.3 – Juin 2011**

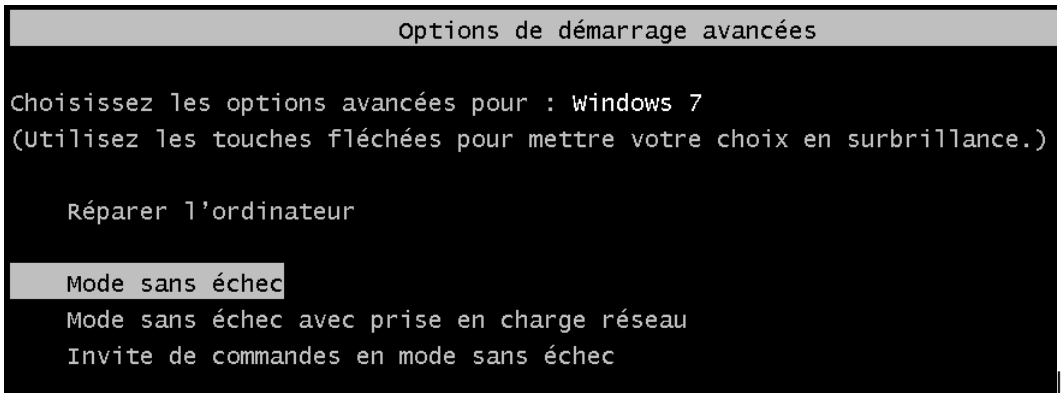
www.cabare.net ©

# TABLE DES MATIÈRES

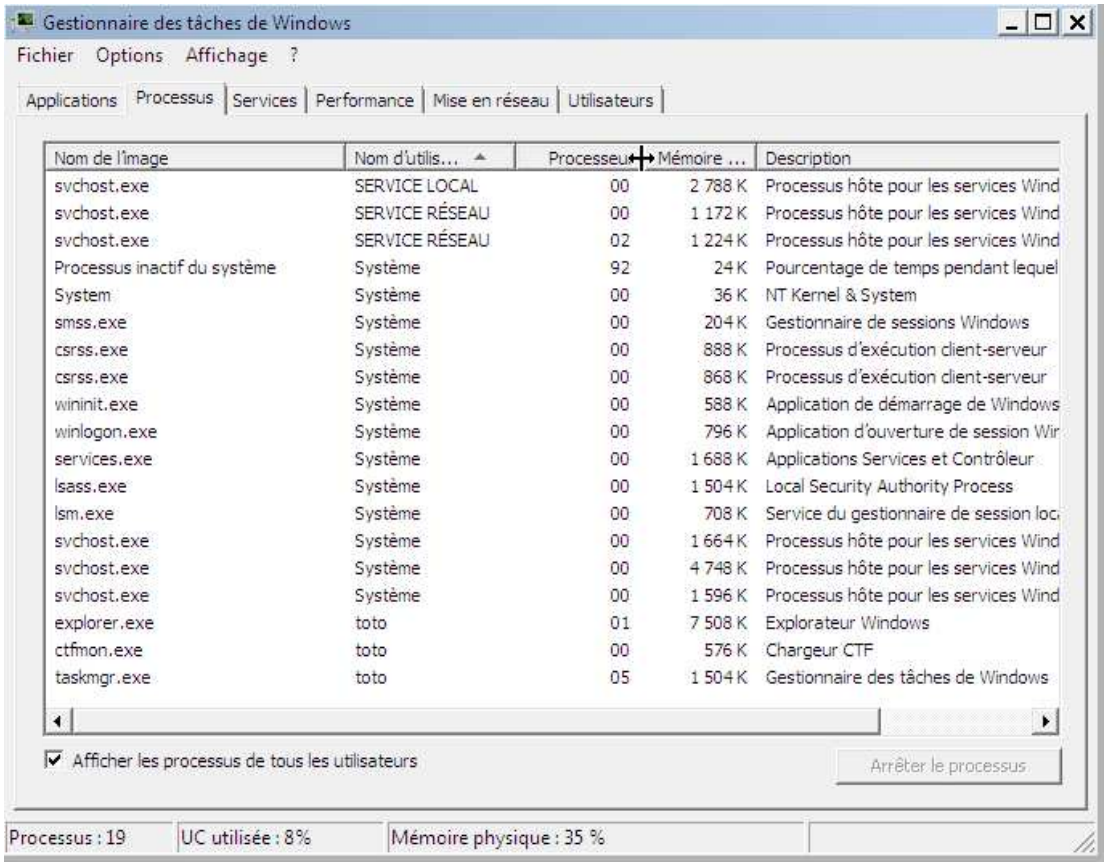
# TRACER DES PROCESSUS…

**Liste par défaut:**

Soit une machine SEVEN sur laquelle on ouvre une session en **mode sans Echec**, (F8 au démarrage)




la liste des processus est bien sûr minimaliste




Si on lance ne serait-ce que wordpad, on obtient alors tout de suite un process de plus

| | | | | |
|---|---|---|---|---|
| wordpad.exe | toto | 00 | 4 368 K | Application Windows Wordpad |
| taskmgr.exe | toto | 08 | 1 520 K | Gestionnaire des tâches de Windows |

De même, si on referme wordpad, et on lance **tasklist** en invite de commande, on obtiendra par rapport aux processus initiaux, 2 nouveaux processus :

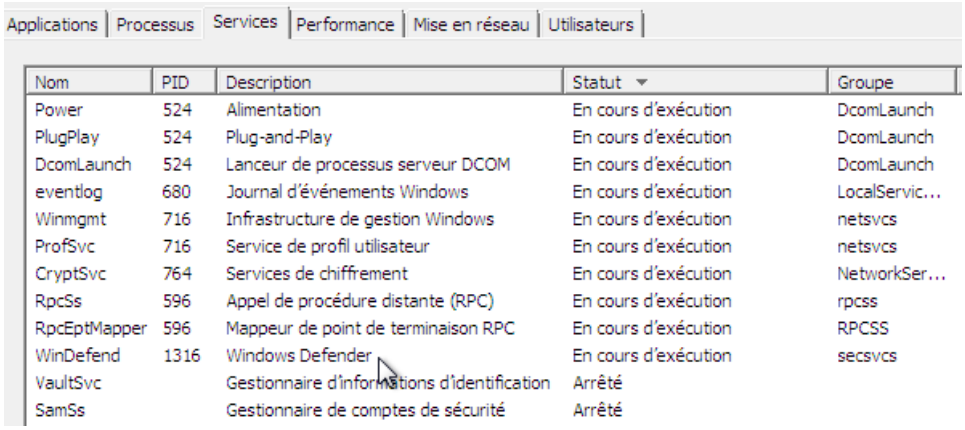
- **cmd.exe** (l'invite de commande)
- et **tasklist** lui-même !

```
C:\Users\toto>tasklist

Nom de l'image                 PID Nom de la sessio Numéro de s Utilisation
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 Ko
System                           4 Services                   0        224 Ko
smss.exe                       204 Services                   0        712 Ko
csrss.exe                      276 Services                   0      2 804 Ko
csrss.exe                      316 Console                    1      7 108 Ko
wininit.exe                    324 Services                   0      3 040 Ko
winlogon.exe                   352 Console                    1      3 512 Ko
services.exe                   412 Services                   0      4 528 Ko
lsass.exe                      420 Services                   0      6 008 Ko
lsm.exe                        428 Services                   0      2 684 Ko
svchost.exe                    524 Services                   0      5 696 Ko
svchost.exe                    596 Services                   0      4 036 Ko
svchost.exe                    680 Services                   0      5 752 Ko
svchost.exe                    716 Services                   0      9 536 Ko
svchost.exe                    764 Services                   0      4 732 Ko
explorer.exe                   928 Console                    1     28 204 Ko
ctfmon.exe                    1004 Console                    1      2 904 Ko
svchost.exe                   1316 Services                   0      5 924 Ko
taskmgr.exe                   1492 Console                    1      6 872 Ko
cmd.exe                        824 Console                    1      2 112 Ko
conhost.exe                    660 Console                    1      2 792 Ko
tasklist.exe                  1488 Console                    1      3 968 Ko
WmiPrvSE.exe                  1312 Services                   0      4 540 Ko
```

Pour mieux voir la correspondance, l'affichage du PID est significatif

| Nom de l'image | ▲ | Nom d'utilisateur | Proces... | Mém... | Description |
|---|---|---|---|---|---|
| Processus inactif ... | 0 | Système | 75 | 24 K | Pourcentage de temps pendant lequel l'ordinateur est inactif |
| System | 4 | Système | 00 | 36 K | NT Kernel & System |
| smss.exe | 204 | Système | 00 | 204 K | Gestionnaire de sessions Windows |
| csrss.exe | 276 | Système | 00 | 888 K | Processus d'exécution client-serveur |
| csrss.exe | 316 | Système | 05 | 924 K | Processus d'exécution client-serveur |
| wininit.exe | 324 | Système | 00 | 588 K | Application de démarrage de Windows |
| winlogon.exe | 352 | Système | 00 | 796 K | Application d'ouverture de session Windows |
| services.exe | 412 | Système | 00 | 1 696 K | Applications Services et Contrôleur |
| lsass.exe | 420 | Système | 00 | 1 500 K | Local Security Authority Process |
| lsm.exe | 428 | Système | 00 | 784 K | Service du gestionnaire de session locale |
| svchost.exe | 524 | Système | 00 | 1 704 K | Processus hôte pour les services Windows |
| svchost.exe | 596 | SERVICE RÉSEAU | 00 | 1 252 K | Processus hôte pour les services Windows |
| conhost.exe | 660 | toto | 00 | 664 K | Hôte de la fenêtre de la console |
| svchost.exe | 680 | SERVICE LOCAL | 00 | 2 788 K | Processus hôte pour les services Windows |
| svchost.exe | 716 | Système | 00 | 4 756 K | Processus hôte pour les services Windows |
| svchost.exe | 764 | SERVICE RÉSEAU | 00 | 1 224 K | Processus hôte pour les services Windows |
| cmd.exe | 824 | toto | 00 | 468 K | Interpréteur de commandes Windows |
| explorer.exe | 928 | toto | 01 | 10 1... | Explorateur Windows |
| ctfmon.exe | 1004 | toto | 00 | 576 K | Chargeur CTF |
| svchost.exe | 1316 | Système | 00 | 1 596 K | Processus hôte pour les services Windows |
| taskmgr.exe | 1492 | toto | 19 | 1 528 K | Gestionnaire des tâches de Windows |

L'onglet Service donnant lui '(ce qui correspondrait à **Tasklist /SVC**)




| Nom | PID | Description | Statut | Groupe |
|---|---|---|---|---|
| Power | 524 | Alimentation | En cours d'exécution | DcomLaunch |
| PlugPlay | 524 | Plug-and-Play | En cours d'exécution | DcomLaunch |
| DcomLaunch | 524 | Lanceur de processus serveur DCOM | En cours d'exécution | DcomLaunch |
| eventlog | 680 | Journal d'événements Windows | En cours d'exécution | LocalServic... |
| Winmgmt | 716 | Infrastructure de gestion Windows | En cours d'exécution | netsvcs |
| ProfSvc | 716 | Service de profil utilisateur | En cours d'exécution | netsvcs |
| CryptSvc | 764 | Services de chiffrement | En cours d'exécution | NetworkSer... |
| RpcSs | 596 | Appel de procédure distante (RPC) | En cours d'exécution | rpcss |
| RpcEptMapper | 596 | Mappeur de point de terminaison RPC | En cours d'exécution | RPCSS |
| WinDefend | 1316 | Windows Defender | En cours d'exécution | secsvcs |
| VaultSvc | | Gestionnaire d'informations d'identification | Arrêté | |
| SamSs | | Gestionnaire de comptes de sécurité | Arrêté | |

```
C:\Users\toto>tasklist /SVC

Nom de l'image                 PID Services
========================= ======== ============================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       204 N/A
csrss.exe                      276 N/A
csrss.exe                      316 N/A
wininit.exe                    324 N/A
winlogon.exe                   352 N/A
services.exe                   412 N/A
lsass.exe                      420 N/A
lsm.exe                        428 N/A
svchost.exe                    524 DcomLaunch, PlugPlay, Power
svchost.exe                    596 RpcEptMapper, RpcSs
svchost.exe                    680 eventlog
svchost.exe                    716 ProfSvc, Winmgmt
svchost.exe                    764 CryptSvc
explorer.exe                   928 N/A
ctfmon.exe                    1004 N/A
svchost.exe                   1316 WinDefend
cmd.exe                        824 N/A
conhost.exe                    660 N/A
tasklist.exe                  1828 N/A
WmiPrvSE.exe                  1864 N/A
```

A titre de comparaison, un tasklist / SVC sur une machine normalement démarrée donnerait

```
Nom de l'image                 PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       216 N/A
csrss.exe                      308 N/A
csrss.exe                      348 N/A
wininit.exe                    356 N/A
winlogon.exe                   384 N/A
services.exe                   444 N/A
lsass.exe                      452 SamSs
lsm.exe                        460 N/A
svchost.exe                    552 DcomLaunch, PlugPlay, Power
svchost.exe                    628 RpcEptMapper, RpcSs
svchost.exe                    720 Audiosrv, Dhcp, eventlog, lmhosts, wscsvc
svchost.exe                    756 AudioEndpointBuilder, CscService, Netman,
                                   SysMain, TrkWks, UxSms, WdiSystemHost
svchost.exe                    780 AeLookupSvc, Appinfo, BITS, gpsvc,
                                   iphlpsvc, LanmanServer, MMCSS, ProfSvc,
                                   Schedule, SENS, ShellHWDetection, Themes,
                                   Winmgmt, wuauserv
svchost.exe                    892 EventSystem, netprofm, nsi, WdiServiceHost
svchost.exe                    980 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc
spoolsv.exe                   1156 Spooler
svchost.exe                   1196 BFE, DPS, MpsSvc
taskhost.exe                  1312 N/A
svchost.exe                   1416 FDResPub, SSDPSRV
dwm.exe                       1444 N/A
explorer.exe                  1460 N/A
rundll32.exe                  2028 N/A
rundll32.exe                   196 N/A
rundll32.exe                   248 N/A
SearchIndexer.exe             1408 WSearch
SearchProtocolHost.exe        1700 N/A
SearchFilterHost.exe          1912 N/A
cmd.exe                       1908 N/A
conhost.exe                   1900 N/A
mscorsvw.exe                   900 clr_optimization_v2.0.50727_32
sppsvc.exe                    1712 sppsvc
svchost.exe                    224 WinDefend
tasklist.exe                   600 N/A
WmiPrvSE.exe                  1964 N/A
```

**Liste détaillée:**

Pour connaître les processus, on peut demander les détails des SVCHOST :

**Tasklist /m**

```
C:\Users\Administrateur>tasklist /M

Nom de l'image                 PID Modules
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       276 ntdll.dll
csrss.exe                      368 ntdll.dll, CSRSRV.dll, basesrv.DLL,
                                   winsrv.DLL, USER32.dll, GDI32.dll,
                                   kernel32.dll, KERNELBASE.dll, LPK.dll,
                                   USP10.dll, msvcrt.dll, sxssrv.DLL, sxs.dll,
                                   RPCRT4.dll, CRYPTBASE.dll
wininit.exe                    436 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   USER32.dll, GDI32.dll, LPK.dll, USP10.dll,
```

Cette option génère beaucoup de sortie, et on peut la filtrer pour limiter sa portée à un suel processus, que l'on identifie par son PID

Par exemple pour le process dont le PID est 524, on demande

**Tasklist /fi "pid eq 524"** avec comme options **/m**

```
C:\Users\toto>tasklist /m /fi "pid eq 524"

Nom de l'image                 PID Modules
========================= ======== ============================================
svchost.exe                    524 ntdll.dll, kernel32.dll, KERNELBASE.dll,
                                   msvcrt.dll, sechost.dll, RPCRT4.dll,
                                   umpnpmgr.dll, SPINF.dll, USER32.dll,
                                   GDI32.dll, LPK.dll, USP10.dll, DEVRTL.dll,
                                   IMM32.DLL, MSCTF.dll, RpcRtRemote.dll,
                                   USERENV.dll, profapi.dll, GPAPI.dll,
                                   CRYPTBASE.dll, umpo.dll, WINSTA.dll,
                                   SETUPAPI.dll, CFGMGR32.dll, ADVAPI32.dll,
                                   OLEAUT32.dll, ole32.dll, DEVOBJ.dll,
                                   pcwum.DLL, rpcss.dll, SspiCli.dll,
                                   credssp.dll, CLBCatQ.DLL, ntmarta.dll,
                                   WLDAP32.dll, wmidcprv.dll, FastProx.dll,
                                   wbemcomn.dll, WS2_32.dll, NSI.dll,
                                   NTDSAPI.dll, wbemprox.dll, CRYPTSP.dll,
                                   rsaenh.dll, wbemsvc.dll, wmiutils.dll,
                                   WINTRUST.dll, CRYPT32.dll, MSASN1.dll,
                                   WTSAPI32.dll
```

Noter que le filtre peut être associé à d'autres options…1

**Tasklist /SVC /fi "pid eq 524"**

```
C:\Users\toto>tasklist /SVC /fi "pid eq 524"

Nom de l'image                 PID Services
========================= ======== ============================================
svchost.exe                    524 DcomLaunch, PlugPlay, Power
```

# STRATEGIE GESTION DRIVERS

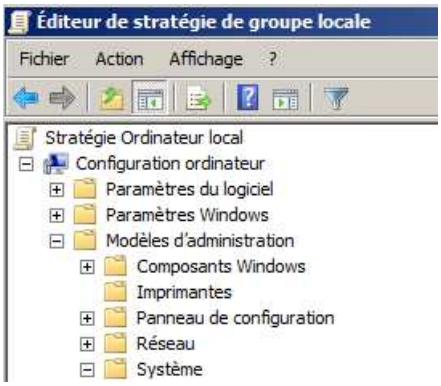
**Stratégies de gestion de drivers & périphériques :**

Comme désormais il est possible d'installer potentiellement un périphérique sans avoir de Droits élevé, de nouvelles **Stratégies** existent via **gpedit.msc**

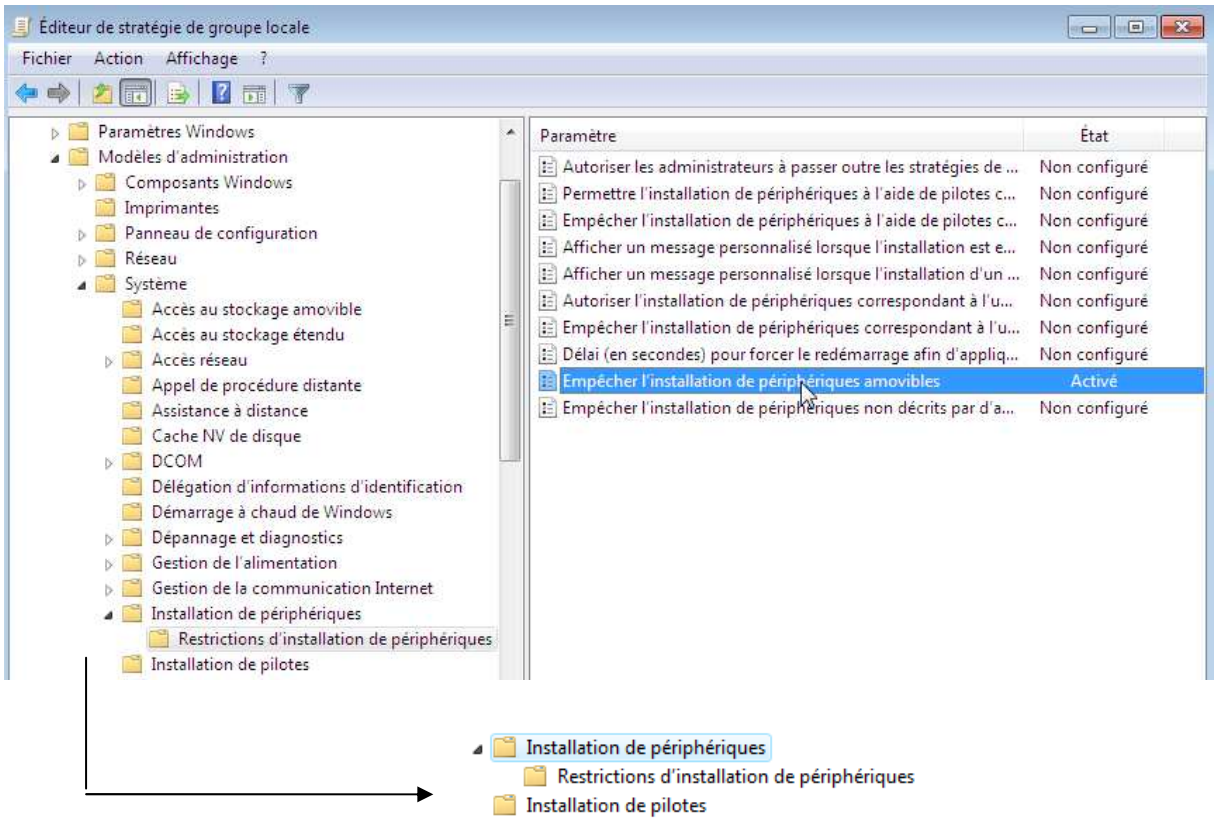
**Configuration ordinateur**

**\Modèles d'administration**

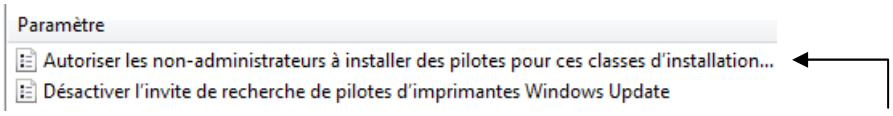
**\ Système**




Deux entrées nouvelles…



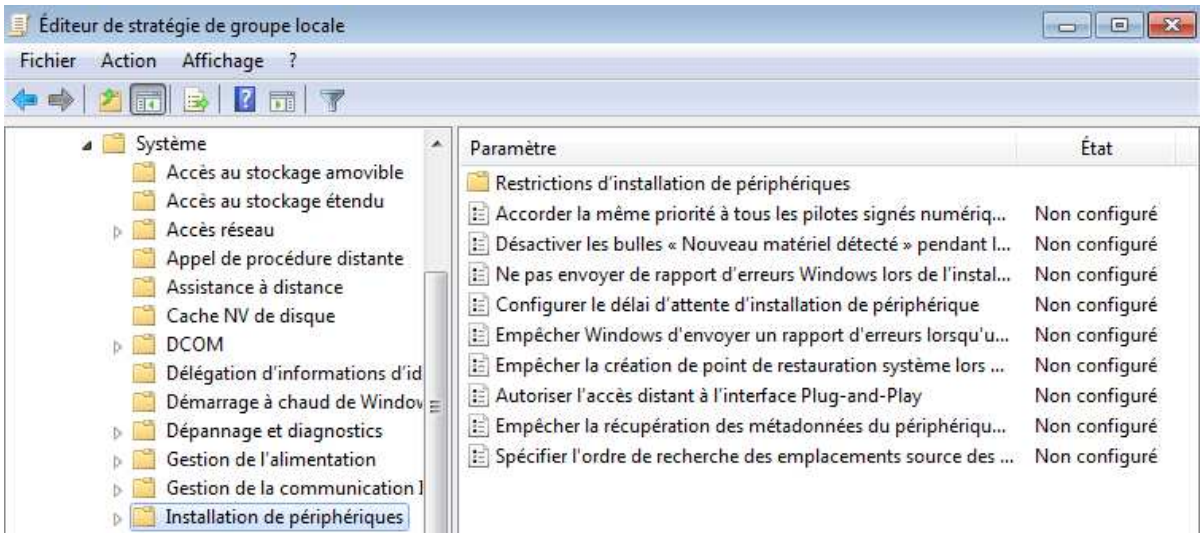

## Stratégie Installation de pilotes



On peut autoriser des Utilisateurs à installer des familles de pilotes

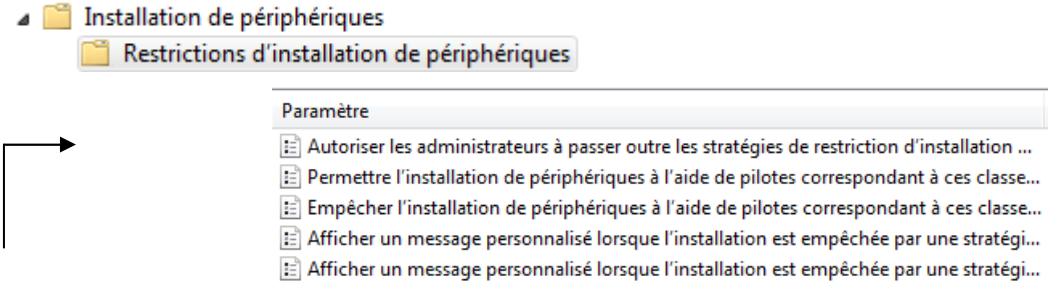
On peut interdire la récupération de drivers via Windows Update…Ne pas se fier à la mention "pilote d'imprimantes"

## Stratégie Installation de périphériques




### Interdire les clés USB :

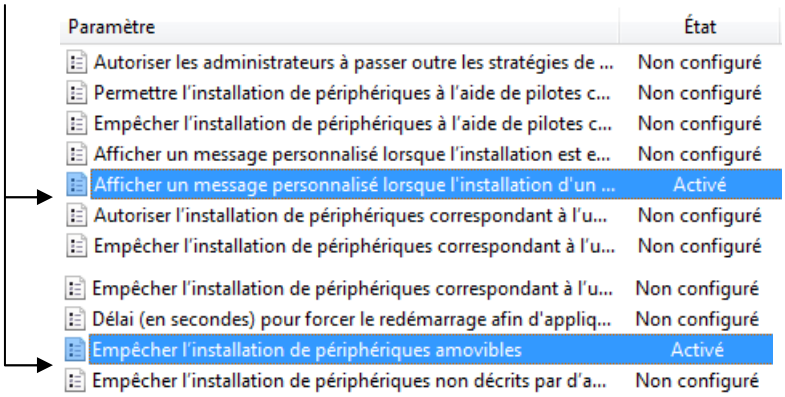
il est possible d'interdire l'installation de certains périphériques…

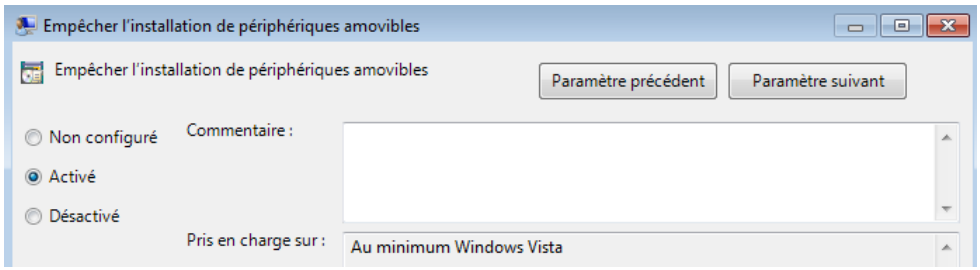



Il peut être bon d'autoriser les administrateurs à outrepasser les restrictions au niveau des installations de drivers…

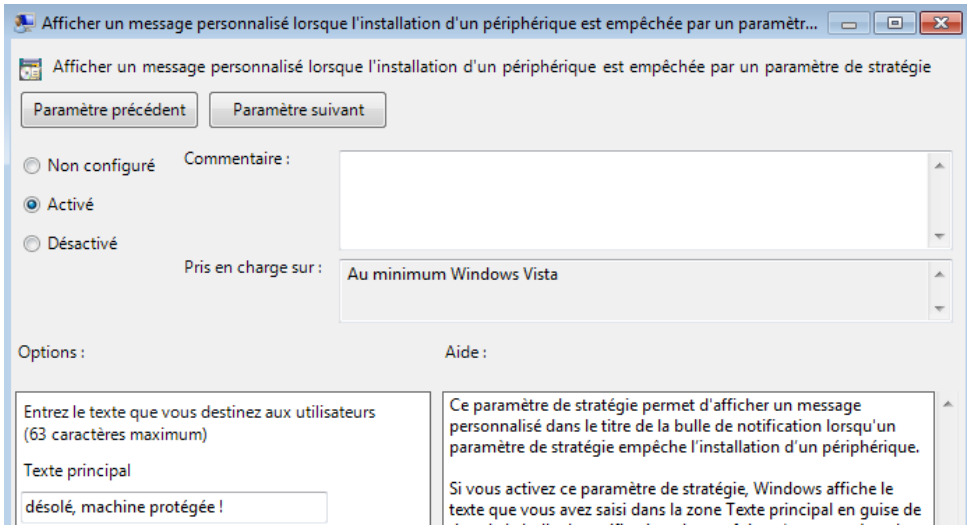
On peut ensuite empêcher l'installation de clé USB désignée comme **Périphériques amovibles.**

Deux stratégies sont présentes :

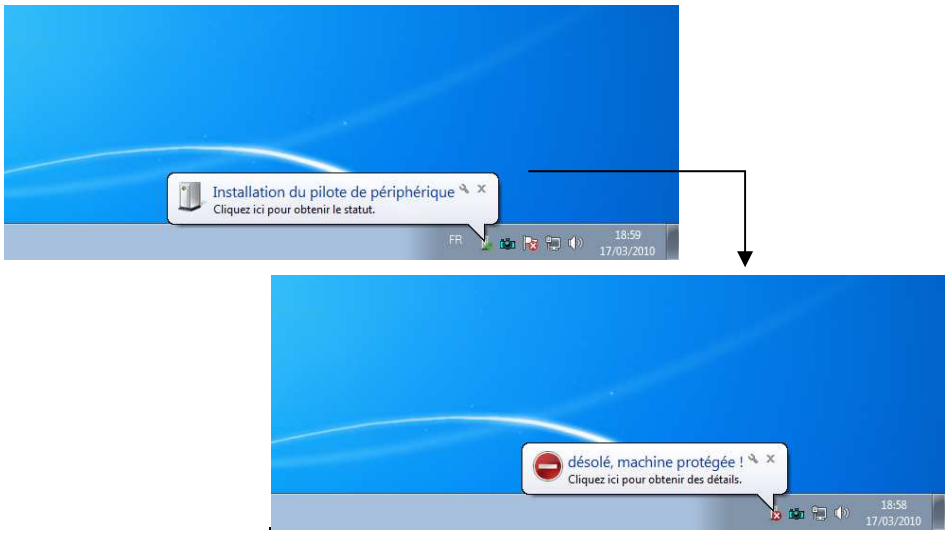




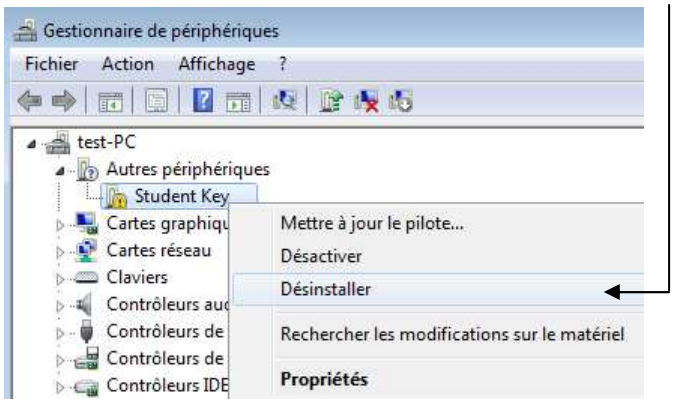

Voire y associer un message explicatif




Donnant lors de l'introduction d'une clé (ou autre périphérique USB…)

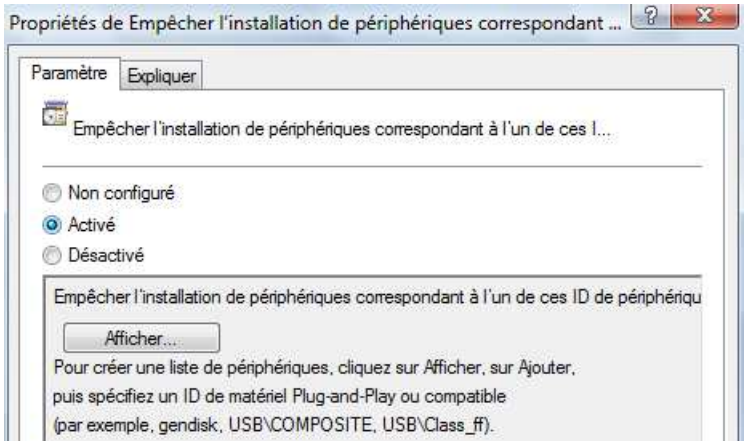



**N.B:** penser que si la clé a été détectée une fois, le message ne se réaffichera pas tant que l'on n'aura pas désinstaller le périphérique…



**ID et classe de Périphérique :**

On peut de manière plus générale empêcher une famille de périphérique :




Pour identifier un périphérique sous SEVEN plusieurs notions existent

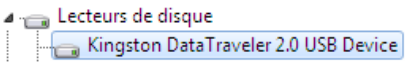
- l'**ID** de périphérique
- le **Nom de la classe** de périphérique.
  **USB, Display** gendisk
- le **GUID de la classe** de périphérique.
  **{36fc9e60-c465-11cf-8056-444553540000}**
  **{4D36E968-E325-11CE-BFC1-08002BE10318}**

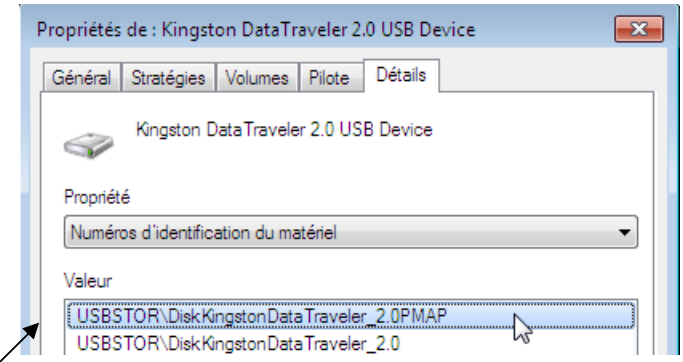
## ID de périphérique :

Chaque fabricant de composant et chaque périphérique possèdent des identificateurs uniques (ID).

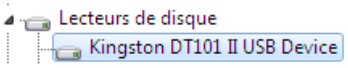
Dans le **Gestionnaire de périphériques**. On sélectionne un périphérique puis on demande **Propriétés / Détails**

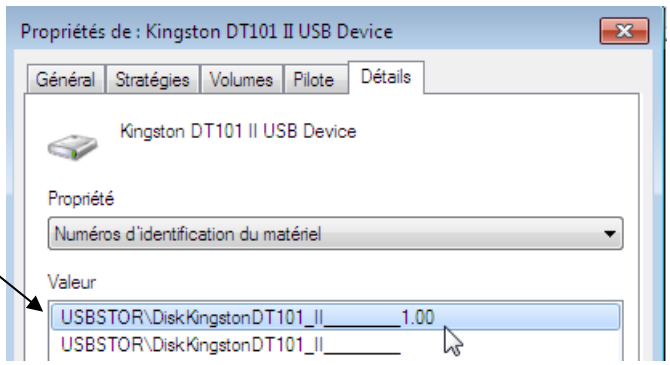
Dans la liste déroulante l'option **Numéro d'identification du matériel**.




Selon la Clé USB, cela change…

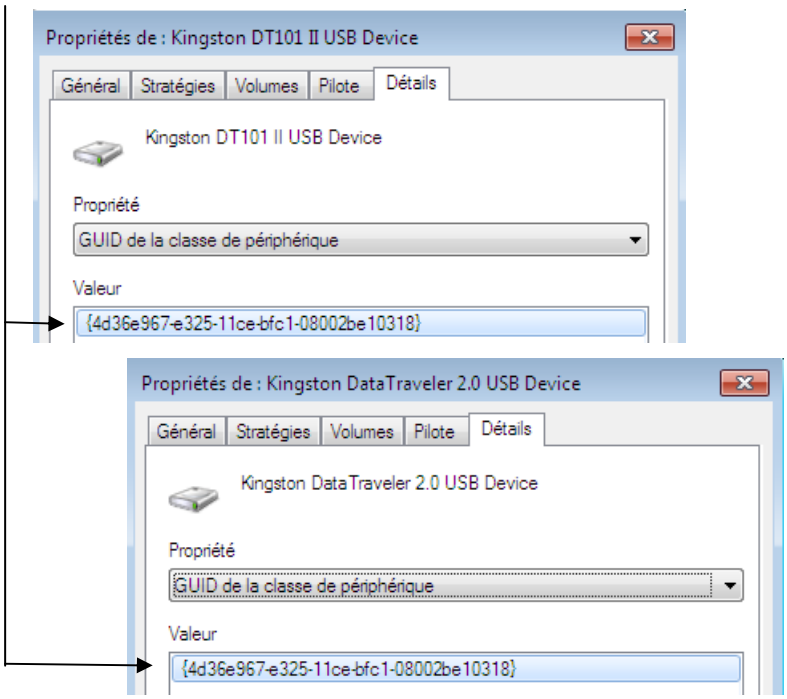


## GUIID de Classe de périphérique :

On peut demander l'option **GUID de la classe de périphérique**

Indépendamment de la Clé USB, c'est le même …




---

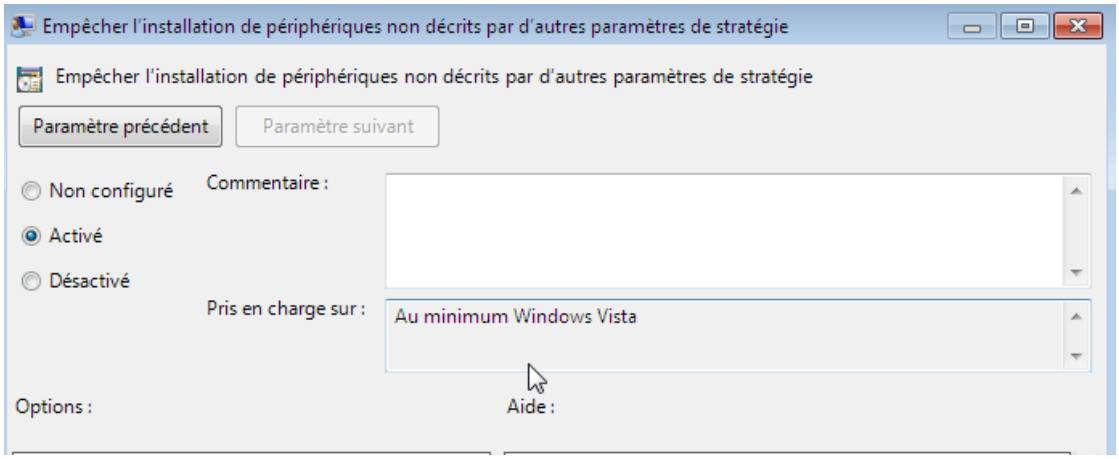
## Autoriser Un modèle de Clé USB:

On achète dans l'entreprise un modèle de clé USB, et on souhaite autoriser uniquement celle-ci.

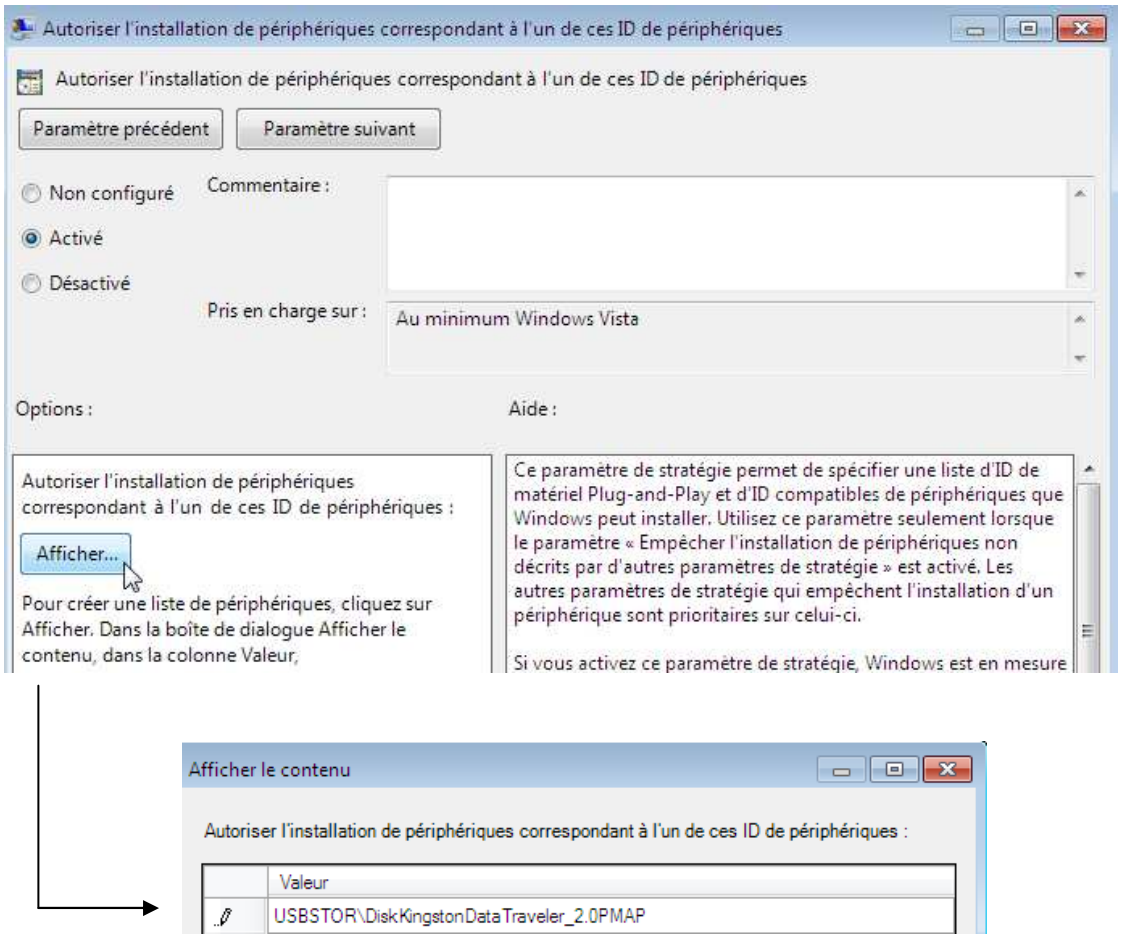
On récupère son numéro d'identification

**USBSTOR\DiskKingstonDataTraveler_2.0PMAP**

Il faut demander de manière générale…




Et autoriser uniquement


Autoriser l'installation de périphériques correspondant à l'un de ces ID de périphériques
Autoriser l'installation de périphériques correspondant à l'un de ces ID de périphériques
Paramètre précédent
Paramètre suivant
Non configuré
Activé
Désactivé
Commentaire :
Pris en charge sur :
Au minimum Windows Vista
Options :
Aide :
Autoriser l'installation de périphériques correspondant à l'un de ces ID de périphériques :
Afficher...
Pour créer une liste de périphériques, cliquez sur Afficher. Dans la boîte de dialogue Afficher le contenu, dans la colonne Valeur,
Ce paramètre de stratégie permet de spécifier une liste d'ID de matériel Plug-and-Play et d'ID compatibles de périphériques que Windows peut installer. Utilisez ce paramètre seulement lorsque le paramètre « Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie » est activé. Les autres paramètres de stratégie qui empêchent l'installation d'un périphérique sont prioritaires sur celui-ci.
Si vous activez ce paramètre de stratégie, Windows est en mesure


Afficher le contenu
Autoriser l'installation de périphériques correspondant à l'un de ces ID de périphériques :
Valeur
USBSTOR\DiskKingstonDataTraveler_2.0PMAP

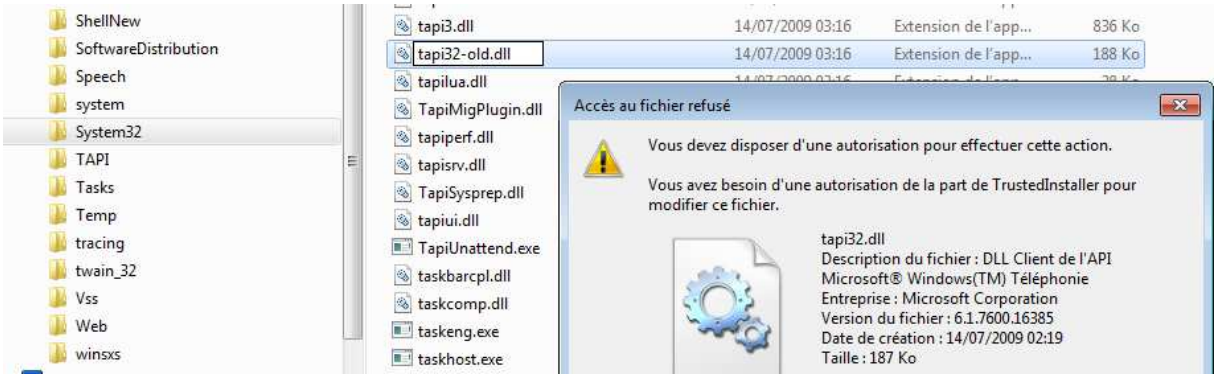
# VERIFIER L'INTEGRITE DU SYSTEME

**Corrompre le système Seven :**

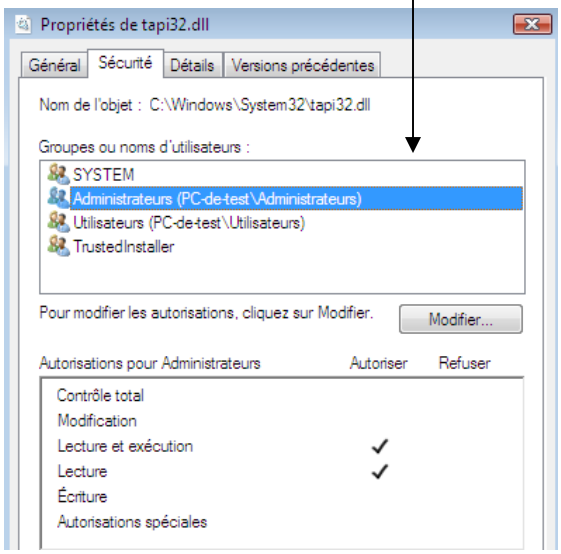
Noter que par exemple la Dll nommée **Tapi32.dll** en **windows\system32** peut être renommée en **Tapi32old.dll**…pour simuler une attaque système.

Les DLL qui sont présentes dans le dossier **Windows\systeme32** ont une sécurité NTFS assez restrictive.

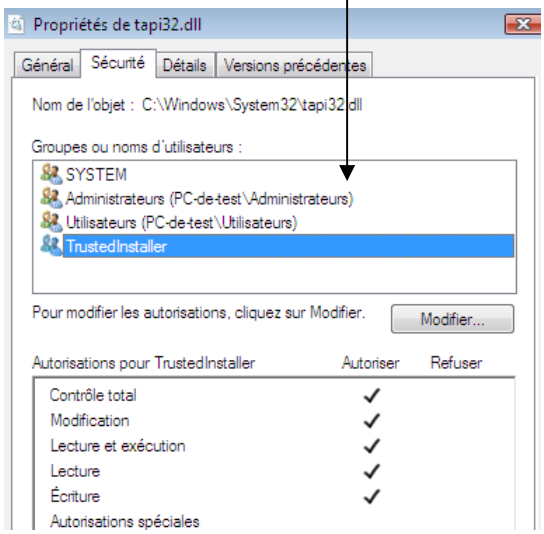
Par défaut ce n'est pas possible !




En effet tant qu'**Administrateur** du système vous avez juste un accès en lecture…



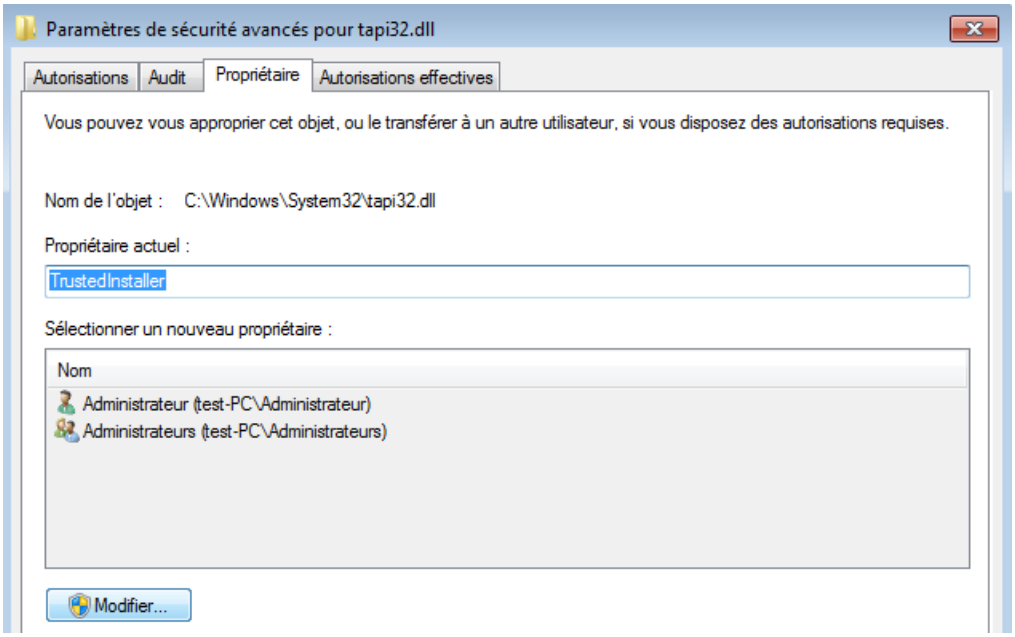

en effet seul le groupe **TrustedInstaller** à les droits complets.



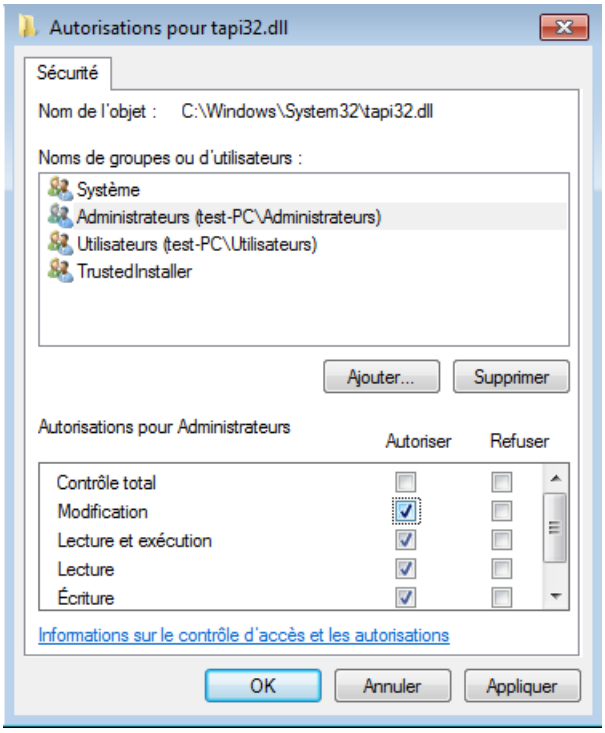

**N.B :** Par conséquent pour modifier une DLL il faut déjà en avoir les droits, et l'administrateur par défaut ne les a pas…

Après avoir changé la sécurité NTFS sur le fichier **tapi32.dll…**

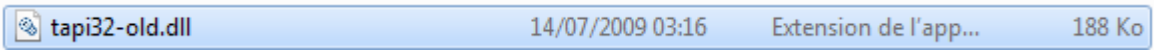
1. appropriation du fichier




2. Ajout des droits de l'administrateur




Renommons cette DLL de téléphonie **tapi32.dll** en **tapi32old.dll**



**Vérifier l'intégrité système Seven :**

Une simple vérification –(et éventuelle réparation) forcée se fera par

**Sfc /scanfile=c:\windows\system32\tapi32.dll**

```
C:\Users\Administrateur>sfc /scanfile=c:\windows\system32\tapi32.dll

La protection des ressources Windows a trouvé des fichiers endommagés et a pu
les réparer. Des détails sont fournis dans le journal CBS.Log
windir\Logs\CBS\CBS.log. Par exemple C:\Windows\Logs\CBS\CBS.log
```

Remodifions notre fichier une deuxième fois…

Une vérification plus complète –(et éventuelle réparation) forcée se fera par

**Sfc /scannow**

```
C:\Users\Administrateur>sfc /scannow

Début de l'analyse du système. Cette opération peut nécessiter un certain temps.

Démarrage de la phase de vérification de l'analyse du système.
La vérification 100% est terminée.

La protection des ressources Windows a trouvé des fichiers endommagés et a pu
les réparer. Des détails sont fournis dans le journal CBS.Log
windir\Logs\CBS\CBS.log. Par exemple C:\Windows\Logs\CBS\CBS.log
```

il existe une trace dans les fichiers de LOG stockés en **C:\Windows\Logs\CBS**


dans lequel il existe un fichier log, traçant la réparation

```
000001ab [SR] Verify complete
000001ac [SR] Repairing 1 components
000001ad [SR] Beginning Verify and Repair transaction
000001ae [SR] Repairing corrupted file [ml:520{260},l:46{23}]"\??\C:\Windows\System32"\[l:20{10}]"tapi32.dll" from store
000001af Repair results created:
```

Et l'on voit que le fichier d'origine est replacé !


**N.B**: si on veut redonner **TrustedInstaller** comme identifiant de sécurité, pour redonner la propriété ou les autorisations de sécurité, il faut spécifier

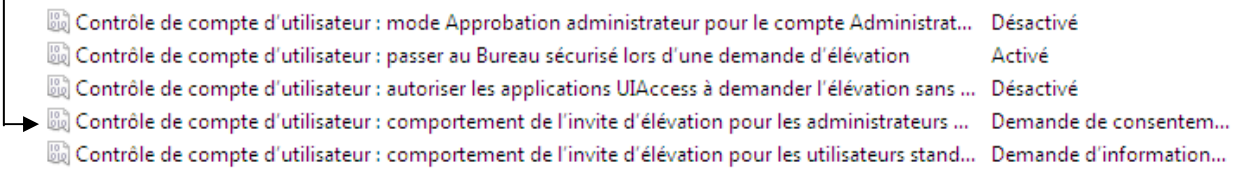
**NT SERVICE\TrustedInstaller**

# SEVEN & UAC – TEST ELEVATION

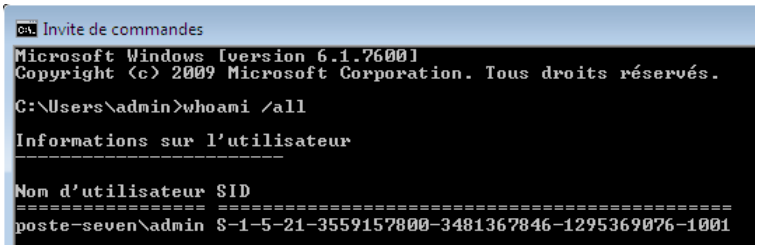
**Mise en Evidence de l'UAC :**

On crée un compte faisant partie du groupe des administrateurs, et on ouvre ensuite une session avec…

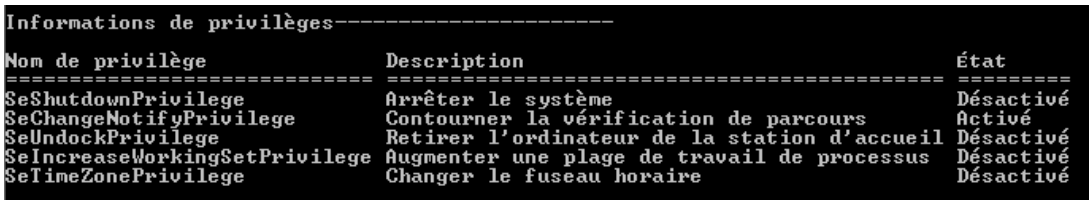
Le réglage par défaut étant maintenu, on devrait avoir une élévation de privilège possible, mais demandée pour ce compte d'administrateur, qui n'est pas le compte intégré…




On lance une invite de commande… **cmd** puis la commande **whoami /all**




Les privilèges sont faibles…



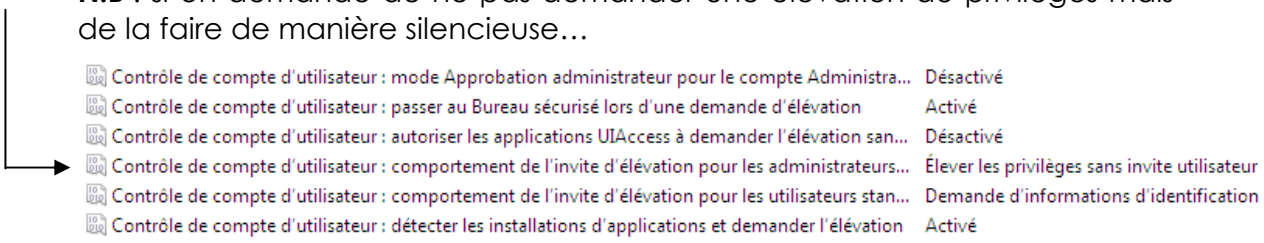

On lance une 2° invite de commande… **cmd** mais en tant qu'administrateur !


Après avoir accepté la demande d'élévation de privilège, on exécute la commande **whoami /all**

Les privilèges sont plus nombreux !!!

```
Informations de privilèges----------------------

Nom de privilège                Description                                                    État
=============================== ============================================================== =========
SeIncreaseQuotaPrivilege        Ajuster les quotas de mémoire pour un processus                Désactivé
SeSecurityPrivilege             Gérer le journal d'audit et de sécurité                        Désactivé
SeTakeOwnershipPrivilege        Prendre possession de fichiers ou d'autres objets              Désactivé
SeLoadDriverPrivilege           Charger et décharger les pilotes de périphériques              Désactivé
SeSystemProfilePrivilege        Performance système du profil                                  Désactivé
SeSystemtimePrivilege           Modifier l'heure système                                       Désactivé
SeProfileSingleProcessPrivilege Processus unique du profil                                     Désactivé
SeIncreaseBasePriorityPrivilege Augmenter la priorité de planification                         Désactivé
SeCreatePagefilePrivilege       Créer un fichier d'échange                                     Désactivé
SeBackupPrivilege               Sauvegarder les fichiers et les répertoires                    Désactivé
SeRestorePrivilege              Restaurer les fichiers et les répertoires                      Désactivé
SeShutdownPrivilege             Arrêter le système                                             Désactivé
SeDebugPrivilege                Déboguer les programmes                                        Désactivé
SeSystemEnvironmentPrivilege    Modifier les valeurs de l'environnement du microprogramme      Désactivé
SeChangeNotifyPrivilege         Contourner la vérification de parcours                         Activé
SeRemoteShutdownPrivilege       Forcer l'arrêt à partir d'un système distant                   Désactivé
SeUndockPrivilege               Retirer l'ordinateur de la station d'accueil                   Désactivé
SeManageVolumePrivilege         Effectuer les tâches de maintenance de volume                  Désactivé
SeImpersonatePrivilege          Emprunter l'identité d'un client après l'authentification      Activé
SeCreateGlobalPrivilege         Créer des objets globaux                                       Activé
SeIncreaseWorkingSetPrivilege   Augmenter une plage de travail de processus                    Désactivé
SeTimeZonePrivilege             Changer le fuseau horaire                                      Désactivé
SeCreateSymbolicLinkPrivilege   Créer des liens symboliques                                    Désactivé
```

**N.B** : si on demande de ne pas demander une élévation de privilèges mais de la faire de manière silencieuse…




Le résultat au niveau de la manip est bien sûr identique… (on a pas les même privilèges selon que l'on lance CMD ou CMD en tant qu'administrateur) mais c'est transparent pour notre administrateur !

- On peut donc demander une invite d'élévation automatique, et laisser l'UAC faire son travail…

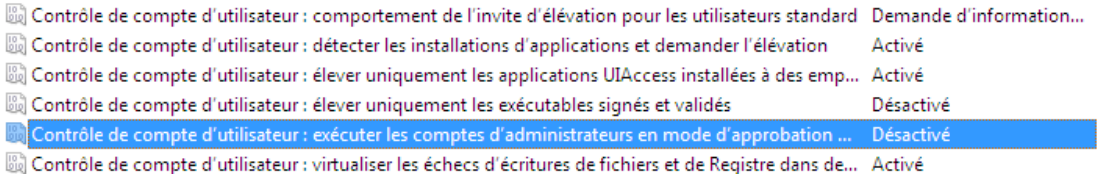
## Administrateur intégré absence d'UAC:

Si on exécute le même test avec le compte Administrateur intégré, alors on remarque qu'il n'y a aucune différence entre un CMD lancé simplement, et un CMD lancé en tant qu'administrateur…

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

## Désactivation de l'UAC :

Si on désactive totalement l'UAC…



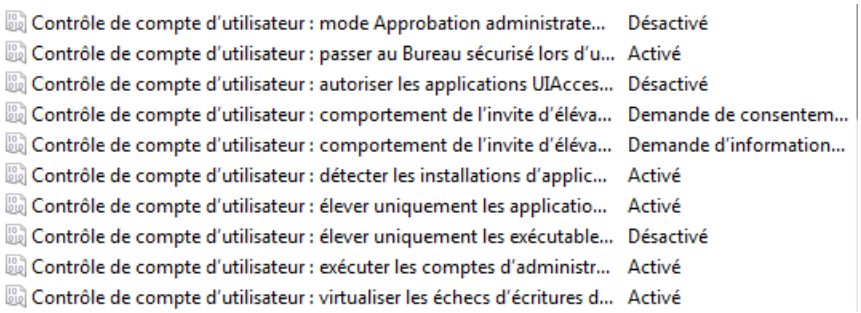

Il n'y a plus aucune différence entre CMD et CMD en tant qu'administrateur…

# SEVEN – VIRTUALISATION & APPLICATIONS HERITEES

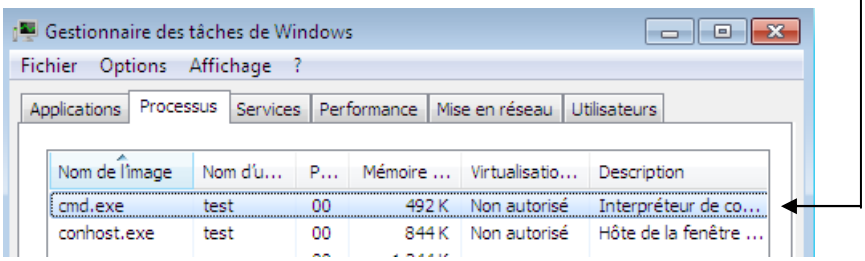
**Pré-requis :**

Pour ce faire il est nécessaire que :

- l'UAC ne soit pas désactivée totalement…

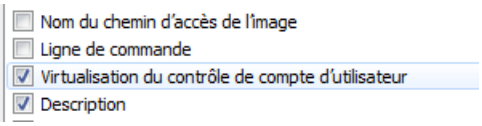



- Utiliser un compte Administrateur (pour pouvoir demander soit même une « virtualisation » du processus) mais pas l'administrateur "Root", pour qui l'UAC est par défaut désactivée… et donc il n'y a pas de possibilité de virtualisation de processus (**Non autorisé**)




- Lancer un processus qui soit « virtualisable », comme l'interpréteur de commande.

On peut modifier l'état de la virtualisation d'un processus …dans le Gestionnaire des tâches, sur la tâche en question, par le menu contextuel en demandant **Virtualisation du contrôle de compte d'utilisateur**

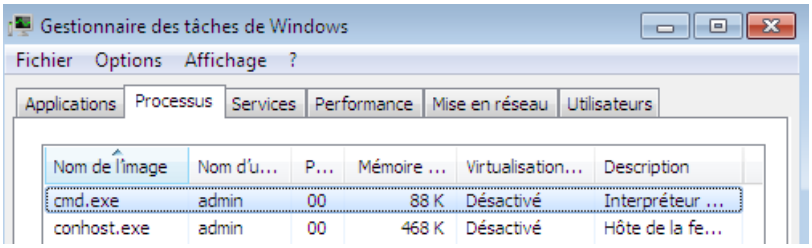


**Mise en Evidence de la virtualisation :**

1. ouvrons une session avec un compte autre que l'administrateur, (par exemple "test")

2. lançons l'interpréteur de commande

   par defaut **cmd** est un processus signé Seven donc la virtualisation est désactivée par défaut




3. essayons d'écrire dans notre répertoire

```
C:\Users\test>dir >affiche.txt

C:\Users\test>
```

   c'est possible,

```
C:\Users\test>dir
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 586A-31A3

 Répertoire de C:\Users\test

18/09/2007  17:17    <REP>          .
18/09/2007  17:17    <REP>          ..
18/09/2007  17:17               864 affiche.txt
07/09/2007  12:30    <REP>          Contacts
07/09/2007  12:47    <REP>          Desktop
```

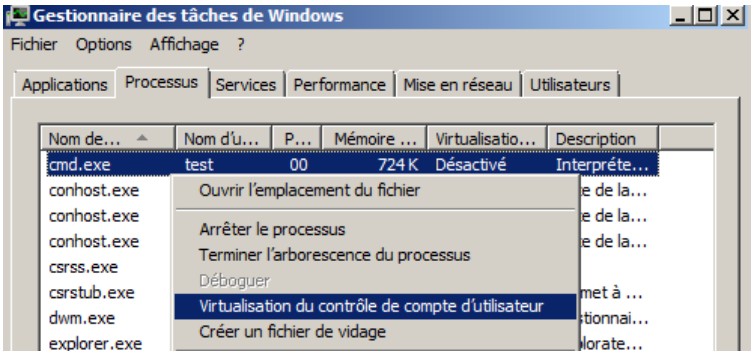
4. plaçons nous dans un dossier système sensible (comme Windows)

```
C:\Users\test>cd \windows
```

   essayons d'écrire dedans, cela ne marche pas !

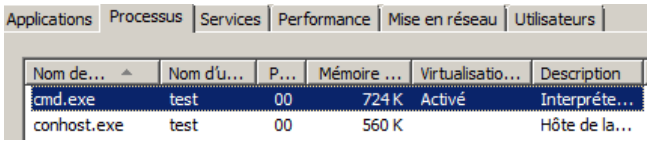
```
C:\Windows>dir >affiche.txt
Accès refusé.
```

5. virtualisons notre processus CMD :




   on confirme…

   pour obtenir



6. réessayons d'écrire dans le dossier réservé...

```
C:\Windows>dir >affiche.txt
```

Cela a l'air de marcher !!!!

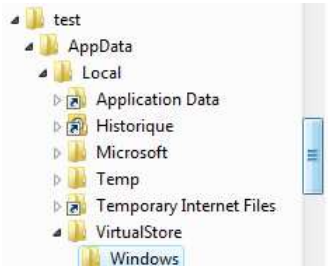
```
C:\Windows>dir
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 586A-31A3

 Répertoire de C:\Windows

18/09/2007  17:25    <REP>          .
18/09/2007  17:25    <REP>          ..
02/11/2006  14:37    <REP>          addins
18/09/2007  17:25             4 034 affiche.txt
12/09/2007  07:08    <REP>          AppPatch
```

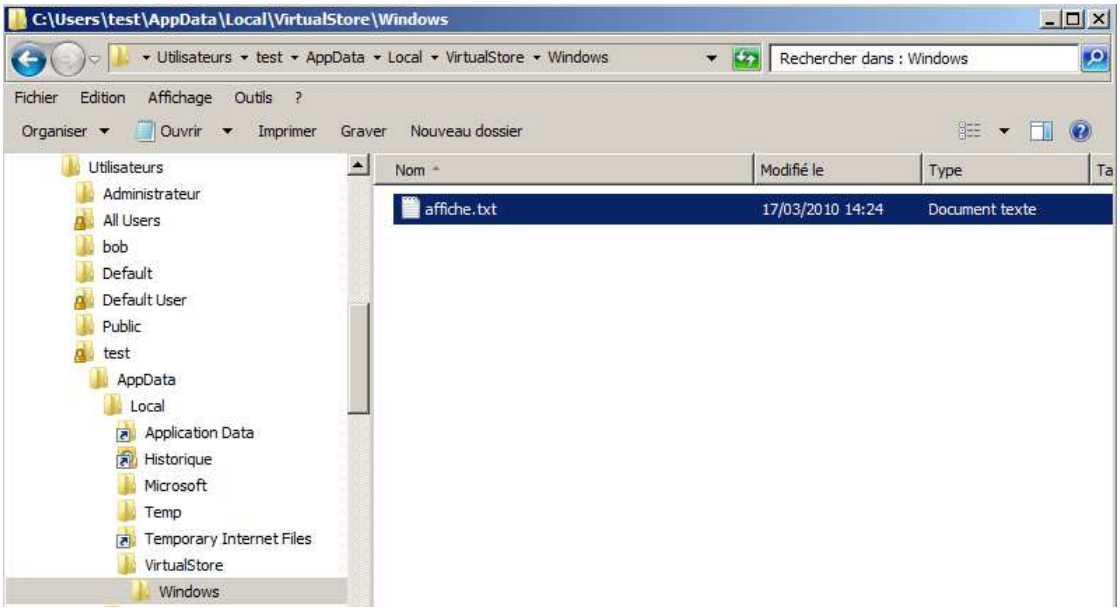
7. maintenant vérifions ou l'on a écrit réellement ....

notre fichier « *affiche.txt* »

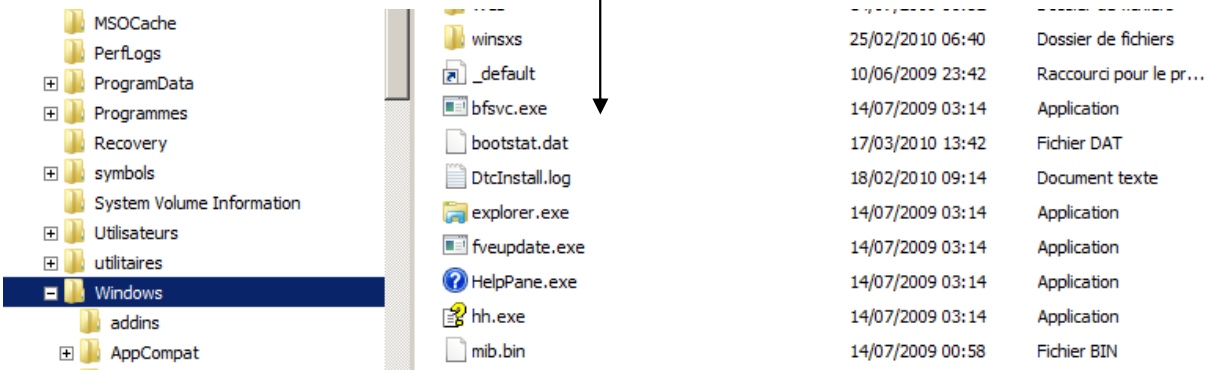
se trouve en

**\User\Test\AppData\local\VirtualStore**Windows



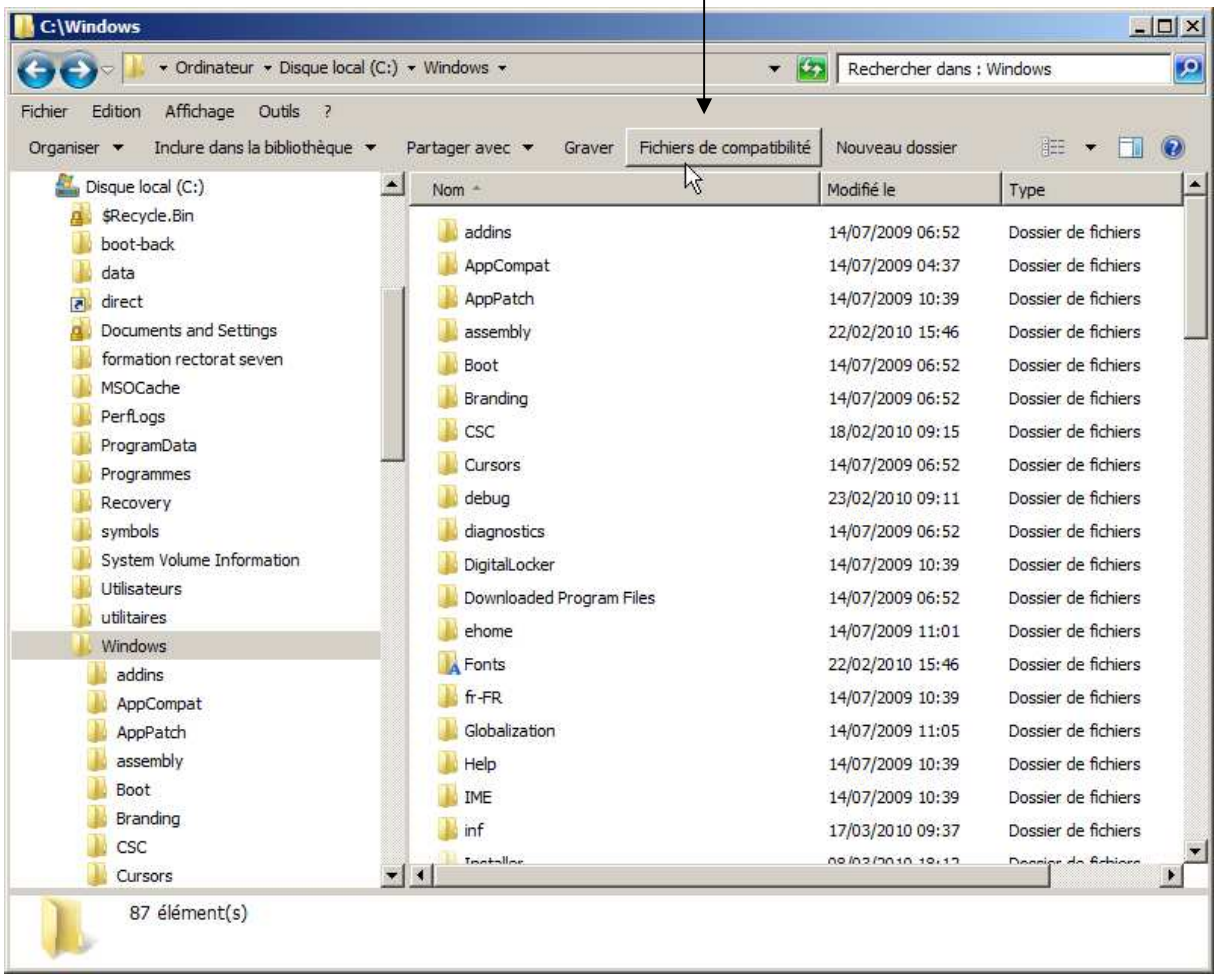




Et sûrement pas en **\Windows** ?



Ceci dit, si on regarde dans le vrai dossier système Windows... le bouton **Fichiers de compatibilité** apparaît, permettant de savoir que quelque chose a été virtualisé…

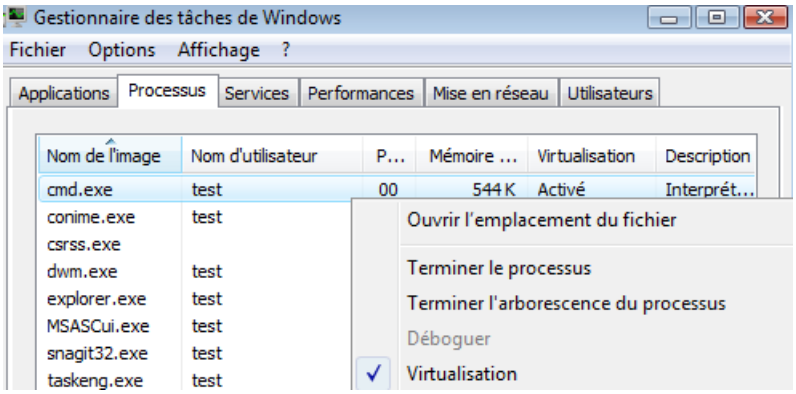
**N.B**: le bouton n'apparaît que s'il y a au moins un fichier, si on a uniquement crée un dossier vide, il ne s'affichera pas…



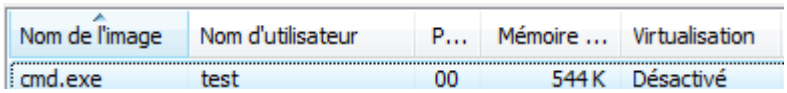

Et en cliquant dessus, on obtient


Et on se trouve immédiatement là ou le fichier a été réellement écris…

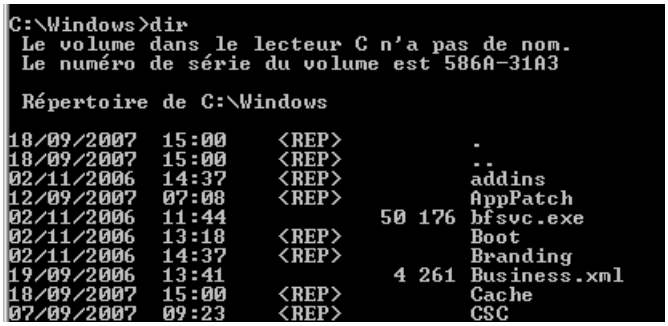
8. Si on arrête la virtualisation,




pour retrouver




alors ensuite **affiche.txt** a disparut !!!!




Ceci dit il reste stocké dans Virtual Store…

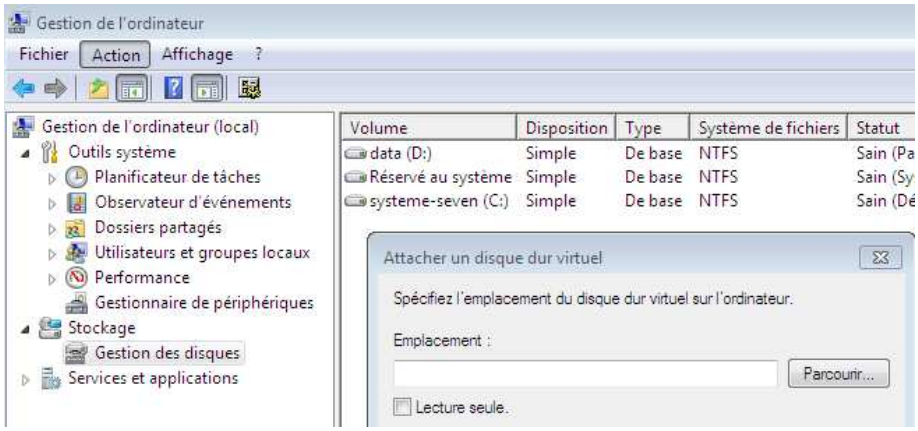
# BOOT DEPUIS UN DISQUE VHD

## Principe du Boot sur VHD

Windows 7 et Windows Server 2008 R2 offrent la possibilité de pouvoir booter un système sur un disque VHD, cette fonctionnalité rendue possible via le "Boot Manager" permet d'exploiter un VHD comme disque amorçable.

Installer un nouveau système d'exploitation se limitera donc à copier le fichier VHD et de le référencer dans notre Boot Manager…

Ici le système stocké dans le VHD ne travaille pas de manière virtualisée, il utilise réellement l'environnement matériel ou il se trouve, la seule différence c'est qu'il va chercher "son" disque via un driver capable de lire les fichiers VHD… C'est un peu le même principe que celui qui consiste à attacher un disque VHD depuis SEVEN ou 2008R2 dans le gestionnaire de disque.



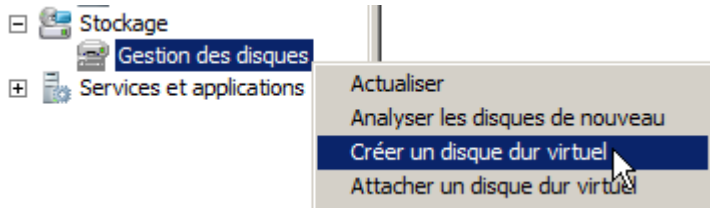

**N.B**: Si toutes les versions de Seven peuvent inclure dans leur Boot un vhd, seules les versions **Enterprise** et **Intégrale** de **SEVEN** prennent en charge le boot depuis VHD, ainsi **toutes les licences 2008R2**

Il en découle plusieurs choses :

- si un VHD est lançable depuis n'importe quel Hyper-V, il n'en est pas de même ici, car l'OS doit être capable de lire les VHD comme disques dur, XP et 2003 ne peuvent pas… seuls SEVEN et 2008R2 le peuvent
- le disque Vhd ne peut contenir qu'une version Entreprise ou Intégrale de Seven, ou un Serveur 2008R2. Sinon un problème de licence existe.
- dans le **bcdedit**, il faut bien rajouter **detectehal = yes** pour que l'OS s'adapte au nouvel environnement matériel…
- Il faut avoir de la place pour que lors du lancement le fichier VHD dynamique puisse prendre la taille requise. (s'il est statique, pas de problèmes.)
- Il faut « installer » le Système dans le VHD pour que l'OS détecte bien le Hard de notre configuration… Ce ne peut être un VHD d'une VM prise sur un Hyper-Viseur

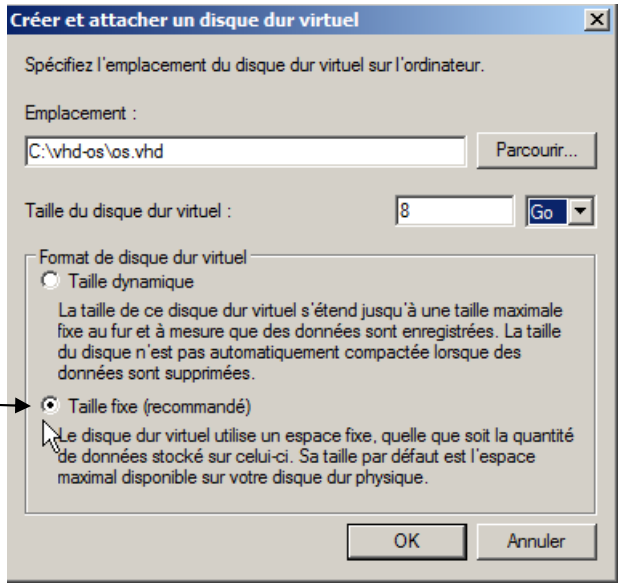
## Réalisation d'un disque VHD

- il faut créer un disque VHD,
- et lancer une installation sur ce VHD…




Par exemple ***windows-7-sp1-entreprise.vhd*** pour un disque **vhd** avec seven sp1 entreprise

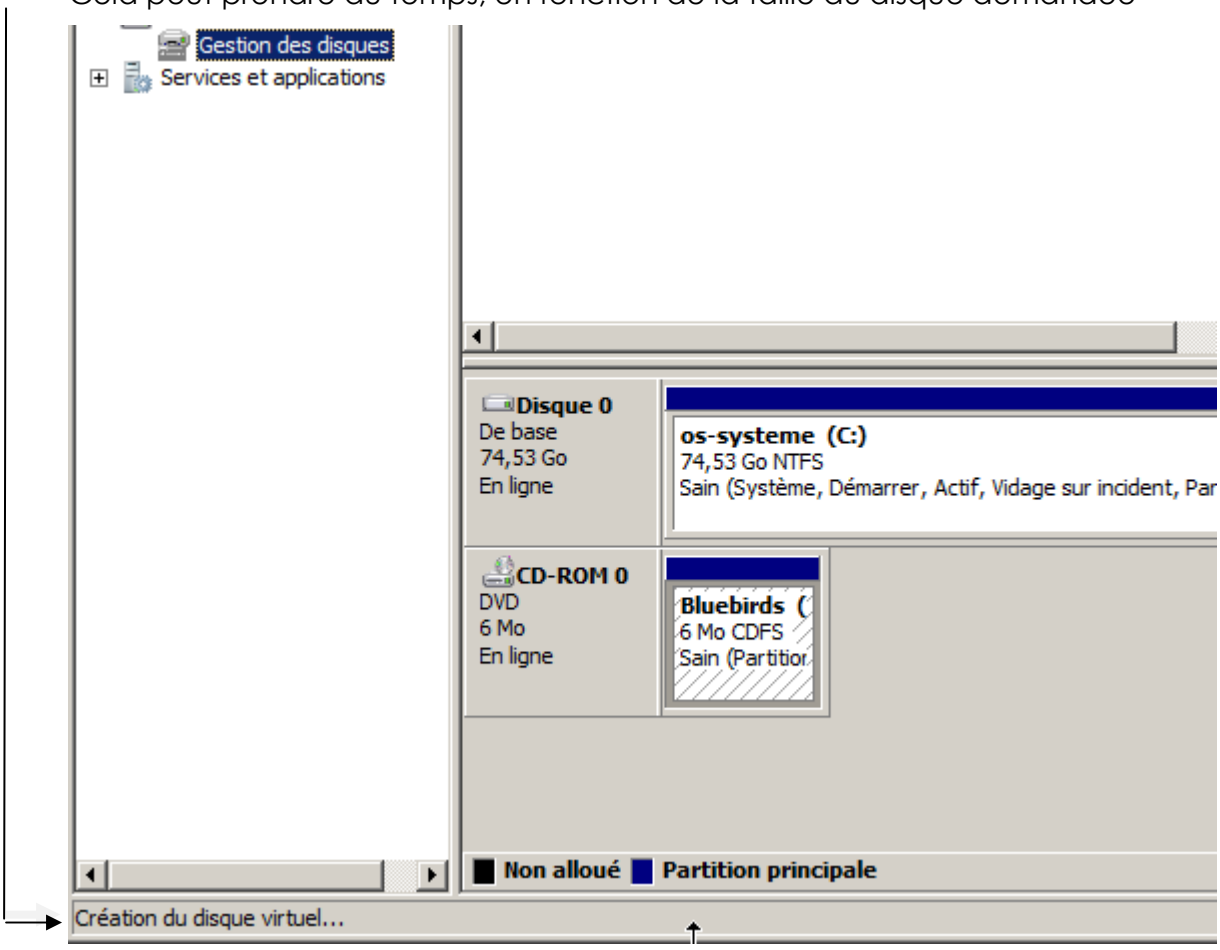
Pour lequel impérativement on demande **Taille Fixe**



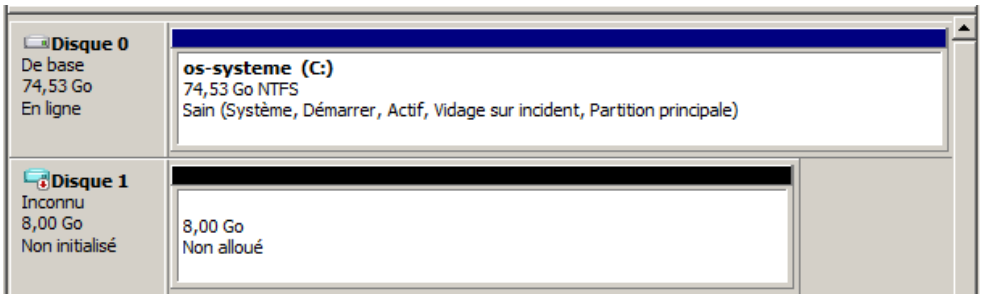

9 Giga min pour un 2008R2

9 Giqa min pour un Windows 7

Cela peut prendre du temps, en fonction de la taille du disque demandée

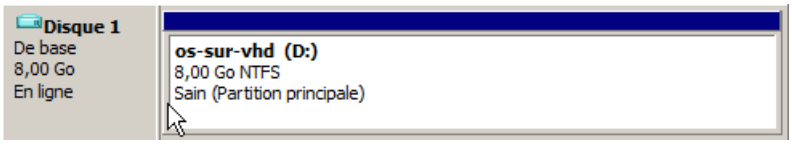


Avant d'obtenir

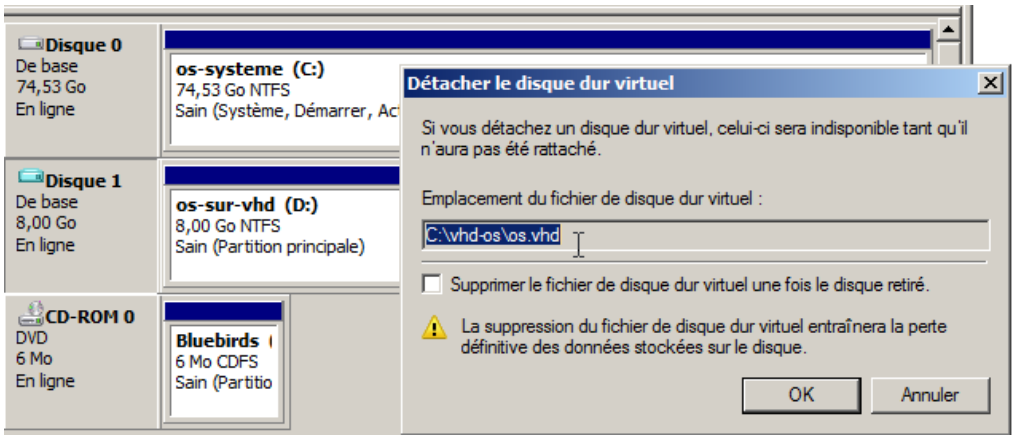



Ensuite on peut initialiser le Disque (facultatif)


On crée une partition, formatage et on donne un label parlant… (facultatif)




Puis on détache notre disque virtuel, sans le supprimer, bien sûr.

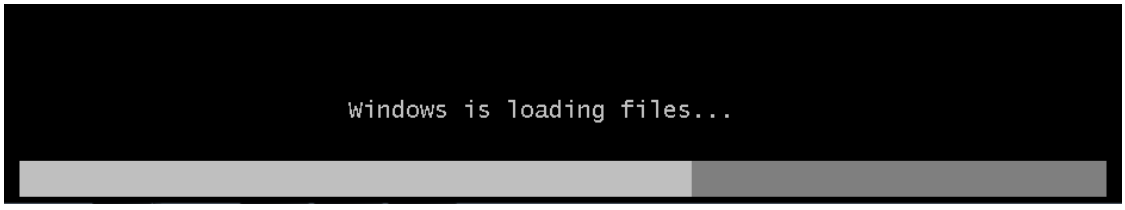



On a maintenant un fichier pour notre disque en **vhd**

| Nom | Modifié le | Type | Taille |
|---|---|---|---|
| os.vhd | 18/04/2013 05:17 | Fichier VHD | 8 388 609 Ko |

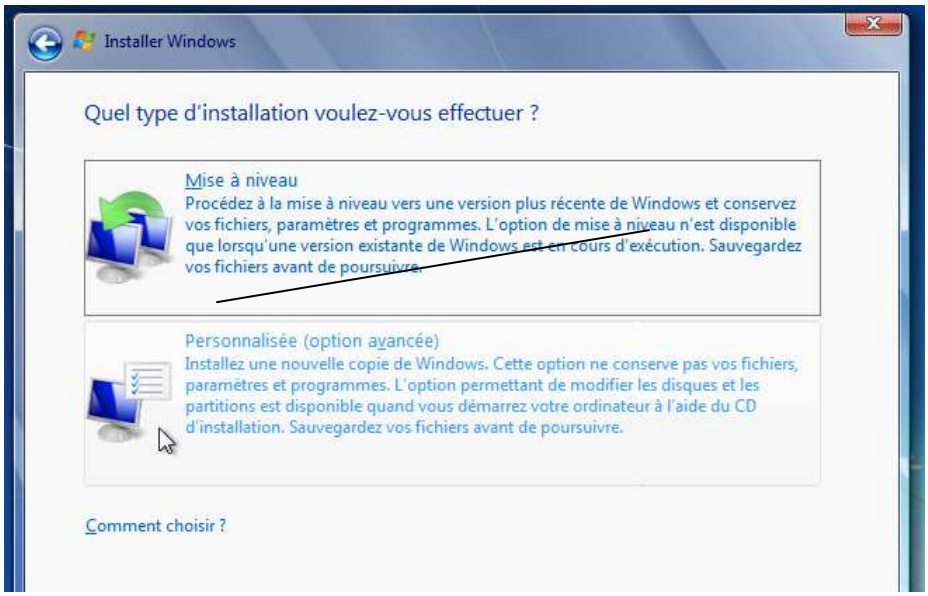
## Installation de l'OS dans le VHD

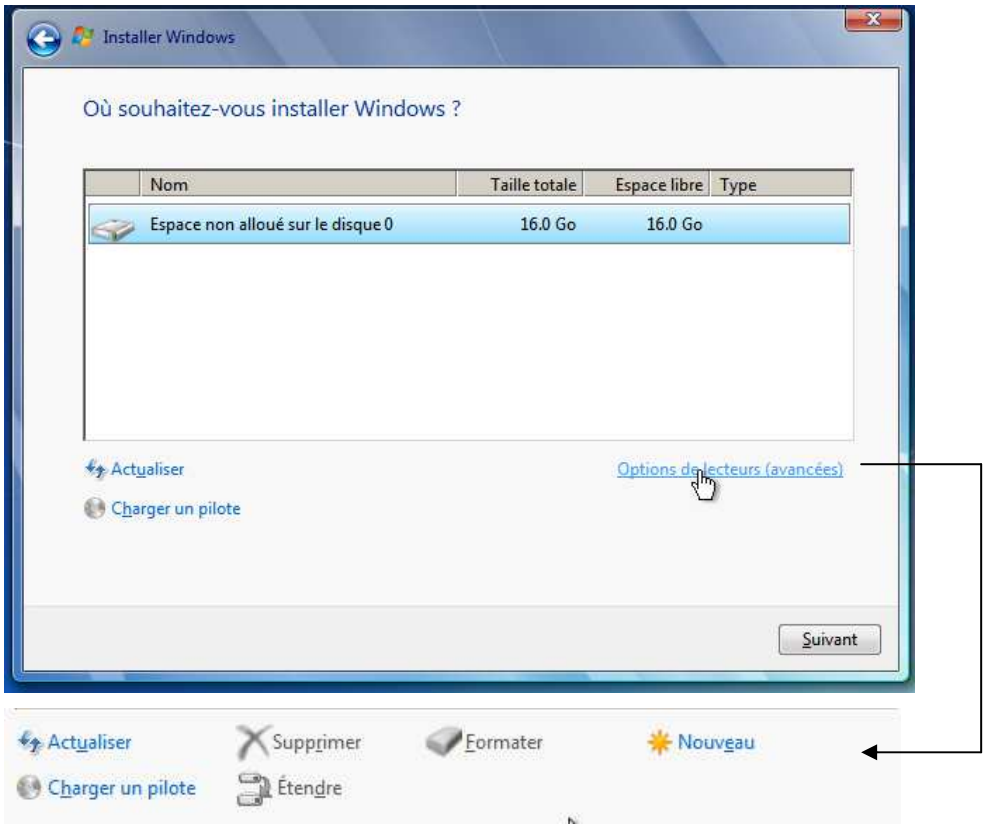
En bootant depuis un DVD, c'est la manière normale d'installation…




On passe avec une interface graphique de manière quasi immédiate…

on demande une Installation **Personnalisée (option avancée).**




Notre disque VHD n'apparaît pas dans la liste car il n'est pas attaché, Il va falloir via diskpart en ligne de commande le faire. On accède à l'invite de commande via **MAJ+F10** et on lance l'utilitaire **Diskpart,**

```
C:\Users\Administrateur>diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
```

Puis si nécessaire **List Disk**

```
DISKPART> list disk

  Nº disque  Statut         Taille   Libre    Dyn  GPT
  ---------  -------------  -------  -------  ---  ---
  Disque 0    En ligne         74 G octets  1024 K octets
  Disque 1    En ligne          9 G octets     9 G octets
```

Suivit d'un **Select Disk=0**

```
DISKPART> Select disk=0

Le disque 0 est maintenant le disque sélectionné.
```

**List Vol**

```
DISKPART> list vol

  Nº volume   Ltr  Nom          Fs     Type        Taille   Statut     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E   Bluebirds    CDFS   DVD-ROM     6146 K   Sain
  Volume 1     C   os-systeme   NTFS   Partition     74 G   Sain       Système
```

On repère la lettre sur laquelle se trouve le fichier VHD à lier, (c'est le disque système sur lequel Seven est installé, (ici dans l'exemple **C**)

puis on tape **Select vdisk file=C:\vhd-os\os.vhd**

Avec la lettre repérée « **C** »: et le nom du disque vhd « ***os.vhd*** »

```
DISKPART> select vdisk file=c:\vhd-os\os.vhd

DiskPart a correctement sélectionné le fichier de disque virtuel.
```

… Diskpart nous informe que le fichier de disque virtuel est sélectionné.

Ensuite on tape **Attach vdisk**

Diskpart nous informe qu'il a attaché e fichier de disque virtuel

```
DISKPART> attach vdisk

  100 pour cent effectués

DiskPart a correctement attaché le fichier de disque virtuel.
```

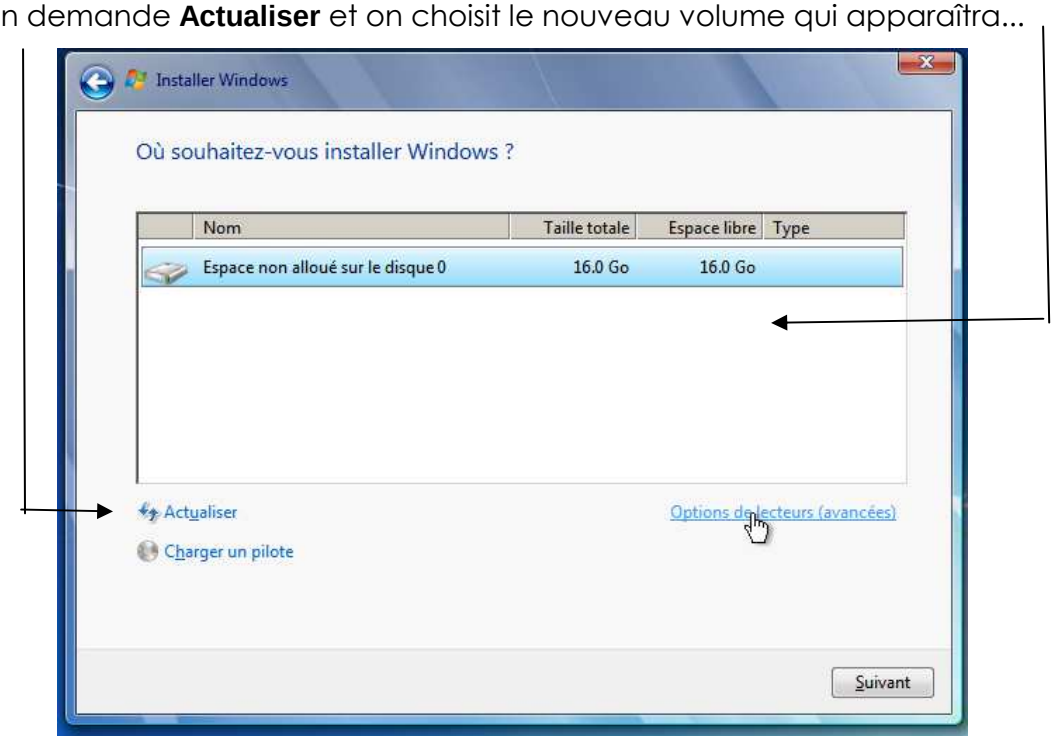
Un **list Vol** confirme cela

```
DISKPART> list vol

  Nº volume   Ltr  Nom          Fs     Type        Taille   Statut     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E   Bluebirds    CDFS   DVD-ROM     6146 K   Sain
  Volume 1     C   os-systeme   NTFS   Partition     74 G   Sain       Système
  Volume 2     D   os-sur-vhd   NTFS   Partition   8189 M   Sain
```

On peut quitter disqpart par **exit**

```
DISKPART> exit

Quitte DiskPart...
```

Puis on quitte la ligne de commande, on revient dans l'interface graphique, on demande **Actualiser** et on choisit le nouveau volume qui apparaîtra...




On termine ensuite l'installation classiquement

## Supprimer un Boot sur VHD

Il suffit dans le magasin d'effacer le chargeur de démarrage avec l'identifiant correspondant à notre OS sur VHD.

Par exemple ici l'identifiant étant

{e34d0d0a-13fa-11e0-a522-aa22f2a4872a}

```
Chargeur de démarrage Windows
-----------------------------
identificateur          {e34d0b0a-13fa-11e0-a522-aa22f2e4872a}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             boot OS depuis VHD
locale                  fr-FR
inherit                 {bootloadersettings}
recoverysequence        {e34d0b08-13fa-11e0-a522-aa22f2e4872a}
recoveryenabled         Yes
osdevice                partition=C:
systemroot              \Windows
resumeobject            {e34d0b06-13fa-11e0-a522-aa22f2e4872a}
nx                      OptIn
```

On le supprimerait par un

**bcdedit /delete { e34d0d0a-13fa-11e0-a522-aa22f2a4872a}**

et ensuite suppression du fichier vhd dans le dossier ***\vhd-os***

**N.B :** si le dernier chargeur est le chargeur par défaut, comme par exemple dans le magasin ci-dessous

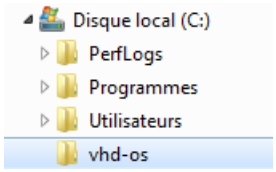
```
Gestionnaire de démarrage Windows
---------------------------------
identificateur          {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  fr-FR
inherit                 {globalsettings}
default                 {default}
resumeobject            {716e0e20-a4d4-11e2-87ca-0010b586d1f9}
displayorder            {default}
                        {current}
toolsdisplayorder       {memdiag}
timeout                 30

Chargeur de démarrage Windows
-----------------------------
identificateur          {default}
device                  vhd=[C:]\vhd-os\os.vhd
path                    \Windows\system32\winload.exe
description             Windows Server 2008 R2
locale                  fr-FR
inherit                 {bootloadersettings}
recoverysequence        {716e0e22-a4d4-11e2-87ca-0010b586d1f9}
recoveryenabled         Yes
osdevice                vhd=[C:]\vhd-os\os.vhd
systemroot              \Windows
resumeobject            {716e0e20-a4d4-11e2-87ca-0010b586d1f9}
nx                      OptOut

Chargeur de démarrage Windows
-----------------------------
identificateur          {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Windows 7
locale                  fr-FR
inherit                 {bootloadersettings}
recoverysequence        {716e0e17-a4d4-11e2-87ca-0010b586d1f9}
recoveryenabled         Yes
osdevice                partition=C:
systemroot              \Windows
resumeobject            {716e0e15-a4d4-11e2-87ca-0010b586d1f9}
nx                      OptIn
```

Pour le supprimer il faut ajouter l'option ***/f***

```
C:\Users\Administrateur>bcdedit /delete {default} /f_
```

## Ajouter Manuellement une entrée Bcdedit sur VHD

Un avantage d'un disque VHD, c'est que c'est un fichier que l'on dépose sur une partition, donc pas besoin de créer une partition distincte pour installer un système d'exploitation en Multi-Boot.




soit un dossier ***vhd-os*** par exemple contenant des fichiers **.vhd** de systèmes d'exploitation alternatifs...

on doit ajouter une entrée dans notre boot manager. On va dupliquer l'entrée actuelle de seven sur une autre entrée pour avoir un nouveau GUID

```
C:\Users\Administrateur>bcdedit /copy {current} /d "boot OS depuis VHD"
L'entrée a été correctement copiée dans {e34d0b0a-13fa-11e0-a522-aa22f2e4872a}.
```

on dispose donc d'une nouvelle entrée

```
Chargeur de démarrage Windows
-----------------------------
identificateur          {e34d0b0a-13fa-11e0-a522-aa22f2e4872a}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             boot OS depuis VHD
locale                  fr-FR
inherit                 {bootloadersettings}
recoverysequence        {e34d0b08-13fa-11e0-a522-aa22f2e4872a}
recoveryenabled         Yes
osdevice                partition=C:
systemroot              \Windows
resumeobject            {e34d0b06-13fa-11e0-a522-aa22f2e4872a}
nx                      OptIn
```

supposons que notre fichier vhd se nomme *os.vhd*


il faut modifier l'entrée DEVICE

```
C:\Users\Administrateur>bcdedit /set {e34d0b0a-13fa-11e0-a522-aa22f2e4872a} devi
ce vhd=[C:]\vhd-os\os.vhd
L'opération a réussi.
```

puis l'entrée OSDEVICE

```
C:\Users\Administrateur>bcdedit /set {e34d0b0a-13fa-11e0-a522-aa22f2e4872a} osde
vice vhd=[C:]\vhd-os\os.vhd
L'opération a réussi.
```

sans oublier l'instruction DETECTHAL forçant le re-détection de la couche d'abstraction matérielle

```
C:\Users\Administrateur>bcdedit /set {e34d0b0a-13fa-11e0-a522-aa22f2e4872a} dete
cthal on
L'opération a réussi.
```

de manière à avoir au final

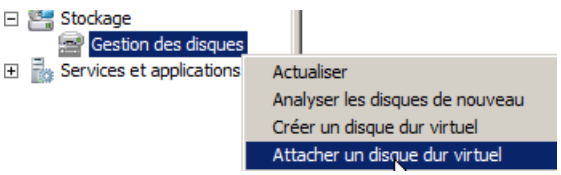
```
Chargeur de démarrage Windows
-----------------------------
identificateur          {e34d0b0a-13fa-11e0-a522-aa22f2e4872a}
device                  vhd=[C:]\vhd-os\os.vhd
path                    \Windows\system32\winload.exe
description             boot OS depuis VHD
locale                  fr-FR
inherit                 {bootloadersettings}
recoverysequence        {e34d0b08-13fa-11e0-a522-aa22f2e4872a}
recoveryenabled         Yes
osdevice                vhd=[C:]\vhd-os\os.vhd
systemroot              \Windows
resumeobject            {e34d0b06-13fa-11e0-a522-aa22f2e4872a}
nx                      OptIn
detecthal               Yes
```

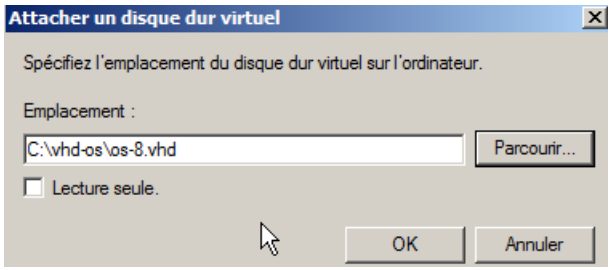
## Boot manager - Os loader Windows 8

Si on construit manuellement un magasin allant chercher un vhd, il faut faire attention à la version de l'OSloader présent sur le poste d'origine. Par exemple la version **osloade**r de Seven, ne peut pas lancer un windows 8. Lorsque l'on installe le Windows 8 sur la machine en direct dans le VHD, l'installation met à jour cet Os loader, et donc pas de soucis. Mais si on ajoute manuellement l'entrée dans BCDEDIT pointant vers notre vhd contenant windows 8, alors au démarrage on aura un message d'erreur.

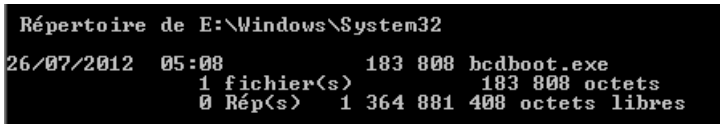
Pour mettre à jour le Boot manager de Seven par celui de Windows 8 il faut utiliser l'outil **BCDBOOT** fournit avec Windows 8… qui est donc situé dans le répertoire \System32 de notre image VHD. **BCDBoot** permet de copier les fichiers de démarrage de l'environnement et la configuration des données de démarrage (BCD), depuis le répertoire \Windows du VHD, vers la partition système C:\.

On va donc attacher le disque .vhd contenant windows 8

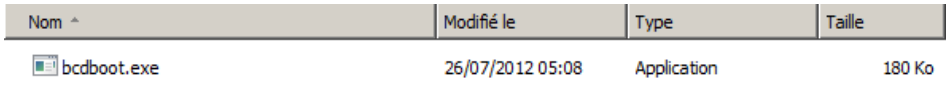



On y trouve un fichier système en windows\system32 nommé **bcdboot.exe**




On fait une copie de ce fichier a la racine du disque c : (par exemple)




En invite de commande ensuite, on tape (attention a la lettre du disque vhd, ici dasn l'exemple le disque vhd est monté dans le lecteur f ☺

**bcdboot f:\windows /s c :**

L'outil BCDboot importe automatiquement les informations de l'installation existante lors de la mise à jour du gestionnaire de démarrage (BCD). L'ordinateur est maintenant mis à jour pour inclure un environnement de démarrage de Windows 8

## Choix du VHD - Licences

La seule restriction concerne les OS contenus dans ces VHD, en effet si depuis Seven toutes versions on sait attacher un disque virtuel, tous les Windows ne sont pas capables de « se booter » depuis un disque VHD

Pour **Seven** : uniquement les versions **Entreprise** et **Ultimate** le peuvent

Pour **2008 R2** : toutes les versions le peuvent

## Clé USB bootable (mode opératoire):

On utilise **diskpart** intégré à Seven ou 2008. En invite de commande on lance **Diskpart**

```
C:\Users\Administrateur>diskpart

Microsoft DiskPart version 6.1.7601
Copyright (C) 1999-2008 Microsoft Corporation.
Sur l'ordinateur : POSTE-WAIK
```

On repère les disques disponibles (dont notre clé USB)

**list disk**

```
DISKPART> list disk

  Nº disque  Statut         Taille   Libre    Dyn  GPT
  ---------  -------------  -------  -------  ---  ---
  Disque 0    En ligne        114 G octets  1024 K octets
  Disque 1    En ligne       3817 M octets      0 octets
```

Disque 1 = clé de 4Gig

On repère le chiffre assigné à la clé USB (par exemple 1)

**select disk=1**

```
DISKPART> select disk=1

Le disque 1 est maintenant le disque sélectionné.
```

Tapez maintenant « clean », les données de partition seront toutes effacées,

**Clean**

```
DISKPART> clean

DiskPart a réussi à nettoyer le disque.
```

Il faut maintenant créer une partition sur le disque " create partition primary"

**create partition primary**

```
DISKPART> create partition primary

DiskPart a réussi à créer la partition spécifiée.
```

La partition générée il faut la sélectionner et la rendre active en général, le fait de l'avoir crée, la sélectionne, mais on peut vérifier et si besoin la sélectionner via **select partition 1**

**select partition 1**

```
DISKPART> select partition 1

La partition 1 est maintenant la partition sélectionnée.
```

On Vérifie que l'on est bien dessus

**List partition**

```
DISKPART> list partition

  Nº partition   Type              Taille   Décalage
  -------------  ----------------  -------  --------
* Partition 1    Principale        3817 M     64 K
```

On la rend active

**active**

```
DISKPART> active

DiskPart a indiqué la partition actuelle comme étant active.
```

On passe maintenant à son formatage en fat32 ou mieux NTFS, donc par

**format fs=fat32** ou mieux **format fs=NTFS LABEL="cle bootable"**

```
DISKPART> format fs=fat32

  100 pour cent effectués

DiskPart a formaté le volume.
```

```
DISKPART> format Fs=NTFS LABEL="cle bootable Winpe"

  100 pour cent effectués

DiskPart a formaté le volume.
```

On termine en forçant l'assignation d'une lettre de lecteur

**assign**

```
DISKPART> assign

DiskPart a correctement assigné la lettre de lecteur ou le point de montage.
```

Une dernière vérification par

**list volume**

```
DISKPART> list volume

  Nº volume   Ltr  Nom          Fs     Type        Taille   Statut     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     E   Bluebirds    CDFS   DVD-ROM     6146 K   Sain
  Volume 1         Réservé au   NTFS   Partition    100 M   Sain       Système
  Volume 2     C   os-7-sp1     NTFS   Partition     29 G   Sain       Démarrag
  Volume 3     D   installatio  NTFS   Partition     85 G   Sain
* Volume 4     W                FAT32  Amovible    3817 M   Sain
```

et on peut quitter l'outil **Diskpart** en saisissant

**exit**

```
DISKPART> exit

Quitte DiskPart...
```

## Copie du DVD Seven (par exemple):

Pour copier les fichiers, on peut utiliser la commande **xcopy**

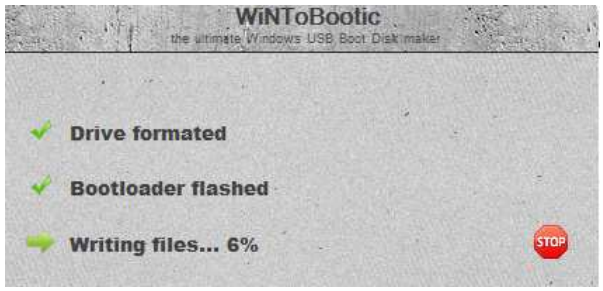
Insérer le DVD d'installation de Windows ainsi que la clé dans un port USB. En invite de commande taper

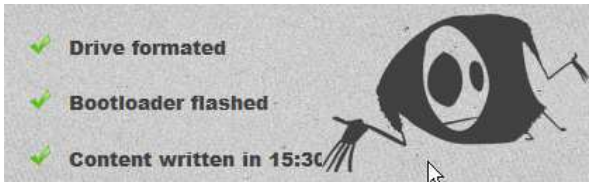
**xcopy d:\ f:\ /e /f**

(avec dans l'exemple **D** : est l'unité du lecteur CD et **F** : la clé USB)

## Utilitaire WinnToBootic:

Si on a une image ISO, on peut utiliser ce petit utilitaire

## Préparation du poste 7

1. On fait un profil type avec le compte Administrateur/Root
2. On fait le ménage compte utilisateur/profils autres…

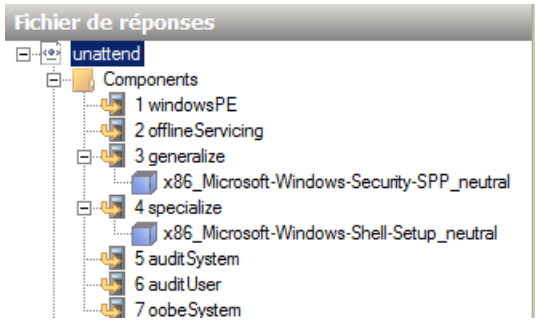
## Sysprep 3.12 obligatoire

Depuis le dossier, **windows\system32\sysprep** on lance la commande

**Sysprep /generalize /oobe**

ou

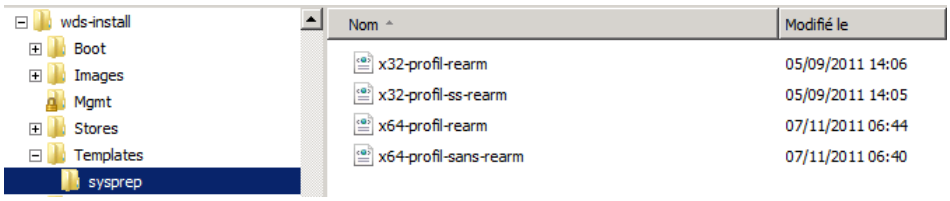
**Sysprep /generalize /oobe /unattend:c:\nom-fich.xml**



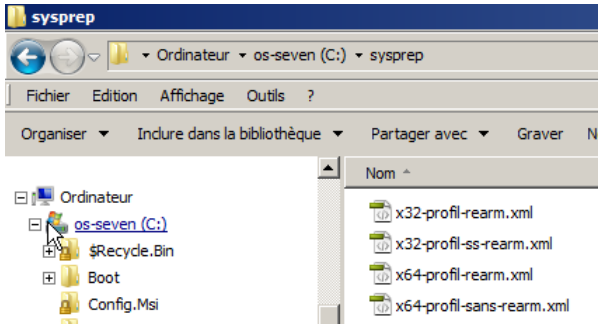

**N.B**: la construction des fichiers de réponse est traitée à part. Il faut juste indiquer ici 2 valeurs, **skiprearm = 1** pour éviter le rearmement du décompte de l'activation de licence
**copyprofile = true** pour créer un profil par défaut sur le poste type

**N.B**: attention à ne pas re-démarrer le poste sur lequel on vient d'exécuter sysprep sans booter sur le CD contenant l'image de capture, sinon la phase mini-install OOBE se déroulera automatiquement...

**N.B**: Une copie du fichier **unattend.xml** version avec rearm ou sans rearm est disponible sur le serveur WDS en version 32 ou 64 bits




à copier à la racine du C:\ de la machine à « syspréper »




pour pouvoir sur un Seven 64bits faire par exemple

**Sysprep /generalize /oobe /unattend:c:\sysprep\x64-profil-rearm.xml**

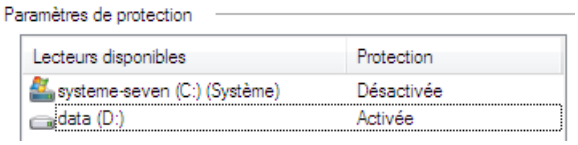
# RESTAURATION DE FICHIERS

## Contexte de travail

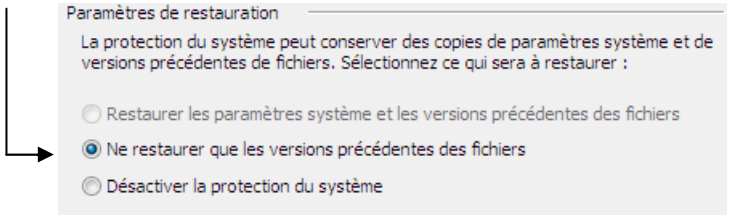
Pour mettre en évidence la possibilité de restaurer une version antérieure d'un fichier, on va travailler avec une sauvegarde de fichiers effectuée manuellement. En désactivant par ailleurs les points de restauration…

Dans les **propriétés** de **ordinateur / protection du système**

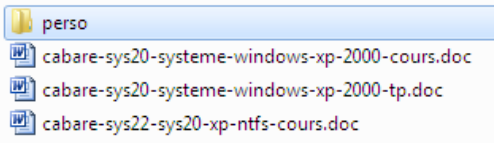
Sur un poste avec un système en C: et des données en D: alors



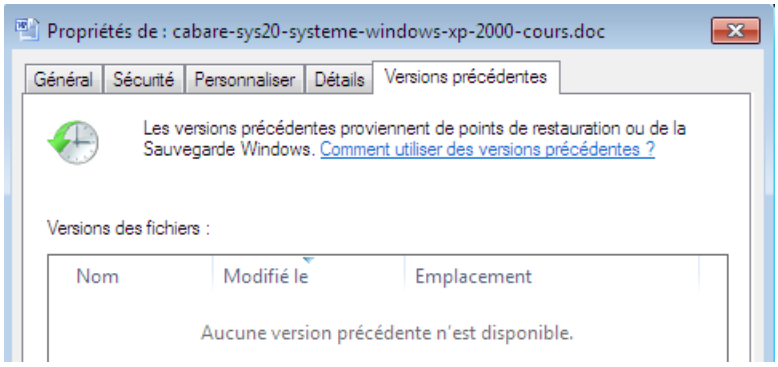

On peut aussi si on dispose d'un seul lecteur C: demander de ne gérer que la **restauration des fichiers**…




Dans un dossier data, on a une structure de fichiers et de dossier du genre



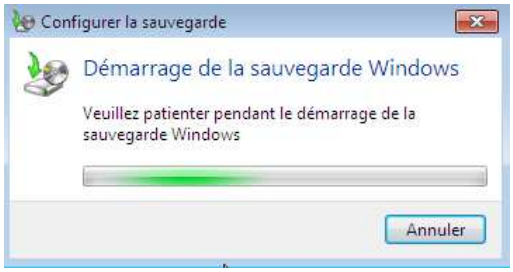

Pour n'importe lequel de ces éléments, fichiers ou dossier, on obtient dans l'onglet **Propriétés / Versions précédentes** le message "**Aucune version précédente n'est disponible**"



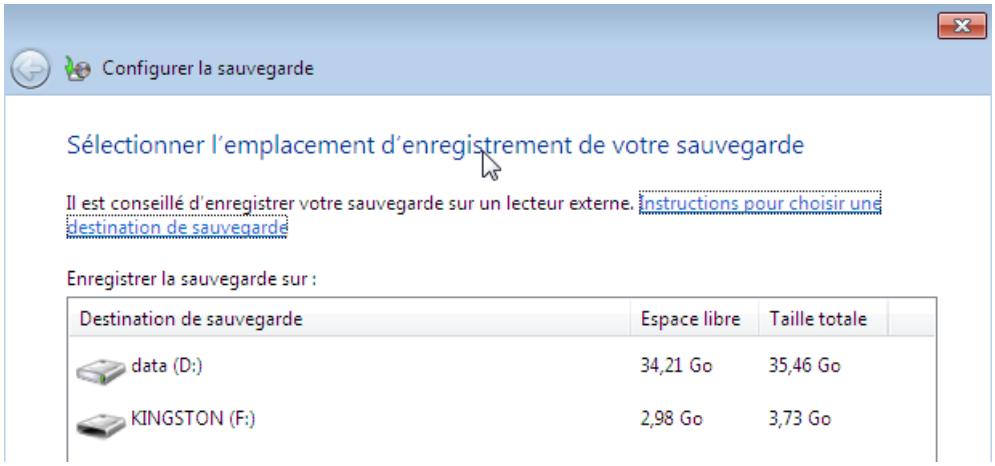
## Réaliser une sauvegarde de fichiers

On réalise une sauvegarde de fichiers.

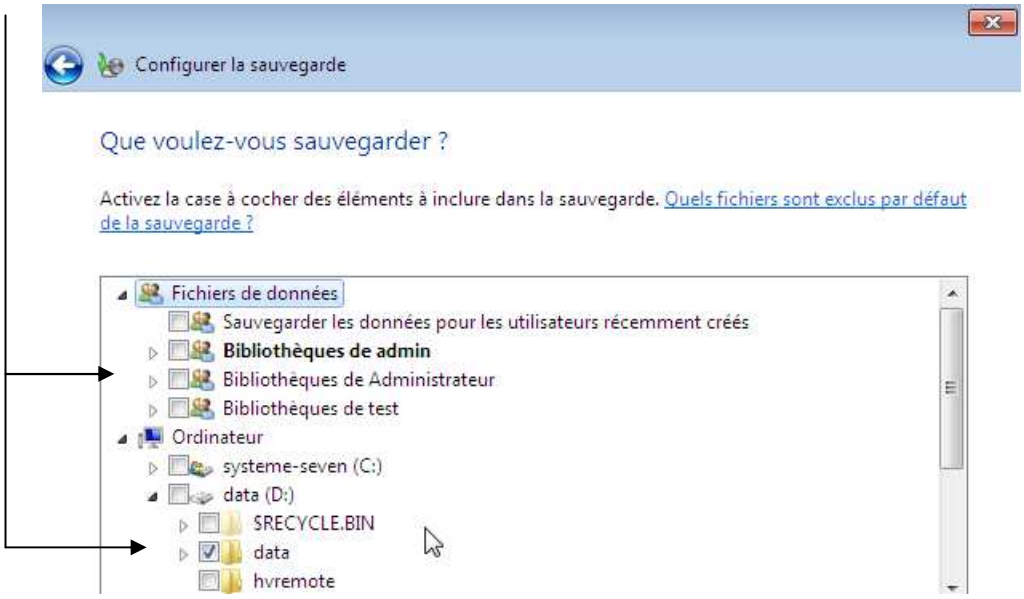
**Démarrer / Tous les programmes / Maintenance / Sauvegarder et Restaurer**



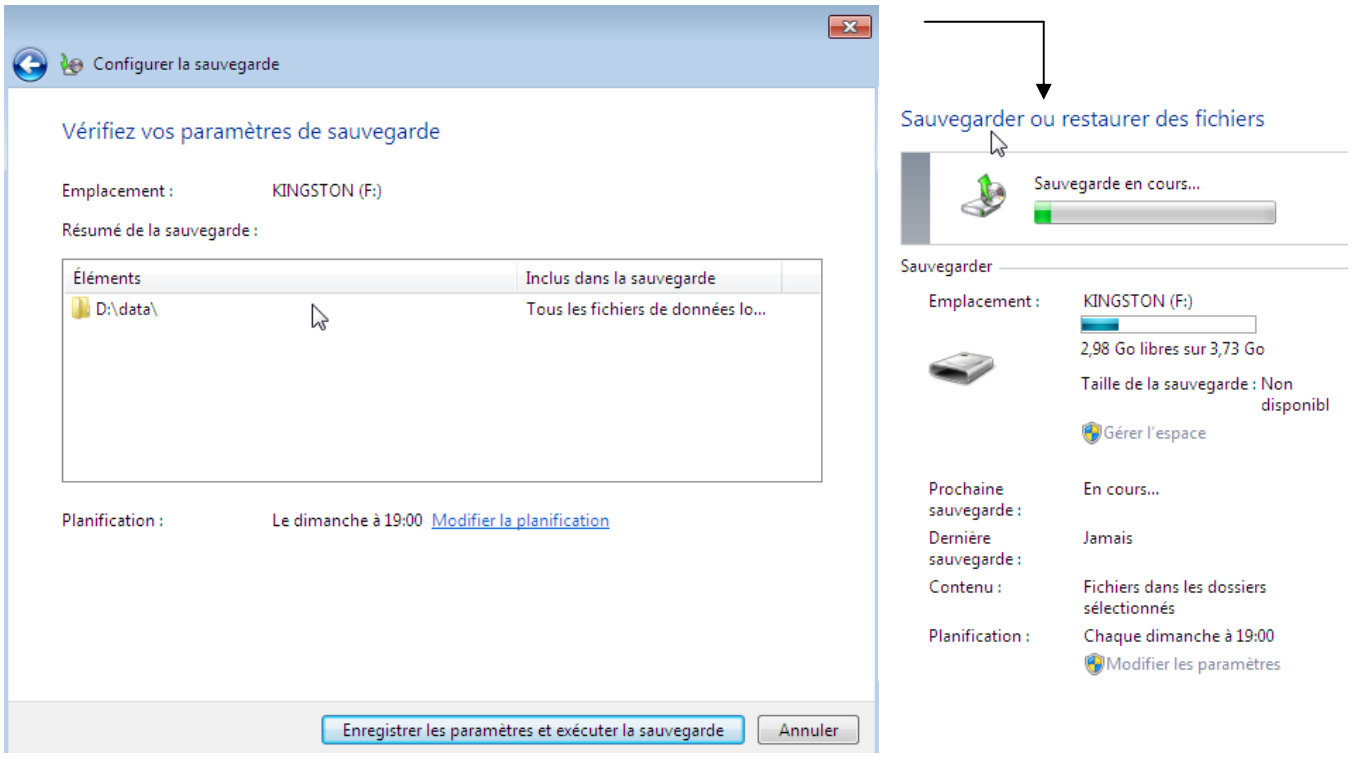

On choisit un emplacement quelconque… (clé USB)




Et on choisit de ne sauvegarder QUE le dossier data préalablement visualisé

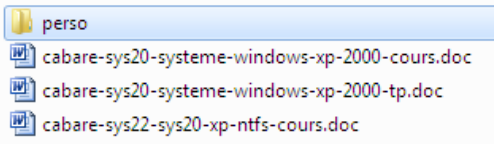



Ce qui donne

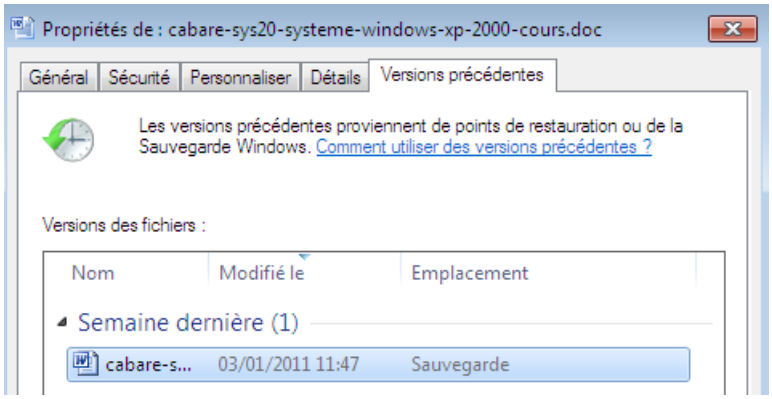



## Utilisation d'une sauvegarde de fichiers

Sans avoir besoin, ou envie de réaliser une "réstauration" de la sauvegarde, il est possible maintenant de constater que lorsque l'on demande les **propriétés / versions précédentes** de nos fichiers - dossiers




On obtient



# DEPLACER LE DOSSIER MES DOCUMENTS

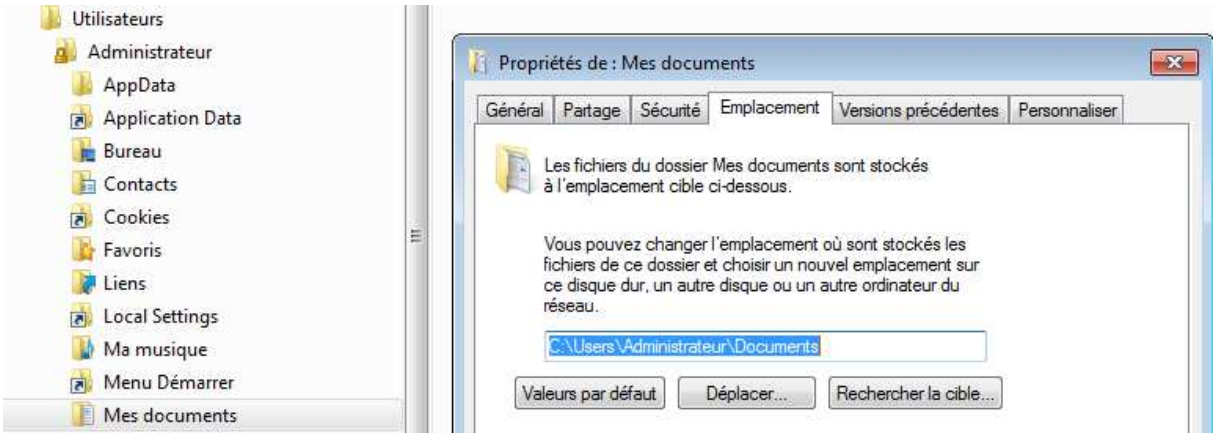
**Objectif:**

Il peut devenir nécessaire de déplacer l'emplacement par défaut du dossier repéré comme « mes documents » pou un utilisateur:

L'objectif est non seulement de déplacer le contenu, mais aussi et surtout de modifier les pointeurs pour les enregistrements ultérieurs par défaut

Il suffit pour cela de se Loguer en tant qu'Utilisateur dont on veut déplacer le dossier mes documents, et se placer sur le dossier **mes documents**

et de demander les **Propriétés**



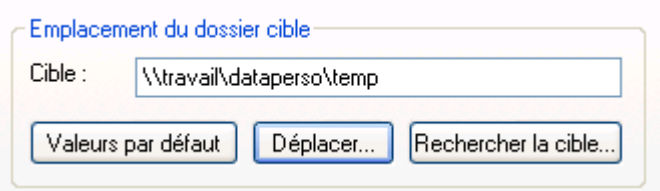

Au niveau de **Rechercher la Cible**, on demande le nouvel emplacement, par exemple **D:\autre**

Puis **Déplacer…**

Et le tour est joué

**Possibilités et… limites:**

Il peut être possible de définir l'emplacement par défaut du dossier repéré sur un chemin réseau…




Toute redirection de ce genre à un effet limité au profil utilisateur en cours !