

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	4 4
Liste détaillée:	7
Stratégie gestion drivers Stratégies de gestion de drivers & périphériques : Stratégie Installation de pilotes	8 8 8
Stratégie Installation de périphériques Interdire les clés USB :	9 9 1 1 2 2
Vérifier l'integrité Du Système	4 4 6
Seven & UAC – Test Elevation	7 7 8 8
Seven – Virtualisation & applications heritées	9 9 20
Boot depuis un disque VHD.2Principe du Boot sur VHD2Réalisation d'un disque VHD.2Installation de l'OS dans le VHD.2Supprimer un Boot sur VHD2Ajouter Manuellement une entrée Bcdedit sur VHD3Boot manager - Os loader Windows 8.3Choix du VHD - Licences.3	24 24 25 26 29 30 31
Clé-Disque USB Bootable	32 32 33 33
Profil par défaut	34 34 34



Restauration de fichiers	35
Contexte de travail	
Réaliser une sauveaarde de fichiers	
Utilisation d'une sauvegarde de fichiers	
Déplacer le dossier mes documents	
Óbjectif:	
Possibilités et limites:	





TRACER DES PROCESSUS...

Liste par défaut:

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



liste des processus est bien sûr minimaliste

om de l'image	Nom d'utilis A	Processeu	Mémoire	Description
vchost.exe	SERVICE LOCAL	00	2 788 K	Processus hôte pour les services Wind
vchost.exe	SERVICE RÉSEAU	00	1 172 K	Processus hôte pour les services Wind
vchost.exe	SERVICE RÉSEAU	02	1 224 K	Processus hôte pour les services Wind
rocessus inactif du système	Système	92	24 K	Pourcentage de temps pendant lequel
ystem	Système	00	36 K	NT Kernel & System
nss.exe	Système	00	204 K	Gestionnaire de sessions Windows
arss.exe	Système	00	888 K	Processus d'exécution dient-serveur
arss.exe	Système	00	868 K	Processus d'exécution client-serveur
ininit.exe	Système	00	588 K	Application de démarrage de Windows
inlogon.exe	Système	00	796 K	Application d'ouverture de session Wir
ervices.exe	Système	00	1 688 K	Applications Services et Contrôleur
ass.exe	Système	00	1 504 K	Local Security Authority Process
m.exe	Système	00	708 K	Service du gestionnaire de session loc
/chost.exe	Système	00	1664 K	Processus hôte pour les services Wind
/chost.exe	Système	00	4 748 K	Processus hôte pour les services Wind
/chost.exe	Système	00	1 596 K	Processus hôte pour les services Wind
xplorer.exe	toto	01	7 508 K	Explorateur Windows
fmon.exe	toto	00	576 K	Chargeur CTF
askmgr.exe	toto	05	1 504 K	Gestionnaire des tâches de Windows
1				

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	Ø	24 K
System	4	Services	Ø	224 K
smss.exe	204	Services	Ø	712 K
csrss.exe	276	Services	Ø	2 804 K
csrss.exe	316	Console	1	7 108 K
wininit.exe	324	Services	Ø	3 040 K
winlogon.exe	352	Console	1	3 512 K
services.exe	412	Services	Ø	4 528 K
lsass.exe	420	Services	Ø	6 008 K
lsm.exe	428	Services	0	2 684 K
svchost.exe	524	Services	Ø	5 696 K
svchost.exe	596	Services	Ø	4 Ø36 K
svchost.exe	680	Services	0	5 752 K
svchost.exe 💦 💦	716	Services	Ø	9 536 K
svchost.exe	764	Services	Ø	4 732 K
explorer.exe	928	Console	1	28 204 K
ctfmon.exe	1004	Console	1	2 904 K
svchost.exe	1316	Services	Ø	5 924 K
taskmgr.exe	1492	Console	1	6 872 K
cmd.exe	824	Console	1	2 112 K
conhost.exe	660	Console	1	2 792 K
tasklist.exe	1488	Console	1	3 968 K
WmiPrvSE.exe	1312	Services	Ø	4 540 K

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

	Nom de l'image		Nom d'utilisateur	Proces	Mém	Description
I	Processus inactif	0	Système	75	24 K	Pourcentage de temps pendant lequel l'ordinateur est inactif
I	System 😡	4	Système	00	36 K	NT Kernel & System
I	smss.exe	204	Système	00	204 K	Gestionnaire de sessions Windows
I	csrss.exe	276	Système	00	888 K	Processus d'exécution client-serveur
I	csrss.exe	316	Système	05	924 K	Processus d'exécution client-serveur
I	wininit.exe	324	Système	00	588 K	Application de démarrage de Windows
I	winlogon.exe	352	Système	00	796 K	Application d'ouverture de session Windows
I	services.exe	412	Système	00	1 696 K	Applications Services et Contrôleur
I	lsass.exe	420	Système	00	1 500 K	Local Security Authority Process
I	lsm.exe	428	Système	00	784 K	Service du gestionnaire de session locale
I	svchost.exe	524	Système	00	1704 K	Processus hôte pour les services Windows
I	svchost.exe	596	SERVICE RÉSEAU	00	1 252 K	Processus hôte pour les services Windows
I	conhost.exe	660	toto	00	664 K	Hôte de la fenêtre de la console
I	svchost.exe	680	SERVICE LOCAL	00	2 788 K	Processus hôte pour les services Windows
I	svchost.exe	716	Système	00	4 756 K	Processus hôte pour les services Windows
I	svchost.exe	764	SERVICE RÉSEAU	00	1 224 K	Processus hôte pour les services Windows
I	cmd.exe	824	toto	00	468 K	Interpréteur de commandes Windows
I	explorer.exe	928	toto	01	10 1	Explorateur Windows
I	ctfmon.exe	1004	toto	00	576 K	Chargeur CTF
1	svchost.exe	1316	Système	00	1 596 K	Processus hôte pour les services Windows
1	taskmgr.exe	1492	toto	19	1 528 K	Gestionnaire des tâches de Windows
-						

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



Applications Processus Services Performance Mise en réseau Utilisateurs

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 N	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	Ø	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



Nom de l'image	PID	Services
=======================================	=======	
System Idle Process	Ø	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, 1mhosts, 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,
		NlaŜvc
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
rund1132.exe	2028	N/A
rund1132.exe	196	N/A
rund1132.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



Système Windows 7 Seven - SYS 20 - Travaux Pratiques - ver 2.3 - http://www.cabare.net Page 6 Cabaré Michel

Liste détaillée:

Tasklist /m

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

C:\Users\Administrateur>tasklist /M						
Nom de l'image	PID	Modules				
	======					
System Idle Process	ខ	N/A				
System	4	N/A				
smss.exe	276	ntdll.dll				
csrss.exe	368	ntdll.dll, CSRSRU.dll, basesrv.DLL, winsrv.DLL, USER32.dll, GDI32.dll,				
		kerne132.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.d11, GDI32.d11, LPK.d11, USP10.d11,				

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

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, RPCR14.dll, umpnpmgr.dll, SPINF.dll, USER32.dll, GDI32.dll, LPK.dll, USP10.dll, DEVRTL.dll, IMM32.DLL, MSCTF.dll, RpcRtRemote.dll, USERENU.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, ubemprox.dll, CRYPTSP.dll, rsaenh.dll, wBemsvc.dll, WMiutils.dll, WITRUST.dll, CRYPT32.dll, MSASN1.dll, WISAPI32.dll

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

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

Tasklist /SVC /fi "pid eq 524"

C:\Users\toto>tasklist /SU	JC ∕fi "pi	id 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**



Deux entrées nouvelles...



Stratégie Installation de pilotes

Paramètre

Autoriser les non-administrateurs à installer des pilotes pour ces classes d'installation...
 Désactiver l'invite de recherche de pilotes d'imprimantes Windows Update





http://www.cabare.net Page 8 3- Cabaré Michel 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

Éditeur de stratégie de groupe locale		
Fichier Action Affichage ?		
 Système Accès au stockage amovible Accès au stockage étendu Accès réseau Appel de procédure distante Assistance à distance Cache NV de disque DCOM Délégation d'informations d'id Démarrage à chaud de Windov Dépannage et diagnostics 	Paramètre Restrictions d'installation de périphériques Accorder la même priorité à tous les pilotes signés numériq Désactiver les bulles « Nouveau matériel détecté » pendant l Ne pas envoyer de rapport d'erreurs Windows lors de l'instal Configurer le délai d'attente d'installation de périphérique Empêcher Windows d'envoyer un rapport d'erreurs lorsqu'u Empêcher la création de point de restauration système lors Autoriser l'accès distant à l'interface Plug-and-Play Empêcher la récupération des métadonnées du périphériqu	État Non configuré Non configuré Non configuré Non configuré Non configuré Non configuré Non configuré Non configuré
 Gestion de l'alimentation Gestion de la communication l Installation de périphériques 	Spécifier l'ordre de recherche des emplacements source des	Non configuré

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 :

Paramètre	État
🖹 Autoriser les administrateurs à passer outre les stratégies de	Non configuré
Permettre l'installation de périphériques à l'aide de pilotes c	Non configuré
Empêcher l'installation de périphériques à l'aide de pilotes c	Non configuré
🖹 Afficher un message personnalisé lorsque l'installation est e	Non configuré
🖹 Afficher un message personnalisé lorsque l'installation d'un	Activé
Autoriser l'installation de périphériques correspondant à l'u	Non configuré
Empêcher l'installation de périphériques correspondant à l'u	Non configuré
Empêcher l'installation de périphériques correspondant à l'u	Non configuré
🗄 Délai (en secondes) pour forcer le redémarrage afin d'appliq	Non configuré
Empêcher l'installation de périphériques amovibles	Activé
Empêcher l'installation de périphériques non décrits par d'a	Non configuré



💁 Empêcher l'installation de périphériques amovibles						
Empêcher l'insta	Ilation de périphérique	s amovibles Paramètre précédent Paramètre suivant				
🔘 Non configuré	Commentaire :		b			
Activé						
Désactivé			r			
	Pris en charge sur :	Au minimum Windows Vista	h			

Voire y associer un message explicatif

Afficher un message personnalisé lorsqu Paramètre précédent Paramètre suiva	e l'installation d'un périphérique est empêchée par un paramètre de stratégi .t	2
 Non configuré Commentaire : Activé Désactivé 		*
Pris en charge sur :	u minimum Windows Vista	*
Options :	Aide :	
Entrez le texte que vous destinez aux utilisate (63 caractères maximum) Texte principal	Ce paramètre de stratégie permet d'afficher un message personnalisé dans le titre de la bulle de notification lorsqu'un paramètre de stratégie empêche l'installation d'un périphérique. Si vous activez ce paramètre de stratégie, Windows affiche le	

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...

Fichier Action Affichage	1 7
⊨ 🔿 🖬 🖬 🔽 🖬	🔍 📴 🍢 🖏
 test-PC Autres périphériqu Student Key 	les
🔉 📲 Cartes graphiqu	Mettre à jour le pilote
Cartes réseau	Désactiver
 Cartes réseau Claviers Contrôleurs auc 	Désinstaller 🗸
Cartes réseau Claviers Claviers Contrôleurs au Contrôleurs de Contrôleurs de	Désactiver Désinstaller Rechercher les modifications sur le matériel



ID et classe de Périphérique :

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

aramètre	Expliquer	
Empê	her l'installation de périphériques correspondant à l'un de ces l	
🔘 Non co	nfiguré	
 Activé 		
🔘 Désact	ivé	
Empêch	r l'installation de périphériques correspondant à l'un de ces ID de périp icher	hériqu
Pour cré	r une liste de périphériques, cliquez sur Afficher, sur Ajouter,	
puis spé	ifiez un ID de matériel Plug-and-Play ou compatible	
(par exer	ple, gendisk, USB\COMPOSITE, USB\Class_ff).	

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**

	Proprietes de : Kingston Data fraveler 2.0 036 Device
Dans la liste déroulante l'option	Général Stratégies Volumes Pilote Détails
matériel.	Propriété
Lecteurs de disque	Numéros d'identification du matériel
Kingston Data I raveler 2.0 USB Device	USBSTOR\DiskKingstonDataTraveler_2.0PMAP USBSTOR\DiskKingstonDataTraveler_2.0
Selon la Clé USB, cela change	Desprétér de Vingeton DT101 II USP Device
Lecteurs de disque	Général Stratégies Volumes Pilote Détails
Kingston DT101 II USB Device	Kingston DT101 II USB Device
	Propriété
	Numéros d'identification du matériel 🔻
	Valeur
	USBSTOR\DiskKingstonDT101_II1.00 USBSTOR\DiskKingstonDT101_II



Système Windows 7 Seven - SYS 20 - Travaux Pratiques - ver 2.3 -

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 ...

Propriétés de : Kingston DT101 II USB Device
Général Stratégies Volumes Pilote Détails
Kingston DT101 II USB Device
Propriété
GUID de la classe de périphérique
Valeur
{4d36e967-e325-11ce-bfc1-08002be10318}
Propriétés de : Kingston DataTraveler 2.0 USB Device
Général Stratégies Volumes Pilote Détails
Kingston Data Traveler 2.0 USB Device
Propriété
La unu de la classe de penphénque
Valeur {4d36e967-e325-11ce-bfc1-08002be10318}

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...

Empêcher l'installation de périphériques	non décrits par d'autres paramètres de stratégie	×				
Empêcher l'installation de périphériques non décrits par d'autres paramètres de stratégie						
Paramètre précédent Paramètre suiv	vant					
O Non configuré Commentaire :		*				
 Activé 						
Désactivé		Ŧ				
Pris en charge sur :	Au minimum Windows Vista	*				
	N	~				
Options :	kờ Aide:					

Et autoriser uniquement



Paramètre précédent Paramètre su	ivant	
 Non configuré Commentaire : Activé Désactivé 		
Pris en charge sur :	Au <mark>minin</mark>	num Windows Vista
Options :		Aide :
Autoriser l'installation de périphériques correspondant à l'un de ces ID de péripl Afficher Pour créer une liste de périphériques, cliq Afficher. Dans la boîte de dialogue Affiche contenu, dans la colonne Valeur,	nériques ; uez sur er le	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 périphéri	ques correspondant à l'un de ces ID de périphériques :
Valeur		





VERIFIER L'INTEGRITE DU SYSTEME

Corrompre le système Seven :

Noter que par exemple la DII 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...

Propriétés de tapi32.dll	(
Général Sécurité Détails Versions précéd	dentes
Nom de l'objet : C:\Windows\System32\tapi	i32.dll
Groupes ou noms d'utilisateurs :	+
& SYSTEM	
Administrateurs (PC-de-test\Administrate	eurs)
🎎 Utilisateurs (PC-de-test\Utilisateurs)	
& TrustedInstaller	
Pour modifier les autorisations, cliquez sur Mo	odifier. Modifier
Autorisations pour Administrateurs	Autoriser Refuser
Contrôle total	
Modification	
Lecture et exécution	~
Lecture	\checkmark
Écriture	

	en	effet	t s	eul		е	g	roup	be
	Trust	edIn	stal	ler	à	le	es.	dro	its
	comp	olets	•						
Proprie	étés de tap	oi32.dll							X
Général	Sécurité	Détails	Versio	ns préc	éden	es			
Nom de	l'objet : C	:\Window	vs\Syste	em32\ta	api32	dll			
Groupe	s ou noms (d'utilisate	urs :						
88 S1	/STEM	m (PC da	teet\ Ae	logioter					
8 Ut	ilisateurs (P	C-de-test	\Utilisat	eurs)	lieurs	,			
Se Tr	ustedInstall	er							
Pourmo	odifier les ai	utorisatior	ns, cliqu	iez sur l	Modifi	er.		Modifier	
Autorisa	ations pour	TrustedIn	staller		A	utorise	er	Refuser	
Cont	rôle total					\checkmark			
Modi	fication					\checkmark			
Lect	ure et exéc	ution				~			
Lecti	ure					~			
Ecrit	ure					\checkmark			
Auto	nsations sp	eciales							

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



1. appropriation du fichier



2. Ajout des droits de l'administrateur

👃 Autorisations pour tapi32.dll		×		
Sécurité				
Nom de l'objet : C:\Windows\Syste	em32\tapi32.dll			
Noms de groupes ou d'utilisateurs :				
& Système				
& Administrateurs (test-PC\Adminis	trateurs)			
& Utilisateurs (test-PC\Utilisateurs)				
RustedInstaller				
	Ajouter	Supprimer		
Autorisations pour Administrateurs	Autoriser	Refuser		
Contrôle total				
Modification				
Lecture et exécution				
Lecture				
Écriture	V			
Informations sur le contrôle d'accès et les autorisations				
ОК	Annuler	Appliquer		

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



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 [m]:520{260},1:46{23}]"\??\C:\windows\system32"\[]:20{10}]"tapi32.dll" from store 000001af Repair results created:

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

👂 🍌 Speech	🚳 tapi3.dll	14/07/2009 03:16	Extension de l'app	836 Ko
闄 system	≡ 🚳 tapi32.dll	14/07/2009 03:16	Extension de l'app	188 Ko
🛛 🍌 System32	🚳 tapi32-old.dll	14/07/2009 03:16	Extension de l'app	188 Ko

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...

📓 Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administrat... Désactivé

🕅 Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation 🛛 🛛 Activé

📓 Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sans ... Désactivé

Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs ... Demande de consentem...
 Demande de consentem...
 Demande d'information...

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

Invite de commandes
Microsoft Windows [version 6.1.7600] Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\admin>whoami /all
Informations sur l'utilisateur
Nom d'utilisateur SID

Les privilèges sont faibles...

Informations de privilèges		
Nom de privilège	Description	État
SeShutdownPrivilege SeChangeNotifyPrivilege SeUndockPrivilege SeIncreaseWorkingSetPrivilege SeTimeZonePrivilege	Arrêter le système Contourner la vérification de parcours Retirer l'ordinateur de la station d'accueil Augmenter une plage de travail de processus Changer le fuseau horaire	Désactivé Activé Désactivé Désactivé Désactivé

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

Invite de commandes	_	Looke and the second se
		Ouvrir
Pense-bête		Exécuter 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
Selecter Sel	Ajuster les quotas de mémoire pour un processus Gérer le journal d'audit et de sécurité Prendre possession de fichiers ou d'autres objets Charger et décharger les pilotes de périphériques Performance système du profil Modifier l'heure système Processus unique du profil Augmenter la priorité de planification Créer un fichier d'échange	Désactivé Désactivé Désactivé Désactivé Désactivé Désactivé Désactivé Désactivé
SeBackupFrivilege SeRestorePrivilege SeShutdownPrivilege SeDabugPrivilege SeChangeNotifyFrivilege SeChangeNotifyFrivilege SeRemoteShutdownPrivilege SeUndockFrivilege SeManageVolumePrivilege SeImpersonatePrivilege SeImpersonatePrivilege SeIncreaseWorkingSetPrivilege SeTimeZonePrivilege SeCreateSymbolicLinkPrivilege	Sauvegarder les fichiers et les répertoires Restaurer les fichiers et les répertoires Arrêter le système Déboguer les programmes Modifier les valeurs de l'environnement du microprogramme Contourner la vérification de parcours Forcer l'arrêt à partir d'un système distant Retirer l'ordinateur de la station d'accueil Effectuer les tâches de maintenance de volume Emprunter l'identité d'un client après l'authentification Créer des objets globaux Augmenter une plage de travail de processus Changer le fuseau horaire Créer des liens symboliques	Desactivé Désactivé Désactivé Désactivé Désactivé Désactivé Désactivé Activé Activé Activé Désactivé Désactivé Désactivé

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

📓 Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Administra... Désactivé

📓 Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation 🛛 🛛 Activé

🐻 Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation san... Désactivé

Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs... Élever les privilèges sans invite utilisateur
 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs stan... Demande d'informations d'identification
 Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation Activé

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...

Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs standard Demande d'information...
 Contrôle de compte d'utilisateur : détecter les installations d'applications et demander l'élévation Activé
 Contrôle de compte d'utilisateur : élever uniquement les applications UIAccess installées à des emp... Activé
 Contrôle de compte d'utilisateur : élever uniquement les exécutables signés et validés Désactivé
 Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation ... Désactivé
 Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre dans de... Activé
 Il n'y a plus aucune différence entre CMD et CMD en tant au'administrateur...



SEVEN – VIRTUALISATION & APPLICATIONS HERITEES

Pré-requis :

Pour ce faire il est nécessaire que :

• l'UAC ne soit pas désactivée totalement...

🛞 Contrôle de compte d'utilisateur : mode Approbation administrate	Désactivé
📓 Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'u	Activé
🕅 Contrôle de compte d'utilisateur : autoriser les applications UIAcces	Désactivé
🖾 Contrôle de compte d'utilisateur : comportement de l'invite d'éléva	Demande de consentem
🕅 Contrôle de compte d'utilisateur : comportement de l'invite d'éléva	Demande d'information
🖾 Contrôle de compte d'utilisateur : détecter les installations d'applic	Activé
🕅 Contrôle de compte d'utilisateur : élever uniquement les applicatio	Activé
🖾 Contrôle de compte d'utilisateur : élever uniquement les exécutable	Désactivé
🔯 Contrôle de compte d'utilisateur : exécuter les comptes d'administr	Activé
🕅 Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures d	Activé

 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)

📮 Gestionnaire des tâches de Windows 📃 🖃 🗾 💌							
Fichier Options	\ffichage ?						
Applications Processus Services Performance Mise en réseau Utilisateurs							
Nom de Îîmage	Nom d'u	P	Mémoire		Virtualisatio.	Descript	ion
[cmd.exe	test	00	493	2 K	Non autorise	é Interpré	iteur de co 🔸
conhost.exe	test	00	84	4 K	Non autorise	é Hôte de	la fenêtre

• 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**

Nom du chemin d'accès de l'image
Ligne de commande
Virtualisation du contrôle de compte d'utilisateur
V Description



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

, 🜉	📮 Gestionnaire des tâches de Windows 📃 💼 📼					
Fic	hier Options /	Affichage	?			
Ap	oplications Proces	sus Services	s Per	formance Mis	e en réseau Utili	isateurs
	Nom de Îîmage	Nom d'u…	P	Mémoire	Virtualisation	Description
	[cmd.exe	admin	00	88 K	Désactivé	Interpréteur
	conhost.exe	admin	00	468 K	Désactivé	Hôte de la fe

3. essayons d'écrire dans notre répertoire

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

c'est possible,

C:\Users\te: Le volume	st>dir dans_le	lecteur C	n'a pas	de nom.
Le numero (de serie	e du volume	est 58	6H-31H3
Répertoire	de C:∖U	lsers\test		
18/09/2007	17:17	<rep></rep>		
18/09/2007	17:17	<rep></rep>		
18/09/2007	17:17		864	affiche.txt
07/09/2007	12:30	<rep></rep>		Contacts
07/09/2007	12:47	<rep></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 :

📮 Gestionnaire des tâches de Windows									
Fichie	er Options Aff	ichage ?							
App	olications Proces	sus Services	Peri	formance 🛛 Mis	e en réseau 🛛 Ut	ilisati	eurs	- 1	
	Nom de 🔺	Nom d'u	P	Mémoire	Virtualisatio	Des	cription		
	cmd.exe	test	00	724 K	Désactivé	Inte	erpréte		
	conhost.exe	Ouvrir l'em	placen	nent du fichier			e de la		
	conhost.exe Arrêter le processus						e de la e de la		
	csrss.exe	Terminer l' Déboquer	arbore	scence du proc	tessus				
	csrstub.exe dwm.exe	Virtualisati	on du		met à tionnai				
	explorer.exe	Créer un f	ichier d	le vidage			lorate		

on confirme...

pour obtenir

 Applications
 Processus
 Services
 Performance
 Mise en réseau
 Utilisateurs

 Nom de... ^
 Nom d'u...
 P...
 Mémoire ...
 Virtualisatio...
 Description

 cmd.exe
 test
 00
 724 K
 Activé
 Interpréte...

 conhost.exe
 test
 00
 560 K
 Hôte de la...



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

C:\Windows>dir >affiche.txt Cela a l'air de marcher !!!!

C:\Windows) Le volume Le numéro	dir dans le de série	lecteur C e du volum	; n'a pas de nom. e est 586A-31A3	
Répertoire	de C:∖ł	lindows		
18/09/2007 18/09/2007 02/11/2006 18/09/2007	17:25 17:25 14:37 17:25	<rep> <rep> <rep></rep></rep></rep>	addins 4 034 affiche.txt	-
12/09/2007	07:08	<rep></rep>	AppPatch	

7. maintenant vérifions ou l'on a écrit réellement





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...

😜 🗢 📕 🔹 Ordinateur 👻 Disque local (Windows -	Rechercher dans :	Windows	
r Edition Affichage Outils ? Iniser 🔻 Inclure dans la bibliothèque 🔻	• P	artager avec 👻 Graver 🛛 Fichiers de comp	patibilité Nouveau dossier	i - 🗖
Lisque local (C:)	<u>.</u>	Nom +	Modifié le	Type
sRecycle.Bin	ſ	adding	14/07/2009 06:52	Dossier de fichiers
boot-back			14/07/2009 00:32	Dossier de fichiers
🍰 data	-	M AppCompat	14/07/2009 04:37	Dossier de fichiers
irect		AppPatch	14/07/2009 10:39	Dossier de fichiers
Bocuments and Settings		assembly	22/02/2010 15:46	Dossier de fichiers
formation rectorat seven		🌙 Boot	14/07/2009 06:52	Dossier de fichiers
MSOCache		🍌 Branding	14/07/2009 06:52	Dossier de fichiers
Braggam Data		🍌 csc	18/02/2010 09:15	Dossier de fichiers
Brogrambata		Lursors	14/07/2009 06:52	Dossier de fichiers
Recovery		a debug	23/02/2010 09:11	Dossier de fichiers
symbols		iagnostics	14/07/2009 06:52	Dossier de fichiers
System Volume Information			14/07/2009 10:39	Dossier de fichiers
Utilisateurs			14/07/2009 06:53	Dossier de fichiers
🚺 utilitaires		Bownloaded Program Files	14/07/2009 06:52	Dossier de fichiers
🔒 Windows		ji enome	14/07/2009 11:01	Dossier de fichiers
🎳 addins		A Fonts	22/02/2010 15:46	Dossier de fichiers
🍶 AppCompat		🍰 fr-FR	14/07/2009 10:39	Dossier de fichiers
🍶 AppPatch		📕 Globalization	14/07/2009 11:05	Dossier de fichiers
🍶 assembly		退 Help	14/07/2009 10:39	Dossier de fichiers
le Boot		🕌 IME	14/07/2009 10:39	Dossier de fichiers
🍰 Branding		inf	17/03/2010 09:37	Dossier de fichiers
USC CSC		1 Installor	00/02/2010 10.12	Dessige de Achiere
Jursors	-			

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,

Gestionnaire des tâches de Windows										
Fichier	Options	Affichag	je ?							
Applica	ations Proces	vices	Perform	nance	s	Mise en rése	au	Utilisateurs		
No	m de l'image	Nom d'u	utilisate	ur	P		Mémoire	Vir	tualisation	Description
cm	d.exe	test		_	00		544 K	Ac	tivé	Interprét
cor csr dw exp MS	nime.exe ss.exe m.exe plorer.exe ASCui.exe	test test test test				O Te Te De	uvrir l'empla erminer le pr erminer l'arb éboguer	cen oce: ores	nent du fichi ssus scence du pr	ier rocessus
tas	keng.exe	test			✓	Vi	rtualisation			

pour retrouver

Nom de l'image	Nom d'utilisateur	P	Mémoire	Virtualisation
cmd.exe	test	00	544 K	Désactivé

alors ensuite affiche.txt a disparut !!!!

C:\Windows> Le volume (Le numéro (lir lans le le série	lecteur C du volum	n'a pas e est 51	s de nom. 86A-31A3
Répertoire	de C:∖\	lindows		
18/09/2007	15:00	<rep></rep>		
18/09/2007	15:00	<rep></rep>		
02/11/2006	14:37	<rep></rep>		addins
12/09/2007	07:08	<rep></rep>		AppPatch
02/11/2006	11:44		50 176	bfsvc.exe
02/11/2006	13:18	<rep></rep>		Boot
02/11/2006	14:37	<rep></rep>		Branding
19/09/2006	13:41		4 261	Business.xml
18/09/2007	15:00	<rep></rep>		Cache
07/09/2007	09:23	<rep></rep>		CSC

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 <u>ne travaille pas de manière virtualisée</u>, 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.

Fichier Action Affichage ?					
 Gestion de l'ordinateur (local) Qutils système Planificateur de tâches Observateur d'événements Observateur d'événements Dossiers partagés Willisateurs et groupes locaux O Performance Gestionnaire de périphériques Stockage Gestion des disques Services et applications 	Volume data (D:) Réservé au système systeme-seven (C:) Attacher un disqu Spécifiez l'emplace Emplacement :	Disposition Simple Simple Simple e dur virtuel	Type De base De base De base	Système de fichiers NTFS NTFS NTFS sur l'ordinateur. Parco	Statut Sain (Pa Sain (Sy Sain (De

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-sp1entreprise.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

Analyser les disques de nouveau

Créer un disque dur virtuel

Attacher un disque dur virtue

Actualiser

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

E Stockage

Gestion des disques

🛨 📷 Services et applications

Gestion des disques		
	De base 74,53 Go En ligne Os-systeme (C:) 74,53 Go NTFS Sain (Système, Démarrer, Actif, Vidage sur inc	ident, Par
	CD-ROM 0 DVD 6 Mo En ligne Bluebirds (6 Mo CDFS Sain (Partition	
	Non alloué Partition principale	
Création du disque virtuel	↑	



ı

http://www.cabare.net Page 25 Cabaré Michel Avant d'obtenir

De base	◆ os-systeme (C:)
74,53 Go	74,53 Go NTFS
En ligne	Sain (Système, Démarrer, Actif, Vidage sur incident, Partition principale)
Disque 1 Inconnu 8,00 Go Non initialisé	8,00 Go Non alloué

Ensuite on peut initialiser le Disque (facultatif)

Disque 1 Inconnu 20,00 Go	20.00.60	
Non initialisé	Initialiser le disque	
	Hors connexion	

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

Disque 1	
De base	os-sur-vhd (D:)
8,00 Go	8,00 Go NTFS
En ligne	Sain (Partition principale)

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

Disque 0		
De base 74,53 Go En ligne	os-systeme (C:) 74,53 Go NTFS Sain (Système Démarrer Aci	Détacher le disque dur virtuel
		Si vous détachez un disque dur virtuel, celui-ci sera indisponible tant qu'il n'aura pas été rattaché.
Disque 1 De base 8,00 Go En ligne	os-sur-vhd (D:) 8,00 Go NTFS Sain (Partition principale)	Emplacement du fichier de disque dur virtuel :
CD-ROM 0 DVD 6 Mo En ligne	Bluebirds (6 Mo CDFS Sain (Partitio	La suppression du fichier de disque dur virtuel entraînera la perte définitive des données stockées sur le disque. OK Annuler

On a maintenant un fichier pour notre disque en vhd

Nom *	Modifié le	Туре	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...

Windows is loadin	ng files

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

on demande une Installation Personnalisée (option avancée).



ise à niveau océdez à la mise à s fichiers, paramèt le lorsqu'une versic s fichiers avant de ersonnalisée (opti stallez une nouvelle ramètres et progra rititions est disponi installation. Sauveg	niveau vers une ver res et programmes on existante de Win poursuivee. on a <u>v</u> ancée) e copie de Window mmes. L'option pe ble quand vous dé	rsion plus récente de Win , L'option de mise à <u>nivea</u> dows est en cours d'exéc s. Cette option ne conser rmettant de modifier les	dows et conservez u n'est disponible ution. Sauvegardez	
rsonnalisée (opti stallez une nouvelle ramètres et progra rtitions est disponi nstallation. Sauveg	on a <u>v</u> ancée) e copie de Window mmes. L'option pe ble quand option dé	s. Cette option ne conser rmettant de modifier leci	e pas vos fichiers	
	aroez vos nemers a	marrez votre ordinateur à avant de poursuivre.	lisques et les l'aide du CD	
sir ?				
taller Windows				×
ouhaitez-vous	installer Wind	lows ?		
Nom	ué sur le disque 0	16.0 Go	16.0 Go	<u> </u>
ct <u>u</u> aliser			Options de lecteur	rs (avancées)
<u>n</u> arger un pilote			U	
	sir ? taller Windows souhaitez-vous <u>Nom</u> Espace non allo ct <u>u</u> aliser <u>h</u> arger un pilote	taller Windows souhaitez-vous installer Wind Nom Espace non alloué sur le disque 0	taller Windows souhaitez-vous installer Windows ? Nom Taille totale Espace non alloué sur le disque 0 16.0 Go ctualiser harger un pilote	taller Windows souhaitez-vous installer Windows ? Nom Taille totale Espace libre Type Espace non alloué sur le disque 0 16.0 Go 16.0 Go Espace non alloué sur le disque 0 16.0 Go

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> li	st disk						
N ^o disque	Statut	Taille	Libre	Dyn	GPT		
Disque Ø Disque 1	En ligne En ligne	74 G o 9 G o	ctets ctets	1024 K 9 G	octets octets		

Suivit d'un Select Disk=0





List Vol

DISKPART> lis	t vol						
N ^o volume Volume Ø Volume 1	Ltr E C	Nom Bluebirds os-systeme	Fs CDFS NTFS	Type DVD-ROM Partition	Taille 6146 K 74 G	Statut Sain Sain Sain	Info 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 udisk							
100 pour	cent effectué	és					
DiskPart a	correctement	attaché	le	fichier	de	disque	virtuel.

Un list Vol confirme cela

DISKPART> lis	t vol						
N ^o volume Volume Ø Volume 1 Volume 2	Ltr E C D	Nom Bluebirds os-systeme os-sur-vhd	Fs CDFS NTFS NTFS	Type DUD-ROM Partition Partition	Taille 6146 K 74 G 8189 M	Statut Sain Sain Sain Sain	Info Système

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...

	l aille totale	Espace libre Type
Espace non alloué sur le disque 0	16.0 Go	16.0 Go
Actualiser		Options delecteurs (avancé

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	<pre></pre>
device	partition=C:
path	\Windows\system32\winload.exe
description	boot US depuis VHD
locale	t P-FK {}
innerit	\DOOTLOAGErSETTINGS/ (-2440-00 420- 44-0 -5000000-4050-3
recoverysequence	\e34d0D08-13fa-11e0-a522-aa22f2e4872a}
recoveryenabled	
osaevice	partition=0:
systempool	\#111UUWS {
resumeonject	Opt In
11X	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 démarra	ge Windows
identificateur device description locale inherit default resumeobject displayorder toolsdisplayorder timeout	<pre>{bootmgr} partition=C: Windows Boot Manager fr-FR {globalsettings} {default} {716e0e20-a4d4-11e2-87ca-0010b586d1f9} {derault} {current} {mendiag} 30</pre>
identificateur device	//////////////////////////////////////
path description locale	\Windows\system32\winload.exe Windows Server 2008 R2 fr-FR
inherit recoverysequence recoveryenabled osdevice	{bootloadersettings} {716e0e22-a4d4-11e2-87ca-0010b586d1f9} Yes uhd=[C:]\uhd-os\os.uhd
systemroot resumeobject nx	\Windows {716e0e20-a4d4-11e2-87ca-0010b586d1f9} OptOut
Chargeur de démarrage W	indows
identificateur device path description locale inherit recoverysequence recoveryenabled osdevice systemroot resumeobject nx	<pre>{current} partition=C: \Windows\system32\winload.exe Windows 7 fr-FR {bootloadersettings} {716e0e17-a4d4-11e2-87ca-0010b586d1f9} Yes partition=C: \Windows {716e0e15-a4d4-11e2-87ca-0010b586d1f9} OptIn</pre>

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

identificateur{e34d0b0a-13fa-11e0-a522-aa22f2e4872a} partition=C:pathWindows\system32\winload.exedescriptionboot OS depuis UHDlocalefr-FRinherit{bootloadersettings}recoverysequence{e34d0b08-13fa-11e0-a522-aa22f2e4872a}recoveryenabledYesosdevicepartition=C:systemroot\Windowsresumeobject{e34d0b06-13fa-11e0-a522-aa22f2e4872a}nxOptIn

supposons que notre fichier vhd se nomme os.vhd



os.vhd pc-2008r2-natif.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=LC:l\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
Chargeur de demarrage identificateur device path description locale inherit recoverysequence recoveryenabled osdevice systemroot	Windows <pre></pre>
resumeobject nx detecthal	\estime=131a=11e0=a522=aa2212e4672a7 OptIn Yes





Système Windows 7 Seven - SYS 20 - Travaux Pratiques - ver 2.3 -

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

🖃 🚰 Stockage	Attacher un disque dur virtuel
 Gestion des disques Services et applications Actualiser Analyser les disques de nouveau Créer un disque dur virtuel Attacher un disque dur virtuel 	Spécifiez l'emplacement du disque dur virtuel sur l'ordinateur. Emplacement : C:\vhd-os\os-8.vhd Parcourir Lecture seule. OK Annuler

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

Répertoire	de E:\Windows\S	ystem32	
26/07/2012	05:08 1 fichier(s)	183 808	bcdboot.exe 183 808 octets
	e Kep(s) 1	364 881	408 octets libres

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

Nom *	Modifié le	Туре	Taille
bcdboot.exe	26/07/2012 05:08	Application	180 Ko

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

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 » <u>depuis</u> 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\Administr	ateur>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 Disque Ø En li Disque 1 En li	gne 114 G octet gne 3817 M octet	e Dyn GPT s 1024 Koctets s 0 octets	Disque 1 = clé de 4Gig

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

se	select disk=1								
DIS	SKPART >	se	elect	t 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	a réussi	à	nettover	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

DIS	KPART> se	Lec	t pa	artition 1			
La	partition	1	est	maintenant	la	partition	sélectionnée.

On Vérifie que l'on est bien dessus

List partition

DISKPART> list partition					
N ^o partition	Туре	Taille	Décalage		
→ * Partition 1	Principale	3817 M	64 K		

On la rend active

active





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

format fs=fat32	ou mieux	forma	at fs=N	TFS L	ABEL="cle	bootable	e"
DISKPART> format fs=	=fat32	DISKPART>	format	Fs=NTF	S LABEL="cle	bootable	W
100 pour cent effe	ctués	100 pour	r cent e	effectu	és		
DiskPart a formaté]	le volume.	DiskPart a	a format	té le v	olume.		

at Fs=NTFS LABEL="cle bootable Winpe" nt effectués maté 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 d	e montage.

Une dernière vérification par

list volume							
DISKPART> lis	t vol	ume					
N ^o volume	Ltr	Nom 	Fs	Туре 	Taille	Statut	Info
Volume Ø Volume 1	Ε	Bluebirds Réservé au	CDFS NTFS	DUD-ROM Partition	6146 K 100 M	Sain Sain	Système
Volume 2	C	os-7-sp1	NTFS	Partition	29 G	Sain	Démarrag
* Volume 4	ŵ	INSCALLACIO	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

ΟU

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

🖃 퉲 wds-install	Nom ^	Modifié le
E Boot	🔿 x32-profil-rearm	05/09/2011 14:06
H Mgmt	x32-profil-ss-rearm	05/09/2011 14:05
🗉 퉲 Stores	👜 x64-profil-rearm	07/11/2011 06:44
🖃 퉲 Templates	🖆 x64-profil-sans-rearm	07/11/2011 06:40
🎍 sysprep		
	sysprep	

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

Pa	aramètres de protection		
	Lecteurs disponibles	Protection	
	🏭 systeme-seven (C:) (Système)	Désactivée	
	👝 data (D:)	Activée	

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



- 🖄 cabare-sys20-systeme-windows-xp-2000-tp.doc
- abare-sys22-sys20-xp-ntfs-cours.doc

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**"

2	Propriétés	de : cabare-sys20-systeme-windows-xp-2000-cours.doc	×
G	iénéral Sér	curité Personnaliser Détails Versions précédentes Les versions précédentes proviennent de points de restauration ou de la Sauvegarde Windows. <u>Comment utiliser des versions précédentes ?</u> s fichiers :	
	Nom	Modifié le Emplacement 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)

Configurer la sauvegarde			
Sélectionner l'emplacement d'enregist	rement de votre sauveg	Jarde	
Il est conseillé d'enregistrer votre seuvegerde sur ur	lecteur externe Instructions r	our choisir und	
Enregistrer la sauvegarde sur :	necteur externe. <u>Instructions p</u>		
Enregistrer la sauvegarde sur : Destination de sauvegarde	Espace libre	Taille totale	
Enregistrer la sauvegarde sur : Destination de sauvegarde at (D:)	Espace libre 34,21 Go	Taille totale	

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

Activez la case à cocher des éléments à inclure dans la sauvegarde. <u>Quels fichiers sont exclus par défi</u> de la sauvegarde ?		
Activez la case à cocher des éléments à inclure dans la sauvegarde. Quels fichiers sont exclus par défi de la sauvegarde ?		
	Activez la case à cocher des éléments à inclure dans la sauvegarde. Quels fichiers sont	exclus par défa
 Fichiers de données Sauvegarder les données pour les utilisateurs récemment créés Bibliothèques de admin Bibliothèques de Administrateur Bibliothèques de test Ordinateur systeme-seven (C:) data (D:) 	de la sauvegarde ?	
 Frchiers de données Sauvegarder les données pour les utilisateurs récemment créés Bibliothèques de admin Bibliothèques de Administrateur Bibliothèques de test Ordinateur systeme-seven (C:) data (D:) 	(1)	
 Sauvegraeries donnees pouries utilisateurs recemment crees Bibliothèques de admin Bibliothèques de Administrateur Bibliothèques de test Ordinateur systeme-seven (C:) data (D:) 	Fichiers de données	
 Bibliothèques de admin Bibliothèques de Administrateur Bibliothèques de test Ordinateur systeme-seven (C:) data (D:) 	Sauvegarder les données pour les utilisateurs récemment crees	
 Bibliotheques de Administrateur Bibliothèques de test Ordinateur systeme-seven (C:) data (D:) 	Districted a second a desired a d	
 ▷ □ ■ Bibliotheques de test ▲ □ Ordinateur ▷ □ ■ systeme-seven (C:) ▲ □ → data (D:) 	Bibliotheques de Administrateur	1
■ Grainateur > □ systeme-seven (C:) ■ □ data (D:)	District de test	
 Systeme-seven (C:) data (D:) 		
a 🔤 🚙 data (D:)	Systeme-seven (C:)	1
	a 🛄 🥪 data (D:)	
b 🛛 🖕 data 🛛 🖓		

Ce qui donne



Vérifiez vos para	amètres de sauvegarde		Sauvegarder ou	restaurer des fichiers
Emplacement : Résumé de la sauveo	KINGSTON (F:)		Sau	vegarde en cours
Éléments		Inclus dans la sauvegarde	Sauvegarder	
\mu D:\data\	2	Tous les fichiers de données lo	Emplacement :	KINGSTON (F:)
	45			2,98 Go libres sur 3,73 Go
				Taille de la sauvegarde : Non dispon
				🌍 Gérer l'espace
Planification :	Le dimanche à 19:00 Mo	lifier la planification	Prochaine sauvegarde :	En cours
Flammeation .	Le dimanche a 19.00 Mol		Dernière sauvegarde :	Jamais
			Contenu :	Fichiers dans les dossiers sélectionnés
			Planification :	Chaque dimanche à 19:00
				🛞 Modifier les paramètres

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

J perso			
👜 cabare-sys20-	systeme-windows-xp-2000)-cours.doc	
👜 cabare-sys20-	systeme-windows-xp-2000)-tp.doc	
👜 cabare-sys22-	sys20-xp-ntfs-cours.doc		
On obtient			
Propriétés de :	cabare-sys20-systeme-wi	ndows-xp-2000-cours.doc	×
Général Sécurit	é Personnaliser Détails	Versions précédentes	
		enert de painte de meteurstien eu de la	
Versions des fic	versions precedentes provie uvegarde Windows. <u>Commen</u> hiers :	t <u>utiliser des versions précédentes ?</u>	
Versions des fic	versions precedences provie uvegarde Windows. <u>Commen</u> hiers : Modifié le	Emplacement	
Versions des fict	hiers : Modifié le	Emplacement	_



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

Utilisateurs Administrateur		Propriétés de : Mes documents
🎍 AppData 🝺 Application Data		Général Partage Sécurité Emplacement Versions précédentes Personnaliser
📔 Bureau		Les fichiers du dossier Mes documents sont stockés à l'emplacement cible ci-dessous.
🔊 Cookies 隆 Favoris	=	Vous pouvez changer l'emplacement où sont stockés les
Liens		tichiers de ce dossier et choisir un nouvel emplacement sur ce disque dur, un autre disque ou un autre ordinateur du réseau.
Ma musique		C:\Users\Administrateur\Documents
Menu Démarrer Mes documents		Valeurs par défaut Déplacer Rechercher la cible

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...

Emplacer	nent du dossi	er cible	
Cible :	\\travail\da	ataperso\temp	
Valeurs	par défaut	Déplacer	Rechercher la cible

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





Système Windows 7 Seven - SYS 20 - Travaux Pratiques - ver 2.3 - http://www.cabare.net Page 39 Cabaré Michel