

Système Windows 8.1 Pro – sys 20 – Cours -

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

Système Windows 8.1 Pro Cours

Michel Cabaré – Ver 1.2 – Juin 2014

<u>www.cabare.net</u>©

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

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

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

Bon Travail

Michel Cabaré

Table des Matières

WINDOWS 81 SEVEN & XP	
POSITIONNEMENT DANS LA FAMILLE MICROSOFT :	8
DUREE DU SUPPORT CHEZ MICROSOFT :	9
Fonctionnalites Windows 8 :	10
CONFIGURATION MATERIELLE	
CONFIGURATION REQUISE :	
HARDWARE COMPATIBILITY LIST :	
QU' EST-CE QU'UN SERVICE PACK :	
PATCHES:	
CENTRE DE PROFIL MICROSOFT :	14
OUTILS MBSA 2.3:	15
NOTIONS POUR INSTALLER 8	
FICHIERS D'INSTALLATION IMAGE - WIM :	
LA HAL - HARDWARE ABSTRACTION LAYER	
Sous Windows XP,	
Sous Windows 8 (Seven)	
LES CATEGORIES DE PARTITION SUR SYSTEME INTEL:	
SYSTEME DE FICHIER NTFS :	
INSTALLATION NOUVELLE/ M.A.J.	
MISE A NIVEAU - INSTALL COMPLETE:	
INSTALL COMPLETE DEPUIS CD :	23
Paramètre régionaux :	
Installer / Réparer	
Licence	
Mise a Jour / Installation Avancee Création des Partitions	
Copie des fichiers	26
Assistant premier démarrage (phase OOBE)	
Configuration Rapide / Personnalisée	
Profils Réseaux	
Mise à Jours Windows Update – Filtres IE	
Aide Débugage Windows 8	
Compatibilité IE, Réseaux Sociaux, Géo-Localisation	
Email - Comple Local – Passeport Microsoft Création Compte Local	
AUTHENTIFICATION WINDOWS 8	
PAR CODE CONFIDENTIEL :	32
PAR TRACE SUR LINE IMAGE .	33
LOGIN SUR SAM OU AD .	33
COMPTE MICROSTORE (NON LOCAL)	34
ECRAN DE VERROUII LAGE	34
ECRAN D'ACCUEIL:	
WINPE 4.0	
WINDOWS PREINSTALLATION ENVIRONMENT:	
UTILISER WINDOWS PE LORS DE L'INSTALLATION SEVEN:	
UTILISER UN MEDIA AMORÇABLE WINDOWS PE:	
3	



SÉQUENCE BOOT & MULTI-BOOT	
BOOT XP & NTLDR:	
BOOT SEVEN & BOOTMGR :	39
MULTI-BOOT SEVEN (BOOTMGR) - XP (NTLDR) :	40
BOOT WINDOWS 8	41
BOOT WINDOWS 8 – ABANDON F8 :	41
METHODES ACCES AU MENU DE DEMARRAGE:	41
MENU OPTIONS DE DEMARRAGE:	42
MENU OPTIONS DE DEMARRAGE - DEPANNAGE:	43
BCDEDIT	44
BCDEDIT ET GESTION DU MAGASIN :	44
Sauvegarde du magasin complet :	44
Reconstruction du Magasin :	44
Structure du magasin:	
BCDEDIT COMMANDE :	
Copier-Dupliquer une entrée du magasin:	
Supprimer une entree au magasin:	47 17
Système par défaut:	47 <i>A</i> 8
Time-out	48
Forcer l'affichage du menu de boot:	
BCDEDIT ET CHARGEUR DE DEMARRAGE – BOAT LOADER :	49
Renommer une entrée :	
BCDEDIT ET CHARGEUR ANCIEN SYSTEME – LEGACY BOAT LOADER :	50
Renommer une entrée :	
BCDEDIT OPTION /STORE :	50
UTILITAIRE BOOTSECT & CHANGEMENT BCDEDIT / NTLDR:	51
INSTALLER WINDOWS 8 A COTE DE XP (MULTI-BOOT)	51
même disque, autre partition :	
autre disque :	
INSTALLER AP A COTE DE WINDOWS 8	
SUPPRIMER UN BOOT SEVEN (RETOUR BOOT SEVEN);	
LES DROCESSUS SOUS WINDOWS	
LES PROCESSUS SOUS WINDOWS	
SEQUENCE POST : POWER ON SELF TEST	55
SEQUENCE DEMARRAGE BOOTMGR	55
VOCABULAIRE SYSTEME SOUS 8-SEVEN :	56
LISTER LES PROCESSUS - GRAPHIQUE:	57
ARRETER UN PROCESSUS, UN SERVICE :	
GESTIONNAIRE DE SERVICES	
LISTER LES PROCESSUS – INVITE DE COMMANDE:	60
Taskiisi (SEVEN - AF). Taskkiili (denuis SEVEN - XP):	
OUELOUES PROCESSUS DE BASE	61
DRIVERS	67
ANCIENS TYPES 2000 - WOM ·	
ANCIENS TTEES 2000 - WDM I es Drivers WDF ·	02 67
MAGASIN DE DRIVERS :	
Mise en place du pilote dans le magasin	
Installation du pilote lors du P&P par Windows 8	
STRATEGIES DE GESTION DE DRIVERS :	64
DRIVERS CERTIFIES :	64
INSTALLATION DE PILOTES NON CERTIFIES :	64
GESTIONNAIRE DE PERIPHERIQUE:	65
VERSIONS - INSTALLATION DE PILOTES :	66



INSTALLATION DRIVER VIA UPDATE : INSTALLATION DRIVER VIA FICHIERS LOCAUX : METHODE PAR DEFAUT INSTALLATION DE DRIVERS : SIGVERIF VERIFICATION DRIVERS SIGNES: DRIVERQUERY VERIFICATION DRIVERS SIGNES:	67 67 69 70 71
INTÉGRITÉ WINDOWS 8	73
LES DLL (DYNAMIC LINK LIBRARIES) : WRP PROTECTION DES DLL : sfc - system file checker	73 73 74
UAC- USER ACCOUNT CONTROL	75
OBJECTIF VISE : IL – INTEGRITY LEVEL : GESTION DE L'UAC (PANNEAU DE CONFIGURATION): GESTION DE L'UAC (STRATEGIES LOCALES): Désactivation de l'UAC (STRATEGIES LOCALES): Désactivation de l'UAC pour les Administrateur : Désactivation de l'UAC pour les Administrateur : Désactivation l'UAC pour les Utilisateurs : Activation l'UAC aussi pour le compte Administrateur Root :	75 75 77 78 78 78 78 79 79
INSTALLATIONS ET VIRTUALISATION	80
PRECONISATION MICROSOFT : VIRTUALISATION DES PROCESSUS :	80 80
COMPATIBILITE AVANT WINDOWS 8	82
EXECUTER EN MODE COMPATIBILITE:	82 83
PROTECTION DEP	84
PRINCIPE DEP DATA EXECUTION PREVENTION: DESACTIVATION COMPLETE DE DEP : DESACTIVATION POUR UNE APPLICATION DE DEP :	84 84 84
WINRE	86
WINDOWS RECOVERY ENVIRONNEMENT: DEMARRER L'ENVIRONNEMENT DE RECUPERATION WINRE: ETAPE 1 SEQUENCE POST Problèmes hardware Problèmes partition- mbr-fichiers manquants ETAPE 2 AFFICHAGE DU « ROND » AVANT SESSION ETAPE 3 APPES L'OUWERTURE DE SESSION	86 87 89 90 90
WINRE - CONSOLE DE RECUPERATION	91
INVITE DE COMMANDE: MODIFIER LES PARTITIONS - UTILITAIRE DISKPART SHRINK DISKPART – REDUIRE UNE PARTITION EXTEND DISKPART – ETENDRE UNE PARTITION OUTIL MDSCHED	92 93 93 93 94 94
CREATION DE WINRE SUR CD - USB	95
CREATION CD WINRE CREATION LECTEUR USB	95 96
TEST MEMOIRE	97
Depuis Windows 8	97
PARAMETRES DE DEMARRAGE – EX F8 Acces aux options avancees : Options principales :	98 98 98



http://www.cabare.net Page 5 - Michel Cabaré -

ACTUALISER – REINITIALISER LE PC	
MENU OPTIONS DE DEMARRAGE - DEPANNAGE:	
ACTUALISER VOTRE PC:	100
IMAGE PERSONALISEE RECIMG:	101
REINITIALISER VOTRE PC:	102
REINSTALLER COMPLETEMENT	
REINSTALLER LE SYSTEME :	103
LES TUILES DE L'ACCUEIL	
ECRAN ACCUEIL PAR DEFAUT	104
GESTION DES TUILES PRE-DEFINIES EN POWERSHELL	105
EPINGLER DES TUILES SUR L'ACCUEIL	107
GESTION WINDOWS STORE	107
POINTS DE RESTAURATION	
PRINCIPE RESTAURATION - DESACTIVATION	109
DESACTIVATION DE LA RESTAURATION	
CREATION D'UN POINT DE RESTAURATION	110
UTILISER ANNULER UN POINT DE RESTAURATION	110
TYPES DE POINT DE RESTAURATION	111
PARAMETRAGES DES POINT DE RESTAURATION : VSSADMIN	112
SAUVEGARDE SYSTEME - FICHIERS	
	112
JEUX OUTILS DE SAUVEGARDE	
AUTOMATISEP VIA WRADMIN	115
REALISER UNE RESTAURATION INTEGRALE SYSTEME	116
	110
HISTORIQUE DES FICHIERS	
MISE EN PLACE	
STOCKAGE	
KESTAURER DES FICHIERS	120
COMPTES UTILISATEURS	
COMPTE D'UTILISATEURS – SESSION:	121
CONNEXION MULTIPLES UTILISATEUR	
DESACTIVER LA BASCULE RAPIDE UTILISATEUR	
SID SECURITY IDENTIFIER :	
	125
COMPTES PRE-DEFINIS :	125
EXECUTER EN TANT QUE:	120
GESTION DES COMPTES:	127
RE-DEFINITION DE MOT DE PASSE	129
CACHER LE DERNIER UTILISATEUR	
GROUPES LOCAUX	
NOTIONS DE CROUDES :	120
ROHONS DE GROUPES :	130
LIENS SYMBOLIQUES – KACCOURCIS – JONCTIONS :	
FKUFIL LUCAL:	132
LWIFLACEMENT FRUFILS LUCAUA SEVEN	132
STRUCTURE D'UN PROFIL I ITU ISATEUR	133



PROFIL PAR DEFAULT	
Méthode Certifiée pour modifier le profil par défaut	
DDDCE DUDUC	
SUPPRIMER TOUS LES PROFILS LOCAUX WINDOWS 8:	
INTERFACE WINDOWS 8 - 7	
PANNEAU DE CONFIGURATION:	
L'EXPLORATEUR WINDOWS:	
INTERFACE AERO:	
NOTE WINDOWS 8:	
MESSAGES DU CENTRE DE MAINTENANCE :	
MENU CONTEXTUEL / ACCUEIL	144
COMPROMIS PERFORMANCES – ARRET SERVICES:	144
SLMGR - ACTIVATION LICENCE	
INSTALLER WINDOWS 8 SANS CLE:	145
REACTIVER WINDOWS 8 - SLMGR:	
Réactivation période de grâce	
TRANSFERT – RE-SAISIE LICENCE:	147
SAISIE LICENCE SLUI 3:	147
INCLASSABLES WINDOWS 8	
MENU ETENDUS (INVITE DE COMMANDE):	
OPTIONS DEMARRAGE MSCONFIG.EXE :	
OUTILS DXDIAG:	
OUTILS SHUTDOWN:	
WHOAMI:	151
CONSOLE MMC	
MICROSOFT MANAGEMENT CONSOLE:	
CREER UNE CONSOLE PERSONNALISEE:	
LIMITER LES FONCTIONS D'UN COMPOSANT LOGICIEL :	154
ENREGISTRER LA CONSOLE UTILISATEUR :	155
SYSPREP	
VERSIONS DE SYSPREP:	156
Sysprep 3.14 pour 8 Seven-2008:	156
SYSPREP MODE GRAPHIQUE:	
Sysprep /generalize:	157
MINI INSTALLATION PASSE OOBE:	
Sysprep /unattend:c:\fichier.xml:	
SYSPREP /UNATTEND COPYPROFILE	
ACTIVATION ET SKIPREARM	
EXEMPLE DE FICHIER DE REPONSE	



WINDOWS 81 SEVEN & XP

Positionnement dans la famille Microsoft :

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

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

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

- système d'exploitation 32 bits multi-tâche, WINDOWS NT:
 - ✓ 4.0 en juillet 96 : Version Workstation et Server
 - 01/01/2005 : arrêt complet du support
- Une mise à jour majeure du système d'exploitation Windows 2000:
 - ✓ 5.0 dit 2000 en fév 2000 Version Pro, Server, Advanced Server 16/06/2003 : arrêt complet du support

Une mise à jour **Windows XP**: starter, familiale, pro, intégrale

✓ 5.1 en sept 2001 Professionnel, Home, Embedded

08/04/2014 : arrêt complet du support

- Une mise à jour majeure du système d'exploitation dit Vista:
 - ✓ 6.0 en janvier 2007 dit Vista, Version Home Basic, Home Premium, Business-Pro, Business-Enterprise, (Ultimate...)

Une mise à jour **7 - Seven**: starter, familiale, pro, intégrale

✓ 6.1 en octobre 2009 ...

Une mise à jour Windows - 8: RT, 8, pro, entreprise

✓ 6.2 en octobre 2012 ...

Une mise à jour Windows - 8.1 : RT, 8, pro, entreprise

✓ 6.3 en mai 2014



Durée du support chez Microsoft :

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





La phase principale de support inclut :

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

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

La phase d'extension de support inclut :

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

Systèmes d'exploitation clients	Dernier Service Pack ဇူu dernière mise à jour	Fin du support standard	Fin du support étendu
Windows XP	Service Pack 3	14 avril 2009	8 avril 2014
Windows Vista	Service Pack 2	10 avril 2012	11 avril 2017
Windows 7 *	Service Pack 1	13 janvier 2015	14 janvier 2020
Windows 8	Windows 8.1	9 janvier 2018	10 janvier 2023





Fonctionnalités Windows 8 :

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

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

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

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

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



CONFIGURATION MATERIELLE

Configuration requise :

Voilà les données pour une utilisation de Windows 8

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

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

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

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

Hardware Compatibility List :

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



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

Désormais les listes Windows 8 et Windows RT sont disponibles



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

Qu' est-ce qu'un Service Pack :

avec Windows 7.

Dans un premier temps on installe Windows puis le service pack existant faute de quoi le fonctionnement correct peut être gravement compromis

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

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

2000 livré 02/2000	5.00.build 2195	SP4 final juin 2003
XP livré 09/2001	5.10.build 2600	SP3 final mai 2008
Vista livré 01/2007	6.00.build 6000	SP2 final mai 2009
Seven livré 07/2009	6.10.build 7600	SP1 mars 2011 build 7601
8 livré 10/2012	6.20.build 9200	pas de Sp à venir
8.1 livré 05/2014	6.30.build 9600	Ś



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

Centre de Service Packs - Microsoft Windows windows.microsoft.com > ... > Microsoft Security Essentials Découvrez les Service Packs Windows et téléchargez les derniers SP pour ... Service Packs consiste à activer Windows Update pour Windows 8, Windows 7 et ...

Ce qui donne

Centre de Service Packs - Microsoft Windows					1
DÉCOUVREZ WINDOWS TÉLÉCHARGER ET A	CHETER	PRISE EN MAIN	ASSIST	ANCE	
Téléchargements gratuits // Sécurité et utilitain	res //	Microsoft Security Es	sentials	Service Packs	Utilitaires

Centre de Service Packs

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

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

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

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

Windows 8 Windows 7 Windows Vista Windows XP

Et on pourra télécharger

Aucun Service Pack disponible actuellement

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

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

Patches:

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

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



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

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

N	licrosoft				Reche	rcher sur le site
Accueil	Newsletters	Flux RSS	Mentions légales	Contactez-nous	Plan d'accès	Plan du site

Newsletters de Microsoft France

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

Newsletter France Newsle		ter produits Newsletters professionnels de l'inform			rmatique
Newsletter pour l'éducation		Newsletter e	ntreprise	Toutes les newsletters	N

Un identifiant passeport microsoft peut être nécessaire...

👏 Windows Liv	ve ID	
Connexion à Site Wel	b Windows Live ID Aide michel@cabare.net	Connexion Connectez-vous maintenant pour consulter ou modifier les paramètres de votre compte.
Mot de passe :	Mot de passe oublié ? Connexion	Pour vous connecter au site à partir duquel vous avez cliqué sur le lien Espace Utilisateurs, cliquez sur le bouton Précédent de votre navigateur, puis connectez-vous. Liens <u>Ouvrijfun compte</u>

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

Technet



Newsletter TechNet

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

Toutes les deux semaines | Inscription à la Newsletter Technet | Un exemplaire de la Newsletter Technet

Alertes de Sécurité



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

Dès qu'une alerte se présente | Inscription aux bulletins de sécurité

Donnant ensuite la possibilité de s'inscrire

Centre de profil Microsoft :

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

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







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

Newsletters disponibles Vos aber Pour vous abonner, sélectionnez la ou les newsletter (s) que vous souhaitez recevoir et appuyez sur S'abonner. Votre ou vos Sélectionner Langue Français (France) Sélection	onnements vos abonnements sont re ez un abonnement et aj ment pour le supprimer	epris ci-dessous. ppuyez sur Annuler r de la liste.
Pour vous abonner, sélectionnez la ou les newsletter Votre ou v (s) que vous souhaitez recevoir et appuyez sur Sélectionn S'abonner. l'abonner	vos abonnements sont re iez un abonnement et aj ment pour le supprimer	epris ci-dessous. ppuyez sur Annuler r de la liste.
Langue Français (France) Sélecti		
[+] Newsletter MSDN [+] Newsletter Windows [+] Newsletter Office [+] Newsletter Office [+] Newsletter Microsoft France [+] Newsletter Education [+] Newsletter TPE-PME [+] Newsletter des Décideurs [+] Newsletter Etudiants.ms [+] MSDN Afrique	ionner tout HTM Sletter Ce de Cation Soft rité	

Outils MBSA 2.3:

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



Il faut donc exécuter ce fichier...





La version 2.3 de MBSA comprend une interface graphique



qui peut effectuer l'analyse locale de systèmes Windows 8

	Microsoft Baseline Security Analyzer 2.3	- 🗆 🗙
Baseline	e Security Analyzer	Microsof
Tâches Analyser un ordinateur Analyser plusieurs ordinateurs <u>Afficher les rapports de</u> <u>sécurté</u> A propos de Microsoft Baseline Security Analyzer	Recherchez dans les ordinateurs les erreurs fréquentes de configuration de sécurité. L'outil Microsoft Baseline Security Analyzer peut analyser des ordinateurs exécutant Microsoft Windows Server 2012 R2, Window Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Win Windows XP. La recherche de mises à jour de sécurité dans les ordinateurs utilise les services WSUS (Windows Server Update Vous devez disposer des privilèges d'administrateur pour chaque ordinateur que vous devez analyser. Microsoft Baseline Security Analyzer ne détecte pas l'applicabilité des mises à jour sur des systèmes configurés dans le cadre d' serveurs SharePoint à systèmes multiples.	vs 8.1, dows Vista, ou Services). 'une batterie de
	Analyser un ordinateur Recherchez un ordinateur utilisant ce nom ou cette adresse IP.	
	Analyser plusieurs ordinateurs Recherchez plusieurs ordinateurs utilisant un nom de domaine ou une plage d'adresses IP.	

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

Quel ordinateur vo	Quel ordinateur voulez-vous analyser ?				
Entrez le nom de l'ordinateur ou se	on adresse IP.				
<u>N</u> om de l'ordinateur :	WORKGROUP\POSTE-SEVE (cet ordinateur)				
A <u>d</u> resse IP :					
Nom du <u>r</u> apport de sécurité :	%D% - %C% (%T%)				
Options : Rechercher les vulnérat Rechercher les mots de Rechercher les vulnérat Rechercher les vulnérat Rechercher les vulnérat Rechercher les vulnérat Rechercher les nises à Configurer les ordina	%D% = domaine, %C% = ordinateur, %T% = date et heure, %IP% = Adresse IP Options : Image: Constraint of the state o				
Options avancées d	Options avancées des services de mise à jour :				
 Analyser en n'utilisant que les serveurs Windows Server Update Services(WSUS) <u>a</u>ssignés Analyser en n'utilisant que <u>M</u>icrosoft Update Analyser avec le catalogue hors connexion uniquement 					

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

Analyse...
Téléchargement des informations de mises à jour de sécurité depuis le site de Microsoft...

Une analyse est rendue

Un résultat est donné avec des indications sur les actions éventuelles





Vulnérabilités d'administration

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

Informations système supplémentaires

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



NOTIONS POUR INSTALLER 8

Fichiers d'installation Image - WIM :

Comme Seven, Windows 8 ne s'installe plus depuis une distribution de fichiers stockés dans une arborescence du CD-DVD d'installation (traditionnellement un dossier i386...), mais depuis une image au format WIM Windows Imaging format

Ce format Wim présente les avantages suivants :

- Réduction considérable de la taille due à la structure mono-fichier de la distribution
- Indépendance du matériel, deux distributions suffiront à couvrir tous le parc, une 64 bits et (éventuellement une 32 bits)
- Orienté fichier, et non secteurs disques, il peut s'installer sans reformater le disque sur des partitions existantes (et garder l'existant)
- Stockage des différentes images dans un fichier Wim, permettant de déployer différentes topologies en économisant de la place car les fichiers communs aux différentes images ne sont stockés que une fois
- Démarrage de l'installation avec Windows PE 4.0, (boot.Wim) permettant de préparer (si besoin) disques et partition...

Il est possible d'installer Windows 8 de 2 manières :

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

La HAL - Hardware Abstraction Layer

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

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

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



Sous Windows XP,

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

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

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

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

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

Sous Windows 8 (Seven)

detectehal

une seule HAL est désormais détectée, dénommée



Windows 8 se déployant à partir d'image, la détection de la base HARDWARE peut se faire directement au lancement de l'OS (et non plus lors de l'installation). On peut forcer la détection de la HAL à travers via 2 nouvelles commandes disponible, dans la section windows boot loader :

Usefirmwarepcisettings No Chargeur de démarrage Windows			
identificateur device path description locale inherit osdevice systemroot resumeobject nx detecthal usefirmwarepcisettings	<pre>Current> partition=C: Windows\system32\winload.exe Microsoft Windows Uista fr-FR Cbootloadersettings> partition=C: Windows {06ac77b7-f447-11dc-a37d-dbb378e90123> OptIn Yes No</pre>		

Yes

Donc

Bcdedit /set {current} detecthal yes

Et Bcdedit /set {current} detecthal no

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



Les catégories de partition sur système INTEL:

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

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



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

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

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

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

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

Donc un disque pourra avoir la structure suivante :

A CONTRACT OF A				
DISQUE PHYSIQUE				
Partition primaire Partition étendue				
	Partition logique	Partition	étendue	
		Partition logique	Partition étendue	
			Partition logique	

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



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

N.B: Avec les outils DOS/Windows, une table de partition ne "pointe" au plus que vers 2 partitions (une logique et éventuellement une étendue), alors qu'elle pourrait en contenir 4. Par conséquent, avec l'administrateur de disque NT4, seule est affichée la 1ère partition étendue, suivie de toutes les autres partitions logiques comme si elles étaient à l'intérieur de cette partition étendue.

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

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



Système de Fichier NTFS :

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

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

Comparaison des tailles de disques et de fichiers

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



INSTALLATION NOUVELLE/ M.A.J.

Mise à niveau - install complète:

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

• Au cours d'une mise à niveau, le programme d'installation **remplace** les fichiers Windows existants mais essaye de conserver vos paramètres et applications actuels. Il est bien sur possible que certaines applications ne soient pas compatibles avec Windows 8

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

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

On peut migrer uniquement dans les cas suivants pour Seven

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

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

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



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

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

Install complète Depuis CD :

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

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

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



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

Paramètre régionaux :

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





Installer / Réparer

Il faut demander d'Installer Windows 8

🖆 Insta	allation de Windows		
	Windows [.] 8		
	Installer maintenant		
<u>R</u> éparer l'ordinateur			
© 2012 Microsoft Corporation. Tous droits réservés.			

Pour obtenir

Démarrage du programme d'installation

Licence

1	🕞 💰 Installation de Windows
	Termes du contrat de licence
	CONTRAT DE LICENCE D'ÉVALUATION DE LOGICIEL MICROSOFT
	WINDOWS 8 ENTREPRISE
	Nous vous remercions d'avoir choisi d'évaluer Microsoft Windows 8 Entreprise. Le présent contrat de licence constitue un contrat entre vous et Microsoft Corporation (ou, en fonction du lieu où vous vivez, l'un de ses affiliés) qui décrit vos droits d'utilisation du logiciel d'évaluation Windows 8. Nous avons structuré le présent contrat en deux parties dans un souci de commodité. La première partie se présente sous forme de questions réponses, suivies par les Conditions Supplémentaires plus détaillées. Vous devez lire l'ensemble du contrat, y compris les liens, car tous les termes sont importants et constituent ensemble le présent contrat, qui s'applique à vous. Vous pouvez consulter les termes liés en collant le lien concerné dans la fenêtre de votre navigateur une fois le logiciel en cours d'exécution. Les Conditions Supplémentaires contiennent une clause d'arbitrage et une renonciation aux actions collectives, qui vous sont
	Vaccepte les termes du contrat de licence
	Suivant

Il faut accepter la licence

Mise à Jour / Installation Avancée

La mise à jour est souvent désactivée (car elle n'est disponible que si on démarre la procédure d'installation depuis l'ancien OS, XP ou Seven...), et donc on demande Personnalisé : installer uniquement Windows (avancé).



\bigcirc	Installation de Windows
	Quel type d'installation voulez-vous effectuer ?
	Mise à niveau : installer Windows et conserver les fichiers, les paramètres et les applications Avec cette option, les fichiers, les paramètres et les applications sont déplacés vers Windows. Cette option n'est disponible que lorsqu'une version prise en charge de Windows est déjà en cours d'exécution sur l'ordinateur.
	Personnalisé : installer uniquement Windows (avancé) Avec cette option, les fichiers, les paramètres et les applications ne sont pas déplacés vers Windows. Pour apporter des modifications aux partitions et aux lecteurs, démarrez l'ordinateur à l'aide du disque d'installation. Nous vous recommandons de sauvegarder vos fichiers avant de continuer.
	<u>C</u> omment choisir ?

Création des Partitions

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

Nom		Taille totale	Espace libre Ty	pe	
> Lecteur 0 Espace r	ion alloué	80.0 Go	80.0 Go		
Act <u>u</u> aliser	C3		Options de lecte	ur (avancées)	
C <u>h</u> arger un pilote					
				Suivant	1
				_	

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

Administrateur : X:\windows\system32\cmd.exe - diskpart	
Microsoft Windows [version 6.2.9200]	^
X:\Sources>diskpart	
Copyright (C) 1999-2012 Microsoft Corporation. Sur l'ordinateur : MINWINPC	k
DISKPART> _	



	Où souhaitez-vous installer Windows ?			×
Une partition « cachée »	Nom Lecteur 0 Partition 1: Réservé au système	Taille totale 350.0 Mo	Espace libre Type 320.0 Mo Système	
système est crée pour	Lecteur 0 Partition 2	19.2 Go	19.2 Go Principal	
stocker des outils de récupération en cas de	Lecteur 0 Espace non alloué	60.5 G	60.5 Go	
crash	 ∳Actualiser ✓ Supprimer ✓ E ✓ Charger un pilote ✓ Étendre 	<u>F</u> ormater	* Nouv <u>e</u> au	

Copie des fichiers

Le programme d'installation poursuit,



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

Windows doit	redémarrer votre ord	inateur pour continu	ier
Redémarrage dan	10 secondes		





Assistant premier démarrage (phase OOBE)

Il demande successivement :

• Le nom machine

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

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

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

• Un choix de couleur

Personnalis	er
Sélectionnez une couleur que vous aim	ez et donnez à votre PC le nom souhaité. Vous pourrez le personnaliser
davantage plus tard.	
davantage plus tard.	▼
davantage plus tard.	
davantage plus tard.	
davantage plus tard.	

Configuration Rapide / Personnalisée

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

€	Paramètres
	 Configuration rapide, ce PC envoie de temps en temps des informations à Microsoft pour : Installer automatiquement les mises à jour importantes et recommandées. Protéger votre PC contre les fichiers et les sites Web dangereux Activez Do Not Track dans Internet Explorer. Contribuer à améliorer les logiciels, services et services de localisation Windows en nous envoyant des informations. Permettre aux applications de vous proposer un contenu personnalisé en fonction de l'emplacement, du nom et de l'avatar de compte de votre PC. Activer le partage et se connecter aux périphériques de ce réseau.
	En savoir plus sur la configuration rapide
	Déclaration de confidentialité
¢	Utiliser la configuration rapide Personnaliser

il vaut mieux demander Personnaliser



Profils Réseaux

E	Paramètres	
	Il s'agit de votre première connexion à ce réseau. Voulez-vous a périphériques sur ce réseau ?	ctiver le partage entre les PC et vous connecter à des
	Oui, activer le partage et se connecter aux périphériques Pour les réseaux domestiques ou d'entreprise	
	Non, ne pas activer le partage ni se connecter aux périphériques Pour les réseaux situés dans des lieux publics	

Mise à Jours Windows Update – Filtres IE

¢	Paramètres
	Protéger et mettre à jour le PC ^{Windows Update}
	Ne pas configurer Windows Update (non recommandé)
	Obtenir automatiquement les pilotes, applications et informations pour les nouveaux périphériques Désactivé
	Protéger votre vie privée et votre PC
	Activer le filtre Windows SmartScreen pour vérifier les fichiers et les applications auprès de Microsoft Désactivé
	Activer le filtre SmartScreen d'Internet Explorer pour vérifier les URL et les téléchargements auprès de Microsoft Désactivé
	Envoyer une demande Do Not Track aux sites Web que vous visitez dans Internet Explorer Désactivé
Ċ	Suivant



Aide Débugage Windows 8

¢	Paramètres
	Envoyer à Microsoft des informations pour contribuer à améliorer Windows et les applications Contribuer à l'amélioration du Windows Store en envoyant des URL relatives au contenu Web utilisé par les applications Désactivé Aider Microsoft à répondre aux applications et programmes malveillants en rejoignant Active Protection Service (MAPS)
	Contribuer à l'amélioration des services Microsoft en envoyant des données d'emplacement lors de l'utilisation d'applications de géolocalisation Désactivé Participer au programme d'amélioration de l'expérience utilisateur pour contribuer à l'amélioration des logiciels et services Microsoft. (Un fichier se téléchargera régulièrement pour collecter de meilleures informations.) Désactivé Contribuer à l'amélioration du contenu de l'aide de Windows en envoyant des informations au programme d'amélioration de l'aide
¢	Désactivé Suivant

Compatibilité IE, Réseaux Sociaux, Géo-Localisation

¢	Paramètres
	Rechercher en ligne des solutions aux problèmes
	Utiliser le rapport d'erreurs Windows pour rechercher des solutions Désactivé
	Améliorer la navigation grâce aux listes de compatibilité d'Internet Explorer Désactivé
	Partager les informations avec des applications
	Permettre aux applications d'utiliser mon nom et l'avatar de mon compte Désactivé
	Activer la plateforme de localisation Windows pour permettre aux applications de demander leur emplacement aux utilisateurs
	Désactivé
Ŷ	Suivant



Email - Compte Local – Passeport Microsoft

E	Vous connecter à votre PC Utilisez votre adresse de messagerie préférée comme compte Microsoft pour vous connecter à Windows. Nous ne vous enverrons pas de courrier indésirable.				
	Adresse de messagerie				
	 Quand vous vous connectez à Windows avec un compte Microsoft, vous pouvez : Télécharger des applications à partir du Windows Store ; Obtenir automatiquement votre contenu en ligne dans des applications Microsoft ; Synchroniser les paramètres en ligne pour donner à des PC la même apparence, notamment pour l'historique du navigateur, l'avatar du compte et la couleur. 				
	Se connecter sans compte Microsoft				
Ċ	Suivant				

On demande de se connecter sans compte microsoft





Création Compte Local

¢	Vous connecter à votre PC				
	Si vous voulez un mot d	le passe, choisissez quelque chose qui soit facile à retenir mais difficile à deviner.			
	Nom d'utilisateur	util			
	Mot de passe	•			
	Entrer de nouveau le mot de passe	•			
	Indication de mot de passe	normal			
сь		Ter	miner		

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

Et l'installation est terminée



AUTHENTIFICATION WINDOWS 8

Par code confidentiel :

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

Charm Bar / Paramètres, et Modifier les paramètres du PC

puis sur Utilisateurs. Et on demande Créer un code confidentiel

Paramètres du PC	Votre compte
Personnaliser	Compte local
Utilisateurs	Vous pouvez utiliser votre adresse connecter à Windows. Vous pour
Notifications	synchroniser des paramètres, etc. Passer à un compte Microsoft
Rechercher	
Partager	Options de connex
Général	Changer votre mot de passe
Confidentialité	Créer un mot de passe image
Périphériques	Créer un code confidentiel

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

E	test	Code 4 chiffre
	Code confidentiel Options de connexion	Options de connexion → ♥

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

C'est Activer la connexion par code confidentiel dans

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

Ouverture de session

Éditeur de stratégie de groupe locale			
Fichier Action Affichage ?			
🗢 🄿 📶 🖬 📾 🕅 📆 🦷			
Det Logon	^	Paramètre	État
Options d'arrêt		Activer la connexion par code confidentiel	Désactivé
Ouverture de session		E Désactiver la connexion par mot de passe image	Non configuré
Panneau de configuration des perfo	:	Affecter un domaine par défaut pour l'ouverture de session	Non configuré



Par Tracé sur une image :

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

Charm Bar / Paramètres, et Modifier les paramètres du PC

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

Paramètres du PC	Votre compte
Personnaliser	test Compte local
Utilisateurs	Vous pouvez utiliser votre adresse connecter à Windows. Vous pour
Notifications	synchroniser des paramètres, etc. Passer à un compte Microsoft
Rechercher	
Partager	Options de connex
Général	Changer votre mot de passe
Confidentialité	Créer un mot de passe image
Périphériques	Créer un code confidentiel

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

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



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

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

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

Ouverture de session

<u>I</u>		Éditeur de stratégie de groupe locale	
Fichier Action Affichage ?			
Net Logon	^	Paramètre	État
Options d'arrêt		E Activer la connexion par code confidentiel	Non configuré
Ouverture de session		Désactiver la connexion par mot de passe image	Activé
Panneau de configuration des pe	it i	E Affecter un domaine par défaut pour l'ouverture de session	Non configuré

Login sur SAM ou AD :

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



Compte Microstore (non local) :

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

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

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

- Applications téléchargées depuis Windows Store.
- Favoris, thèmes, préférences linguistiques.

• Mise à jour de votre réseau social Facebook, Hotmail, Twitter... Photos et autres fichiers stockés sur des services tels que SkyDrive, Flickr...

Charm Bar / Paramètres, et Modifier les paramètres du PC

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

Paramètres du PC	Certains paramètres sont gérés par votre administrateur système. Votre compte		
Personnaliser	test		
Utilisateurs	Vous pouvez utiliser votre adresse de messagerie comme compte Microsoft pour vous		
Notifications	conspecte à Windows. Vous source a nessignir comme complex marcon pour rous connecter à Windows. Vous source accéder à des fichiers et des photos où que vous soyez, synchroniser des paramètres, etc.		
Rechercher	Passer à un compte Microsoft		

Ecran de Verrouillage:

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



N.B : on peut choisir un autre fond, mais on ne peut rien « poser » dessus Via Charm bar, paramètres, Modifier les Pamarètres du PC, Personnaliser



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



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

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

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



Ecran d'accueil:

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





Windows Preinstallation Environment:

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

Windows PE 2.0 basé sur le noyau de Vista, fut le précurseur

Windows PE 4.0 est basé sur le noyau de Windows 8 (Windows PE 3.0 était basé sur le noyau de Seven) . Avec Windows PE on peut:

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

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

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

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

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

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



ens rapides Présentation Configuration requise Le Kit de déploiement et d'évaluation Windows® (Windows ADK) est un ensemble d'outils que vous pouvez utiliser pour personnaliser, évaluer et déployer les systèmes d'exploitation Windows sur de nouveaux ordinateurs.

Utiliser Windows PE lors de l'installation Seven:

Au démarrage apparaît l'écran qui vous accueille lorsque vous installez Windows 8, Mais la combinaison de Touche **MAJ+F10** permettra d'ouvrir une fenêtre d'invite de commande (en plus de l'habituel wizard d'installation...)




Utiliser un média amorçable Windows PE:

Le CD Windows 8 contient déjà un environnement de démarrage sous Windows PE Utiliser un média contenant <u>uniquement</u> Windows PE peut être assez pratique car :

- 1. Il permet de démarrer n'importe quelle machine, y compris un poste sous Windows 2000 ou sous Windows XP sans utiliser une copie de Windows 8
- Grâce à la très petite taille de l'environnement Windows PE 4.0, il est envisageable de le placer sur une simple clef USB.
 N.B : un minimum de 256 Mo de RAM est nécessaire
- 3. Il est naturellement possible d'ajouter ses propres outils à l'image ISO générée par les outils Windows PE.

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

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



SÉQUENCE BOOT & MULTI-BOOT

Boot XP & ntldr:

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

Windows NT4 ne reconnaît pas les partitions formatées en FAT32.

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

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

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

Donc le secteur de boot de la MBR charge le programme NT Loader (**NTLDR**). Ce dernier affiche un menu de sélection basé sur le fichier de configuration **BOOT.INI**. La structure de ce fichier texte est relativement simple.

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

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

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

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





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

Mise sous tension « Séquence POST »

	Ntldr		
	Boot.ini		
	(fichier texte de choix options)		
	Bootsect.dos (Si autre OS que NT)		
,	′Ntdetect.com		
	Détection du matériel		
	Ntoskrnel		
	HAL		
	F8 + profils matériels		
,	Chargement drivers (/SOS ds boot.ini)		

Boot Seven & Bootmgr :

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

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

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

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

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

Mise sous tension « Séquence POST »

Bootmgr

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

Winload.exe

(crée l'environnement d'execution pour SEVEN)

Détection hard HAL

- F8+profils matériels
- Appels drivers



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

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

Mise sous tension « Séquence POST »



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





BOOT WINDOWS 8

Boot Windows 8 – abandon F8 :

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

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

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

Méthodes accès au menu de démarrage:

- Windows 8 à des comportements automatiques qui affichent automatiquement le menu des options de démarrage chaque fois qu'un problème susceptible d'empêcher le PC de démarrer correctement sous Windows se pose.
- 2. Appel via la Charm bars / Paramètres

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



Soit on demande Modifier les paramètres du PC



Système Windows 8.1 Pro - Cours - ver 1.2 - http://www.cabare.net Page 41 - Michel Cabaré -



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

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

Shutdown /r /o	arrêt immédiat
C:\Users\Administrateur)	>shutdown ∕r ∕o_
Ou encore mieux	
Shutdown /r /o /f /t 0	

Menu Options de démarrage:

Les 3 options de bases toujours présentes sont



e option Nindows 8	Continuer : Si on est ici par inadvertance (ou que le comportement automatique de 8 nous y amène), mais que l'on ne souhaite rien faire,
ou le réinitialiser, ou ncés	Dépannage : C'est lui qui nous intéresse
re PC	Eteindre : Toujours la logique du démarrer / arrêter

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



Menu Options de démarrage - Dépannage:

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



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





Les paramètres de votre ordinateur seront remplacés par leurs valeurs par défaut.

BCDEDIT

BCDEDIT et gestion du magasin :

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

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

Ce magasin ne peut se visualiser qu'avec la commande

bcdedit ou bcdedit /enum ou encore

bcdedit /enum all

Sauvegarde du magasin complet :

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

bcdedit /export <chemin> comme dans

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

et pour le récupérer il faut lancer

bcedit /import <chemin> comme dans

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

Reconstruction du Magasin :

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

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

A éviter tout de même...



Structure du magasin:

	Administrateur : C:\Windows\sy	stem32\cmd.exe
Section Gestionnaire de démarrage :	C:\Users\test>bcdedit Gestionnaire de démarrage Windows	
Bootmgr il permet de gérer le boot et les multi-boot.	identificateur device description locale inherit default resumeobject displayorder toolsdisplayorder timeout	<pre><bootmgr> partition=D: Windows Boot Manager fr-FR {globalsettings> {current> {324e1371-5d1b-11dc-8bf1-d6f4bef89e58> {ntldr> {current> {30</bootmgr></pre>
Section Legacy (éventuellement) renvoi à NTLDR et ancien boot.ini	Chargeur de système d'ex identificateur device path description Chargeur de démarrage Wi	xploitation Windows d'ancienne génération {ntldr} partition=D: \ntldr Version antérieure de Windows indows
Section Chargeur démarrage Windows Winload.exe existe pour chaque version de 8-Seven-2012-2008 installée	identificateur device path description locale inherit nointegritychecks osdevice systemroot resumeobject nx	<pre>{current} {current} partition=C: \Windows\system32\winload.exe Microsoft Windows Vista fr-FR {bootloadersettings} No partition=C: \Windows {324e1371-5d1b-11dc-8bf1-d6f4bef89e58} OptIn</pre>

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

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

Gestionnaire de	démarrage Windows	
identificateur	{bootmgr}	

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

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

contenant notamment les éléments : Device - Path - Description

• Chargeur démarrage Windows / Windows Boot Loader: (un pour chaque installation de 8-Seven, stocké dans \Windows\system32)

Chargeur de démarrage Windows identificateur {current}

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



BCDEDIT commande :

Une aide en ligne est disponible via

Bcdedit / ?

et les commandes sont nombreuses :

🔤 Administrateur : C:\Windows\system32\cmd.exe				
C:\>bcdedit /? /TOPICS				
RUBRIQUE DE CE FICHIER D'AIDE				
Pour afficher l'aide <rubrique> représen</rubrique>	Pour afficher l'aide d'une rubrique, exécutez « bcdedit /? <rubrique> », où ≺rubrique> représente l'une des valeurs suivantes :</rubrique>			
bootdebug	Commande /bootdebug.			
bootems	Commande /bootems.			
bootsequence	Commande /bootsequence.			
copy	Commande /copy.			
create	Commande /create.			
createstore	Commande /createstore.			
dbgsettings	Commande /dbgsettings.			
depug	Commande /debug.			
default	Commande /default.			
	Commande /delete.			
	Commande /deletevalue.			
alsplayorder	Commande /alsplayorder.			
	Commanue /ens.			
emssettings	Commande Zemssettings.			
enun	Commanue Zenum.			
ЕХРОРС ЕОРМАТС	Commanue /export.			
	Identificateuns noum les entmées			
impost	Commande /impost			
set	Commande /set			
stove	Ontion de ligne de commande /stowe			
timeout	Commande /timeout			
toolsdisnlauorder	Commande /toolsdisnlauorder			
TYPES	Types qui s'appliquent à toutes les entrées.			
TYPES BOOTAPP	Types relatifs aux applications de démarrage. Parmi elle	es		
	figurent le gestionnaire de démarrage, l'application de			

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

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

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

bool	Valeur booléenne	. Les valeurs suivantes correspondent à TRUE (vrai) :
	1, ON, YES,	TRUE
	Les valeurs suiv	vantes correspondent à FALSE (faux) :
	Ø, OFF, NO,	FALSE
device	Périphérique, qu	i peut être de l'un des types suivants :
	BOOT PARTITION=<1 FILE=[<paren RAMDISK=[<pa< td=""><td>lecteur> ut>l<chemin> urent>l<chemin>,<idoptions></idoptions></chemin></chemin></td></pa<></paren 	lecteur> ut>l <chemin> urent>l<chemin>,<idoptions></idoptions></chemin></chemin>
	Les options pour	ces types sont :
	<lecteur></lecteur>	Lettre de lecteur suivie d'un deux-points et sans harre oblique inverse à la fin.
	<parent></parent>	(Obligatoire) Peut représenter BOOT ou une lettre de lecteur avec un deux-points. Les crochets n'indiquent pas qu'il est facultatif mais constituent des éléments littéraux de la suntave
	<chemin></chemin>	Chemin d'accès au fichier (ou au fichier .wim) à partir de la racipe du périphérique parent
	<idoptions></idoptions>	de la racine de periphérique Identificateur de l'entrée d'option de périphérique qui contient les options d'image de déploiement du système (SDI) du disque virtuel. Il s'agit en général de {ramdisksdioptions}.
id	Identificateur d des données de c pour plus d'info	l'entrée qui fait référence à une entrée du magasin configuration de démarrage. Exécutez « bcdedit /? ID » prmations sur les identificateurs.



Copier-Dupliquer une entrée du magasin:

Dans notre magasin, avant de modifier l'entrée de Windows 8-Seven (par exemple), nous souhaitons en effectuer une copie...

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

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



Supprimer une entrée du magasin:

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

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

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

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

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

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

bcdedit /delete {ntldr} /f

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

BCDEDIT et Gestionnaire de démarrage - Boot Manager :

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

- cette entrée existe toujours,
- et elle est unique

Gestionnaire de démar	Prage Windows
identificateur	{bootmgr}
device	partition=\Device\HarddiskVolume1
description	Windows Boot Manager
locale	fr-FR
inherit	{globalsettings}
default	{current}
resumeobject	{6900ba1b-1c65-11df-9c4e-9f716fb9c591}
displavorder	{current}
1 3	{6900ba1f-1c65-11df-9c4e-9f716fb9c591}
toolsdisplavorder	{memdiag}
timeout	30

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

bcdedit / ? types bootmgr



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

Système par défaut:

Il faut changer la valeur default {identificateur}

Aide avec bcdedit /default / ?

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

Time-out:

Il faut changer la valeur timeout {entier}

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

Forcer l'affichage du menu de boot:

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

Avec le type voulu derrière

C:\>bcdedit /set /?								
Cette commande déf de configuration d	ette commande définit une valeur d'option d'entrée dans le magasin des données le configuration de démarrage.							
bcdedit [/store <r< td=""><td>nomfichier>] /set [{{id>}] {typedonnées> {valeur></td></r<>	nomfichier>] /set [{{id>}] {typedonnées> {valeur>							
<nomfichier></nomfichier>	Spécifie le magasin à utiliser. Si cette option n'est pas spécifiée, le magasin système est utilisé. Pour plus d'informations, entrez « bcdedit /? store ».							
<id></id>	Spécifie l'identificateur de l'entrée à modifier. S'il n'est pas spécifié, {current> est utilisé. Pour plus d'informations sur les identificateurs, entrez « bcdedit /? ID ».							
<typedonnées></typedonnées>	Spécifie le type de données de l'option qui sera créée ou modifiée. Entrez « bcdedit /? TYPES » pour plus d'informations sur les types de données.							
<valeur></valeur>	Spécifie la valeur à affecter à l'option. Le format de <valeur≻ de="" données="" du="" dépend="" entrez<br="" spécifié.="" type="">« bcdedit /? FORMATS » pour plus d'informations sur les formats de données.</valeur≻>							

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

Comme dans

Bcdedit /set {bootmgr} displaybootmenu on



BCDEDIT et Chargeur de démarrage – Boat Loader :

L'entrée du magasin correspondante est {current}

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

Chargeur de démarrage	e Windows
identificateur	{current}
device	partition=C:
path description	Nyindows Nystem32 Nyinioda.exe Micwosoft Windows Uista
locale	fp-FR
inherit	{bootloadersettings}
nointegritychecks	No
osdevice	partition=C:
systemroot	Windows
resumeobject	{324e1371-5d1b-11dc-8bf1-d6f4bef89e58}
nx	Uptin

Renommer une entrée :

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

Comme dans

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

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

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

Bcdedit /set description « Windows Seven Pro »

donc cela donne

Chargeur de démarrage	Windows
identificateur device path description locale inherit recoverysequence recoveryenabled osdevice systempoot resumeobject nx	<pre> {current}</pre>

et dans l'interface graphique on retrouve

Démarrage et récupération	—X —
Démarrage du système	
Système d'exploitation par défaut :	
Windows Seven Pro	▼
Afficher les systèmes d'exploitation pendant :	30 🚔 secondes
Afficher les options de récupération pendant :	30 secondes



BCDEDIT et Chargeur ancien système – Legacy Boat Loader :

L'entrée du magasin correspondante est {ntldr}

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

Renommer une entrée :

On veut renommer notre « Ancien Windows »

Chargeur	de	système	d'exploitatio	on Windows	d' (ancienne	génération
identific device path descripti	at: ion	eur	{ntldr} partition ∖ntldr Version a	n=D: antérieure	de	Windows	

donc <id> devra prendre la valeur {ntldr}

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

donc cela donne

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

et dans l'interface graphique on retrouve

Démarrage et récupération	×
Démarrage du système	
Système d'exploitation par défaut :	
Vista 6.0 business	-
Windows X.P. sp2	
Vista 6.0 business	ides

BCDEDIT option /store :

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

Imaginons effectuer une copie de notre magasin...

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

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

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

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

Dupliquer une entrée...

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



Utilitaire Bootsect & changement bcdedit / ntldr:

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

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

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

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

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

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

- Windows XP étant installé sur la première partition Active...
- Il faut installer Windows 8 dans une <u>autre</u> partition principale (voire un autre disque), ayant au mois 12 Giga de libre
 Il n'est plus possible de faire cohabiter Windows 8 et Xp dans une même partition.
- Il faut booter sur le CD de Windows 8 (pour désactiver la mise à niveau) et demander d'installer avec les options avancées
- Il faut choisir une nouvelle partition, la formater et lancer l'installation
- N.B : il est conseillé de préparer sa partition disque dur depuis XP, en effet le Setup d'installation de Windows 8 ne donne pas toutes les possibilités de création de partions de reformatage voulues, et parfois refusera une installation sur un disque non préparé (volume dynamiques...)

même disque, autre partition :

Le résultat fonctionne, la partition active est inchangée ! (mais le lettrage est modifié dans Windows 8 qui se trouve



en C : et la partition principale active passe en D :...)

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



autre disque :

Ce sera sans doute le cas le plus fréquent.

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



Disposition

Simple

Simple

Type

De base

Debase NTFS

De base CDFS

NTFS

Système de fichiers

Statut

Sain (Dé

Sain (Sv

Sain (Pa

Le résultat fonctionne, la partition **active** est inchangée! (mais le lettrage est surprenant dans Windows 8 qui se trouve installé en C: et avec la partition principale active décalée en D: ...)

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

<		*
Disque 0 De base 38,29 Go En ligne	(C:) 38,28 Go NTFS Sain (Démarrer, Fichier d'échange, Vidage sur in	ncident, Pai
Disque 1 De base 37,27 Go En ligne	disque-xp (D:) 37,26 Go NTFS Sain (Système, Actif, Partition principale)	11 Mo Non allo

Installer XP à coté de Windows 8

Si vous voulez installer une version antérieure du système d'exploitation Windows sur un ordinateur Windows 8, c'est beaucoup plus complexe, et <u>non garantit</u> <u>sur la fiabilité de l'opération !</u>

Volume

isque-xp (D:)

LRMBVOL FR CD1 (E:) Simple

(C:)

En effet le programme d'installation remplace tout le contenu de la MBR, du secteur de démarrage et des fichiers de démarrage. Par conséquent, la version antérieure du système d'exploitation Windows perd sa compatibilité en aval avec Windows 8.

Supprimer un boot Seven (retour boot Xp):

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

- ✓ Il faut utiliser Bootsect.exe pour restaurer la MBR du disque et le secteur de boot qui transmet le contrôle au Gestionnaire de démarrage Windows ancienne version (NTLDR).
- ✓ II faut effacer toutes traces de Windows 8

On pourrait imaginer le mode opératoire suivant :



Système Windows 8.1 Pro - Cours - ver 1.2 - 1. En invite de commandes :

lecteur:\Boot\ Bootsect.exe -NT52 All

- N.B: lecteur représente le lecteur dans lequel se trouve le media d'installation de Windows 8.
 (Le dossier \Boot figure sur le Média Windows 8.)
- 2. Redémarrez l'ordinateur et donc uniquement Xp apparaît au boot.
- 3. Supprimer la partition sur laquelle Windows 8 était installé
- 4. Faire le ménage des fichiers amenés par Windows 8 sur la partition qui reste (ou se trouve Windows XP) notamment :
 - un dossier **\boot** à la racine (il faut d'abords s'approprier le dossier en NTFS, pour se donner les droits dessus)
 - un fichier **bootmgr** à la racine (il faut d'abords s'approprier le dossier en NTFS, pour se donner les droits dessus)

Supprimer un boot XP (retour boot Seven):

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

- ✓ Il faut utiliser **Bootsect.exe** pour restaurer la MBR du disque et le secteur de boot qui va chercher bootmgr
- ✓ II faut effacer toutes traces de XP
- il faut transférer sur la future partition active les fichiers nécessaire au boot vista (actuellement stockés dans la partition active qui contient xp, vue en D:...) c'est à dire le dossier \boot et le fichier bootmgr
 - N.B: (Le dossier **\Boot** contient une partie de la base de registre sur laquelle Seven est lancé, il faut faire cette manipulation depuis la console de recup Seven Pour que la base ne soit pas lue)
 - N.B: La « console » se lance en bootant sur le CD Seven puis réparer l'ordinateur - dans la boite de dialogue « options de récupération système » suivant, puis invite de commande...
 - N.B: toujours dans La « console » vérifier le lettrage utilisé, en fait il faut repérer les lettre qui correspondent a telle ou telle partition, car <u>ce</u> <u>ne sont pas forcément les mêmes qu'utilise Seven en mode OS</u> <u>normal !</u>

Donc sachant que

dir /A

(affiche fichier- dossier cachés)

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



mkdir C:\Boot D :

xcopy D:\Boot C:\Boot /c /h /o /s /e xcopy D:\bootmgr C:\ /h

(copie de tout le dossier) (copie du fichier)

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

2. Il faut activer la future partition active C : (à la place de l'ancienne D :)

Via dans le gestionnaire de disque, menu contextuel en pointant la partition Marquer la partition comme active

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

lecteur:\Boot\ Bootsect.exe -NT60 All

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

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

Pour que le changement soit effectif, redémarrer le poste

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

Bcdedit /delete {ntldr} /f

Bcdedit /set {bootmgr} device partition=c:

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



LES PROCESSUS SOUS WINDOWS

Séquence POST : Power On Self Test

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



Vocabulaire système sous 8-SEVEN :

Schématiquement on peut distinguer :



- LA HAL Oou couche d'abstraction matérielle : fournie des fonctions pour contrôler le bus système, canaux DMA, déclenchement des interruptions, horloge système... toutes ces fonctions sont utilisées dans les autres parties du noyau
- L'exécutif

 (serveur noyaux) : c'est l'ensemble des services système de gestion mémoire – périphériques –fichiers – appellé donc threads système. Chaque service système progresse à son propre rythme
- les services noyaux sous systèmes environnement

 : il s'agit de supporter différentes interfaces...: win32 – posix – Os2... par exemple l'executif de windows défini un ensemble de fonction nommée API (Access Programming Interface).

 Un programme utilisateur fait appel à des API système pour dialoguer avec l'OS.
- les services noyaux systèmes

 nécessaires comme le spool
 d'impression, task manager ... et les services de sécurité associés
- Certaines applications peuvent utiliser directement des **DLL Dynamic Link** Library... qui elles feront appel si nécessaire aux API système

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



Lister les Processus - graphique:

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

P	Gestionnaire des tâches								-		×	
Fichier O	Fichier Options Affichage											
Processus	Performance	Historique des a	applications	Déma	arrage	Utilisa	teurs	Détails	Services			
63	*					2%		30%	09	6	0	%
Nom			Statut		Proc	esseur	M	émoire	Disqu	e	Rése	au

Plusieurs onglets sont disponibles, l'onglet Processus regroupe

Des Application :

Programme lancé par l'utilisateur, ou lancé automatiquement au démarrage de Windows. Tourne dans une interface fenêtre, normalement sans incidence Fichier Options Affichage

sur le fonctionnement de Windows 8

Des Processus :

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

Processus Performance Historique des applications Démarrage Utilisateurs Déf Statut Nom Applications (3) Bloc-notes Explorateur Windows Gestionnaire des tâches Processus en arrière-plan (7) Application sous-système spouleur Indexeur Microsoft Windows Search 2 KMS Connection Broker Applications (3)

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

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

Bloc-notes	
Explorateur Windows	
👂 🕎 Gestionnaire des tâches	1
Processus en arrière-r	Développer Fin de tâche
Application sous-syst	Valeurs de ressources
👂 🔒 Indexeur Microsoft W	Créer un fichier de vidage
KMS Connection Bro	Accéder aux détails
Processus hôte pour	Ouvrir l'emplacement du fichier

Processus Performa	ance Historiq	ue des applications	Démarrage Utilisateu	rs Déta	ils Services			
Nom	PID	Statut	Nom d'utilisateur	Pro	Mémoire (Description		
wlms.exe	1312	En cours d'exé	Système	00	276 Ko	Service de contrôle des licence		
winlogon.exe	532	En cours d'exé	Système	00	496 Ko	Application d'ouverture de ses		
wininit.exe	468	En cours d'exé	Système	00	372 Ko	Application de démarrage de V		
😰 Taskmgr.exe	2344	En cours d'exé	Administrateur	00	9 768 Ko	Gestionnaire des tâches		
💷 taskhostex.exe	1940	En cours d'exé	Administrateur	00	756 Ko	Processus hôte pour Tâches W		



Système Windows 8.1 Pro - Cours - ver 1.2 -

http://www.cabare.net Page 57 - Michel Cabaré -

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

Fichier Options Affichage						
Processus Performance Historique des applications Démarrage Utilisateurs Détails Services					Services	
Nom	PID	Description	S	tatut		Groupe
SstpSvc TermService		Service SSTP (Secure Socket Services Bureau à distance		Arrêté Arrêté		LocalService NetworkSe
🔍 CryptSvc	484	Services de chiffrement		En cours d'exécution		NetworkSe
😳 Spooler	336	Spouleur d'impression		n cours d'exéc	ution	
🤹 LanmanWorkstati	484	Station de travail	En cours d'exécution		ution	NetworkSe

Arrêter un Processus, un service :

 Fichier
 Options
 Affichage

 Processus
 Performance
 Historique des applications
 Démarrage
 Utilisateur

 Nom
 Statut
 Processeur
 1

 Applications (1)
 Image: Comparison of the state of the

Cela peut se faire soit depuis l'onglet Processus...

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

Fichier Op	tions Affi	chage					
Processus Performance		ce Histori	Historique des applications		Utilisate	eurs Détails	
Nom	*	PID	Statut	Nom d'util	Pro	Mémoire (
👰 Taskmgr.	.exe	2124	En cours d'exé	Administr	00	6 896 Ko	
💷 taskhoste	ex.exe	Fin de t	Fin de tâche 16 Ko				
💷 System		Termin	Terminer l'arborescence du processus 🛛 🖌 😽 😽				

depuis l'onglet Détails... on peut accéder aux services

Fichier Options Affichage							
Processus	Performance	Historiq	ue des applications	Démarrage	Utilisate	eurs Détails	Services
Nom	*	PID	Statut	Nom d'util	Pro	Mémoire (Description
👰 Taskmg	r.exe	2124	En cours d'exé	Administr	02	7 880 Ko	Gestionnaire des tâc
💷 taskhost	ex.exe	1976	En cours d'exé	Administr	00	1 000 Ko	Processus hôte pour
System		4	En cours d'exé	Système	02	72 Ko	NT Kernel & System
🔳 svchost.	exe	652	En cours d'exé	Système	00	1 360 Ko	Processus hôte pour

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



Fichier Options Affichage					
Processus Performance Histo	orique des	applications Démarrage	Utilisateurs	Détails Servio	es
Nom	PID	Description	9	Statut	Groupe
🕼 Power	652	Alimentation	E	En cours d'exé	DcomLaunch
🔍 PlugPlay	652	Plug-and-Play	E	En cours d'exé	DcomLaunch
🔍 LSM	652	Gestionnaire de session lo	cale E	En cours d'exé	DcomLaunch
🔍 DeviceInstall		Service d'installation de pé	riphér A	Arrêté	DcomLaunch
🔍 DcomLaunch	652	Lanceur de processus serv	eur DC E	En cours d'exé	DcomLaunch
BrokerInfrastructure	652	Service d'infrastructure de	s tâch E	n cours d'exé	DcomLaunch
🔍 defragsvc		Optimiser les lecteurs	4	Arrêté	defragsvc

Dans l'onglet Services Performance Historique des applications Démarrage Utilisateurs Détails Services

on peut	Nom	PID	Description		Statut	Gr
Arrêter/Démarrer un	🔍 Power	652	Alimentation		En cours d'exé	De
service: solon son átat	🔍 PlugPlay	652	Plug-and-Play		En cours d'exé	De
Service. Selon son end	🔍 LSM	652	Gestionnaire de session l	ocale	En cours d'exé	De
	🕼 DeviceInstall		Service d'installation	- 2.:1. 2.	A	5c
	🔍 DcomLaunch	652	Lanceur de processu	Démarr	er	De
Et accéder à la	🔍 BrokerInfrastructure	652	Service d'infrastructu	Arrêter		De
gestion des services via	🔍 defragsvc		Optimiser les lecteur	Redéma	arrer	le
Ouvrir les services	🔍 vmicrdv		Service de virtualisati	0		c
	🔍 vmicheartbeat	1712	Service Pulsation Mic	Ouvrir I	es services	c
	C stieve		Acquisition d'image	Rechero	he en ligne	

Gestionnaire de Services

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

Gestionnaire des tâches – 🗖 🗙								
Fichier Options Affichage	e							
Processus Performance H	listorique de	s applications I	Démarrage 🛛 l	Jtilisateurs	Détails S	Services		
Nom	PID	Description			Statut	Gr	oupe	^
WSearch WMPNetworkSvc	1036	Windows Sear Service Partag	rch je réseau du L	ecteu /	En cours d'e Arrêté	xé		~
Moins de détails 🍇	Ouvrir les se	rvices						

Services et applications
 Services
 Contrôle WMI

mais aussi Clic droit - Ordinateur / Gérer / Services



OU Panneau de configuration / Outils d'administration /

🍇 Services				_				
$ \underline{Action} Affichage \underline{]} \leftarrow \rightarrow \implies \boxed{ } \boxed{ \end{array}{ } \boxed{ } \boxed$								
Arbre	Nom 🔺	Description	État	Type de démarrage	C 🔺			
Services (local)	🖓 Affichage des messages	Envoie et reçoit les messages transmis	Démarré	Automatique	Ŀ			
040	🦓 Agent de stratégie IPSEC	Gère la stratégie de sécurité IP et déma	Démarré	Automatique	- D			
	Appel de procédure distante (RPC)	Fournit le mappeur du point de sortie et	Démarré	Automatique	L.			
	Avertissement	Informe les utilisateurs et les ordinateur		Manuel	Li 🔰			
	Carte à puce	Gère et contrôle l'accès à une carte à p…		Manuel	Li 🔰			
	Client de suivi de lien distribué	Envoie des notifications relatives aux fic	Démarré	Automatique	_ L/			
	Client DHCP	Gère la configuration réseau en inscriva	Démarré	Automatique	L)			
	Client DNS	Résout et met en cache les noms DNS.	Démarré	Automatique	Ŀ			
	Configuration sans fil	Permet le contrôle d'accès réseau authe		Manuel	Ŀ			
	Connexions réseau	Prend en charge les objets dans le dossi	Démarré	Manuel	Li			



September 2 - Se Tient à jour une liste des ordinateurs présents sur votre réseau ... Démarré Automatique on peut demander via les propriétés Propriétés de Explorateur d'ordinateur (Ordinateur local) ? × Général Connexion Récupération Dépendances Nom du service : Browser Explorateur d'ordinateur Nom affiché : Tient à jour une liste des ordinateurs présents sur votre Description : Chemin d'accès des fichiers exécutables : C:\WINNT\System32\services.exe Automatique -Type de démarrage : Essentiellement Automatique pour le prochain Manuel Statut du service : Désactivé démarrage dυ poste Arrêter Suspendre Vous pouvez spécifier les paramètres qui s'appliquent pour le démarrage du service. et on peut avoir une idée des dépendances... Propriétés de Explorateur d'ordinateur (Ordinateur local) ? × Général Connexion Récupération Dépendances Certains services dépendent d'autres services. Si un service est arrêté ou ne fonctionne pas correctement, les services dépendants peuvent en être affectés. 線 Serveur Station de travail De qui ce service dépend... Qui dépends de Ces services dépendent de "Explorateur d'ordinateur" 😲 <Pas de dépendances> ce service...

Lister les Processus – invite de commande:

Tasklist (SEVEN - XP):

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

Tasklist

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

Si ces options fonctionnent, les autres options ont l'air plus délicates à utiliser... Tasklist /SVC Tasklist /M



Taskkill (depuis SEVEN - XP):

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

Taskkill

C:\Documents and Settings\Administrateur>taskkill /? IASKKILL [/S système] [/U utilisateur [/P mot_de_passe]]] { [/FI filtre] [/PID ID_processus ¦ /IM image] } [/F] [/T]

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

Taskkill /PID x

Εt

Taskkill /PID x /F

Et

Taskkill /PID x /F /T

Quelques Processus de base

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

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



anciens types 2000 - wdm :

Windows 2000 – wdm

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

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

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

Les Drivers WDF :

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

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



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



Magasin de drivers :

Sous XP, il fallait installer le périphérique avant le driver

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

Depuis SEVEN, il existe deux étapes distinctes

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

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

Mise en place du pilote dans le magasin

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



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

- Si le périphérique n'est pas connecté par des outils comme **pnputil.exe**, **drvload.exe**,
- En modifiant l'image via l'utilitaire **DISM** des outils de déploiement **WAIK-ADK**
- En les déployant avec WSUS
- Si le périphérique est connecté, " à la volée" avec le disque et l'assistant ajout de matériel (mais avec des droits d'administration)

Installation du pilote lors du P&P par Windows 8

- 1. on connecte le périphérique
- 2. le service Plug and Play le détecte
- 3. Windows 8 cherche le pilote dans le magasin, si un pilote est présent, il installe le périphérique sans autres formes de procédure.
- 4. Si un pilote n'est pas présent, Windows cherche dans les chemins fournis MAIS vérifie que l'utilisateur dispose des autorisations nécessaires, et vérifie à la volée le Drivers, avant de le stocker dans le magasin, puis de l'installer.



Stratégies de gestion de drivers :

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

gpedit.msc... Puis

Configuration ordinateur \Modèles d'administration\Système



Drivers certifiés :

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

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

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

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

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

Propriétés de : 3Com EtherL	ink 10/100 PCI TX NIC (3C905B-TX)	×
Général Pilote Détails	Ressources	
3Com EtherLink 10	1/100 PCI TX NIC (3C905B-TX)	Voici un driver accepté par
Foumisseur du pilote :	3Com	Windows datant de
Date du pilote :	04/06/2003	2003 !
Version du pilote :	4.41.0.0	ll est signé
Signataire numérique :	Microsoft Windows Hardware Compatibil Publisher	bility

Installation de pilotes non certifiés :

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

/ Dépannage / Options Avancées / paramètres / F7



Puis F7 - Désactiver le contrôle obligatoire de signature des pilotes



Soit en invite de commande

Bcdedit /set nointegritychecks ON

Administrateur : C:\Windows\system32\cmd.exe

C:\Users\Administrateur>bcdedit /set nointegritychecks ON Opération réussie.

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

identificateur	{current}
device	partition=C:
path	\Windows\system32\winload.exe
description	Windows 8
locale	fr-FR
inherit	{bootloadersettings}
recoverysequence	{c238da97-a685-11e2-9346-ce022367f00a}
integrityservices	Enable
recoveryenabled	Yes
nointegritychecks	Yes
allowedinmemorysettings	0x15000075
osdevice	partition=C:
systemroot	\Windows

Puis redémarrage, et installation du driver non signé...

Pour re-protéger ensuite le système il faut

Bcdedit /set nointegritychecks OFF



et redémarrage

Gestionnaire de périphérique:

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



panneau de configuration le gestionnaire de périphérique :

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







Les familles de périphériques sont listées

(par exemple Cartes graphiques)

Ainsi que leurs composants

(par exemple NVIDIA GeForce 6200)

Versions - Installation de pilotes :

On demande les propriétés du composant sélectionné





Installation driver via Update :

On demande les propriétés du composant sélectionné

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



Puis Afficher les mises à jour installées

Windows Update / Afficher l'historique des mises à jour

 Windows Update

 Rechercher des mises à jour pour l'ordinateur

 Toujours installer les dernières mises à jour pour améliorer la sécurité et les performances de l'ordinateur.
 Rechercher les mises à jour

 Dernière recherche de mises à jour :
 Hier à 10:27

 Des mises à jour ont été installées :
 Hier à 10:28. Afficher l'historique des mises à jour

 Vous avez configuré Windows pour :
 Installer automatiquement les nouvelles mises à jour chaque jour à 03:00 (recommandé)

 Vous recevez les mises à jour :
 Pour Windows et d'autres produits à partir de Microsoft Update

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

3Com - net - 3Com EtherLink 10/100 PCI For Complete PC Management NIC (3C905C-TX
Date d'installation : 12/09/2007 06:56
État de l'installation : Réussite
Type de mise à jour : Recommandée
Driver update provided by 3Com for support of 3Com EtherLink 10/100 PCI For Complete PC Management NIC (3C905C-TX)

Installation driver via Fichiers locaux :

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

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

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

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





Contenant la définition du driver et son installation

W9X90XBC.INF - Bloc-notes		x
Fichier Edition Format Affichage ?		
; This is the Setup information file to ; Copyright (c) 2002 3Com Corporation	install hardware components	Â
[version] signature Compatible Class ClassGUID provider CatalogFile DriverVer	<pre>="\$CHICAGO\$" = 1 = Net = {4D36E972-E325-11CE-BFC1-08002BE10318} = %V_MS% = w9x90xbc.cat = 06/04/2003,04.41.0000.0</pre>	
[Manufacturer] %V_3COM%	= 3COM	Ŧ

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

Mettre à jour le pilote... Mettre à jour le pilote logiciel de ce périphérique.

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

Rechercher automatiquement un pilote logiciel mis à jour Windows va rechercher sur votre ordinateur et sur Internet le pilote logiciel le plus récent pour votre périphérique.	Ne pas demander Rechercher auto car cela revient à Windows Update
Rechercher un pilote logiciel sur mon ordinateur	

Recherchez et installez manuellement le pilote logiciel.

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

F:\3Com\4.41 ✓ Inclure les sous-dossiers		Pa
✓ Inclure les sous-dossiers		
· more is sour obsider		
Me laisser choisir parmi une liste de pilotes	es de nérinhéric	nues sui
intertaisser enoisin parmi ane liste de priotes	.5 de periprierie	1465 54
and the second		

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



Sélectionnez la carte réseau

- . . /

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



A ce moment la Windows décode le xxx.inf

t si nec	essaire nous propose un choix	
	Afficher les matériels compatibles	
	Carte réseau :	
	3Com 3C920 Integrated Fast Ethemet Controller (3C905C-TX Compatible)	
	3Com EtherLink 10/100 PCI For Complete PC Management NIC (3C905C-	TX)
	👾 Ce pilote a une signature Authenticode(tm).	Disque fourni

Méthode par défaut installation de drivers :

Dans les propriétés du poste de travail, paramètres systèmes avancé

puis onglet **Matériel**

Paramètres d'installation des périphériques





Sigverif vérification drivers signés:

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

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



signé

siāné

el90xbc5, svs

storprop.dll



2:6.1

1:4.90.2:5.00

04/06/2003

Microsoft Windows

Microsoft Windows Hardware Compatibility

nt5.cat

w9x90xbc.cat

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

<pre>[c:\windows\system32]</pre>	drivers]		-	
acpi.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
afd.sys	14/07/2009	2:6.1	Signé	nt5.cat
agilevpn.sys	14/07/2009	2:6.1	Signé	nt5.cat
asyncmac.sys	14/07/2009	2:6.1	Signé	nt5.cat
atapi.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
ataport.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
blbdrive.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
cdrom.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
cng.sys	14/07/2009	2:6.1	Signé	nt5.cat
compositebus.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Cl
csc.sys	14/07/2009	2:5.1,2:5.2,2:6.	0,2:Signé	Microsoft-Windows-Of
discache.sys	14/07/2009	2:6.1	Signé	nt5.cat
disk.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
drmk.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Cl
drmkaud.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Cl
dxgkrn1.sys	14/07/2009	2:6.1	Signé	nt5.cat
el90xbc5.sys	04/06/2003	1:4.90,2:5.00	Signé	w9x90xbc.cat
fdc.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co
flpydisk.sys	14/07/2009	2:5.1	Signé	Microsoft-Windows-Co

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

DriverQuery vérification drivers signés:

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

Syntaxe

5

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

Les paramètres les plus intéressants étant

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

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

C:\Users\util>driverquery /si			
DeviceName	InfName	IsSigned	Manufacturer
Volume générique Gestionnaire de volume Pilote d'énumérateur de lecteu	volume.inf machine.inf machine.inf	TRUE TRUE TRUE	Microsoft (Périphériques système st (Périphériques système st

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

C:\Users\util≻driverquery /s 19	92.168.1.10 /u	administ	rateur /p zk29 /si
DeviceName	InfName	IsSigned	Manufacturer
Volume générique	volume.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.inf	TRUE	Microsoft
Cliché instantané de volume gé	volsnap.int	TRUE	Microsoft
Cliche instantane de volume ge	volsnap.inf	IRUE	Microsoft



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

C:\Users\util≻driverquery /s 19	92 .168.1.111 /u	i cabare-i	intra\administrateur	/p zk281 /s
DeviceName	InfName	IsSigned	Manufacturer	
Volume générique Volume générique	volume.inf volume.inf	TRUE TRUE	Microsoft Microsoft	

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

- 🖉 Gestion à distance des tâches planifiées (RPC)
- Gestion à distance des tâches planifiées (RPC-EPMAP)
- Gestion à distance du Pare-feu Windows (RPC)
- Gestion à distance du Pare-feu Windows (RPC-EPMAP)
- Gestion des services à distance (NP-Entrée)
- Gestion des services à distance (RPC)
- 🕑 Gestion des services à distance (RPC-EPMAP)

Gestion à distance des tâches ... Gestion à distance des tâches ... Gestion à distance du Pare-fe... Gestion à distance du Pare-fe... Gestion des services à distance Gestion des services à distance Gestion des services à distance


INTÉGRITÉ WINDOWS 8

les DLL (Dynamic Link Libraries):

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

Plusieurs avantages sont présents :

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

Des inconvénients existent :

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

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

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

WRP Protection des DLL :

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

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

%systemroot%Winsxs

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

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



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

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

sfc - system file checker

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

C:\Users\Adminis	trateur/sfc /help
Vérificateur de Copyright (c) Mi	ressources Microsoft(R) Windows(R) version 6.0 icrosoft Corporation. Tous droits réservés.
Analyse l'intégn les versions inc	rité de tous les fichiers système protégés et remplace correctes par les versions Microsoft appropriées.
SFC [/SCANNOW] [/VERIFYFIL] [/OFFWINDIR= /OFFBOOTDI]	Z∕UERIFYONLY] [/SCANFILE= <fichier>] =<fichier>] <<répertoire connexion="" hors="" windows=""> R=<répertoire connexion="" hors="" windows="">]</répertoire></répertoire></fichier></fichier>
⁄scannow	Analyse l'intégrité de tous les fichiers système protégés et répare les fichiers endommagés dès que possible
∕VERI FYONLY	Analyse l'intégrité de tous les fichiers système protégés, Aucune réparation n'est effectuée.
∕SCANFILE	Analyse l'intégrité du fichier référencé et le répare si des problèmes ont été identifiés. Spécifiez le chemin d'accès commilet dans «fichier».
VERIFYFILE	Vérifie l'intégrité du fichier ayant comme chemin complet {fichier} Aucune réparation p'est effectuée
∕OFFBOOTDIR	Pour les réparations hors connexion, spécifier l'emplacement du répertoire de démarrage hors connexion.
∕OFFWINDIR	Pour les réparations hors connexion, spécifier l'emplacement du répertoire Windows hors connexion.

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



UAC-USER ACCOUNT CONTROL

Objectif Visé :

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

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

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

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

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

IL – Integrity Level :

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

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

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

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

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

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



Propriétés de snagit32.exe	X
Général Compatibilité Sécurité Détails Versions précédentes	
Si vous rencontrez des problèmes avec ce programme alors qu'il fonctionnait correctement sur une version antérieure de Windows, sélectionnez le mode de compatibilité adapté à cette version antérieure.	
Mode de compatibilité	
Exécuter ce programme en mode de compatibilité pour :	
Windows XP (Service Pack 2)	
Paramètres	51
Exécuter en 256 couleurs	
Exécuter avec une résolution d'écran de 640 x 480	
Désactiver les thèmes visuels	
Désactiver la composition du Bureau	
Désactiver la mise à l'échelle de l'affichage pour les résolutions élevées	
Niveau de privilège	
Exécuter ce programme en tant qu'administrateur	

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

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

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



Dans cette optique pax exemple, lorsque

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

lexplorer : avec un II d'utilisateur (pour stocker ses favoris...)

lexplorer : avec un II bas pour executer les activex et autres...

P				Gestionnaire des	tâches			×
Fichier Op	otions Afficha	age						
Processus	Performance	Histori	que des applications	Démarrage Utilisat	eurs Dét	ails Services		
Nom	*	PID	Statut	Nom d'utilisateur	Pro	Mémoire (Description	^
dwm.exe	2	740	En cours d'exé	DWM-1	00	18 480 Ko	Gestionnaire de fenêtres du Bureau	
📄 explorer.	exe	1928	En cours d'exé	Administrateur	00	22 988 Ko	Explorateur Windows	
🤮 iexplore.	exe	2936	En cours d'exé	Administrateur	00	4 460 Ko	Internet Explorer	
🥘 iexplore.	exe	3024	En cours d'exé	Administrateur	00	5 824 Ko	Internet Explorer	

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



Gestion de l'UAC (panneau de configuration):

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

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

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

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

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



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



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



Gestion de l'UAC (stratégies locales):

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

Dans le Panneau de Configuration / Outils d'administration /

🐨 Outils d'administration

Puis Stratégies de sécurité locales 📠 Stratégie de sécurité locale

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

🚡 Paramètres de sécurité	Stratégie
Stratégies de comptes	Contrôle de compte d'utilisateur : mode Approbation administrateur pour le compte Adminis
a 📴 Stratégies locales	Contrôle de compte d'utilisateur : passer au Bureau sécurisé lors d'une demande d'élévation
District Stratégie d'audit	Contrôle de compte d'utilisateur : autoriser les applications UIAccess à demander l'élévation sur
Attribution des droits utilisateur	Contrôle de compte d'utilisateur : comportement de l'invite d'élévation nour les administrate
Options de sécurité	Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les utilisateurs st
Pare-feu Windows avec fonctions av	Contrôle de compte d'utilisateur : comportement de l'invite d'elevation pour les duissateurs st
Stratégies du gestionnaire de listes d	Contrôle de compte d'utilisateur : detecter les instanations d'applications et demander relevat
Stratégies de clé publique	Controle de compte d'utilisateur : elever uniquement les applications DiAccess installees a des
Stratégies de restriction logicielle	Controle de compte d'utilisateur : elever uniquement les executables signes et valides
Stratégies de contrôle de l'applicatio	Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approba
Stratégies de sécurité IP sur Ordinate	Contrôle de compte d'utilisateur : virtualiser les échecs d'écritures de fichiers et de Registre da
Configuration avancée de la stratégi	📓 Contrôleur de domaine : conditions requises pour la signature de serveur LDAP

Désactivation de l'UAC :

Sans doute le plus ... radical

🖾 Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur





N.B : re-démarrage du PC obligatoire

Désactivation de l'UAC pour les Administrateur :

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

📓 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Ad..

Propri	étés de : Contrôle de compte d'utilisateur : c	?
Param	ètre de sécurité locale Expliquer	
	Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	
	Demande de consentement pour les binaires non Windows	~
	Élever les privilèges sans invite utilisateur Demande d'informations d'identification sur le bureau sécurisé Demande de consentement sur le bureau sécurisé Demande d'informations d'identification Demande de consentement Demande de consentement pour les binaires non Windows	6

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

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



http://www.cabare.net Page 78 - Michel Cabaré -

Désactivation l'UAC pour les Utilisateurs :

Lorsque les logiciels anciens deviennent incompatibles

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

Activation I'UAC aussi pour le compte Administrateur Root :

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

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

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

DONC... il ne faut jamais utiliser le compte Administrateur intégré pour travailler avec Windows 8, puisque un compte administrateur "autre" bénéficiera de l'effet protecteur de l'UAC sans occasionner de gêne (il suffit de demander une élévation de privilège silencieuse).

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

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



INSTALLATIONS ET VIRTUALISATION

Préconisation microsoft :

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

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

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

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

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

Virtualisation des processus :

Si un programme d'installation se lance sans tous les droits administrateurs comme il va tenter d'écrire dans des dossiers systèmes ou protégés il court à l'échec. Pour prévoir ce type de problème, Microsoft a créé tout un système de virtualisation de dossier dans Windows 8.

- Sous Windows XP, dans un environnement limité, vous lanciez l'installation jusqu'au moment où un fichier a besoin d'être écrit dans un espace protégé Cette opération va faire "crasher" l'installation rendant le logiciel à moitié installé et donc inutilisable
- Windows 8 déroule toute l'installation pour savoir si il a besoin d'aller écrire dans les dossiers système ou des parties réservées du registre. Si c'est le cas, et que l'installateur n'a pas les autorisations suffisantes, alors un système de dossiers virtuels est mis en place.

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

Ensuite une application, devant être exécutée avec les privilèges administrateur parce qu'elle va écrire dans **Program Files** ou dans la clef de registre **HKLM**, est exécutée avec un jeton "restreint", il n'y aura aucune erreur de la part du système.



Lors du lancement de l'application, celle-ci ira dans un premier temps regarder dans le dossier virtuel du profil, et si elle ne trouve rien, elle chargera les paramètres dans le Program Files réel. Grâce à ce système, près de 90% des applications non réécrites pour Windows 8 allant écrire dans **Program Files** ou dans des dossiers systèmes fonctionnent. On parle de « **programmes hérités** »

Windows 8 traite un processus comme « virtualisable » si :

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

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

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

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

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

				1				
Processus Performance	Histo	rique des applic	ations	Démarrage	Utilisate	urs Détails	s Services	
Nom	PID	Statut		Nom d'utilisa	teur	Proc	Mémoire (Description
os. cmd.exe	1540	En cours d'é	exé	Administrate	ur	00	384 Ko	Interpréteur
os. conhost.exe	1016	En cours d'é	exé	Administrate	ır	00	916 Ko	Hôte de la f
Csrss.exe	368	En cours		Sélectio	onner d	es colonn	nes 🛛 🗙	ocessus d
csrss.exe	3016	En cours						ocessus d
💷 dwm.exe	1416	En cours	Sélec	tionnez les colon	ines qui a	pparaîtront d	lans la table.	stionnair
🥃 explorer.exe	1544	En cours						plorateur
Interruptions système	-	En cours		Octets de lecture	e d'E/S		^	pels de p
sass.exe	540	En cours		Octets d'écriture	d'E/S	-		cal Secur
MsMpEng.exe	1204	En cours		Octets d'autres (opération	s d'E/S		ntimalwar
Processus inactif du		En cours	En cours				urcentag	
🔏 SearchIndexer.exe	1596	En cours	cours Contexte du système d'exploitation				dexeur M	
services.exe	512	En cours					plication	
smss.exe	280	En cours		Élevé				stionnair
spoolsv.exe	736	En cours	urs Virtualisation du contrôle de compte d'utilisateur				plication	
SppExtComObj.Exe	1984	En cours		escription				IS Conne
sppsvc.exe	1468	En cours		Prévention de l'e	xécution	des données	×	rvice de l
Nant Processus Performance H	listorique	e des applications	Dém	arrage Utilisater	urs Détai	ls Services		/
Nom F	DID :	Statut	Nom	d'utilisateur	Proc	Mémoire (. Virtualisation	Descriptio
cmd.exe 1	540	En cours d'exé	Admi	nistrateur	00	384 Ko	Non autorisé	Interpréte
conhost.exe 1	016	En cours d'exé	Admi	nistrateur	00	916 Ko	Non autorisé	Hôte de la
csrss.exe 3	68	En cours d'exé	Systèr	me	00	832 Ko	Non autorisé	Processus
csrss.exe	016	En cours d'exé	Systèr	me	00	908 Ko	Non autorisé	Processus

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



COMPATIBILITE AVANT WINDOWS 8

Exécuter en mode compatibilité:

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

RDISK 23/03/2005 10:17 Application

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

0	Propriétés de : Bginfo.exe	×	
Généra	Compatibilité Signatures numériques Sécurité Détails		
Sice p de Wi compa	programme ne fonctionne pas correctement sur cette version ndows, essayez en lançant la résolution des problèmes de atibilité.		
Lar	ncer la résolution des problèmes de compatibilité		
Comm	ent choisir manuellement les paramètres de compatibilité ?		
Mod	le de compatibilité		
E	Exécuter ce programme en mode de compatibilité pour :		
Wir	ndows XP (Service Pack 3) V		
Para	amètres		
	Mode couleur réduit		
Соц	aleur 8 bits (256) 🗸 🗸		
E	Exécuter avec une résolution d'écran de 640 x 480		
	Désactiver la mise à l'échelle de l'affichage pour les ésolutions élevées		
Nine			
	Exécuter ce programme en tant qu'administrateur		
N	Nodifier les paramètres pour tous les utilisateurs		
	OK Annuler	Appliquer	
npe	ut specifier		
•	si il y a besoin d'exécuter avec un pr	ivilège d'administrateu	r
•	On peut choisir un mode de compat	ibilité	
	Mode de compatibilité		
	Exécuter ce programme en mode de compatibilité pour :		
	Windows XP (Service Pack 3)		
	Windows 95		
	Windows 98 / Windows Me Windows XP (Service Pack 2)		
	Windows XP (Service Pack 3) Windows Vista		
	Windows Vista (Service Pack 1)		
	Windows Vista (Service Pack 2) x 480		



Séquence possible:

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

Il se peut qu'il faille désactiver l'UAC

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



PROTECTION DEP

Principe DEP Data Execution Prevention:

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

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

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

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

Désactivation Complète de DEP :

La fonctionnalité DEP, permettant de sécuriser Windows 8 contre les virus, peut être responsable de crashs intempestifs sur votre système

bcdedit.exe /set {current} nx AlwaysOff

Puis re démarrage

La réactivation de la protection se fait par

bcdedit.exe /set {current} nx Optin

(et re démarrage)

Désactivation pour une application de DEP :

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

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

P	ropriétés système			
	Nom de l'ordinateur			Matériel
	Paramètres système avancés	Protection du	u système	Utilisation à distance
	Vous devez ouvrir une session ces modifications. Performances	n d'administrat	eur pour eff	ectuer la plupart de
	Effets visuels, planification d mémoire virtuelle	u processeur,	utilisation d	e la mémoire et
				Paramètres



onglet "prévention de l'exécution des données".

Options de performances	×
Effets visuels Avancé Prévention de l'exécution des données	
La prévention de l'exécution des données vous aide à vous protéger des virus et autres risques de sécurité. <u>Comment cela fonctionne-t-il ?</u>	
 Activer la prévention d'exécution des données pour les programmes et les services Windows uniquement 	
 Activer la prévention d'exécution des données pour tous les programmes et les services, sauf ceux que je sélectionne : 	
Ajouter Supprimer Le processeur de votre ordinateur prend en charge la prévention de l'exécution des données au niveau matériel.	
OK Annuler Appliquer	

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



Windows Recovery Environnement:

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

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

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

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

Pourquoi ? Les raisons sont multiples :

- L'accès à une procédure de réparation demandant une authentification stockée dans la base de regitre du poste à Secourir suppose que celui-ci ne soit pas trop gravement atteint (et que donc sa base de registre soit toujours lisible !)
- La sécurisation des données par mot de passe local ont démontré leurs limites lors des attaques réelles, et donc ne protège pas réellement. Désormais la sécurité des données passe par des procédés de chiffrement
 - 1. renforcement du système EFS
 - 2. Algorithme de chiffrement plus robustes
 - 3. Apparition de BitLocker associant chip TPM et clé USB

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



Démarrer l'environnement de récupération WinRE:

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



Puis on demande Réparer l'ordinateur

<u>1</u>	Installation de Windows
	Windows [.] 8
	Inst <u>a</u> ller maintenant
	Déo aras l'asdiosteur
	Reparer Toroinateur In © 2012 Microsoft Corporation. Tous droits réservés.



et on tombe sur le menu options de démarrage



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





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

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

à ce niveau on peut avoir des :

- Problème HARDWARE
- Problèmes dans la Partition MBR du disque
- Fichiers de démarrage absents endommagés
- 2. **ETAPE 2** : « rond » jusqu'à l'ouverture de session.

à ce niveau on peut avoir des :

- Problème HARDWARE
- Pilotes Services defectueux mal configurés
- 3. **ETAPE 3** : Après l'ouverture de session.

à ce niveau on peut avoir des :

- Programmes de démarrages
- Programmes instancés automatiquement

Les méthodes de récupérations diffèrent selon les étapes de défaillance

Etape 1 séquence POST

Les problèmes à ce niveau peuvent être matériels ou logiciels:

Problèmes hardware

Les causes fréquentes peuvent être

- des problèmes mémoire:
- des problèmes de disque dur

On peut essayer de "prévenir" une panne de disque dur... Windows 8 peut s'interfacer avec la technologie SMART des disques récents pour informer l'administrateur de l'état d'un disque dur... dans l'observateur d'évènement on trouve donc une trace des rapports consigné par cette technologie.

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

soit en interface graphique,

Dossiers	~	🐲 Propriétés de Disque local (C:)
Bureau Administrateur Administrateur Public Codinateur Eccteur de disquettes (A:) Cisque local (C:) Cisque local (C:)	4 III	Général Outils Matériel Partage Sécurité Versions précédentes Quota Vérification des erreurs Cette option vérifiera le volume. Image: Cette option vérifiera le volume. </td



Problèmes partition- mbr-fichiers manquants

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



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

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

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

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

C:\	Invite de commandes Utiliser l'invite de commandes pour un dépannage avancé

Notamment avec BootRec.exe (en invite de commande) suivit des options

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

Cf chapitre suivant "WinRE console de récupération"

Etape 2 affichage du « rond » avant session

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

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

€	Réparation automatique
	Choisir un système d'exploitation cible.
	Windows 8

On peut surtout tenter de passer par les "options de démarrage" / options avancées /- paramètres ex F8 (Cf chapitre suivant "Options de démarrage F8")

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



Etape 3 après l'ouverture de session

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

Stratégies de groupe, Scripts de démarrage, programmes/services en HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run PKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run PKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run ProgramData\Microsoft\Windows\Start Menu\Programmes\Démarrage X:\User\%username%\AppData\RoamingMenu\Microsoft\Windows\ Start Menu \ Programmes\Démarrage

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

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



WINRE - CONSOLE DE RECUPERATION

invite de commande:

L'accès aux outils manuels est toujours disponible

C-4.	Administrateur : X:\windows\SYSTEM32\cmd.exe	×
Microsoft Wir	ndows [version 6.2.9200]	^
X:\Sources>_	▶	

Les commandes disponibles sous Windows RE sont les suivantes :

Console Récupération XP	Windows RE
ATTRIB	
ватсн	
CD	
CHDIR	
СНКДЅК	marque les secteurs défectueux
CLS	
СОРҮ	
DEL	
DELETE	
DIR	
DISABLE	Plus disponible
DISKPART	
ENABLE	Plus disponible
EXIT	
EXPAND	
FIXBOOT	BootRec /Fixboot
	écrire le nouveau code du secteur de démarrage de Windows
FIXMBR	BootRec /FixMbr
	réparer le secteur de démarrage principal
FORMAT	
HELP	
LISTSVC	Plus disponible
LOGON	Plus disponible
МАР	Diskpart
MD	



http://www.cabare.net Page 92 - Michel Cabaré -

MKDIR	
MORE	
RD	
REN	
RENAME	
RMDIR	
SYSTEMROOT	
ТҮРЕ	

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

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

Modifier les partitions - Utilitaire Diskpart

Depuis Vista, il est possible de modifier la taille des partitions sans perdre leur contenu. Cela peut par exemple faire de la place pour une installation de Windows 8 sur une machine ou XP utilise tout le disque dur....

L'utilitaire Diskpart en ligne de commande est accessible :

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

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

On sort de l'utilitaire via exit



Shrink Diskpart – réduire une partition

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

C:\Users\Admin	nistrateur≻diskj	part					
Microsoft DiskPart version 6.0.6000 Copyright (C) 1999-2007 Microsoft Corporation. Sur l'ordinateur : PC-DE-TEST							
DISKPART> list	t disk						
Nº disque	Statut	Taille	Libre		Dyn	GPT	
Disque Ø	En ligne	37 G oc	tets	1689 K	octet	s	

Ensuite II faut sélectionner le disque 0

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



http://www.cabare.net Page 93 - Michel Cabaré - On demande de lister les partitions

DISKPART> list p	artition		
N ^o partition	Туре	Taille	Décalage
Partition 1	Principale	37 G	1024 K

Ensuite II faut sélectionner la partition 1

DIS	SKPART> se	lect	t pa	rtition=1			
La	partition	1ε	est	maintenant	la	partition	sélectionnée.

On demande de lister les volumes

DISKPART> lis	t vol	ume					
N ^o volume	Ltr	Nom	Fs	Туре	Taille	Statut	Info
* Volume Ø Volume 1	C D		NTFS	Partition DVD-ROM	37 G Ø o	Sain Ø média	Système

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

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

On peut demander de récupérer par exemple 10G via

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

Extend Diskpart - étendre une partition

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

DISKPART> extend size=5000

Outil mdsched





CREATION DE WINRE SUR CD - USB

Création CD WinRe

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

Nécupération de fichiers Windows 7

On demande Créer un disque de réparation Système



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



Création Lecteur USB

Via le menu panneau de Configuration / Récupération

🌮 Récupération

On demande Créer un lecteur de récupération



Copie des utilitaires

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



TEST MEMOIRE

Depuis Windows 8

Via le menu panneau de Configuration / Outils d'administration

On demande **Diagnostic de mémoire Windows**

Analyseur de performances
 Configuration du système
 desktop.ini
 Diagnostic de mémoire Windows



F1 permet d'executer des tests plus complets...

Correspondant à l'outil mdsched.exe



PARAMETRES DE DEMARRAGE – EX F8

Accès aux options avancées :

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

/ Dépannage / Options Avancées / paramètres / F4



Options principales :

Dans l'ordre d'intêret

F4 - Mode sans Echec (avec ou sans réseau) :

permet de lancer uniquement le noyau et les drivers principaux

Utilisation : après une installation posant problème, on peut prendre la main « a minima »



F6 - Invite de commande en mode sans Echec :

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

F2 Activer la journalisation au demarrage :

permettant de Créer un journal spécifique de tous les pilotes et services chargés ou non par le système

Utilisation : Fichier journal Ntbtlog.txt dans le dossier racine de Windows 8



F3 Activer la video en basse résolution :

pilote VGA en 640x480

F7 Désactiver le contrôle obligatoire de la signature des pilotes :

permet d'installer des drivers non signés

F8 Désactiver la protection du logiciel anti-programmes malveillants:

permet de ne pas langer windows defender et autres



ACTUALISER – REINITIALISER LE PC

Menu Options de démarrage - Dépannage:

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



Actualiser votre PC:

Sont sauvegardés

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

Ne sont pas sauvegardés

• Paramètres Pare-Feu

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

🕖 Applications supprimées.html





Applications supprimées lors de la restauration des performances de votre PC

Nom de l'application		Éditeur	Version
Adobe Reader X (10.1.0) MUI		Adobe Systems Incorporated	10.1.0
IZArc 4.1.6		Ivan Zahariev	4.1.6
Kit d'évaluation et de déploiement	R	Microsoft Corporation	8.59.25584
McAfee Agent		McAfee, Inc.	4.6.0.2988
McAfee VirusScan Enterprise		McAfee, Inc.	8.8.03000
Microsoft Baseline Security Analyzer 2.2		Microsoft Corporation	2.2.2170
Microsoft SQL Server 2008 Setup Support Files		Microsoft Corporation	10.1.2731.0



Image personalisée Recimg:

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



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

C:\Users\Admini:	strateur>reci	ng /showcurrent	-
Aucune image de Code d'erreur :	récupération 0x80070490	personnalisée	active.

On crée une image via la commande

recimg /createimage c:\temp

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



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

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

Une fois la commande terminée

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

on peut vérifier de nouveau par recimg /showcurrent

C:\Users\Administrateur>recimg /showcurrent \\?\GLOBALROOT\device\harddisk0\partition1\temp RecImg : opération terminée

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

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

recimg /setcurrent c:\temp-new

Réinitialiser votre PC:

Rien n'est sauvegardé

- Ni les données
- Ni aucune application

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





REINSTALLER COMPLETEMENT

Réinstaller le système :

Il est possible de réinstaller complètement Windows 8 (en raison de l'apparition de dysfonctionnements du système par exemple) sans reformater la partition d'origine système

Installer Windows	X
La partition sélectionnée contient peut-être les fi précédente. Dans ce cas, ces fichiers et dossiers s nommé Windows.old. Vous pourrez accéder aux mais vous ne pourrez pas utiliser votre la précéde	ichiers d'une installation Windows seront placés dans un dossier informations de Windows.old, ente version de Windows.
	OK Annuler

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

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



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

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

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



LES TUILES DE L'ACCUEIL

Ecran Accueil par défaut

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



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



Les tuiles suivantes peuvent apparaître :

Courrier IE Windows Store Bing Calendrier Cartes Skydrive



Gestion des tuiles pré-définies en Powershell

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

Σ	Administrateur : Windows PowerShell	
PS C:\Users\Administrateur> get-module -ListAvailable		
	Répertoire : C:\Windows\system32\WindowsPowerShell\v1.0\Modules	

On importe le module

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

On peut vérifier les les commandes importées par un

(Get-Module appx).exportcommands

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

Кеу	Value
Add-AppxPackage	Add-AppxPackage
Get-AppxPackage	Get-AppxPackage
Get-AppxPackageManifest	Get-AppxPackageManifest
Remove-AppxPackage	Remove-AppxPackage
Get-AppxLastError	Get-AppxLastError
Get-AppxLog	Get-AppxLog

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

Get-AppxPackage

(respectivement Get-appxprovisionedPackage –online)

Name	<pre>: windows.immersivecontrolpanel</pre>
Publisher	: CN=Microsoft Windows, O=Microsoft Corporation,
Architecture	: Neutral
ResourceId	: neutral
Version	: 6.2.0.0
PackageFullName	: windows.immersivecontrolpanel_6.2.0.0_neutral_
InstallLocation	: C:\Windows\ImmersiveControlPanel
IsFramework	: False
PackageFamilyName	🔹 windows.immersivecontrolpanel_cw5n1h2txyewy 👘
PublisherId	: cw5n1h2txyewy
Name	: WinStore
Publisher	: CN=Microsoft Windows, O=Microsoft Corporation,
Architecture	: Neutral
ResourceId	: neutral
Version	: 1.0.0.0
PackageFullName	: WinStore_1.0.0.0_neutral_neutral_cw5n1h2txyewy
InstallLocation	: C:\Windows\WinStore
IsFramework	: False
PackageFamilyName	: WinStore_cw5n1h2txyewy
PublisherId	: cw5n1h2txyewy
Name	: Microsoft.BingFinance
Publisher	: CN=Microsoft Corporation, O=Microsoft Corporat
Architecture	: X64
ResourceId	:
Version	: 1.2.0.135

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

Remove-AppxPackage fullname

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

puis pour les autres users (a venir...)

Remove-AppxProvisionedPackage -online -PackageName:fullname

Path : Online : True <u>Restar</u>t Needed : False

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



PS C:\Users\Administrateur> Remove-AppxProvisionedPackage -online

http://www.cabare.net Page 105 - Michel Cabaré -

-PackageName Microsoft.BingFinance_1.2.0.135_x64__8

On peut supprimer sans état d'ames les packages suivants





Voire si on supprime en plus



les 4 sont supprimables via

microsoft.windowscommunicationsapps_16.4.4206.722_x64__8wekyb3d8bbwe





microsoft.microsoftskydrive_16.4.4204.712_x64__8wekyb3d8bbwe

ce qui devient assez radical...



Epingler des tuiles sur l'accueil

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



Gestion Windows Store

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



on pourra par stratégie

gpedit.msc

Configuration Utilisateur / Modèles d'administration / Composants Windows





chercher l'entrée Windows Store

Windows PowerShell	Windows Store	
Windows Store	Désactiver l'application Windows	Paramètre
Dossiers partagés	Store	Désactiver l'application Windows Store

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

stratégies de sécurité locale /



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

🗟 Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur	Activé
donc	
Paramètre de sécurité locale Expliquer	
Contrôle de compte d'utilisateur : exécuter les comptes d'administrateurs en mode d'approbation d'administrateur	
Activé	
◯ Désactivé	
même si on peut demander une élévation automatique, donc	
📓 Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Admini	Élever les privilèges sans invite
donc	
Paramètre de sécurité locale Expliquer	
Contrôle de compte d'utilisateur : comportement de l'invite d'élévation pour les administrateurs en mode d'approbation Administrateur	

v

Élever les privilèges sans invite utilisateur



Système Windows 8.1 Pro - Cours - ver 1.2 - http://www.cabare.net Page 108 - Michel Cabaré -
POINTS DE RESTAURATION

Nom de l'ordinateur

Paramètres système avancés

Restaurer le système

Principe Restauration - désactivation-

Les points de restauration sont créés par le système, et permettent une

Propriétés système

mémorisation d'un état du système, à un instant donné. Leur utilisation est permet de "retrouver" un système dans un état passé.

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

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

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

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



Protection du système

Utilisez la protection du système pour annuler des modifications système non souhaitées et restaurer des versions précédentes de

fichiers. Qu'est-ce que la protection du système ?

x

Matériel

Utilisation à distance

Désactivation de la Restauration

Il faut demander Configurer	A Protection système pour Disque local (C:)
Puis au choix	Paramètres de restauration La protection du système peut conserver des copies de paramètres système et de versions précédentes de fichiers. Sélectionnez ce qui sera à restaurer : Restaurer les paramètres système et les versions précédentes des fichiers Ne restaurer que les versions précédentes des fichiers Désactiver la protection du système
N.B: L'espace disque disponible pour la restauration est ajustable, et détermine le nombre de point de restauration qui peuvent être crées. (la config par défaut peut stocker plusieurs semaines de points de restauration.)	Utilisation de l'espace disque



Création d'un point de restauration

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

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

aramètres de protection	
Lecteurs disponibles	Protection
🏭 Disque local (C:) (Système)	Activée
Configurez des paramètres de restaura l'espace disque et supprimez des poin restauration.	ition, gérez ts de Configurer
Créez un point de restauration immédia pour les lecteurs dont la protection du est activée.	stement système Créer 🗲

un assistant nous demande de nommer le point

Protection du système	
Créez un point de restauration	
Entrez une description pour vous aider à identifier le point de restauration. La date et l'heure actuelles sont ajoutées automatiquement.	Protection du système
test-formation	Le point de restauration a été créé.
Créer Annuler	Eermer
puis on demande Créer et on devrait obt	enir

Utiliser Annuler un point de restauration

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



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

Choisir un point de restau La restauration du systèn par ailleurs, le processus	ration ne n'entraîne aucune modification ou suppression de vos documents ; est réversible.	Ń
Cliquez sur le point de restaur	ation à utiliser, puis sur Suivant. <u>Comment choisir un point de restaurat</u>	ion ?
Fuseeu boraire actuel : Darie	Madrid	
rusedu nordire actuer. Paris,		
Date et heure	Description	
20/03/2008 16:00:10	Description Manuelle : suite-formation	
20/03/2008 16:00:10 20/03/2008 15:58:46	Description Manuelle : suite-formation Manuelle : test-formation	



Afficher d'autres points de restauratio	Red	hercher les programmes concernés	
	< Précé	ident Suivant > Annuler	
A titre d'information, p le choix du point de	oour aider dans Restauration, le	Restaurer le système Description : test-formation	
bouton Rechercher le concernés est assez uti	es programmes le	Date : 18/03/2010 16:03:39 Les programmes qui ont été ajoutés depuis la création du de seront supprimés et ceux qui ont été supprimés seront resta Programmes et pilotes qui seront supprimés :	rnier point de restauration uurés.
apràs quair chaisit	il cuffit do	Description	Туре
demander suivant		Services Bureau à distance Microsoft (Printer) 06/21/20	Pilote
🌮 Restauration du système			
	Confirmer le poir Votre ordinateur sera re dans le champ Descripti Date et heure : 18/0	nt de restauration estauré dans l'état où il était avant l'événement ion ci-dessous.)3/2010 16:03:39 (Paris, Madrid)	
	Description : Manu Lecteurs : Dis	eque local (C:) (Système)	

Eventuellement préciser le lecteur, puis confirmer

Annuler une restauration

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

Types de point de restauration

3 Types de points de restauration existent

- 1. **Points contrôle système** : crées toutes les 24 heures, et après 10 heures de fonctionnement à la suite.
- Points de restauration d'installation de programmes / pilotes: crées lors d'une installation de programme, évidemment, mais aussi lors des mises à jours automatiques de Seven, de récupération à l'aide de l'utilitaire de sauvegarde..

N.B: lors de la restauration suite à une installation défaillante, l faut savoir que les fichiers éventuels de l'application ne sont pas supprimés... seules les entrées dans le registre sont effacées.

3. Points manuels : crée par l'utilisateur.



Paramétrages des point de restauration : Vssadmin

Ce paramétrage se fait via une commande en ligne

Vssadmin

On peut demander un état des lieux via

Vssadmin list shadowstorage

C:\Users\Administrateur>vssadmin list shadowStorage vssadmin 1.1 - Outil ligne de commande d'administration du service de cliché instantané de volume (C) Copyright 2001-2005 Microsoft Corp. Association de stockage de cliché instantané Pour le volume : (C:>\\?\Volume{a5248ba1-f05e-11dc-af8a-806e6f6e6963}\ Volume de stockage de cliché instantané : (C:>\\?\Volume{a5248ba1-f05e-11dc-a f8a-806e6f6e6963}\ Espace du volume de stockage de cliché instantané utilisé : 400.016 MB. Espace du volume de stockage de cliché instantané : 5.59 GB Association de stockage de cliché instantané Pour le volume : (D:>\\?\Volume{d99de527-f67a-11dc-8173-0080c8e6c311}\ Volume de stockage de cliché instantané : 5.97 GB Association de stockage de cliché instantané Pour le volume : (D:>\\?\Volume{d99de527-f67a-11dc-8173-0080c8e6c311}\ Volume de stockage de cliché instantané : (D:>\\?\Volume{d99de527-f67a-11dc-8 173-0080c8e6c311}\ Espace du volume de stockage de cliché instantané : (D:>\\?\Volume{d99de527-f67a-11dc-8 173-0080c8e6c311}\ Espace du volume de stockage de cliché instantané : (D:>\\?\Volume{d99de527-f67a-11dc-8 173-0080c8e6c311}\ Espace du volume de stockage de cliché instantané : 300 MB. Espace maximal du volume de cliché instantané : 1.465 GB

l'option la plus intéressante est

Vssadmin resize shadowstorage



Comme dans

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

avec

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

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

/MaxSize= permet de spécifier la taille maximale allouée



SAUVEGARDE SYSTEME - FICHIERS

Deux Outils de Sauvegarde :

Windows 8 propose deux nouveaux types de sécurisation pour votre machine:

- Une sauvegarde type image disque (configuration complète)
 A L'initiative de l'utilisateur
 Automatisable via l'utilitaire wbadmin.exe
- Une sauvegarde type fichier (récupération des versions précédentes)
 A l'occasion des points de restauration (s'ils sont en place),

Lors de la sauvegarde Windows (si elle est effectuée ou programmée)

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

Image système - vhd :

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

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

Via le menu panneau de Configuration / Historique des fichiers

🖟 Historique des fichiers

On demande Créer une image système



Ici avec Sauvegarde d'image système un assistant se déclenche

<section-header><form></form></section-header>		Créer une image système			
In image systeme est une copie des lecteurs nécessaires à l'exécution de Windows. Elle peut auxis profession de libre: Image systeme est une copie des lecteurs nécessaires à l'exécution de Windows. Elle peut auxis profession de libre: Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une copie des lecteurs : 1/10/2014 08:16:16 Image systeme est une image systeme Image systeme est une image systeme est une systeme est une de less spons codes a lecteurs : 1/10/10/11/10/11 Image systeme est une image systeme est une une de less spons acceder a lecteurs : 1/10/10/11 Image: Image: Image systeme est une une de less spons acceder a lecteurs : 1/10/10/11 Image: Image: Image systeme est une une de less spons acceder a lecteurs : 1/10/10/11 Image: Image: Ima	C)ù voulez-vous enregistrer	la sauvegarde ?		
Sur un disque dur in data (D): 291,98 Go de libre: Survegarde la plus récente sur le lecteur: TUD/2014 08:16:19 in et un ou plusieurs DVD in et et un DVD RW (E) in et un partage réseut in et un apartage réseut in et un apartage réseut in et données sauvegardé-poste-8-1-image-systemel Isoure données de voor fichies de sauvegardé et porte dés de manière securisée pour une cible réseut in et données sauvegardé es ne peuvent pas être protégées de manière securisée pour une cible réseut in et données de voor fichies de sauvegarde et entres lie informations divertifications reseut indigues l'emplecement réseut indigues l'emplecement réseut de voor fichies de sauvegarde et entres lie informations divertification réseut indigues l'emplecement réseut de voor fichies de sauvegarde et entres lie informations divertification réseut indigues l'emplecement réseut de voor et es sauvegarde et entres lie informations d'informations de lie resplacement. Indigues l'emplecement réseut de voor es sauvegarde et entres lie informations d'informations de lie resplaceme	U o p	ne image système est une copie de omprendre des lecteurs supplémen rdinateur si votre lecteur de disque ouvez pas sélectionner d'éléments	:s lecteurs nécessaires à l'e itaires. Une image système ou ordinateur s'arrête de f individuels à restaurer.	xécution de Windo e peut servir à resta fonctionner. Ceper	ows. Elle peut aussi uurer votre ndant, vous ne
Image:	C) Sur un disque dur			
Suvegarde la plus récente sur la lacterir 1/10/12014 08:16:19 Sur un ou plusieurs DVD I cateur DVD RW (E)		ata (D:) : 291,98 Go de libres	5	~	
Image: Instant of the second of		Sauvegarde la plus récente sur le	lecteur : 11/01/2014 08	8:16:19	
Image: Control provided in the second interval of the secon	C) Sur un ou plusieurs DVD		2	
<form></form>		Lecteur DVD RW (E:)		~	
● Sur un partage réseau VMAS/data-nas/sauvegardée poste-8-1-image-systeme! Selectionner Image: Survegardées au vegardées ne peuvent pas être protégées de manière sécurisée pour une cible réseau Survant Annu Image: Survegardées ne peuvent pas être protégées de manière sécurisée pour une cible réseau Survant Annu Image: Survegardées ne peuvent pas être protégées de manière sécurisée pour une cible réseau Survant Annu Image: Survegardée poste-8-1-image: systeme! Selectionner une emplacement réseau Bacours de certe les informations didentification réseau Image: Image: metter téses informations didentification réseau Bacours du vois fichiers de voite sauvegarde. Parcourir Survegardée Windows a Second no non d'utilisateur et do mot de passe pour accéder à l'emplacement réseau lors de l'emergistrement de voite sauvegarde. Nem d'utilisateur: Imarkadmin Mot de passe: Imarkadmin Imarkadmin Imarkadmin Imarkadmin Mot de passe: Imarkadmin Imarkadmin Imarkadmin Imarkadmin Imarkadmin Mot de passe: Imarkadmin Imarkadmin <td></td> <td></td> <td></td> <td></td> <td></td>					
Image: source of the second) Sur un partage réseau		C/Is at is a sec	1
Les données sauvegardées ne peuvent pas être protégées de manière sécurisée pour une cible réseau. Suivant Annut Sélectionner un emplacement réseau Indiquez l'emplacement réseau de vos fichiers de sauvegarde et entres les informations d'dentification permettant à la sauvegarde Windows d'accéder à l'emplacement. Emplacement réseau WAS/data-nas/sauvegarde-poste-8-1-image-systeme\ Remple: \\terveut\partage Informations d'identification réseau La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de vote sauvegarde. Nom d'utilisateur: maix-dmini Mot de passe: Clefer une image système Quels lecteurs souhaitez-vous inclure dans la sauvegarde? Lesteure vious enregistres al reduction de unities par défaut. Vous ne pouvez pas inclure le lecteur ou vous enregistres la seuvegarde. Vot sauvegardes un IVAS/data-na/sauvegarde-poste-8-1-image-systeme\. Vot sauvegardes sont enregistres un VIVAS/data-na/sauvegarde? Vot sauvegardes al reduction de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur ou vous enregistres au vivAJS/data-na/sauvegarde-poste-8-1-image-systeme. Letteur Taille totale Epsee utiliéé Gor-windows-8-1 (C) (Systeme) 453,76 60 173,78 60		\\INAS\data-nas\sauvegarde-po	iste-8-1-Image-systeme\	Selectionner	
✓ Créer une image système Sélectionner un emplacement réseau Indiquer l'emplacement réseau de vos fichiers de sauvegarde et entrez les informations d'identification permettant à la sauvegarde Windows d'accéder à l'emplacement. Emplacement réseau: [\NAS\data-nas\sauvegarde-poste-8-1-image-systeme] Parcourir Exemple : \\serveu/upartage Informations d'identification réseau La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur: as\admin Mot de passe :					Suivant Annu
Schectionner un emplacement réseau Lidiquez l'emplacement réseau de vos fichiers de sauvegarde et entrez les informations didentification permettant à la sauvegarde Windows d'accéder à l'emplacement. Emplacement réseau MASS data-nas/sauvegarde-poste-8-1-image-systemel. Dermotions d'identification réseau Bauvegarde Windows a becoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur: mass de passe Vet de passe de vote sauvegarde. Vet feer une image système Leuteurs) 🔄 🎼 Créer une image systè	me		
Sélectionner un emplacement réseau Indiguez l'emplacement réseau de vos fichiers de sauvegarde et entrez les informations d'identification permettant à la sauvegarde Windows d'accéder à l'emplacement. Emplacement réseau INNAS/data-nas/sauvegarde-poste-8-1-image-systeme/ Exemple: '\serveur/partage Informations d'identification réseau La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur: matrix Mot de passe: OK Annuler Ver Créer une image système Cuels lecteurs souhaitez-vous inclure dans la sauvegarde. Us suevegarde sont enregistres sur (NASI data-nas/sauvegarde-poste-8-1-image-systeme).					
Indiquez l'emplacement réseau de vos fichiers de sauvegarde et entrez les informations d'identification permettant à la sauvegarde Windows d'accéder à l'emplacement. Emplacement réseau :		Sélectionner un emplace	ement réseau		
Emplacement réseau :		Indiquez l'emplacement réseau d'identification permettant à la	de vos fichiers de sauvegarde e sauvegarde Windows d'accéde	et entrez les informatio r à l'emplacement.	ons
Image: systeme Parcourir Exemple: \\Serveur\partage Informations d'identification réseau La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur:: Image: systeme Image: systeme Image: systeme OK Annuler Image: systeme Image: systeme Image: systeme Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Image: systeme Image: systeme Us sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Image: systeme Image: systeme Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Image: systeme Image: systeme Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-goste-8-1-image-systeme\. Image: systeme Image: systeme Us sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Image: systeme Image: systeme Us sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-goste-8-1-image-systeme\. Image: systeme Image: systeme Image: sont enregistrée sur \\NAS\data-nas\sauvegarde-goste-8-1-image-systeme\. Image: sont enregistrée sur \\NAS\data-nas\sauvegarde-goste-8-1-image-systeme\. Image: sont enregistrée sur \\NAS\data-nas\sauvegarde-goste-8-1-i		Emplacement réseau :			
Exemple: \\Serveur\partage Informations d'identification réseau La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur: nasladmin Mot de passe : OK Annuler X Créer une image système Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistre's la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Taille totale Espace utilisé os auvegardes totale (D:) 465,76 Go 36,45 Go Atta (D:)		\\NAS\data-nas\sauvegarde-p	ooste-8-1-image-systeme\	Pa	rcourir
Informations d'identification réseau La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur: nas\admin Mot de passe : ••••••• OK Annuler Implacement réseau lors de l'enregistrement de votre sauvegarde. ••••••• OK Annuler Implacement réseau lors de l'enregistrement de votre sauvegarde. ••••••• OK Annuler Implacement réseau lors de l'enregistrement de votre sauvegarde. ••••••• OK Annuler Implacement réseau lors de l'enregistrement de votre sauvegarde. ••••••• OK Annuler Implacement réseau lors de l'enregistrement de votre sauvegarde. ••••••• OK Annuler Implacement réseau lors de l'enregistrement de votre sauvegarde. ••••••• OK Annuler Implacement réseau lors de l'enregistres survival de la sauvegarde. •••••••• Ouels lecteurs souhaitez-vous inclure dans la sauvegarde. •••••••••• Implacement de la sauvegarde. •••••••••• Vos sauvegardes sont enregistres sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. <		Exemple : \\serveur\partage			
La Sauvegarde Windows a besoin du nom d'utilisateur et du mot de passe pour accéder à l'emplacement réseau lors de l'enregistrement de votre sauvegarde. Nom d'utilisateur : nas\admin Mot de passe :		Informations d'identification ré	seau		
Nom d'utilisateur :: nas\admin Mot de passe ::		La Sauvegarde Windows a beso	vin du nom d'utilisateur et du m	ot de passe pour accé	der à
Mot de passe : Mot de passe : OK Annuler CK Annuler		l'emplacement réseau lors de l'	enregistrement de votre sauveg	arde.	
OK Annuler Créer une image système Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistrez la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Taille totale Espace utilisé es os-windows-8-1 (C:) (Système) 465,76 Go 36,45 Go data (D:) 465,76 Go 173,78 Go		l'emplacement réseau lors de l' Nom d'utilisateur : r	enregistrement de votre sauveg nas\admin	arde.	
OK Annuler X Créer une image système Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistrez la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur		l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : •	enregistrement de votre sauveg nas\admin	arde.	
Créer une image système Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistrez la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Control Con		l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : •	enregistrement de votre sauveg nas\admin	arde.	
Créer une image système Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistres la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur		l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : •	enregistrement de votre sauveg nas\admin 	arde.	OK Annuler
Quels lecteurs souhaitez-vous inclure dans la sauvegarde ? Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistrez la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Taille totale Espace utilisé W souvegarde-sott-8-1-image-systeme\. Lecteur Taille totale Espace utilisé W souvegardes on enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Taille totale Espace utilisé W dota (D:) deta (D:) 465,76 Go 173,78 Go		l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : •	enregistrement de votre sauveg nas/admin	arde.	OK Annuler
Les lecteurs nécessaires à l'exécution de Windows seront inclus par défaut. Vous ne pouvez pas inclure le lecteur où vous enregistrez la sauvegarde. Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Taille totale Espace utilisé os-windows-8-1 (C:) (Système) 465,76 Go 36,45 Go data (D:) 465,76 Go 173,78 Go	•	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : •	enregistrement de votre sauveg nas\admin 		OK Annuler
Vos sauvegardes sont enregistrées sur \\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\. Lecteur Taille totale Espace utilisé Image: systeme in the systeme in the systeme intervence in the systeme intervence inte	e) 🤞	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : •	enregistrement de votre sauveg nas/admin	?	DK Annuler
Lecteur Taille totale Espace utilisé So-windows-8-1 (C:) (Système) 465,76 Go 36,45 Go data (D:) 465,76 Go 173,78 Go	D 🏟 Qu Les	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : • Créer une image système els lecteurs souhaitez-vous incl lecteurs nécessaires à l'exécution de Winc sur où vous enregistrez la sauvegarde.	enregistrement de votre sauveg nas/admin	? Yous ne pouvez pas in	DK Annuler X
Image: Solution of the	C 🔅	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : • Créer une image système els lecteurs souhaitez-vous incl lecteurs nécessaires à l'exécution de Winc eur où vous enregistrez la sauvegarde. sauvegardes sont enregistrées sur \\NAS	enregistrement de votre sauveg nas/admin	? 'ous ne pouvez pas in-	OK Annuler X
□ 🛹 data (D:) 465,76 Go 173,78 Go	C C C	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : • Créer une image système els lecteurs souhaitez-vous incl lecteurs nécessaires à l'exècution de Wine eur où vous enregistrez la sauvegarde. sauvegardes sont enregistrées sur \\NAS cteur	enregistrement de votre sauveg nas\admin ure dans la sauvegarde Jows seront inclus par défaut. V (data-nas\sauvegarde-poste-8- Taille totale	? 'ous ne pouvez pas in: 1-image-systeme\. Espace utilis	OK Annuler X
	QL Les lect Vos	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : • Créer une image système els lecteurs souhaitez-vous incl lecteurs nécessaires à l'exécution de Wine eur où vous enregistrez la sauvegarde. sauvegardes sont enregistrées sur \\NASI cteur •	enregistrement de votre sauveg nas\admin ure dans la sauvegarde Jows seront inclus par défaut. V (data-nas\sauvegarde-poste-8- Taille totale 465,76 Go	? Yous ne pouvez pas inv 1-image-systemel. Espace utilis 36,45 Go	OK Annuler ×
	Cu Les lect	l'emplacement réseau lors de l' Nom d'utilisateur : r Mot de passe : • Créer une image système els lecteurs souhaitez-vous incl lecteurs nécessaires à l'exécution de Winc eur où vous enregistres la sauvegarde. sauvegardes sont enregistrées sur \\NAS' cteur * souvegardes sont enregistrées sur \\NAS' cteur * souvegardes sont enregistrées sur \\NAS' cteur *	enregistrement de votre sauveg nas\admin ure dans la sauvegarde Jows seront inclus par défaut. V (data-nas\sauvegarde-poste-8- Taille totale 465,76 Go 465,76 Go	? 'ous ne pouvez pas int 1-image-systeme\. Espace utilis: 36,45 Go 173,78 Go	OK Annuler X



×	
Confirmez les paramètres de sauvegarde.	
Emplacement de sauvegarde :	🤹 Créer une image système – 🗆 🗙
\\NAS\data-nas\sauvegarde-poste-8-1-image-systeme\	La sauvegarde est en cours d'enregistrement
La sauvegarde peut occuper 37 Go d'espace disque.	
Line seule image système par ordinateur peut être conservée dans l'emplacement de sauvegarde.	Sauvegarde de os-windows-8-1 (C:)
Les lecteurs suivants seront sauvegardés :	
s-windows-8-1 (C:) (Système)	
	Arrêter la sauvegarde

Cela crée

(→ ▼ ↑) ► Réseau ► NAS ► data-nas ► sau	vegarde-poste-8-1-image-systeme 🕨		
A 🔝 NAS	Nom	Modifié le	Туре
4 🕌 data-nas	WindowsImageBackup	11/01/2014 09:02	Dossier de fichiers
4 🔀 sauvegarde-poste-8-1-image-systeme	-		
WindowsImageBackup			
4 🌗 travail-8			
🌗 Backup 2014-01-11 080226			
🎳 Catalog			

Avec une nature de fichier .VHDX

BackupSpecs.xml

d2820dc0-4c5c-11e4-825d-806e6f6e6963.vhdx

e75a402e-7f7f-4323-b489-4dfbda4fcfb8_AdditionalFilesc3b9f3c7-5...

Automatiser via wbadmin

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

L'option la plus intéressante étant

wbadmin start backup

Itilisation : WBADMIN S	TART BACKUP
-backupTarget:{Volu	meCible ¦ PartageRéseauCible>
-include:Volumesàlı	clure
[-noVerify]	
[-quiet]	

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

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

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

wbadmin get status

			-	• .						
C:\Users\	Admini	istrateur>wJ	padr	nin get	status					
wbadmin 1	.0 - 0)util de lic	rne	de com	mande de	e sauvegard	le			
(C) Conur	ight S	004 Michoso	£+	Cown		J				
(0) OOPAL	Tâuc 5	.001 11101030		001 p.						
-			-	,		(100 00 M				
La sauveg	farde d	tu volume Ré	esei	rvê au s	système	(100.00 Mo	12 a	a abouti	L.	
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(56%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(56%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(57%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(57%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(57%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(57%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(57%)	copiés.
Création	d'une	sauvegarde	du	volume	Disque	local(C:)	en	cours,	(57%)	copiés.



Réaliser une Restauration Intégrale Système

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

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

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



Il faut s'authentifier, puis

Récupération o	le l'image système
Choisissez un compte pour continuer.	
• Administrateur	l i i
• util	

Cela déclenche un assistant

Réimager l'ordinateur	Sélectionner une sauvegarde d'image système Cet ordinateur sera restauré à l'aide de l'image système. Tout ce qui se trouve sur cet ordinateur sera remplacé par les informations incluses dans l'image système.	×
	Utiliser la dernière image système (recommandé) Emplacement : Date et heure : Ordinateur : Sélectionner une image système	
	Celection in a dire innege systeme Source of the sector	

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



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

Si l'image système es Cliquez sur Avancé p périphérique de sauv	t sur DVD, insérez le dernier DVD de la sa our ajouter un emplacement réseau ou ir egarde s'îl ne figure pas dans la liste ci-d	auvegarde de lîmage système. Istaller un pilote pour un essous.
Fuseau horaire actue	el : GMT+01:00	
Emplacement	Image système la plus récente	Ordinateur
	3	
Avancé		Actualiser
•	< Précédent	Suivant > Annuler
	Réimager l'ordinateur	×
Chercher une ima Établir une connexion	age système sur le réseau au réseau pour rechercher l'image à restau	rer.

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

 Spécifiez l'emplacement de l'image système.

Dossier réseau :

\\nas-1\commun| Exemple : \\serveur\partage



HISTORIQUE DES FICHIERS

Mise en place

Via le menu panneau de Configuration / Historique des fichiers

🔄 Historique des fichiers 🚽

Il faut mettre en place un lecteur de stockage ...



On demande de Sélectionner un lecteur

Sélectionner un lecteur d'historique des fichiers

Sélectionnez un lecteur dans la liste suivante ou entrez un emplacement réseau.

Lecteurs disponibles		Espace libre	Espace total
雬 \\NAS-1\commun		99,6 Go	915 Go
	ß		
			Aiouter un emplacement réseau

Et on active

Conservez un historique de vos fichiers.

L'historique des fichiers enregistre des copies de vos fichiers ; vous pouvez ainsi les récupérer s'ils sont perdus ou endommagés.

L'historique des fichi	ers est activé.
Copier les fichiers à partir de :	bibliothèques, bureau, contacts et favoris
Copier les fichiers vers :	\\NAS-1\commun\ 99,6 Go disponible(s) sur 915 Go
	L'historique des fichiers enregistre des copies de vos fichiers pour la première fois. Arrêter

6

Désactiver



On peut demander de gérer les paramètres avancés



Désactiver

Pour définir la fréquence des synchronisations

Enregistrer les copies des fichiers :	Toutes les 10 minutes	~
Taille du cache hors connexion :	5 % d'espace disque (par défaut)	Ý
Conserver les versions enregistrées :	1 mois	~

On peut demander d' Exclure des dossiers



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

Exclure de l'historique des fichiers

Si vous ne voulez pas enregistrer de copies de dossiers ou de bibliothèques spécifiques, ajoutez-les ici. Dossiers et bibliothèques exclus :

📑 Vidéos

Stockage

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



Que l'on peut retrouver donc

🌗 Data	Nom *	Modifié le
\rm с	▲ Non spécifié(e) (3)	
Users Administrateur	bof (2013_05_03 11_49_22 UTC).txt	03/05/2013 13:48
Contacts	bof (2013_05_03 12_00_58 UTC).txt	03/05/2013 14:00
퉬 Desktop	e-bof (2013_05_03 11_49_22 UTC).txt	03/05/2013 13:48
Documents		
infos		



Système Windows 8.1 Pro - Cours - ver 1.2 -

Restaurer des fichiers

Via le menu panneau de Configuration / Historique des fichiers



On a une interface qui se suffit à elle - même

%	Page d'accueil - Historique des fichiers	- 🗆 🗙
÷	↑ Page d'accueil ✓ C Rechercher dans Tout	P 🛉 🌣
	vendredi 3 mai 2013 13:49 2 sur 2	
	Bibliothèque (3) Documents Imales Musique	
	Bureau Contacts Favoris	
	6 élément(s)	



COMPTES UTILISATEURS

Compte d'utilisateurs - session:

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



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

Le mot de passe peut contenir jusqu'à 127 caractères

Le nom utilisateur peut contenir jusqu'à 20 caractères

Administrateur util

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

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

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

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

Configuration

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



Système Windows 8.1 Pro - Cours - ver 1.2 -

http://www.cabare.net Page 121 - Michel Cabaré -

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

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

Winlogon.exe

Ouverture de session

Séquence authentifiée 1

Fermeture de session

Ouverture de session

Séquence authentifiée 2

Fermeture de session

Arrêt Poste

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

Connexion multiples Utilisateur

Sur un poste Windows 8 (comme XP) il est possible de changer d'utilisateur connecté sur le poste, sans fermer sa session (les travaux et la tâches initiés continuent...) c'est-à-dire que l'on peut autoriser sur un poste plusieurs sessions en parallèle de différents utilisateurs...

 Il n'est plus nécessaire de fermer la session d'un autre utilisateur pour ouvrir sa propre session....



• Autrement dit deux utilisateurs peuvent ouvrir chacun une session et se passer la connexion sans arrêter leur travaux respectifs....

Winlogon.exe



Arrêt Poste

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

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



Gestionnaire des tâches										×
Fichier O	ptions Affich	age								
Processus	Performance	Historique d	des applications	Démarrage	Ut	tilisateurs	Détails	Services		
	~			1	%	43	%	7%	0%	
Utilisateur			Statut	Processe	eur	Mémoi	re	Disque	Réseau	
D P Ad	ministrateur (6)		Déconnecté	(0%	12,3 N	10	0 Mo/s	0 Mbits/s	
Image: Partie	I (9)			(0%	42,2 N	10 (),2 Mo/s	0 Mbits/s	

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

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

Désactiver la bascule rapide Utilisateur

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

¢	Verrouiller Se déconnecter Modifier un mot de passe Gestionnaire des tâches		e	 Verrouiller Changer d'utilisateur Se déconnecter Modifier un mot de passe Gestionnaire des tâches
Soit o	n utilise gpedit.msc			 Éditeur d'objets de stratégie de groupe Fichier Action Affichage ?
Con d'ad	figuration ordinateur ministration	1	Modèles	 Stratégie Ordinateur local Configuration ordinateur Paramètres du logiciel Paramètres Windows Modèles d'administration Configuration utilisateur Paramètres du logiciel Paramètres du logiciel

puis

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





ou alors II faut passer par la base de registre

Regedt32.exe

💣 Édite	ur du Reg	istre		
Fichier	Edition	Affichage	Favoris	?
⊿ - <u> </u> ∎ (Ordinateu	r		
Þ	HKEY_	CLASSES_RO	от	
Þ - 🛛	HKEY_	CURRENT_U	SER	
Þ 📔	HKEY_	LOCAL_MAC	HINE	

Et dans la clé

$HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current\Version\Policies\System$

Il faut créer la valeur DWORD : HideFastUserSwitching

🕮 HideFastUserSwitching 🛛 REG_DWORD

0x00000000 (0)

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

Modifier la valeur DWORD 3	2 bits 🔣
Nom de la valeur :	
HideFastUserSwitching	
Données de la valeur :	Base
1	Hexadécimale
	Décimale
	OK Annuler

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

SID Sécurity identifier :

Le **SID** est un numéro d'identification unique sur un poste Windows comportant 38 digits et représentant un compte utilisateur ou un nom de groupe.

Créé automatiquement à chaque déclaration de nouveau groupe ou utilisateur, il reste stocké dans la machine même si le groupe ou l'utilisateur qui en était à l'origine est supprimé. Ce qui fait que si on supprime puis on recrée un compte ayant le même nom, le SID attribué la deuxième fois sera différent de celui utilisé lors de la 1° création, et par conséquent on ne pourra réutiliser les ressources droits et permissions allouées lors de la première utilisation





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

Whoami :

en tant que quoi on est logué ? whoami

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

et SID à titre d'information whoami /user

Comptes pré-définis :

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

Sous Windows 8 il existe 2 Comptes Utilisateurs prédéfinis

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

Le Compte Administrateur (celui d'origine):

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

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

Le Compte Invité :

Sert pour des utilisateurs occasionnels ayant un minimum de droits s

• Ce compte par défaut est inactivé



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

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

Exécuter en tant que:

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



Paramètres Windows	Afficher la commande « Executer		Palametre	Eldi
Modèles d'administration	en tant qu'utilisateur différent » dans le menu Démarrer		🖹 Supprimer l'accès aux menus contextuels pour la barre des t	Non con
Configuration utilisateur			📰 Masquer le zone de notification	Non con
Paramètres du logiciel	Modifier le paramètre de stratégie	^	Empêcher les utilisateurs de désinstaller des applications à p	Non con
Paramètres Windows			🗄 Supprimer le lien vers le dossier utilisateur du menu Démarrer	Non con
Modèles d'administration	Configuration requise :		🗈 Supprimer le nom d'utilisateur du menu de démarrage	Non con
Bureau	Au minimum Windows Server 2012 Windows 8 ou		🖹 Supprimer les liens et l'accès à Windows Update	Non con
Composants Windows	Windows RT		🗈 Changer le bouton d'alimentation du menu Démarrer	Non con
Dossiers partagés			🗈 Afficher la barre d'outils Lancement rapide dans la Barre des	Non con
a 📋 Menu Démarrer et barre des tâches	Description :		E Supprimer le bouton « Retirer » du menu Démarrer	Non con
Notifications	Ce parametre de strategie affiche		Afficher la commande « Exécuter en tant qu'utilisateur différ	Non con
Panneau de configuration	commande « Exécuter en tant T		Ajouter la commande Exécuter au menu Démarrer	Non con
Réseau	qu'utilisateur différent » dans la		Supprimer la fermeture de session dans le menu Démarrer	Non con
Système	barre d'application du menu		Supprimer l'icône du Centre de maintenance	Non con
🌇 Tous les paramètres	Démarrer.		E Supprimer l'icône de mise en réseau	Non con



http://www.cabare.net Page 126 - Michel Cabaré -

Étai A



Utilisateurs locaux:

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

La meilleure façon pour faire cela se trouve dans le menu

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

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



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



🔚 Gestion de l'ordinateur	
Fichier Action Affichage ?	
🗢 🄿 🖄 🖬 🙆 🖬	
Gestion de l'ordinateur (local) Cutils système Difficateur de tâches Difficateur d'événements Di	Pour créer un nouvel utilisateur il suffit de demander clic droit sur le dossier Utilisateurs , Puis Nouvel utilisateur
Services et applications	Nouvel utilisateur
Iouvel utilisateur	Groupes Nouvel utilisateur
Nom d'utilisateur :	Stoupes Nouvel utilisateur
Image: Services et applications Image: Services et applications <td>Stoupes Nouvel utilisateur</td>	Stoupes Nouvel utilisateur
Image: Services et applications	
Image: Services et applications Image: Services et applications <td></td>	
Image: Services et applications Jouvel utilisateur Nom d'utilisateur : Image: Services et applications Description : Image: Services et applications Mot de passe : Confirmer le mot de passe :	
Image: Services et applications Iouvel utilisateur Nom d'utilisateur : Image: Services et applications Nom d'utilisateur : Image: Services et applications Image:	Jie de session
Image: Services et applications Image: Services et applications Image: Services et applications Image: Services et applications Nom d'utilisateur : Image: Services et applications	Ire de session
Image: Services et applications Image: Services et applications Image: Services et applications Image: Services et applications Nom d'utilisateur : Image: Services et applications Nom d'utilisateur : Image: Services et applications	re de session

Gestion des Comptes:

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

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

	Propriétés de Administ	trateur 🔋 💌
	Général Membre de	Profil
	Administrate	eur
	Nom complet :	
	Description :	Compte d'utilisateur d'administration
	L'utilisateur doit ch	anger le mot de passe à la prochaine ouverture de session
	Le mot de passe n'expire jamais	
Authinistrateur	Le compte est dés	activé

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



Re-définition de mot de passe

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

Nom	Nom complet	Description
👰 Administrateur _		Compte d'utilisateur d'administration
bob	Définir le mot	de passe

Cacher le dernier Utilisateur

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

Stratégies de sécurité locales / Stratégies locales / Options de sécurité

Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur	Désactivé
Propriétés de : Ouverture de session interactive : ne pas afficher I 😢 🗙	
Parametre de securite locale Expliquer	
Ouverture de session interactive : ne pas afficher le dernier nom d'utilisateur	
O Activé	
Désactivé	

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



GROUPES LOCAUX

Notions de groupes :

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

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

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

Un groupe possède un symbole qui est



Groupes Locaux Prédéfinis :

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

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

Dans SEVEN on distingue trois types de comptes utilisateur

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



PROFILS UTILISATEURS

Liens Symboliques – Raccourcis – Jonctions :

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

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

Différence entre liens symboliques et raccourcis:

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

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

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

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

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

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

Objectif:

Les profils d'utilisateur présentent plusieurs avantages :

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





Les profils permettent de mémoriser notamment les paramètres suivants:

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

Profil Local:

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

Le profil local peut être créé à partir d'un profil local par défaut (modèle) stocké dans un dossier **Default** (sous Windows 8) ou **Default User** (sous XP)

Emplacement Profils Locaux Seven:

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

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

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

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

Clic-Droit / Ouvrir une fenêtre de commandes ici







N.B: on ne peut plus «accéder» à **Documents and Settings**... ¹ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **user**...

Emplacement non disponible	
C:\Documents and Settings n'est pas accessible. Accès refusé.	La commande en invite dir /a ou mieux dir /al liste les jonctions
OK	
C:∖>dir ∕al Le volume dans le lecteur C n'a pas de nom. Le numéro de série du volume est F2F4-F37C	
Répertoire de C:\	
14/07/2009 05:53 <jonction> Documents 0 fichier(s) 0</jonction>	and Settings [C:\Users]

Structure des Profils Windows 8:

- Cours - ver 1.2 -

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

🌗 Utilisateurs	
🎒 Administrateur	2 nouveaux dossiers système :
실 All Users	Default et Public
퉬 Default	2 jonctions pour compatibilité XP-2000 :
<table-of-contents> Default User</table-of-contents>	
퉬 Public	Default User et All Users
a test	Et les dossier profils des utilisateur crées : Administrateur , test, xxxxx

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

	Système Windows 8.1 F	Pro http://	www.cabare.net	Page 133
14/07/2009 14/07/2009	05:53 <\$YMLINKD> A 05:53 <jonction> I 0 fichier(s) 2 Rép(s> 6 714 511 3</jonction>	111 Users [C:\Pro Default User [C:\ Ø octets 360 octets libres	gramData] Jsers\Default]	←
Répertoir	e de C:\Users			
	ОК	d jo	ir /a ou mieux onctions	dir /al liste les
C:\Use Accès	ers\Default User n'est pas accessible. refusé.	L	a commande e	n invite
Emplacement r	non disponible	×		

- Michel Cabaré -

Structure d'un profil Utilisateur

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

XP (Document and Settings)	Windows 8 -7 (Users ou "Utilisateurs")
Pour un compte Donné	Pour un compte Donné "Administrateur"
nommé "Administrateur"	Une partie se trouve sous
Tout se trouve dans	C:\Users\Administrateur
Document and Settings \ Administrateur	Et une partie dans
	C:\Users\Administrateur \Appdata\Roaming\Microsoft\Windows

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



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

膧 Bureau			
 Contacts Favoris Liens Ma musique Mes documents Mes images Mes vidéos Parties enregistrées Recherches Téléchargements 	<rep> <rep> <rep> <rep> <rep> <rep> <rep> <rep> <rep> <rep> <rep> <rep> <rep></rep></rep></rep></rep></rep></rep></rep></rep></rep></rep></rep></rep></rep>	Contacts Desktop Documents Down loads Favorites Links Music Pictures Saved Games Searches Videos	Noms réels régionalisatio gestionnaire fichier Seven

dυ ation » lire de 'nen

« hors

certaines entrées stockées sous XP directement dans le profil utilisateur • sont maintenant sous Windows 8 dans un sous dossier du profil utilisateur \AppData\Roaming\Microsoft\Windows... comme par exemple



Menu Démarrer

Appdata\Roaming\Microsoft\Windows\Start Menu

Modèles

Appdata\Roaming\Microsoft\Windows\Templates

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

Profil par Défault

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

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

C:\Users>di Le volume Le numéro	r ∕al dans le] de série	lecteur C n'a j du volume est	pas de nom. 1440-3A67
Répertoire	de C:\Us	ers	
19/01/2008 19/01/2008	15:23 15:23	<symlinkd> <jonction></jonction></symlinkd>	All Users [C:\ProgramData] Default User [C:\Users\Default]

Méthode Certifiée pour modifier le profil par défaut

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

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

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

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

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

Méthode Non Certifiée pour modifier le profil par défaut

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

- 1. Créer un utilisateur "test" (ou mieux "test-xyz") ayant des droits d'administration sur le poste
- 2. Ouvrir une session avec, et faire tous ses réglages...
- 3. Fermer la session de l'utilisateur test et ouvrir une session admin



- 4. Installer l'utilitaire "windows enabler"
- 5. Copier le profil test en C:\Users\Default avec les droits Tout le mode

rofils enregistrés sur cet or	dinateur :				Copier dans	
Nom	Taille	Туре	Statut	Мо	Copier le profil dans	
Profil par défaut test-PC\Administrateur	1,51 Mo 4,21 Mo	Local Local	Local Local	18 16	C: \Users \Default	
test-PC\test	29,1 Mo	Local	Local	16	Parcourir	
					Autorisé à utiliser	
					\Tout le monde	
Modif	ier le type	Sup	orimer Co	opier dans	Modifier	

 Sélectionner la branche HKLM et lancer regedit, demander Fichier / Charger la ruche et aller chercher la ruche ntuser.dat du profil par défaut (donc depuis c:\user\default).

Donner	υn	nom	à	la	clé	quelconque,	mais	unique,	comme	"maj-profil"
Chargement	de la i	ruche				— ×				
Nom de la clé	é :									

-	
Nom de la clé :	
maj-profil	
	OK Annuler

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

a 👰 Ordinateur	Nom		
HKEY_CLASSES_ROOT	ab (par défaut)		
HKEY_CURRENT_USER			
🖟 📗 HKEY_LOCAL_MACHI			
A 📗 HKEY_USERS			
DEFAULT	Rechercher	— ———————————————————————————————————	
Imaj-profil	Parkershare bart		
⊳ 퉲 S-1-5-18	Rechercher : test	Rechercher le suivant	
🍌 🌗 S-1-5-19	Regarder dans	Annuler	
⊳ 퉬 S-1-5-20			
I in a constraint			

effacer toutes les occurrences trouvées...

 se replacer sur la ruche nettoyée "maj-profil" (si on l'a appelée ainsi au point 6) demander Fichier /décharger la ruche Fichier Edition Affichage Favoris ?

Henner Edition Amenage Tavons :	
🛛 📲 Ordinateur	-
HKEY_CLASSES_ROOT HKEY_CURRENT_USER	Confirmer le déchargement de la ruche
HKEY_LOCAL_MACHINE	Voulez-vous décharger la clé actuelle et toutes ces sous-clés ?
→ → → maj-profil → → → S-1-5-18	Oui Non

9. reboot du PC



Profil Public

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

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

C:\Users>di Le volume Le numéro	r ∕al dans le] de série	lecteur C n'a j du volume est	pas de nom. 144A-3A67
Répertoire	de C:\Us	sers	
19/01/2008 19/01/2008	15:23 15:23	<symlinkd> <jonction></jonction></symlinkd>	All Users [C:\ProgramData] Default_User [C:\Users\Default]

XP (Document & Settings)	Windows 8 (ProgramData et Users)		
All users	En partie dans C:\ProgramData plus exactement		
	C:\ProgramData\Microsoft\Windows\		
	Et C:\Users\Public		

Ce dossier ProgramData contient tous les liens pour compatibilité antérieure

Répert	oire de C:\F	ProgramData	
14/07/2	2009 05:53 010 09:25	<jonction></jonction>	Application Data [C:\ProgramData] Bureau [C:\lsers\Public\Deskton]
14/07/2	009 05:53	<jonction></jonction>	Desktop [C:\Users\Public\Desktop]
14/07/2 18/02/2	009 05:53 010 09:25	<jonction> <jonction></jonction></jonction>	Documents [C:\Users\Public\Documents] Favoris [C:\Users\Public\Favorites]
14/07/2	009 05:53	<jonction></jonction>	Favorites [C:\Users\Public\Favorites]
18/02/2 18/02/2	010 09:25 010 09:25	<junction> <jonction></jonction></junction>	Menu Demarrer IC:\ProgramData\Microsoft\Windows\Start Menu] Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2	009 05:53	<jonction></jonction>	Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2	2009 05:53	<pre><jonction></jonction></pre>	Templates IC:\ProgramData\Microsoft\Windows\Templates]

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

<u>1° partie</u> : stockée en ProgramData\Microsoft\Windows

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

- pour modifier le menu démarrer il faut aller en c:\ProgramData\Microsoft\Windows\Start Menu
- pour donner une modèle il faut aller en c:\ProgramData\Microsoft\Windows\Templates
- pour exécuter un programme à l'ouverture de session c:\ProgramData\Microsoft\Windows\Start Menu\Programs\startup

(ProgramData → Microsoft → Windows → Menu Démarrer → Programmes → Démarrage

<u>2° partie</u> : stockée en Users\Public

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

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



Supprimer tous les profils locaux Windows 8:

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

Configuration ordinateur \ modèles d'administration \ Système





INTERFACE WINDOWS 8 - 7

utilisateurs

utilisateur

Panneau de Configuration:

Affichage Windows 8 par catégories

Ajuster les paramètres de l'ordinateur



Système et sécurité Consulter l'état de votre ordinateur Enregistrer des copies de sauvegarde de vos fichiers à l'aide de l'Historique des fichiers Rechercher et résoudre des problèmes



Réseau et Internet Afficher l'état et la gestion du réseau Choisir les options de groupe résidentiel et de partage



Matériel et audio Afficher les périphériques et imprimantes Ajouter un périphérique

Pro

Programmes

Désinstaller un programme



Apparence et personnalisation Modifier le thème Modifier l'arrière-plan du Bureau Modifier la résolution de l'écran

🛞 Configurer le contrôle parental pour un

Comptes et protection des

🗑 Modifier le type de compte

Afficher par : Catégorie 🔻



Horloge, langue et région Ajouter une langue Modifier les méthodes d'entrée Modifier les formats de date, d'heure ou de nombre



Options d'ergonomie Laisser Windows suggérer les paramètres Optimiser l'affichage

Affichage Windows 8 par petites icones

Ajuster les paramètres de l'ordinateur

- Affichage
 Centre de synchronisation
 Clavier
 Contrôle parental
 Exécution automatique
 Gestionnaire de périphériques
 Historique des fichiers
 Langue
- 😪 Langue
- Prions d'indexation
- administration
- Périphériques et imprimantes
- Programmes et fonctionnalités
 Récupération
- Résolution des problèmes
- 🕎 Système
- 攂 Windows To Go

- 🖳 Barre des tâches
- 🕎 Centre Réseau et partage
- 🍇 Comptes d'utilisateurs
- 骨 Date et heure
- 🗾 Flash Player (32 bits)
- Gestionnaire d'identification
- 🔜 Icônes de la zone de notification
- Options d'alimentation
- 📔 Options des dossiers
- 🌌 Paramètres de localisation
- 🖉 Personnalisation
- 🔣 Programmes par défaut
- 🍓 Récupération de fichiers Windows 7
- 🛋 Son
- 🛄 Téléphone et modem
- 🐼 Windows Update
- Centre de maintenance
 Chiffrement de lecteur BitLocker
 Connexions distantes
 Espaces de stockage
 Gestion des couleurs
 Groupement résidentiel
 Informations et outils de performance
 Options d'ergonomie
 Options Internet
 Pare-feu Windows
 Polices
 Reconnaissance vocale
 Souris
 Windows Defender

2





Afficher par : Petites icônes 🔻

L'explorateur Windows:

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



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

	Applic	ations					
	Actualités	Interne	et Explorer	Sport	Access	soires Windows	6
	Bing	Jeux		Vidéo		Bloc-notes	
	Bureau	Lecteu	r 💼	Voyage		Calculatrice	4
	Calendrier	() Messa	ges 🤮	Windows Store		Connexion Bureau à distance	
-	Programmes et fonctionnalités	Météo				Enregistreur d'actions utilisateur	4
	Options d'alimentation Observateur d'événements	Mozilla	a Firefox		J	Journal Windows	
	Systeme Gestionnaire de périphériques Gestion du disque	Musiq	ue		O	Lecteur Windows Media	
	Gestion de l'ordinateur Invite de commandes Invite de commandes (admin)	Photos	5		×.	Magnétophone	c
	Gestionnaire des tâches Panneau de configuration	SkyDri	ive	q		Outil Capture d'écran parametres de	
	Explorateur de fichiers Rechercher Exécuter				l'ordinateur p	oour activer Windows.	
	Bureau						

Ce qui donne





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



Volets de Navigation Afficher tous les dossiers Pas de Favoris

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



Afficher le chemin d'accès complet Ne pas masquer les extensions Ne pas masquer les fichiers cachés Ne pas masquer les lecteurs vides Ne pas masquer les fichiers systèmes Ne pas utiliser l'assistant partage

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





http://www.cabare.net Page 141 - Michel Cabaré -

Interface Aero:

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

Propriétés système		×				
Nom de l'ordinateur Matériel						
Paramètres système avancés	Protection du système	Utilisation à distance				
Vous devez ouvrir une session ces modifications.	n d'administrateur pour eff	fectuer la plupart de				
Performances						
Effets visuels, planification de mémoire virtuelle	u processeur, utilisation d	e la mémoire et Paramètres	donnant			
Options de performanc	ces					
Effets visuels Avancé	é Prévention de l'exécutio	on des données				
Sélectionnez les parar de Windows sur cet or	mètres que vous voulez uti rdinateur.	iser pour l'apparence et le	s performances	Pour Désac demande	tiver AERO: d'obtenir	on Ies
Laisser Windows d	hoisir la meilleure configura	tion pour mon ordinateur		meilleures p	erformances	
Ajuster afin d'obte	enir la meilleure apparence					
Ajuster afin d'obte	enir les meilleures performa	nces		- (sans ettet 3	,D a gogo)	
Paramètres persor	nnalisés :					
 Activer la compos Activer l'affichage Afficher des minia 	sition du Bureau e transparent atures au lieu d'îcônes					

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

Note Windows 8:

Dans les propriétés de Ordinateur

Informations système générales



professionnelles 3D

Taux de transfert des données sur le disque

Disque dur principal :

Déterminé par le

5,7

sous-indice le plus bas



Messages du Centre de Maintenance :

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

On peut gérer les messages via clic/droit

ΟU

Panneau de configuration / Centre de Maintenance

🚩 Centre de maintenance

Modifier les paramètres du centre de maintenance...



ОК

Annuler

1 message important 2 messages au total

Activez Windows Defender (Important) Modifier les paramètres de Windows Update

Ouvrir Centre de maintenance

- 😼 🖢 🈡

Menu Contextuel / Accueil

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

Programmes et fonctionnalités
Options d'alimentation
Observateur d'événements
Système
Gestionnaire de périphériques
Gestion du disque
Gestion de l'ordinateur
Invite de commandes
Invite de commandes (admin)
Gestionnaire des tâches
Panneau de configuration
Explorateur de fichiers
Rechercher
Exécuter
Bureau

Compromis Performances – arrêt services:

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

Il faut arrêter le service : Windows Search

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

Propriétés de Windows Search (Ordinateur local)					
Général Connexion Récupération Dépendances					
Nom du service : WSearch					
Nom complet : Windows Search					
Description : Fournit des fonctionnalités d'indexation de contenu, de mise en cache des propriétés, de résultats de					
Chemin d'accès des fichiers exécutables : C:\Windows\system32\SearchIndexer.exe /Embedding					
Type de démarrage : Automatique (début différé)					
Obtenir de l'aide pour configurer les options de démarrage des services.					
État du service : Démarré					
Démarrer Arrêter Suspendre Reprendre					
Vous pouvez spécifier les paramètres qui s'appliquent au démarrage du service.					


SLMGR – ACTIVATION LICENCE

Installer Windows 8 sans Clé:

Pour des raisons diverses (habitudes, économie et surtout organisation) on peut vouloir installer Windows 8 sans saisir de clé	 ▲ Envoi des mises à jour facultatives - dysfonctionneme ▲ Il se peut que vous soyez en présence d'un logiciel contrefait.
30 jours sont ensuite disponibles sans avoir à rentrer une clé puis Windows Server 2008 R2 Standard Numéro 7600	Pour accéder à toutes les fonctionnalités de Microsoft Windows®, telles que toutes les mises à jour de Windows Update, obtenir les dernières mises à jour et une assistance technique, votre copie de Microsoft Windows® doit être validée. <u>Me connecter et valider maintenant</u>
FR 10:28 06/01/2011	Eermer ■

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

Activation de Windows	
🛞 🎇 Nombre de jours avant l'activation	: 27. Activez Windows maintenant
ID de produit : 89576-236-0200005-71380	🗑 Modifier la clé de produit

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

Réactiver Windows 8 - slmgr:

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

On peut demander SImgr / ?

Outils de gestion des licences logicielles Windows Utilisation : slmgr.vbs [NomOrdinateur [Utilisateur MotDePasse] [<option>] NomOrdinateur : Nom de l'ordinateur distant (ordinateur local par défaut) Utilisateur : Compte bénéficiant des privilèges nécessaires sur</option>
l'ordinateur distant MotDePasse : Mot de passe du compte précédent
Options globales : -ipk <clé produit=""> Installer la clé de produit (remplace la clé existante) -upk</clé>
Désinstaller la clé de produit -ato
Activation de Windows -dli [ID d'activation All] Afficher les informations de la licence (par défaut : licence active)
-dlv [ID d'activation] All]
Afficher les informations détaillées de la licence (par défaut : licence active) -xpr
Date d'expiration de l'état actuel de la licence
Options avancées :
-cpky Effacer la clé de produit du Registre (évite sa divulgation en cas d'attaque) -ilc <fichier de="" licence=""> Installer la licence</fichier>
-ric Réinstaller les fichiers de licence système
-rearm Réinitialiser l'état de la licence de l'ordinateur
l:klkkkkk.k.k.k.k.k



en tant qu'administrateur, il	Windows	Script Host	×
faut en ligne de commande taper sImgr –dli donnant par exemple	Nom : V Descript Clé de p État de l Temps r	Vindows(R) 7, Professional edition ion : Windows Operating System - Windows(R) 7, RETAIL channe roduit partielle : PW487 a licence : période de grâce initiale estant : 1680 minute(s) (1 jour(s))	el
		ОК	
30 iours sont ensuite dispor	aibles	Windows Script Host	×
sans avoir à rentrer une clé peut avoir en clair le calcul de période de grâce » par	et on e « la	Windows(R) 7, Professional edition: La période de grâce initiale se termine le 20/03/2010 09:58:4	8

slmgr –xpr

OK

X

ОK

Réactivation période de grâce

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

C∶∖Us	ers\Administrateur>slmgr -rearm_
après	s un petit délais on obtient
	Windows Script Host
	La commande a été exécutée. Redémarrez le système pour que les modifications soient prises en compte.

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

Dans la base de registre en

HKEY LOCAL MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CurrentVersion\SL

SL SL	-	Nom	Туре	Données
SPP SPP		ab (par défaut)	REG_SZ	(valeur non définie)
Superfetch		📖 SkipRearm	REG_DWORD	0x00000000 (0)
SystemRestore		🐯 VLActivationInterval	REG_DWORD	0x00000078 (120)
Time Zones		N VLRenewalInterval	REG_DWORD	0x00002760 (10080)
Tracing		[ab] WAUSetupLocation	REG_SZ	

la valeur SkipRearm doit valoir 1 pour autoriser le réarmement



Transfert – Re-saisie licence:

slmgr en ligne de commande permet pas mal de manipulations, parmi lesquelles on peut trouver intéressant de désinstaller une clé et la re-installer sur un autre poste.

Pour récupérer la situation actuelle	Windows Script Host	×
au niveau de la licence	Version du service de licences logicielles : 6.1.7601.17514	
slmgr /dlv ────►	Nom : Windows(R) 7, Professional edition Description : Windows Operating System - Windows(R) 7, RETAIL channel ID d'activation : e838d043-63ed-4a0h-9fh1-47152908acc9	
on note l'ID d'activation	ID d'application : 55c92734-d682-4d71-983e-d6ec3f16059f PID étendu : 00371-00170-177-000006-00-1036-7601.0000-1082013 Identificateur d'installation : 017713497195177034454234883502477876067892013961055333	
	URL du certificat du processeur : http://go.microsoft.com/fwlink/?LinkID=88338 URL du certificat de l'ordinateur : http://go.microsoft.com/fwlink/?LinkID=88339	
	URL de licence d'utilisation : http://go.microsoft.com/fwlink/?LinkID=88341 URL du certificat de dé de produit : http://go.microsoft.com/fwlink/?LinkID=88340 Clé de produit partielle : PW487	
	État de la licence : période de grâce initiale Temps restant : 21600 minute(s) (15 jour(s)) Nombre de réinitialisations de Windows restant : 0 Heure approuvée : 29/04/2013 08:56:07	

pour récupérer cette licence et « désactiver » notre poste on tape

slmgr /upk e838d943-63ed-4a0b-9fb1-47152908acc9

pour ré-installer une licence (ne pas confondre une clé d'activation et un n° de licence) sur notre poste on tape

slmgr /ipk 7KBVM-9NWFB-QJVXT-VHV9C-7CBQP-XZK28

puis on l'active via

slmgr /ato

Saisie licence slui 3:

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





INCLASSABLES WINDOWS 8

Menu étendus (invite de commande):

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

Menu contextuel

lata Progr	Affichage	•
Utilisa Wind BOOT	Trier par Regrouper par Empiler par Actualiser	* * *
	Coller Coller le raccourci	
	Nouveau Propriétés	+

MAJ + Menu contextuel

rog	Explorer	
tilis	Ouvrir	
/inc	Ouvrir une fenêtre de commandes ici	
	Rechercher	
	Partager	
	Restaurer les versions précédentes	
	Copier en tant que chemin d'accès	
	Envoyer vers	+
	Couper	
	Copier	
	Créer un raccourci	
	Supprimer	
	Renommer	
	Propriétés	

2 commandes pratiques apparaissent

Ouvrir une fenêtre de commande ici

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



Copier en tant que chemin d'accès

Permettant de récupérer la chaîne entre guillemet du chemin

"C:\data"

Options démarrage msconfig.exe :

Disposant de 5 onglets fort pratiques Général

Configuration du système
Général Démarrer Services Démarrage Outils
Sélection du mode de démarrage © Démarrage normal Charger tous les pilotes de périphérique et tous les services © Démarrage en mode diagnostic
Charger seulement les pilotes de périphérique et les services de base
Démarrage sélectif
✓ Charger les services système
☑ Charger les éléments de démarrage
Utiliser la configuration de démarrage d'origine
OK Annuler Appliquer Aide



Démarrer

Configuration du système			X
Général Démarrer Services Démar	rage Outils		
Microsoft Windows Vista (C:\Windows	s) : Système d'exploitation actuel		
Options avancées F Options de démarrage	Par défaut Supprime	r Dé <u>l</u> ai :]
 Démarrage sécurisé Minimal Autre environnement Réparer Active Directory Réseau 	 Ne pas démarrer l'interface utilisateur graphique Journaliser le démarrage Vidéo de bas<u>e</u> Inf<u>o</u>rmations sur le démarrage du système 	45	secondes e permanents <u>t</u> ous les ètres de démarrage

Services

Service	Fabricant	Statut	Date désactivée
Expérience d'application	Microsoft Corporation	En cour	_
📝 Service de la passerelle de la co	Microsoft Corporation	Arrêté	
Gestion d'applications	Microsoft Corporation	Arrêté	
🔽 Générateur de points de termina	. Microsoft Corporation	En cour	
Audio Windows	Microsoft Corporation	En cour	
🗹 Moteur de filtrage de base	Microsoft Corporation	En cour	
Service de transfert intelligent e	Microsoft Corporation	En cour	
Explorateur d'ordinateurs	Microsoft Corporation	En cour	
Propagation du certificat	Microsoft Corporation	Arrêté	
Microsoft .NET Framework NGEN	 Microsoft Corporation 	Arrêté	
Application système COM+	Microsoft Corporation	Arrêté	
otez que certains services Microsoft s	écurisés peuvent ne pas être	Activer to	Désactiver tou

Démarrage

Configuration du système				×
Général Démarrer Services Déma	rrage Outils			
Élément de démarrage	Fabricant	Commande	Emplacement	Date
Windows Defender	Microsoft Corp	%ProgramFiles	HKLM\SOFTWARE\M	
Système d'exploitation Microsof.	. Microsoft Corp	C:\Program Fil	HKCU\SOFTWARE\	
Système d'exploitation Microsof.	. Microsoft Corp	rundll32.exe o	HKCU\SOFTWARE\	
•				- F
		Activer tout	Désactiver tou	+
		Acavel tout	Desacuver tou	
		Annular		ida
	OK		Appilquer	ide



Outils

2	Configuration du système	×
Général Démarrer Services D	émarrage Outils	
Nom de l'outil	Description	^
Informations système	Afficher les informations avancées sur les paramètres matériels et logicie	
Observateur d'événements	Afficher des messages d'analyse et de dépannage.	
Programmes	Lancer, ajouter ou supprimer des programmes et des composants Windc	
Propriétés système	Afficher les informations de base sur les paramètres système de votre o	
Options Internet	Afficher les propriétés Internet.	
Configuration du protocole I	Afficher et configurer les paramètres d'adresse réseau.	
Analyseur de performances	Analyser les performances des ordinateurs locaux ou distants.	
Moniteur de ressource	Surveiller les performances et l'utilisation des ressources de l'ordinateur	
Gestionnaire des täches	Afficher des informations détaillées sur les programmes et les processus	
Commande sélectionnée :		
C:\Windows\System32\msinfo3	2.exe	
	Exécuter	
	OK Annuler Appliquer Aide	2
		-

Dont msinfo32.exe

Outils dxdiag:

Pour tester les pb directx, en ligne de commande dxdiag

😵 Outil de diagnostic DirectX
Système Affichage Son 1 Son 2 Entrée
Cet outil vous permet d'obtenir des informations détaillées sur les composants et pilotes DirectX installés sur votre système.
Si vous connaissez l'origine de ce problème, diquez sur l'onglet approprié. Sinon, diquez sur Page suivante ci-dessous pour afficher chaque page l'une après l'autre.
Informations système
Date/heure du jour : vendredi 19 mars 2010, 06:01:37
Nom de l'ordinateur : TEST-PC
Système d'exploitation : Windows 7 Professionnel 32 bits (6.1, version 7600)
Langue : français (Paramètres régionaux : français)
Fabricant du système : System manufacturer
Modèle du système : P5QL PRO
BIOS: BIOS Date: 07/01/09 17:37:27 Ver: 08.00.14
Processeur: Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz (4 CPUs), ~2.7GHz
Mémoire: 2048MB RAM
Fichier de pagination : 664 Mo utilisé(s), 3429 Mo disponible(s)
Version DirectX : DirectX 11
Rechercher les signatures numériques WHQL
DxDiag 6.01.7600.16385 32 bits Unicode Copyright © 1998-2006 Microsoft Corporation. Tous droits réservés.
Aide Page suivante Enregistrer toutes les informations Quitter



Outils shutdown:

En ligne de commande **shutdown**

Shutdown /m \\nomposte /t 0

arrêt dans 30 secondes

Shutdown /Is /t 0

Shutdown /s /t 30

fermeture de session immédiate

arrêt du pc \\nomposte « immédiat »

N.B : Les 2 options -r -f semblent obligatoires avec l'option -m

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



Une interface graphique est également disponible

Shutdown /i

Arrêt à distance	×
Or <u>d</u> inateurs :	
	Ajout <u>e</u> r
	<u>S</u> upprimer
	Pa <u>r</u> courir
Quelles tâches voulez-vous que ces ordinateurs exécutent :	
Redémarrer 💌	
Avertir les utilisateurs de l'action	
Afficher l'avertissement pendant 30 secondes	
Moniteur d'événements de mise hors tension	
Sélectionnez l'option qui décrit le mieux la raison pour laquelle voulez arrêter les ordinateurs.	VOUS
Option :	✓ <u>P</u> lanifié
Autre (planifié)	-
Un redémarrage ou un arrêt pour une raison inconnue	
Comm <u>e</u> ntaire : (obligatoire pour la raison que vous avez sélec	tionnée.)
	*
<u> </u>	<u>A</u> ide

Whoami:

En ligne de commande whoami permet de connaître son login

C:\Users\Administrateu	r>whoami
test-pc\administrateur	

N.B: à ce propos on peut lancer une tache avec un autre login (équivalent de RUNAS en ligne de commande) avec **Pointer + SHIFT + Clic DROIT**



CONSOLE MMC

Microsoft Management Console:

Dite plus couramment **MMC**, cette console d'administration n'est en fait qu'un coquille vide, ne faisant rien si ce n'est unifier et homogénéiser l'aspect des différents outils de gestion que l'on doit employer.

La MMC sert donc à fournir une interface commune pour tous les outils d'administrations sous Windows

Chaque MMC peut recevoir (ou on peut lui ôter) des outils d'administrations via ce que l'on appelle des « **snap-in** » ou encore des « **composant logiciels enfichables** ». Il existe un **snap-in** pour chaque outils de gestion.

Les consoles contiennent de manières générale un ou plusieurs snap-in et sont enregistrées dans des fichiers dotés de l'extension **.msc** stockés par défaut dans le dossier Outils d'Administration **Winnt\System32**

S'il est évident qu'il existe déjà un certain nombre de consoles prédéfinies, il est tout aussi évident que l'on peut se créer ses propres consoles personnalisées

Si on a besoin que d'une partie seulement d'une console (par exemple le gestionnaire de disques), ll peut donc être avantageux de lancer uniquement la partie intéressante, en exécutant le fichier d'extension .msc associé

,	
Fichier	Rôle
certmgr.msc	Certificats
ciadv.msc	Service d'indexation
devmgmt.msc	Gestionnaire de périphériques
dfrg.msc	Défragmenteur de disques
diskmgmt.msc	Gestion des disques
dnsmgmt.msc	Gestionnaire de DNS
eventvwr.msc	Observateur d'événements
faxserv.msc	Gestion du service de télécopie
fsmgmt.msc	Dossiers partagés
gpedit.msc	Stratégie de groupe
ias.msc	Service d'authentification Internet
lusrmgr.msc	Utilisateurs et groupes locaux
ntmsmgr.msc	Stockage amovible
ntmsoprq.msc	Demandes de l'opérateur de stockage amovible
perfmon.msc	Analyseur de performances
secpol.msc	Paramètres de sécurité locaux
services.msc	Services
wmimgmt.msc	Infrastructure de gestion Windows (WMI)
comexp.msc	Service de composants
iis.msc	Services Internet
msinfo32.msc	Informations système

Créer une console personnalisée:

Il faut demander **Executer /** Et taper mmc

Ou rechercher MMC



Système Windows 8.1 Pro – Cours - ver 1.2 - http://www.cabare.net Page 152 - Michel Cabaré -

🚡 Console1 - [Racine de la	console]		
🚟 Fichier Action Affic	hage Favoris Fenêtre ?		_ 8 ×
⇐ ➡ 🔲 🗟 🖡			
📔 Racine de la console	Nom		Actions
	Aucun élément à afficher dans cet apercu.		Racine de la console 🔺
			Autres actions

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

Fichier / Ajouter - Supprimer un composant logiciel enfichable

Ajouter ou supprimer des composants logiciels enfichables			
Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disponibles sur votre ordinateur, et les configurer. Pour les composants logiciels enfichables extensibles, vous pouvez spécifier quelles extensions doivent être activées.			
Composants logiciels enfichables disponibles :		Composants logiciels enfi. sélectionnés :	
Composant logiciel enfi Fournisseur		Racine de la console	Modifier les extensions
Analyseur de perfor Microsoft Cor			Supprimer
Configuration du clie Microsoft Cor	E		Monter
Contrôle ActiveX Microsoft Cor Contrôle WMI Microsoft Cor	Aigutor		Descendre
Dossier Microsoft Cor	Ajouter		
Bediteur d'objets de s Microsoft Cor			
Gestion de l'impression Microsoft Cor			
Gestion de la straté Microsoft Cor			

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

Gestion de l'ordinateur	×
Sélectionnez l'ordinateur devant être géré par ce composant logiciel enfichable. Ce composant logiciel enfichable gérera toujours : C L'ordinateur local (l'ordinateur sur lequel cette console s'exécute)	
C Un autre ordinateur : Pa	rcourir

Et l'on voit que notre console se personnalise !





Pour peu que l'on ait placé le fichier .msc dans le bon dossier...



N.B: on peut placer le fichier sur le bureau... ou ailleurs...

Limiter les fonctions d'un composant logiciel :

Lorsque l'on crée une console avec un composant, celui-ci peut donner accès à plein de fonctionnalités différentes. Si on veut ce composant, mais avec moins de fonctionnalités, (en quelque sorte on veut le « brider ») Il suffit de :

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

Désactiver des extensions de la console :

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

Ajouter ou supprimer des composants logiciels enfichables	
Vous pouvez sélectionner des composants logiciels enfichables parm composants logiciels enfichables extensibles, vous pouvez spécifier	i ceux disponibles sur votre ordinateur, et les configurer. Pour les quelles extensions doivent être activées.
Composants logiciels enfichables disponibles : C	Composants logiciels enfi. sélectionnés :
Composant logiciel enfi Fournisseur Standyseur de perfor Microsoft Cor Certificats Microsoft Cor Configuration du clie Microsoft Cor Configuration et an Microsoft Cor Contrôle ActiveX Microsoft Cor Contrôle WMI Microsoft Cor	Racine de la console Gestion de l'ordinateur (local) Modifier les extensions Supprimer Monter Descendre
ار	Extensions pour Gestion de l'ordinateur
On demande Modifier les extensions pour obtenir alors	 Vous pouvez indiquer quelles extensions doivent être activées afin d'ajouter ou de supprimer des fonctionnalités à votre console, composant logiciel enfichable ou extension. Si une extension n'est pas installée, vous pouvez l'installer en la sélectionnant et en cliquant sur Installer. Toujours activer toutes les extensions disponibles Toutes les extensions disponibles, et toutes les extensions installées ultérieurement, seront activées.
on demande de n'activer que les extensions sélectionnées	N'activer que les extensions sélectionnées Seules les extensions sélectionnées ci-dessous seront activées. Les extensions installées ultérieurement ne seront pas activées.
et ensuite on faite sa sélection	
	Description :
	OK Annuler



Enregistrer la console utilisateur :

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

Options 💌	
Console Nettoyage de disque	
Console 1 Changer l'icône	
Ces options prendront effet lorsque vous ouvrirez une nouvelle session MMC,	
Mode de console :	Mode de console :
Mode auteur	Mode utilisateur - accès total
μ <u>σ</u>	

Demander de passer en Mode utilisateur...

Empêche les utilisateurs d'ajouter ou de supprimer des composants
ogiciels enfichables ou de changer les options du fichier de console de
composants enfichables. Les utilisateurs bénéficient d'un accès sans
imites à l'arborescence.

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





SYSPREP

Versions de Sysprep:

L'outil **Sysprep** (**System Preparation**) prépare un ordinateur pour l'acquisition d'images ou la livraison à un client en configurant l'ordinateur de manière à créer un nouvel identificateur de sécurité (SID) d'ordinateur lors du redémarrage de ce dernier.

En outre, Sysprep nettoie les paramètres et les données spécifiques à l'utilisateur et à l'ordinateur qui ne doivent pas être copiés vers un ordinateur de destination.

La version de Sysprep installée avec l'image système Windows est la seule utilisable. Autrement dit, un Sysprep fournit avec Seven SP1 (ou Seven) ne peut travailler avec un XP, et vice-versa.

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

Se trouvant dans \Windows\system32\sysprep\...

• **Sysprep 2.0** XP Sp3 – XP Sp2

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

Sysprep 3.14 pour 8 Seven-2008:

A partir de seven, **Sysprep** est installé avec chaque version de Windows et doit toujours être exécuté à partir du dossier **%WINDIR%\system32\sysprep**

Image: sysprep Image: sysprep Image: fr-FR Image: sysprep Image: panther Image: sysprep Dans le dossier panther Image: sysprep trouvera 2 fichiers journaux Image: sysprep	er 02/11/2006 18:06 ep 02/11/2008 16:52 p 02/11/2006 11:45
▶ fr-FR ▶ Panther ▶ Panther ▶ Syspre Dans Le dossier panther, on ▶ sysprep trouvera 2 fichiers journaux ▶ fr-FR	er 09/07/2008 16:52 p 02/11/2006 11:45
Panther Syspre Dans le dossier panther , on Sysprep trouvera 2 fichiers journaux Sysprep	p 02/11/2006 11:45
Dans le dossier panther , on b sysprep trouvera 2 fichiers journaux b fr-FR	
permettant de tracer l'action de sysprep, surtout setuperr.log	비료 @diagerr.xml @diagwrn.xml

Action de sysprep :

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

Lors du démarrage suivant de l'ordinateur,

- 5. un nouvel ID de sécurité (SID) est créé,
- 6. l'horloge d'activation de Windows est réinitialisée, (si cette horloge n'a pas déjà été réinitialisée à trois reprises)



Sysprep mode graphique:

Un double clic sur sysprep amène

Outil de préparation système v.3.14	
L'outil de préparation du système (Sysprep) prépare l'ordinateur pour son autonomie matérielle et son nettoyage.	
Action de nettoyage du système	_
Entrer en mode OOBE (Out-of-Box Experience)	
🔲 Généraliser 🗧	
Options d'extinction Arrêter le système	

Mode OOBE : re déclenche l'assistant de premier démarrage de Windows

Mode Audit : démarre le poste directement

Généraliser : Impérativement nécessaire, pour demander de régénérer les **SID** lors du redémarrage

Mais dans laquelle il faut toujours demander

Sysprep /generalize:

Si vous avez l'intention de transférer une image système Windows vers un autre ordinateur, vous devez exécuter la commande **sysprep /generalize**

sysprep /generalize

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

sysprep /generalize /oobe

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

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

Administrateur : C:\Windows\system32\cmd.exe			
C:\Windows\System32\sysprep}sysprep ∕generalize ∕oobe			
Sysprep est en cours d'exécution	×		
Traitement des plug-ins Sysprep de la phase de généralisation			
	32\cmd.exe sysprep /generalize /oobe Sysprep est en cours d'exécution Traitement des plug-ins Sysprep de la phase de généralisation		

sysprep /audit

- Arrêt mais pas de rebbot immédiat après le sysprep.
- Lorsque l'on demande /audit après re-démarrage du postye suite au sysprep, on se logue en tant que admin et on peut effectuer quelques manip sur le nouveau poste....

Entrer en mode OOBE (Out-of-Box Experience)	
🔲 Généraliser	
Options d'extinction	
Arrêter le système	-

OOBE : à demander après le premier redémarrage suite au sysprep / audit sur la machine que l'on vient d'installer

N.B: Le mode audit permet d'effectuer des personnalisations et des configurations supplémentaires. Une fois ces opérations terminées, il faudra exécuter **sysprep /generalize /oobe**



Mini installation passe OOBE:

Suite à une demande via **sysprep** de terminer en installation **OOBE** (**Out Of Box Experience**), lorsque le poste redémarre on a :

- Installation re-détectant l'environnement matériel et les périphériques plug& play présent sur la nouvelle machine
- Reboot

Puis une mini installation se déclenche, demandant :

- Régionalisation
- nom utilisateur / nom machine
- mot de passe utilisateur
- (clé activation du produit)
- accepter la licence
- type de protection par défaut
- horodatage
- type connexion réseau (si carte réseau détectée)

Sysprep /unattend:c:\fichier.xml:

Si on veut automatiser la phase de mini installation consécutive à un sysprep, ou bien incorporer des réglages spécifiques, on peut lui indiquer au moment de la commande d'incorporer un fichier de réponses via l'option **/unattend** comme dans

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

Le fichier de réponse est crée de manière analogue aux autres fichiers de réponse, par l'outil WSIM

on peut le nommer comme on le souhaite

ici dans l'exemple

rep-sysprep.xml



- N.B: Ce fichier (dans l'exemple c:\rep-sysprep.xml) est en fait automatiquement recopié dans le dossier c:\windows\panther\ sous le nom unattend.xml... Une fois la commande sysprep passée, ce fichier rep-sysprepr.xml peut être supprimé, car lors du reboot c'est sa copie en %windir%\panther qui est utilisée...
- N.B: Dans la liste des emplacements possible pour le fichier de réponse, %windir%\panther\rep-sysprep.xml est en haut de la hiérarchie.



Sysprep /unattend copyprofile

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

Copyprofile à True

C'est un paramètre qui s'indique en **passe4 Specialize** dans le module **Microsoft-Windows-Shell-Setup_neutral**. Elle ne s'exécutera donc <u>que lors du</u> <u>re-boot après que le sysprep se soit executé</u>, de la phase mini oobe, passe specialize !

Name successory west Windows Success Tennes Manager					
rep-sysprep.xm - windows System Image Manager					
Fichier Edition Insérer Ou	tils ?				
😫 🇀 🔚 📕 🐐 🖹 🔲 🗡 🔎 🞯 🥵					
Partage de distribution		Fichier de réponses			
Sélectionner un dossier partagé d	Components Components				
Image Windows					
x86_Microsoft-Windows-SharedAccess_6.1.7600.16385_neutral					
□··· □ x86_Microsoft-Windo	ws-Shell-Setup_6.1.7601.17514_neutral				
	Ajouter le paramètre à la passe 1 windowsPE				
Display	Ajouter le paramètre à la passe 2 offlineServicing				
	Ajouter le paramètre à la passe 3 generalize				
	Ajouter le paramètre à la passe 4 specialize				
H Notification	Ajouter 🕏 paramètre à la passe 5 auditSystem				

donnant

Fichier de réponses	P	ropriétés de Microso	oft-Windows-Shell-Setup
E. 💽 prof-sysprep		Propriétés	
		AppliedConfiguration Pass	4 specialize
🛂 1 windowsPE		Enabled	True
🖣 2 offline Servicing	Ð	ld	x86_Microsoft-Windows-Shell-Set
		Paramètres	
🖃 🖣 4 specialize		Bluetooth Taskbarlcon Ena	
		ComputerName	
		CopyProfile	true 🔹
📲 6 auditUser		DisableAutoDaylightTimeS	
		DoNotClean TaskBar	
Packages		ProductKey	

La procédure pour créer un profil par défaut est la suivante

- 1. Créer un fichier de réponse nommé par exemple prof-sysprep.xml. contenant la commande CopyProfile=True
- 2. Ouvrir une session sur la machine "type" avec le compte **Administrateur** par défaut du poste (celui qui est dévalidé lors de l'installation...) et
 - a. Supprimer tous les comptes existants autres que l'administrateur.
 - b. Supprimer tous les profils existants éventuellement sur le poste.
 - c. Effectuer le paramétrage du profil en cours de l'administrateur.
- 3. Lancer la commande sysprep avec l'options /unattend comme dans:

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



Activation et SkipRearm

Il existe des limites au nombre d'exécutions de Sysprep sur un ordinateur, 3 sur seven, 7 sous windows 8. Cependant, l'horloge de l'Activation de produit Windows commence son décompte la première fois que Windows est lancé.

La commande **sysprep /generalize** réinitialise l'activation du produit et elle ne peut le faire qua à trois reprises maximum. Après trois exécutions de **sysprep** /generalize, l'horloge ne peut plus être réinitialisée...

On peut ignorer la réinitialisation de l'horloge d'activation à l'aide du paramètre **SkipRearm** dans le composant **Microsoft-Windows-Security-SPP** (anciennement vista **Microsoft-Windows-Security-Licensing-SLC**)

Fichier de réponses	Propriétés de Microsoft-Windows-Security-SPP		
prof-2-sysprep		Propriétés	
🖻 🚽 Components		AppliedConfiguration Pass	3 generalize
🔃 📲 1 windowsPE		Enabled	True
	Ð	ld	x86_Microsoft-Windows-Security-SPP_
🖻 🖣 3 generalize		Paramètres	
		SkipRearm	0
🕀 📲 4 specialize			

Microsoft recommande d'utiliser le paramètre SkipRearm avec la valeur du paramètre SkipRearm égale à 1 si on prévoit d'exécuter Sysprep /generalize à plusieurs reprises sur un ordinateur. Après avoir testé cette image, utilisez la commande Sysprep /generalize avec la valeur SkipRearm égale à 0.

Exemple de fichier de réponse

Avec les 2 commandes

Génération du profil par défaut et non - réarmement



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

setupact.log - Bloc-notes				
Fichier Edition Format Affichage ?				
2014-10-04 19:12:30, Info	[0x0f0041] SYSPRP WinMain:A∂ocessing system shutdown request.			
2014-10-04 19:12:30, Info	[0x0f0074] SYSPRP ProcessShutdown:Successfully enabled the sh			
2014-10-04 19:12:30, Info	[0x0f0076] SYSPRP ProcessShutdown:Successfully called Initiat			
2014-10-04 19:12:30, Info	[0x0f0052] SYSPRP Shutting down SysPrep log			
2014-10-04 19:12:30, Info	[0x0f004d] SYSPRP The time is now 2014-10-04 19:12:30			