ADMINISTRATION ET DÉPANNAGE WINDOWS 7

REDIGE PAR GUILLAUME MATHIEU CONSULTANT ARCHITECTURE & INTEGRATION PROSERVIA (MANPOWERGROUP SOLUTIONS)

http://msreport.free.fr - La connaissance s'accroît quand on la partage

Plan de cours 1/2

1. Configuration avancé de Windows 7:

- Configuration réseau, services, disques, ajout de composant.
- La base de registre Windows 7, les fichiers systèmes / démarrage.

2. Authentification Windows 7 :

- Un peu de théorie (SID, TGT, TGS)
- Présentation de la base SAM et de l'annuaire Active Directory.
- Comment une station de travail détecte un contrôleur de domaine.

3. Partager des fichiers sous Windows 7:

- Sécurisation d'un dossier avec des permissions NTFS / création de partages
- Les bonnes pratiques pour sécuriser un dossier avec des ressources Active Directory

4. Internet Explorer :

Les protocoles d'authentification, les zones de sécurité, le mode compatibilité

5. Les outils d'administration de Windows 7 :

- Les consoles MMC / RSAT.
- PowerShell.
- Prise en main à distance avec le Bureau à distance et l'assistance à distance.

Plan de cours 2/2

- 6. Gestion de la configuration station de travail Windows 7 :
- Les stratégies de groupe
- Les scripts de login.

7. Sécuriser une station de travail avec Windows 7 :

- Le pare feu
- L'UAC
- Les risques liés au virus et aux failles de sécurité.
- APPLOCKER
- 8. Déploiement Windows 7 :
- WAIK, WDS , MDT
- 9. Dépannage Windows 7 :
- Méthodologie
- Les outils de diagnostics.

1. Configuration avancé Windows 7

Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

Ouverture session avec Windows 7

A SAVOIR :

- Windows 7 Home (Familiale) ne permet pas de joindre une machine dans le domaine.
- Le champ « Se connecter A » n'existe plus.
- Pour se connecter à la base SAM local sur Windows Server 2008, taper : *nom_machine\utilisateurbasesam .\utilisateur_base_sam*
- Si la machine est membre d'un domaine, se connecter au domaine en tapant : *Nom_NETBIOS\login_utilisateur_pre_Windows_2000 login@nom_dns_domaine*



Interface graphique

CONFIGURATION DE L'EXPLORATEUR WINDOWS

- Configurer Windows 7 pour afficher le menu, les extensions de fichiers, afficher les fichiers systèmes et les icônes poste de travail, panneau de configuration sur le bureau.
- Aller dans Organiser | Disposition et cocher Barre de menus.
- Aller ensuite dans Organiser | Disposition. Dans « Options des dossiers », dans l'onglet Affichage, décocher les cases « Masquer les extensions des fichiers dont le type est connu », « Masquer les fichiers protégés du système d'exploitation » et sélectionner « Afficher les fichiers, dossiers et lecteurs cachés ».
- Aller dans Panneau de configuration | Personnalisation | Changer icônes bureau.

0	→ Vrdinateur → System (C:) → U	Itilisa	teurs ▶ admin ▶		-		
Org	aniser ▼ Inclure dans la bibliothèque ▼		Partager avec 🔻 🛛 Grav	rer Nouveau d	ossier	Options des dossiers	
	Annuler Couper Copier Coller Annuler Rétablir Sélectionner tout Disposition Options des dossiers et de recherche Supprimer Renommer Supprimer les propriétés Propriétés Fermer		Barre de menus Volet de visualisation Volet de navigation	Aodifié le 3/12/2012 11:33 17/12/2012 08:57 17/12/2012 08:57 17/12/2012 08:57 17/12/2012 08:57 17/12/2012 08:57 12/12/2012 08:57 12/12/2012 08:57 12/12/2012 08:57 12/12/2012 08:57 12/12/2012 10:03	Type Dossier de fichi Dossier de fichi	Général Affichage Rechercher Vous pouver applquer le bye d'affichage (es détals ou les icônes, par exemple) de ce dossiers Image: control Panel + Al Control Panel + Al Control Panel Items - Personalization Image: control Panel + Al Control Panel Items - Personalization Image: control Panel + Al Control Panel Items - Personalization Image: control Panel + Al Control Panel Items - Personalization Image: control Panel + Al Control Panel + Al Control Panel Items - Personalization Image: control Panel + Al Contr	ol Pane
						OK Annuler Appliquer See also OK Cancel	l l

Configuration réseau :

LES NOTIONS FONDAMENTALES :

- Adressage IP privé / publique : <u>http://fr.wikipedia.org/wiki/Adresse_IP</u>
- NAT : <u>http://fr.wikipedia.org/wiki/Network_address_translation</u>
- Routage : <u>http://fr.wikipedia.org/wiki/Routage</u>

CONFIGURATION RÉSEAU WINDOWS 7 :

 Aller dans Panneau de Configuration | Centre réseau et partage et cliquer sur Modifier les paramètres de la carte.

CLIENT VPN PRISE EN CHARGE NATIVEMENT PAR WINDOWS 7

- VPN L2TP IPSEC
- DirectAccess (nouveauté) : <u>http://www.microsoft.com/en-us/download/details.aspx?id=24144</u>



Configuration réseau :

IPV6

- Par défaut IPV6 est activé sur Windows 7.
- IPV6 est prioritaire sur IPV4.
- IPV6 est nécessaire pour les technologies comme DirectAccess (déconseillé de le désactiver).

Configurer IPV4 comme prioritaire sur IPV6 :

 Créer la valeur DWORD 32 Bits DisabledComponents avec la valeur 20 (hexadécimal). <u>http://support.microsoft.com/kb/929852/en-us</u>

Désactiver IPV6 complètement (non préconisé) :

 Créer la valeur DWORD 32 Bits DisabledComponents avec la valeur FFFFFFF (hexadécimal). <u>http://support.microsoft.com/kb/929852/en-us</u>

🖞 Local Area Connection 4 Properties 🛛 🗙	🙀 Éditeur du Registre			_[
Networking Sharing	Fichier Edition Affichage Favoris ?	Nem	Turne	Deprés
Connect using: Broadcom BCM5709C NetXtreme II GigE (NDIS VBD Clier Configure This connection uses the following items: Client for Microsoft Networks QoS Packet Scheduler File and Printer Sharing for Microsoft Networks Internet Protocol Version 6 (TCP/IPv6) Internet Protocol Version 4 (TCP/IPv4) Link-Layer Topology Discovery Mapper I/0 Driver Link-Layer Topology Discovery Responder	Interfaces I	Nom	I Type REG_SZ REG_BINARY REG_DWORD its ase I Hexadécimale I Décimale OK Annule	Jonnees (valeur non définie) 00 01 00 01 13 0a a6 dc 00 24 e8 fa 77 d9 0xffffffff (4294967295)
- Description	Ordinateur HKEY_LOCAL_MACHINE SYSTEM (C	CurrentControlSet\services\TCPIP6\Pa	arameters	

Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

Gestion des fonctionnalités :

POUR AJOUTER DES FONCTIONNALITÉS SOUS WINDOWS 7

- Aller dans Panneau de configuration | Programmes et fonctionnalités | Activer ou désactiver des fonctionnalités Windows.
- Windows 7 intègre un site web IIS / FTP. Contrairement à IIS sous Windows 2008 R2, il n'est possible que de créer un seul site web.
- RSAT : permet de gérer un serveur Windows 2008 R2 depuis une machine Windows 7 : <u>http://www.microsoft.com/en-us/download/details.aspx?id=7887</u>

ā	Programmes et fonctionnalités						
G	🗸 🖂 👻 Panneau de config	uration \star Tous les Panneaux de configuration \star Program	mes et fonctionnalités	▼ 🐓	Recherche	r dans : I	: Programmes et fon
	Page d'accueil du panneau de	Désinstaller ou modifier un programme				E	🖻 🗹 🕌 Services Internet (IIS)
	Afficher les mises à jour installées	Pour désinstaller un programme, sélectionnez-le da	ns la liste et cliquez sur Désins	taller, Modifier ou Répa	arer.		 With a diaministration Web Ompatibilité avec la gestion IIS 6
۲	Activer ou désactiver des fonctionnals <u>Windows</u>	Organiser 🔻					Console de gestion IIS
	Installer un programme à partir du	Nom 🔺 🗸	Éditeur	▼ Install ▼ Ta	aille 🚽 🔪	/ersion	Service de gestion IIS
	réseau	ATI Catalyst Install Manager	ATI Technologies, Inc.	07/12/2012	13,8 Mo 3	3.0.736.	🖃 🛃 Serveur FTP
		💿 Google Chrome	Google Inc.	13/12/2012	2	23.0.12	Extensibilité FTP
		🚟 Intel(R) Management Engine Interface	Intel Corporation	07/12/2012			Service FTP
		Ma-Config.com	Cybelsoft	13/12/2012	8,62 Mo 6	5.5.009	🖃 🛃 📕 Services World Wide Web
		5 Microsoft .NET Framework 4 Client Profile	Microsoft Corporation	07/12/2012	38,8 Mo 4	4.0.303:	Etat de santé et diagnostics
		🔡 Microsoft Office Standard 2007	Microsoft Corporation	07/12/2012	1	12.0.45	Journal ODBC
		🥪 Microsoft Silverlight	Microsoft Corporation	13/12/2012	20,5 Mo 4	4.1.103	Journalisation HTTP
		Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	07/12/2012	428 Ko 8	3.0.563	Journalisation personnalisée
			Microsoft Corporation	07/12/2012	2,93 Mo 4	4.0.303:	Observateur de demandes
		🚮 Technologie d'administration active Intel®	Intel Corporation	07/12/2012			🗹 🍌 Outils de journalisation
		🖔 Wisdom-soft ScreenHunter 6 0 Free	Wisdom Software Inc	13/12/2012			Sulvi Sulvi
							Fonctionnalités de développement d'applications
							ASP ASP
							ASP.NET
							CGI
							Extensibilité .NET
							Extensions IS/PI
							Filtres ISAPI
							SSI (Server-Side Includes)

La base de registre 1/2 :

A SAVOIR :

- Base de registre = base de configuration de Windows.
- REGEDIT / REGEDT32 : éditeur base de registre.
- Ruche : ensemble de clés et de valeurs qui correspondent à un fichier au niveau du système.
- Clés : c'est un conteneur de valeur.
- Valeur : variable. Il existe différent type de valeur (binaire, chaîne de caractères, tableaux de chaines de caractères...).
- La base de registre est organisée en deux grandes sections HKEY LOCAL MACHINE et HKEY USERS.
- La ruche HKEY_CURRENT_CONFIG est une sous ruche de HKEY_LOCAL_MACHINE
- Il est possible de charger des ruches (fichier NTUSER.DAT d'un autre utilisateur...).
- Il est possible de définir des permissions au niveau des clés de registre



Réduire	
Nouveau 🕨 🕨	Clé
Rechercher	Valeur chaîne
Supprimer	Valeur binaire
Renommer	Valeur DWORD 32 bits
Exporter	Valeur QWORD (64 bits) Valeur de chaînes multiples
Autorisations	Valeur de chaîne extens <mark>ib</mark> le
Copier le nom de clé	Ŋ

🕵 Éditeur du Registre						
Fichier	Edition	Affichage	Favoris	?		
Éditeur du Registre Fichier Edition Affichage Eavoris 2						
Image Payons Image Payons						
÷ •	I SECU SOF HKEY_U HKEY_CU	J Déveloj T Nouveau Recherch 55 Supprime J Renomm	pper 1 her er er	•		
		Exporter Autorisa	tions			

Autorisations pour SAM								
Sécurité								
Noms de groupes ou d'utilisateurs :								
Système								
Administrateurs (FORMATION3)	Administrateurs)							
	Ajouter	Suppri						
Autorisations pour Système	Autorise	r Refu						
Contrôle total								
Lecture	\checkmark							
Autorisations spéciales								

Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

La base de registre 2/2 :

A SAVOIR

- Les paramètres de HKEY_USERS correspondent à la configuration spécifique au niveau des utilisateurs.
- Les paramètres de HKEY_LOCAL_MACHINE correspondent à la configuration de la machine (commune pour tous les utilisateurs).
- Dans HKEY_LOCAL_MACHINE | SYSTEM | CurrentControlSet | Services, on retrouve la configuration des services.
- Dans HKEY_LOCAL_MACHINE | SOFTWARE, on retrouve la configuration des logiciels communs à tous les utilisateurs.
- Dans HKEY_USERS | SOFTWARE, on retrouve la configuration des logiciels spécifiques à un utilisateur.



🎪 Éditeur du Registre	🙀 Éditeur du Registre 👘 Éditeur du Registre				
Fichier Edition Affichage Favoris ?	Fichier Edition Affichage Favoris ? Fichier Edition Affichage Favoris ?				
Image: HKEY_USERS Image: DEFAULT Image: S-1-5-18 Image: S-1-5-19 Image: S-1-5-20 Image: S-1-5-21-1241569958-1998640802-1357695591-500_Classes	HKEY_LOCAL_MACHINE BCD0000000 HARDWARE SAM SECURITY SOFTWARE SYSTEM ControlSet001 CurrentControlSet U CurrentControlSet Enum Hardware Profiles Policies Services	SAM SECURITY SOFTWARE SYSTEM ControlSet001 ControlSet002 CurrentControlSet Control Control Control CurrentControlSet Hardware Profiles Policies Services MountedDevices RNG Select			

Les services 1/2 :

A SAVOIR

- Services = programmes (ex :LSASS.EXE pour le service NETLOGON).
- Un service peut démarrer manuellement (démarrer au lancement d'une application) ou automatiquement (avant ou après ouverture de session)
- Un service s'exécute avec les droits d'un compte utilisateur : Local System Account (System), Local Service ou un compte utilisateur standard.
- Possibilité de définir un comportement en cas de défaillance d'un service (redémarrage du service, redémarrage de l'ordinateur,...).
- Les virus SASSER et BLASTER faisait planté le service « Remote Procedure Call » et la machine redémarrait automatiquement (comme configuré dans l'onglet RECOVERY) : <u>http://support.microsoft.com/kb/826955/en-us</u>

Netlogon Properties (Local Computer)	×	Remote Procedure Call (RPC) Properties (Local Computer)	X
General Log On Recovery Dependencies	1	General Log On Recovery Dependencies	
Service name: Netlogon		Select the computer's response if this service fails. Help me set up re actions	Netlogon Properties (Local Computer)
Display name: Netiogon Description: Maintains a secure channel and the domain controller fo	between this computer r authenticating users	First failure: Restart the Computer Second failure: Restart the Computer	General Log On Recovery Dependencies
Path to executable: CAWindows/system32\sass.exe		Subsequent failures: Restart the Computer Reset fail count after:	Log on as:
Help me configure service startup options.		Restart service after: 1 minutes Enable actions for stops with errors. Restart Computer Option	Allow service to interact with desktop
Service status: Stopped Start Stop Pa	use Resume	Run program Program	This account: Browse
You can specify the start parameters that apply from here.	when you start the service	Command line parameters:	Password:
Start parameters:		Append fail count to end of command line (/fail=%1%)	Confirm password:
ОК	Cancel Apply	OK Cancel	Apply Help me configure user account log on options.

Les services 2/2 :

NOTIONS AVANCEES :

- La configuration des services se trouve dans la base de registre à l'emplacement suivant : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services
- Les services IPV4 (TCP) et IPV6 (TCP6) ne sont configurables que par la base de registre.
- L'entrée de registre « *DependOnService* » permet de définir des dépendances.
- L'entrée de registre « Start » permet de définir le mode de démarrage du service.

Registry Editor							
File Edit View Favori	ites Help						
	mrxsmb 10	Name	Туре	Data			
.	mrxsmb20	(Default)	REG_SZ	(value not set)	Netlogon Properties (Local Computer)		
	msahci	DependOnService	REG_MULTI_SZ	LanmanWorkstation			
	msdsm	ab Description	REG_SZ	@%SystemRoot%\System32\netlogon.dll,-103	General Log On Recovery Dependencies		
	MSDTC	ab DisplayName	REG_SZ	@%SystemRoot%\System32\netlogon.dll,-102			
	MSDTC Bridge 3.0.0.0	8 ErrorControl	REG_DWORD	0x00000001(1)	Some services depend on other services, system drivers or load order		
	MSDTC Bridge 4.0.0.0	ab Group	REG_SZ	MS_WindowsRemoteValidation	aroune if a system component is stopped, or is not running property		
	mshidkmdf	ab ImagePath	REG_EXPAND_SZ	%systemroot%\system32\sass.exe	dependent services can be affected		
	msisadry	ab ObjectName	REG_SZ	LocalSystem	dependent services can be anected.		
	MSISCST	88 Start	REG_DWORD	0x0000003 (3)	Netlogon		
T.	msiserver	🛍 Type	REG_DWORD	0x00000020 (32)			
	MSKSSRV	Edit Multi-Stving		X	This service depends on the following system components:		
	msoidsvc	cure mane-sering					
	MSPCLOCK	Value name:					
Ē	MSPQM	DependOnService			Erowser Support Driver		
	MsRPC	Value data:			Wetwork Store Interface Service		
E	MSSCNTRS	value data.					
±	mssmbios	Lanman Workstation	1		E SMB 2.0 MiniBedirector		
	MIConfig						
	Mun						
	MyWiFiDHCPDNS						
	napagent				The following system components depend on this equiper		
	NativeWifiP				The following system components depend on this service.		
	NDIS						
Ē	NdisCap						
Ē	NdisTapi			V			
.	Ndisuio				NS 1		
	Noiswan		0	Cancel			
	NetBT						
	Netlogon						
	Parameters						
L ⊨]	Netman 📃						
					OK Cancel Apply		
Computer HKEY_LOCAL_M	MACHINE\SYSTEM\CurrentControlSet\services\Wetlog	on					

Licences et activation :

3 TYPES DE LICENCE WINDOWS 7 :

- OEM : coût unitaire faible, 1 numéro de licence par machine, la licence rattachée à la machine (perte licence si mise rebus machine / virtualisation machine), activation manuelle (5 fois maximum).
- DETAIL / OPEN : coût unitaire important, 1 numéro de licence par machine, la licence n'est pas rattachée à la machine (support virtualisation), activation manuelle (nombre d'activation illimité).
- VOLUME : coût unitaire moyen. 1 numéro de licence unique pour toutes les machines Windows 7, la licence n'est pas rattachée à la machine (support virtualisation), activation manuelle à l'aide du clé MAK ou via serveur KMS, on déclare à Microsoft tous les ans nombre de licences requise.

ACTIVATION CLÉ VOLUME :

- Clé MAK : activer manuellement Windows 7 avec clé MAK.
- Clé KMS : installer un serveur KMS et l'activer avec clé KMS (5 activations maximum). Windows 7 s'active sur le serveur KMS avec la clé système intégrée par défaut. Windows 7 doit se réactiver au moins 1 fois tous les 180 jours auprès du KMS. Si la machine est hors réseau > 180 jours, activer avec une clé MAK.
- SLMGR.VBS : gestion de l'activation sous Windows 7 / 2008 R2
- Lire : <u>http://msreport.free.fr/?p=153</u>

Gestion des disques 1/2 :

A SAVOIR :

- Windows 7 gère nativement le format de fichier VHD. Ce format de fichiers est utilisé par le système de sauvegarde de Windows 7 et par la solution de virtualisation Hyper-V. Il est donc possible de charger le disque de sauvegarde d'une machine Windows 7 ou un disque d'une machine virtuelle sous forme de disque dur supplémentaire.
- Windows 7 permet d'augmenter ou de réduire la taille d'une partition.

E Gestion de l'ordinateur							
Fichier Action Affichage ?							
🜆 Gestion de l'ordinateur (local)	Volume	Disposition	Туре	Système de fichiers	Statut		
🔺 🎁 Outils système	📼 Data (D:)	Simple	De base	NTFS	Sain (Partition principale)		
Planificateur de tâches	System (C:)	Simple	De base	NTFS	Sain (Système, Démarrer, Fichier d'écł		
Observateur d'événements							
Dossiers partagés							
b 🜆 Utilisateurs et groupes locaux							
Performance							
📇 Gestionnaire de périphériques							
🔺 🚝 Stockage							
🚘 Gestion des disques							
Services et applications							

Gestion des disques 2/2:

TYPES DE DISQUE :

- **Disque de base :** 4 partitions principales maximum. 2 To pour partition NTFS.
- Disque dynamique : partition = volume. Nouveauté Windows 2000. Ne pas utiliser car nombreuses fonctionnalités non compatibles.
- Disque GPT : recommandé nouveautés Windows 2003 SP1. Permet prise en charge partition de plus de 2 To et supprime limite des 4 partitions.

SYSTÈME DE FICHIERS SOUS WINDOWS 7 :

- FAT16 : taille maximum d'une partition = 4 Go. Pas de permissions de fichiers. Voir <u>http://fr.wikipedia.org/wiki/FAT16</u>.
- FAT32 : taille maximum partition : 2 To. Pas prise en charge des fichiers de plus de 4 Go. Pas de permissions de fichiers. Voir <u>http://fr.wikipedia.org/wiki/FAT32</u>
- NTFS : recommandé, taille maximum partition 2 To (disque de base), 16 Exaoctet (disque GPT) :

http://blogs.technet.com/b/askcore/archive/2010/02/18/understanding-the-2-tblimit-in-windows-storage.aspx et http://msdn.microsoft.com/enus/library/windows/hardware/gg463525.aspx

FAT 16, POURQUOI UNE TAILLE MAXIMALE DE 4 GO ?

 Table d'allocation de fichiers contient un maximum de 2^16 blocs. La taille d'un bloc en FAT16 est de 64 Ko, on a 64 * (2^16) = 4194304 Ko

Fonctionnement interne Windows 1/2 :

2 MODES D'EXECUTION :

- Mode utilisateur : les applications tournent en mode utilisateur (Word, Excel...). Les applications n'ont aucun accès direct au matériel (mémoire, disque, CPU...) et ne peuvent générés théoriquement de défaillance système générale.
- Mode noyau : les applications en mode noyau (ordonnanceur, pilotes, certains services) ont un accès direct au matériel. Un pilote défectueux peut donc entraîner une défaillance générale du système d'exploitation.
- Voir <u>http://sebastien-</u> viardot.imag.fr/Enseignements/SEPC/ <u>Documents/windows.pdf</u>



Fonctionnement interne Windows 7 2/2 :

GESTION DES PROCESSUS:

 L'affectation des ressources aux processus est gérée par le noyau. Cela permet d'éviter qu'une application s'octroie toutes les ressources et pénalise les autres (théoriquement). Il est possible de modifier manuellement la priorité d'un processus.

LES SOUS SYSTEMES :

 Plusieurs sous systèmes pour prise en charge par Windows d'applications Windows 16 bits (WIN16), d'applications Windows 32 bits (WIN32), d'applications Windows 64 bits Windows (WIN64), d'applications .Net Framework, d'applications POSIX (compatibilité limitée avec les applications Unix).

LES PILOTES :

- Elément critique car en mode noyau.
- Pilotes génériques : permettent d'exploiter des périphériques sortis après Windows 7. Incluent fonctions de base (prise en charge 2D pour carte graphique uniquement).
- Pour la détection des pilotes, aller sur le site suivant : <u>http://www.touslesdrivers.com/index.php?v_page=29</u>
- WHQL : Microsoft certifie les pilotes (par défaut : installation que des pilotes signés). Installation pilote non signé :

http://www.commentcamarche.net/faq/19651-windows-7-installer-un-pilote-nonsigne

Démarrage Windows 7 :

GESTION DU DÉMARRAGE / CRÉATION D'UN DUAL BOOT :

- Le fichier boot.ini a été remplacé par le BCD.
- BCDEDIT, BCDBOOT : permet de gérer démarrage du système Windows 7. Voir <u>http://technet.microsoft.com/fr-</u> fr/library/dd799299(v=ws.10).aspx
- BOOTREC : permet de reconstruire le BCD : <u>http://support.microsoft.com/kb/92</u> <u>7392/en-us</u>
- Exemple d'une machine avec double boot (capture de droite).

c:\>bcdedit

Windows Boot Manager identifier device description locale inherit default resumeobject displayorder

toolsdisplayorder timeout

Windows Boot Loader

identifier device path description locale inherit recoverysequence recoveryenabled osdevice systemroot resumeobject nx

Windows Boot Loader

identifier device path description locale inherit recoverysequence recoveryenabled osdevice systemroot resumeobject nx c:\>

{bootmgr> partition =\Device\HarddiskVolume2 Windows Boot Manager en=US {globalsettings> {current> {0a70ba24-ff91-11e1-8533-8ff3543fc38c> {current> {0a70ba28-ff91-11e1-8533-8ff3543fc38c> {mendiag} 30

{current}
partition=C:
\Windows\system32\winload.exe
Windows 7
en-US
{bootloadersettings}
{0a70ba26-ff91-11e1-8533-8ff3543fc38c}
Yes
partition=C:
\Windows
{0a70ba24-ff91-11e1-8533-8ff3543fc38c}
OptIn

{0a70ba28-ff91-11e1-8533-8ff3543fc38c}
partition=D:
\Windows\system32\winload.exe
Windows 7 Technip
en-US
{bootloadersettings}
{0a70ba29-ff91-11e1-8533-8ff3543fc38c}
Yes
partition=D:
\Windows
{0a70ba24-ff91-11e1-8533-8ff3543fc38c}
OptIn

TP: Installation Windows 7

ACTIONS (1/2) :

- Effectuer une installation par défaut.
- Le nom machine est généré automatiquement. Renommer la machine (Panneau de configuration | Système ou Windows+Pause).
- Configurer la machine en IP fixe. A quoi sert un masque de sous réseau, une passerelle, un serveur DNS, un serveur Wins ?
- Désactiver le pare feu, l'UAC.
- Configurer IPV4 comme protocole prioritaire sur IPV6.
- Activer le bureau à distance et accéder à la station de travail d'un autre stagiaire.
- Démarrer le service « Explorateur d'ordinateur ».
- Taper la commande SLMGR.VBS /DLV pour valider configuration activation.
- Taper REGEDT32 pour accéder base de registre.
- Aller dans HKEY_LOCAL_MACHINE | SAM | SAM. Faire un clic droit sur le dossier SAM et cliquer sur « *Autorisation* ». Ajouter les droits *Control Total* au groupe *Administrateurs* de la base SAM locale. Visualiser le contenu de la base SAM locale. Faire la même chose sur la clé Security.
- Créer un compte utilisateur appelé « *testregistre* » dans la base SAM.
- Ouvrir une session avec le compte administrateur local sur cette station de travail. Lancer l'éditeur de base de registre.

TP: Installation Windows 7

ACTIONS 2/2 :

- Sélectionner « HKEY_USERS » puis aller dans le menu « Fichier » et cliquer sur « Charger la ruche ». Aller dans « c:\Documents and settings\testregistre » et sélectionner le fichier « NTUSER.DAT ». A quoi correspond ce fichier ?
- Rechercher dans « *HKEY_LOCAL_MACHINE* » la clé « PROFILEIMAGEPATH ». A quoi sert cette clé. On se rend compte que toute la sécurité est basé sur le SID. Il est possible de réassocier un compte utilisateur avec le profil d'un autre utilisateur. Appliquer la procédure suivante <u>http://msreport.free.fr/?p=86</u>
- Aller dans c:\windows\system32\config. On y retrouve tous les fichiers des ruches de la base de registre.
- Lancer la console Gestion de l'ordinateur. Aller dans « Gestion des disques ».
- Créer un nouveau disque virtuelle. Initialiser les disques et le formater.
- Effectuer les exercices suivants :

http://allcomputers.us/windows_7/managing-hardware-in-windows-7-(part-1)--managing-memory---managing-disks.aspx http://allcomputers.us/windows_7/Managing-Hardware-in-Windows-7-(part-2)---

Managing-BIOS---Managing-Devices.aspx

 Lancer le Gestionnaire de périphérique. Aller dans le menu Affichage | Afficher les périphérique cachés pour voir les pilotes cachés (matériel non connecté ou pilotes systèmes). Les antivirus ajoutent des pilotes systèmes pour s'interfacer avec le système.

2. Authentification Windows 7

Les comptes utilisateurs / annuaires :

LES BASES DE COMPTES UTILISATEURS :

- Authentification locale avec la base SAM (System Account Manager) : c'est la base de compte présente par défaut sous Windows 7. La base de compte peut être géré dans la console « Gestion de l'ordinateur » ou dans « Panneau de configuration | Utilisateurs »
- Authentification avec un domaine : nécessite d'intégrer la machine dans un domaine (Active Directory / Samba / NT4). La gestion des comptes se fait alors depuis le contrôleur de domaine. Pour intégrer une machine dans le domaine : « Panneau de configuration | Système | Nom de l'ordinateur | Modifier »
- Authentification avec une base Novell : nécessite le déploiement du client Novell sur Windows 7.

Gestion de l'ordinateur		A. Ht	System Properties	×	Computer Name/Domain Changes		
Fichier Action Affichage ?	2 📅		Computer Name Hardware Advanced System Protection Remote Windows uses the following information to identify your computer on the network.		You can change the name and the membership of this computer. Changes might affect access to network resources. <u>More information</u> Computer name:		
Gestion de l'ordinateur (local)	Nom	Nom complet	For example: "Kitchen Computer" or "Mary's		Guillaume-PC		
 ¹ ¹	 admin asupprimer GLFAdm gmmathieu Invité msreport 	asupprimer gmmathieu msreport	Computer". Full computer name: Guillaume-PC Workgroup: WORKGROUP To use a wizard to join a domain or workgroup, click Network ID Network ID. To rename this computer or change its domain or Change		Full computer name: Guillaume-PC Member of Obmain: msreport.intral Workgroup: WORKGROUP OK Cancel		
Services et applications			OK Cancel Apply				

Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

Comparatif annuaire SAM / AD :

Un service d'annuaire (base de comptes utilisateurs) permet :

- D'identifier des ressources.
- Offre une méthode cohérente pour nommer, décrire, rechercher, accéder, gérer et sécuriser l'accès aux ressources de l'entreprise.

Différence base SAM avec AD :

- AD est annuaire centralisé. Plusieurs machines peuvent accéder aux même annuaires.
- Une base SAM est un annuaire local. Pour pouvoir s'authentifier avec le même compte sur différente machine, il faut recréer le même compte sur différentes machines.

🗳 Active Directory Users and Computers								
🖉 Eile Action View Window Help								
← → 🖻 📧 🖆 🖸 🗟 😫 💷 🦉 🖉 🏷 🍕 🗑								
Active Directory Users and Computer	Users 18 objects							
Hand Saved Queries	Name	Туре	Description					
msproba.nec	🕵 Administrator	User	test					
	🕵 Cert Publishers	Security Group	Members of this group are					
Compacers Domain Controllers	🕵 DnsAdmins	Security Group	DNS Administrators Group					
	🕵 DnsUpdateProxy	Security Group	DNS clients who are permi					
	🕼 Domain Admins	Security Group	Designated administrators					
🗄 🧭 Migration	🕵 Domain Computers	Security Group	All workstations and serve					
	💯 Domain Controllers	Security Group	All domain controllers in th					
	💯 Domain Guests	Security Group	All domain guests					
	💯 Domain Users	Security Group	All domain users					
	💯 Enterprise Admins	Security Group	Designated administrators					
	💯 Group Policy Creator	Security Group	Members in this group can					
	5 Guest	User	test					
	1920 HelpServicesGroup	Security Group	Group for the Help and Su					
	💯 RAS and IAS Servers	Security Group	Servers in this group can					
	🕵 Schema Admins	Security Group	Designated administrators					
	5UPPORT_388945a0	User	test					
	🕵 TelnetClients	Security Group	Members of this group ha					
	🖸 Tigrou Mathieu	User						

SID, TGT, TGS, NTP 1/2 :

SID (Security Identifiant)

- SID (Security Identifiant) : la sécurité sous Windows 7 repose intégralement sur les SID.
- Chaque compte utilisateur, groupe, compte ordinateur dispose d'un SID unique.
- Permission sur un dossier (NTFS) : on affecte les permissions à des SID pas à des noms d'utilisateurs. Quand on supprime un compte utilisateur, les SID non résolus apparaissent au niveau des dossiers.

TGT (TICKET GRANT TICKET) :

- Généré lors de l'ouverture de session d'un utilisateur.
- Contient le SID du compte utilisateur et des groupes dont le compte utilisateur est membre directement ou indirectement. Si l'utilisateur A est membre d'un groupe B qui lui-même est membre d'un groupe C, le TGT contient les SID de A, B et C.
- Voir <u>http://technet.microsoft.com/en-us/library/bb742516.aspx</u>
- Valide pendant 10 heures par défaut. Un utilisateur doit donc fermer sa session, utiliser l'outil KLIST ou attendre 10 heures pour que les modifications d'appartenance aux groupes soient prises en compte.
- Taille maximum TGT : 1014 entrées après modification dans la base de registre: <u>http://support.microsoft.com/kb/327825/en-us</u>
- Sur IIS : <u>http://support.microsoft.com/kb/2020943</u>

SID, TGT, TGS, NTP 2/2 :

TGS (TICKET GRANT SERVICE) :

- L'utilisateur présente son TGT au serveur de ressource qui lui génère alors un TGS avec la liste des accès.
- Valide pendant 10 heures.

NTP (NETWORK TIME PROTOCOL) :

- Par défaut, l'authentification Kerberos autorise un maximum de 5 minutes de décalage horaire.
- Les stations de travail se synchronise au contrôleur de domaine via le service W32Time.



Authentification avec un domaine AD :

A SAVOIR :

- Un domaine Active Directory a deux noms, un nom NETBIOS et un nom DNS.
- Toujours joindre une machine Windows 7 avec le nom DNS du domaine Active Directory (AD).
- Les stations de travail localisent les contrôleurs du domaine ORGA2.LAN en effectuant des requêtes sur les enregistrements DNS _ldap._tcp.orga2.lan et _ldap._tcp.le_nomsitead.orga2.lan.
- Pour changer un mot de passe depuis une machine Windows 7 (CTRL + ALT
- + SUPPR | Changer mot de passe), Windows 7 résout l'entrée DNS __ldap._tcp.pdc._msdcs.orga2.lan



TP : authentification

ACTIONS

- Créer un compte dans la base SAM appelé MSREPORT
- Créer un dossier c:\test et affecter des permissions (contrôle total) au compte MSREPORT.*
- Supprimer le compte local appelé MSREPORT
- Fermer la session et la rouvrir.
- Aller dans les propriétés du dossier c:\test.
- Le SID du compte va apparaître au niveau du dossier c:\test. Conclure
- Joindre la machine dans le domaine Active Directory.
- Ouvrir une session avec un compte du domaine.

Isreport Properties			?	X
General Sharing Security	Web S	haring Custor	mize	
Group or user names:				
🖗 Account Unknown(S-1	1-5-21-12	29272821-202	5429265-682	
🛛 🙍 Administrator (SRVXP)	02\Admin	iistrator)		
🖉 🚮 Administrators (SRVXF	PO2\Admi	nistrators)		
SYSTEM				
		1		.
Dennissians (ex Alexand)		Add	Remove] [
Unknown(S-1-5-21-1229272	2821-2	Allow	Deny	
Full Control				
Modify		\checkmark		
Read & Execute		\checkmark		
List Folder Contents				
Head]
Special Permissions				
For special permissions or fo	or advanc	ed settings,	Advanced	ı I
click Advanced.				
	ОК	Cancel	Apply	

Profil utilisateur 1/3 :

LE PROFIL :

- Profil d'un utilisateur Windows 7 : dossier portant le nom de l'utilisateur (par défaut) dans C:\Users.
- Ce dossier contient : AppData (fichiers liés aux applications), Contacts (les contacts Windows), Desktop (tous les dossiers / fichiers du bureau), Downloads (le dossier de téléchargement par défaut d'Internet Explorer), Favorites (les favoris Internet Explorer), My Documents (le dossier Mes documents), NTUSER.DAT (les paramètres de configuration de la session de l'utilisateur).
- Sous XP, tous les profils utilisateurs sont sous c:\Documents and Settings. Ce répertoire existe toujours sous Windows 7 pour la compatibilité avec les applications (lien physique vers c:\Users).
- Accès à c:\Documents and Settings : accès refusé
- Accès à c:\Documents and Settings\nomutilisateur : cela fonctionne.
- Première connexion d'un utilisateur sur une machine : le nouveau profil utilisateur est généré à partir d'une copie du profil par défaut (C:\Users\Default).
- C:\Default User : profil par défaut sous Windows XP. Existe sous Windows 7 pour la compatibilité avec les applications (lien physique vers c:\Users\Default).
- Accès à C:\Default User : accès refusé
- Accès à C:\Users\Default User\AppData : cela fonctionne.
- UtilisateurA et le groupe Administrateurs disposent des droits sur le dossier c:\users\utilisateurA correspondant au profil de l'utilisateur A.

Profil utilisateur 2/3 :

Le fichier NTUSER.DAT :

- C'est une ruche de la base de registre.
- Contient tous les paramètres de la session de l'utilisateur (fond d'écran, imprimantes, configuration des logiciels spécifiques à l'utilisateur).
- A l'ouverture de session la ruche c:\users\nomusers\NTUSER.DAT est chargée dans la base de registre sous HKEY_USERS.
- Seul l'utilisateur associé au profil et le groupe Administrateurs disposent des droits sur le profil.

Registry Editor				
File Edit View Favorites Help				
File Edit View Favorites Help Image: Solution of the state o		Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ for 7-Zip ames: TED (Guillaume-PC\Guillaum	Data (value not set) fr C:\Program Files (x86)\7-Zip C:\Program Files (x86)\7-Zip
	-]	& Guillaume	tors (Guillaume-PC\Adm	ninistrators)

Profil utilisateur 3/3 :

A SAVOIR

- Au niveau de la base de registre, c'est l'entrée ProfileImagePath (ProfileList).
- Au niveau interface : Panneau de configuration | Système | Paramètres systèmes avancées. Aller dans l'onglet Avancé puis cliquer sur Propriétés dans la section « Profil utilisateur »
- A l'ouverture de session la ruche c:\users\nomusers\NTUSER.DAT est chargé dans la base de registre sous HKEY_USERS. On retrouve dans cette ruche tous les paramètres de la session de l'utilisateur (fond d'écran, imprimantes, configuration des logiciels spécifiques à l'utilisateur).

Registry Editor				On proin utilisateur stocke les parametres de votre bureau et d'autres informations liées à votre compte d'utilisateur. Vous pouvez créer un profil différent sur d'aque ordinateur que vous utilisez ou vous pouvez sélectionner un profil itinérant qui sera le même partout.	
Price ProfileList ProfileList S-1-5-18 S-1-5-19 S-1-5-20 S-1-5-21-2882737045-3759444556-2855104356-1000 S-1-5-21-2882737045-3759444556-2855104356-1004 ProfileLoader ProfileNotification related.desc SecEdit Computer \HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows	Name (Default) (Defa	Type REG_SZ REG_DWORD REG_EXPAND_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_BINARY REG_DWORD	Data (value not set) 0x0000000 (0) C:\Users\Guillaume 0x00000000 (0) 0x00000000 (0) 0x00000000 (1) 0x00000000 (0) 01 05 00 00 00 00 00 05 15 0(0x00000100 (256) 45-3759444556-2855104356-1000	Profile erregistrés sur cet ordinateur Nom Ta Profil par défaut 1,511 SEVEN3/jadmin 25,81 SEVEN3/jadmin 35,81 Vou must be logged on as an Administrator to make most of these char SEVEN3/msreport 22,91 Modifier le type Modifier le type Pour créer de nouveaux comptes d'ut Comptes d'utilisateurs dans le Pannee Startup and Recovery System startup, system failure, and debugging information Settings.	y
				OK Cancel #	

Le coffre fort Windows 7 :

LE COFFRE FORT :

- Windows 7 permet d'enregistrer des mots de passe pour l'accès à des ressources dans le coffre fort. Cela permet que le mot de passe ne soit plus demandé.
- Si accès à une machine d'un autre domaine non approuvé / groupe de travail, il faut s'authentifier. On peut alors cocher la case « Mémoriser ces informations ».
- Accès coffre fort : Panneau configuration | Gestionnaire identification.
- Retour expérience : quand on change de mots de passe pour le compte réseau, il faut aller dans le coffre fort pour modifier / supprimer l'entrée.



Appliquer

OK

Annuler

3. Partage de fichiers Windows 7

Permissions NTFS :

PERMISSION NTFS :

- Onglet sécurité : permet de définir des permissions NTFS.
- Deux affichages pour les permissions NTFS : simplifiés (5 permissions), complexes (13 permissions).
- Héritage : les permissions du dossier parent héritent sur les dossiers enfants.
- Pour supprimer permissions héritées : casser l'héritage.
- Permissions héritées : apparaissent grisées.
- Permissions définis sur l'objet : apparaissent en noir.

📙 Propriétés de : Test2	Paramètres de sécurité avancés pour Test2	
Général Partage Sécurité Versions précédentes Personnaliser	Autorisations Audit Propriétaire Autorisations effectives	
Nom de l'objet : D:\Test2	Double-cliquez pour voir les détails de l'autorisation. Pour modifier, cliquez sur Modifier les autorisations. Nom de l'objet : D:\Test2	
Noms de groupes ou d'utilisateurs :	Entrées d'autorisations ·	
& Utilisateurs authentifiés & Système	Type Nom Autorisation Héritée de Appliquer à	
Administrateurs (SEVEN3\Administrateurs) Utilisateurs (SEVEN3\Utilisateurs)	Autoriser Administrateurs (SEVEN3 Contrôle total D:\ Ce dossier, les sous-dossi Autoriser Système Contrôle total D:\ Ce dossier, les sous-dossi Autoriser Utilisateurs authentifiés Modification D:\ Ce dossier, les sous-dossi	
Pour modifier les autorisations, cliquez sur Modifier. Modifier	Autoriser Utilisateurs (SEVEN3\Utili Lecture et exécution D:\ Ce dossier, les sous-dossi	×
Autorisations pour Utilisateurs authentifiés Autoriser Refuser	Autorisations Aventisement : si vuo continues, les autorisations pouvant Pour afficher ou modifier les détails d'une autorisation, sélecti Nom de l'objet : D: Test2	t être héritées ns héritées de bjet.
Contrôle total Modification Lecture et exécution Affichage du contenu du dossier Lecture Écriture	Modifier les autorisations Inclure les autorisations pouvant être hé Gestion des entrées d'autorisations	iées de l'objet amètres d'héritage.
Pour les autorisations spéciales et les paramètres avancés, cliquez sur Avancé Avancé.	Ajouter Modifier Suprimer	
Informations sur le contrôle d'accès et les autorisations OK Annuler Appliquer	Gestion des entrées d'autorisations OK Annuler Appliquer	×⊖ ⊽:

Permissions de partage :

PERMISSION DE PARTAGE :

- Dans l'onglet Partage | Permissions.
- Ces permissions s'appliquent quand on accède aux dossiers par le chemin UNC <u>\\nommachine\nompartage</u>.

🐌 Propriétés de : Test	23
Partage avancé	
✓ Partager ce dossier	
Paramètres	
Nom du partage :	
Test	
Ajouter	
Limiter le nombre d'utilisateurs simultanés à : 20 👻	
Commentaires :	finir
Autorisations Mise en cache	
OK Annuler Appliquer	
Fermer Annuler	Appliquer

Comment sécuriser un dossier ?

BONNES PRATIQUES :

- Casser l'héritage au niveau du dossier parent.
- Créer 1 groupe local (base SAM ou Active Directory) pour chaque type d'accès : lecture, écriture, contrôle totale.
- Définir les permissions sur ce dossier pour les 3 groupes locaux, le compte system et le groupe « Administrateurs » de l'ordinateur.
- Ajouter les utilisateurs ou les groupes de services (groupes globaux dans l'annuaire Active Directory) en tant que membre des groupes locaux / locaux de domaine.
- Partager le dossier. Définir les permissions de partage sur Contrôle Total pour Utilisateurs authentifiées (pas de contrôle sur permissions de partages).
- Laisser l'héritage sur les dossiers enfants sauf si besoin de droits spécifiques.
- Eviter de trop personnaliser les droits dans les arborescences. Il faut limiter le nombre de groupe car la taille du TGT maximum est de 1014 SID. Il faut éviter de devoir appartenir à 100 groupes pour accéder à un répertoire projet par exemple.

4. Internet Explorer

Internet Explorer et la sécurité

ZONES DE SECURITE INTERNET EXPLORER :

- 4 zones pour les sites web avec des réglages différents : Internet, Intranet local, Sites web de confiance, Sites sensibles. Chaque zone dispose de ses propres réglages de sécurité (activation des cookies, ActiveX...).
- Mode protégé : un peu comme l'UAC pour Internet Explorer. Il bloque les scripts qui nécessitent des privilèges d'administration. Le but est d'empêcher qu'un script ActiveX formate une partition ou modifie une entrée dans la base de registre.
- Zone Intranet local : l'authentification intégré (géré par IIS) permet d'envoyer le login / mot de passe utilisé pour ouvrir une session au serveur web. Pour des raisons de sécurité, le site web doit être dans la zone Intranet Local. Dans le cas contraire, l'utilisateur devra s'authentifier de nouveau.

	Options Internet	
	Général Sécurité Confidentialité Contenu Connexions Programmes Avancé	Paramètres
	Cliquez sur une zone pour afficher ou modifier les paramètres de sécurité.	INET Framework Applications du navigateur XAML Activer Demander Désactiver
	Internet Internet Cette zone est destinée aux sites Web Internet, à l'exception de ceux répertoriés dans les zones Sites de confiance et Sites sensibles.	Octiments Ars Octiments Ars Octiments Ars Octiments Ars Octiments Ars Octiments Octim
Intranet local X		AMU ISOIE
Utilisez les paramètres ci-dessous pour définir les sites Web à inclure dans la zone Intranet local.	Niveau de sécurité pour cette zone Niveaux autorisés pour cette zone : Moyen à Haut - - - - Moyen-haut - - - Adoté orue la plupart des sites Web	O Demander O Désactiver
Détecter automatiquement le réseau Intranet	- Hessages avant le téléchargement de contenu potentiellement dangereux - Les contrôles ActiveX non signés ne seront pas téléchargés	Connexion
Inclure tous les sites locaux (intranet) non mentionnés dans d'autres zones	Activer le mode protégé (redémarrage d'Internet Explorer requis)	*Ne prend effet 🖓 après le redémarrage d'Internet Explorer
🗖 Indure tous les sites qui n'utilisent pas de serveur proxy	Personnaliser le niveau Niveau par défaut	
🔲 Indure tous les chemins d'accès au réseau (UNC)	Rétablir toutes les zones au niveau par défaut	Rétablir : Haute (Par défaut)
Que sont les paramètres intranet 2 Avancé OK Annuler	OK Annuler Appliquer	OK Annuler

Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

Internet Explorer

LES PROTOCOLES D'AUTHENTIFICATION :

- Authentification intégrée : basée sur le protocole KERBEROS / NTLM.
- Authentification de base : le mot de passe est envoyé en clair par le réseau. Si le trafic web n'est pas chiffré (HTTPS), il est possible de retrouver le mot de passe via un outil comme WIRESHARK (<u>http://www.wireshark.org/download.html</u>).

ADMINISTRATION / DEPLOIEMENT INTERNET EXPLORER:

- Internet Explorer est configurable par stratégie de groupes (Internet Explorer Maintenance dans stratégie utilisateur).
- Il est possible de déployer une version préconfiguré d'Internet Explorer à l'aide de l'IEAK.



Internet Explorer (confidentialité / interface)

MECANISMES DE SECURITE INTERNET EXPLORER :

 Internet Explorer permet de purger le cache de navigation à la fermeture. Pour cela, cocher la case « Supprimer l'historique de navigation en quittant le navigateur » dans Options Internet.

CONFIGURATION DE L'INTERFACE :

- Pour configurer Internet Explorer 9 pour afficher le menu : cliquer sur Affichage | Barre d'outils | Barre de menu.
- Pour Configurer Internet Explorer 9 pour afficher la barre d'adresse sur une seule ligne : faire un clic droit en dessous de la barre d'adresses et cocher la case
 « Afficher les onglets dans une ligne séparée »

File Edit	View Favorites	Tools Help		
<u>k</u>	Toobars		🕨 🗸 Menu bar	
	Quick tabs	Ctrl+Q	 Favorites bar 	
Outlo	Explorer bars		 Command bar 	
Outio	C		 Status bar 	
	Go to		avast! WebRep	
Messad	Stop	Esc		
	Refresh	F5	Lock the toolbars	
Download Remote Server Administration Tools for Windows 7 with SP1 from Official Microsoft Down - Windows Inter				
		n/en-us/download/details.aspx?id=70		
Download Remote	e Server Ad 🗙		Menu bar	
File Edit View	Command bar			
≱			✓ Status bar	
	Microsoft		avast! WebRep ✓ Lock the toolbars	
			Snow taps on a separate row	

Options Inte	ernet ?X
Général S	écurité Confidentialité Contenu Connexions Programmes Avancé
Page de d	émarrage
	Pour créer des onglets de page de démarrage, entrez une adresse par ligne.
	http://go.microsoft.com/fwlink/?LinkId=69157
	Page actuelle Par défaut Page vierge
Historique	e de navigation
Ð	Supprimer les fichiers temporaires, l'historique, les cookies, les mots de passe enregistrés et les données de formulaires Web.
	Supprimer l'historique de navigation en quittant le navigateur
	Supprimer Paramètres
Recherch	es
\wp	Modifier les paramètres de recherche par défaut. Paramètres
Onglets	
	Modifier la présentation des pages Web dans les onglets. Paramètres
Apparenc	e
	Couleurs Langues Polices Accessibilité
	OK Annuler Appliquer

5. Outils d'administration Windows 7

Guillaume MATHIEU - http://msreport.free.fr - La connaissance s'accroît quand on la partage

Les outils d'administration graphiques 1/2 :

OUTIL D'ADMINISTRATION :

- Les consoles MMC : permet de gérer les fonctionnalités d'une machine locale et distante. S'appuie sur le protocole RPC.
- Protocole RPC : connexion initiale sur le port TCP 135. Négociation d'un port dynamique (1024 – 65535) pour le trafic des données. Chaque application RPC a un numéro unique. Pose de nombreux problèmes avec les pare feu. Forefront TMG sait gérer de manière sécuriser ce type de trafic (en filtrant les numéros d'application).
- Voir <u>http://technet.microsoft.com/en-us/library/cc738291(v=ws.10).aspx</u>
- Consoles MMC prédéfinis : fichier .MSC présent dans c:\windows\system32.
- Composant logiciel enfichable : chaque service (IIS, DNS...) dispose de son composant logiciel enfichable.
- MMC.EXE : permet de créer une console MMC vierge et d'ajouter des composants logiciels enfichables.
- De nombreux composants logiciels enfichables ne sont pas présent dans les consoles MMC prédéfinis (comme magasin de certificat).

			Allouter ou supprimer des composantes logicieus enne	Askehity of St.
Console1 - [Racine de la console]		Vous pouvez sélectionner des composants logiciels enfichables parmi ceux disc		
📸 Fichier Action Affichage Favoris Feni	être ?		Composants logicels enfichables disponibles :	Composant
(= -> 📅 🔄 🖬			Composant logiciel enfi Fournisseur	Racine
Racine de la console	Nom		Analyseur de perfor Microsoft Cor	
		Aucun élément à afficher dans cet aperçu.	2 Configuration du clie Microsoft Cor	
			Configuration et ana Microsoft Cor	
			Contrôle WMI Microsoft Cor	>

Les outils d'administration graphiques 2/2 :

OUTIL D'ADMINISTRATION :

- Microsoft va vers l'abandon du RPC qui est remplacé par le protocole Windows Remote Management (WIN RM) qui s'appuie sur le protocole HTTP / HTTPS.
- Ce protocole est une implémentation du protocole standard WS-MANAGEMENT.
- Sous Windows 7, le service WINRM s'appelle WINMGMT



TP : outils d'administration graphiques :

ACTIONS :

- Créer une console vierge en exécutant MMC.EXE
- Ajout le composant logiciel certificat (Fichier | Ajouter et supprimer un composant logiciel enfichable).
- Sélectionner le composant certificat.
- Sélectionner certificat pour le compte utilisateur.
- Enregistrer la console sur le Bureau (lab1.msc).
- Il est possible de configurer le fait que la console ne soit plus modifiable sauf si on l'ouvre en mode auteur). Cela se règle dans Fichier | Options.
- Installer le service IIS sous Windows 7. Le composant logiciel enfichable IIS est maintenant disponible.
- Installer les RSAT pour Windows Seven SP1 (fichiers Windows6.1-KB958830x86-RefreshPkg.msu ou Windows6.1-KB958830-x64-RefreshPkg.msu).
- Aller dans Panneau de configuration | Programmes et fonctionnalités | Activer ou désactiver des fonctionnalités Windows. Aller dans la section Outils d'administration à distance. Activer la console DNS et DHCP.
- Ajouter les composants logiciels enfichable DNS et DHCP et se connecter à une machine Windows Server 2008 R2 avec les services DHCP / DNS installés.

PowerShell

Présentation PowerShell :

- Installé de base sous Windows 7.
- Nouvelle interface ligne de commande / s'appuie sur le .Net Framework.
- Format de commande simple : commutateur-objet
- Liste commutateur : Get, new, Add, Remove, Set...
- Liste objets : ChildItem, QADuser, QADobjet
- Exemple de commande : Get-QADuser (liste tous les comptes utilisateurs du domaine).
- Extensible (ajout de CMDLETs via chargement PSSNAPINs). Quest fournit un plugin gratuit pour gérer les ressources Active Directory (ActiveRoles Management Shell).
- Les opérateurs (< > | where –ne), les variables \$_.attributs et les filtres
- Le pipe « | » : permet de chaîner deux commandes. La commande Get-QADuser | Set-QADuser – description Msreport va définir Msreport dans le champ description de tous les utilisateurs de la forêt.

Les commandes PowerShell indispensables :

- Get-Help nom_cmdlet : Get-Help get-aduser –full Get-Help get-aduser -examples
- Get-pssnapin : pour avoir la liste des composants de PowerShell
- Select-object : permet de sélectionner que certains attributs de l'objet de sortie

TP: Powershell:

ACTIONS :

- Lancer PowerShell.
- Taper Get- puis appuyer sur la touche TAB. PowerShell va proposer de compléter la commande.
- Lister les alias de la commande Get-ChildItems en tapant : Get-Alias Get-ChildItems
- Installer Quest ActiveRoles Management Shell pour gérer l'Active Directory : <u>http://www.quest.com/powershell/activeroles-server.aspx</u>
- Lancer le PowerShell avec les addins QUEST.
- Taper les commandes suivantes sur un environnement de tests : New-QADUser -SamAccountName melanie.mathieu -FirstName Mélanie -LastName "Mathieu Bertrand" -Description "Compte utlisateur de Mélanie MATHIEU BERTRAND" -ParentContainer "OU=GLF,DC=MSPROBA,DC=NET" -name melanie.mathieu | Set-QADUser -UserPassword P@ssword

Get-QADUser -SearchRoot "OU=GLF,DC=MSPROBA,DC=NET" | Format-Table – Property SamAccountname,Description

[PS] C:\Users∖administrator>Get-QADUser -SearchRoot escription	"OU=GLF,DC=MSPROBA,DC=NET" Format-Table -Property SamAccountname,D
SamAccountName	Description
Wissam manar.hamor eugene.tosenda melanie.mathieu	test compte utilisateur de Manar hamor Mon premier compte utilisateur avec PowerShell Compte utlisateur de Mélanie MATHIEU BERTRAND

PMAD sous Windows 7 :

Deux solutions natives :

- Bureau distance (Terminal Server mode administration à distance) : port à ouvrir en entrée TCP 3389. Très fluide, peu gourmant au niveau réseau. Permet la redirection des imprimantes, du son et des lecteurs disques. 1 seul utilisateur peut se connecter en bureau à distance. L'autre utilisateur est déconnecté. Pas de mode observation sous Windows 7 (seule une personne peut voir l'écran).
- Assistance à distance : basé sur le protocole RDP, port à ouvrir en entrée TCP 3389 et TCP 445. Nécessite l'approbation de l'utilisateur pour établir la connexion.
 2 personnes peuvent visualiser l'écran en même temps, possibilité de mettre en pause l'affichage écran, envoie de fichiers, messagerie instantanée.
- Une version de client à distance pour chaque évolution du protocole Bureau à distance / Terminal Server : <u>http://support.microsoft.com/kb/2592687/en-us</u>
- Une connexion d'Assistance à distance peut être créé via l'aide de Windows (échange d'un fichier, <u>http://support.microsoft.com/kb/981004/fr</u>) ou via un client dédié (nécessite configuration station de travail, méthode recommandée). Voir <u>http://www.rigolet.fr/articles/print.php?id=3</u>

Solutions tierces :

 TeamViewer / LOGMIN : A et B établissent une connexion sortante (HTTPS) vers le serveur de TEAMVIEWER. Les serveurs de TeamViewer établissent la relation entre les A et B et permettent le partage d'écran. Comme le trafic HTTPS est rarement bloqué, le partage d'écran à travers un proxy est possible.

TP : utilisation du bureau à distance

ACTIONS:

- Sur la machine A, aller dans Panneau de configuration | Système | Paramètres systèmes avancées. Dans la fenêtre Propriétés Systèmes, cocher la case « Autoriser la connexion des ordinateurs exécutant n'importe quelle version du bureau à distance ». Déterminer l'IP de la machine A.
- Sur la machine B, taper Démarrer | Exécuter | MSTSC.EXE. Cliquer sur me bouton options et cliquer sur l'onglet « Display » et configurer la résolution sur 800 * 600, 16 bits. Cliquer sur l'onglet « Local Ressources » et sur le bouton « More ». Configurer le client bureau à distance pour connecter le disque C.

Propriétés système	Remote Desktop Connection	Remote Desktop Connection
Nom de l'ordinateur Matériel Paramètres système avancés Protection du système Utilisation à distance	Remote Desktop Connection	Remote Desktop Connection
Assistance à distance Autoriser les connexions d'assistance à distance vers cet ordinateur Que se passet il lorsque l'active l'Assistance à distance ? Options avancées	General Display Local Resources Programs Experience Advanced Display configuration Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen. Small	General Display Local Resources Programs Experience Advanced Remote audio Configure remote audio settings. Settings
Bureau à distance Cliquez sur une option puis spécifiez qui peut se connecter.	1024 by 768 pixels	Keyboard Apply Windows key combinations: Image: Only when using the full screen Image: Example: ALT+TAB
 Autoriser la connexion des ordinateurs exécutant n'importe quelle version du Bureau à distance (moins sûr) N'autoriser gue la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (plus sûr) 	Choose the color depth of the remote session. Highest Quality (32 bit)	Local devices and resources Choose the devices and resources that you want to use in your remote session. Printers Clipboard
Comment choisir ? Sélectionnez des utilisateurs OK Annuler Appliquer	Options Connect Help	More Options Connect Help

Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

TP : assistance à distance

OBJECTIFS:

A se connecte sur la machine de B.

ACTIONS :

- Sur B, dans « *Propriétés systèmes* », cocher la case « *Assistance à distance* ».
- Créer une stratégie de groupe pour activer l'assistance à distance sur les stations de travail. Activer les paramètres « Activer la journalisation de session », « Activer l'optimisation de la bande passante » et « Proposer l'assistance à distance ».
- Définir le groupe qui a le droit de proposer une assistance à distance. Ajouter l'utilisateur A dans ce groupe.
- Sur A, exécuter la commande C:\Windows\System32\msra.exe /offerRA

📑 Stratégie assistance à distance [^y aramètre	État	Propriétés système		×
 Stratégie assistance à distance [Configuration ordinateur Stratégies Paramètres du logiciel Composants Windows Composants Windows Composants Windows Microsoft InfoPath 2010 (ordinateur) Microsoft PowerPoint 2010 (ordinateur) Microsoft PowerPoint 2010 (ordinateur) Réseau Système Accès au stockage amovible Accès réseau Appel de procédure distante Assistance à distance Assistance à distance 	aramètre Activer la journalisation de session Activer la journalisation de la bande passante Personnaliser les messages d'avertissement Assistance à distance sollicitée Proposer l'Assistance à distance Activer le contract à distance Proposer l'Assistance à distance Proposer l'Assistence à distance Proposer l'Assistence Proposer l'Assistence à distance Proposer l'Assistence Proposer l'Assistence à distance Proposer l'Assistence Proposer l'Assistence à distance Proposer l'Assistence Proposer l'Assist	État Non configuré Activé Non configuré Non configuré Non configuré Activé	Propriétés système Nom de l'ordinateur Paramètres système avancés Protect Assistance à distance Image: Context and the system avancés Protect Assistance à distance Image: Context and the system avancés Protect Que se passe till term Image: Context and the system avancés Image: Context and the system avancés Bureau à distance Image: Context and the system avancés Image: Context and the system avancés Image: Context and the system avancés Bureau à distance Image: Context and the system avancés Image: Context and the system avancés Image: Context and the system avancés Comment choisir ? Image: Context and the system avancés Image: Context and the system avancés Image: Context and the system avancés	Matériel tion du système Utilisation à distance address. What settings are needed? ere name or IP address:	an connect directly using either the computer
	Dr Conten Ork	Annuler Appliquer			Maxt Carrel

6. Gestion configuration station de travail

Guillaume MATHIEU - http://msreport.free.fr - La connaissance s'accroît quand on la partage

Qu'est ce qu'une stratégie de groupe ?

QU'EST CE QU'UNE STRATÉGIE DE GROUPE :

- Les stratégies de groupes (GPO) sont des clés et valeurs de registre.
- Deux sections pour les stratégies de groupe : Configuration ordinateur (modifie HKEY_LOCAL_MACHINE) et Configuration utilisateur (modifie HKEY_USERS).
- Les stratégies de groupe peuvent être définies localement et/ou via un domaine Active Directory.

LES STRATÉGIES DE GROUPE PERMETTENT :

- De déployer des logiciels : déploiement fichier MSI uniquement, pas de rapport, pas de gestion bande passante.
- D'exécuter des scripts au démarrage / arrêt de la machine (sous compte SYSTEM).
- De configurer les stratégies de mots de passe : <u>http://msreport.free.fr/?p=156</u>.
- De configurer les paramètres de sécurité (qui peut ouvrir une session localement, arrêter la machine ...).
- De configurer les paramètres des logiciels et du système (Windows Update, interface utilisateur, configuration des logiciels).

EXTENSION :

 Les GPO sont extensibles : via ajout fichiers ADM / ADMX pour paramétrer des logiciels comme Office, Adobe Acrobat, CitrixXenApp) : <u>http://www.microsoft.com/downloads/details.aspx?familyid=92d8519a-e143-4aee-8f7a-e4bbaeba13e7&displaylang=en</u>

ADMINISTRATION DES GPO :

GPO LOCAL :

- Sous Windows 7, exécuter MMC.EXE. Ajouter le composant logiciel enfichable « Objets de stratégie de groupe ».
- La GPO ne s'applique qu'à la machine.
- Pas de support de la fonctionnalité déploiement de logiciel.
- GPO local = éditeur base registre.

GPO CRÉÉ DEPUIS UN CONTRÔLEUR DE DOMAINE :

- Création via console Gestion des stratégies de groupe (GPMC)
- Possibilité d'appliquer la GPO à plusieurs machines / comptes utilisateurs.



🛃 Gestion de stratégie de groupe		
🛃 Fichier Action Affichage Fenêtre ?		
🗢 🔿 🖄 🖬 🙆 📔 🖬		
📓 Gestion de stratégie de groupe	Default Domain Controllers Policy	
🖃 🔬 Forêt : formation10.lan	Étendue Détails Paramètres Délégation	
🖂 📑 Domaines		
E 📰 Formation10.lan	Default Domain Controllers Policy	
Default Domain Policy	Données recueillies le : 10/06/2010 19:47:01	afficher tout
Administration des ventes	Configuration ordinateur (activée)	masquer
🕀 🧧 Comprabilitie	Charlie	
Default Domain Controllers	Sudleyles	masquer
Formation	Paramètres Windows	masquer
Production	Paramètres de sécurité	masquer
I I I Vente		
🗉 📴 Objets de stratégie de groupe	Strategies locales/Attribution des droits u	itilisateur <u>masquer</u>
🕀 🙀 Filtres WMI	Stratégie	Paramètre
표 🛅 Objets GPO Starter	Accéder à cet ordinateur à partir du réseau	BUILTIN\Accès compatible pré-Windows
🕀 📑 Sites		2000, AUTORITE NT\ENTERPRISE
🔯 Modélisation de stratégie de groupe		DOMAIN CONTROLLERS, AUTORITE
🞼 Résultats de stratégie de groupe		NT\Utilisateurs authentifiés,

Comment s'appliquent les GPO ?

- Une GPO « Configuration Ordinateur » s'applique à une machine (si compte ordinateur est dans OU où est liée la GPO et si le compte ordinateur a les droits « Lire » et « Appliquer la stratégie de groupe »).
- Une GPO « Configuration Utilisateur » s'applique aux utilisateurs (si compte utilisateur est dans OU où est liée la GPO et si le compte utilisateur a les droits « Lire » et « Appliquer la stratégie de groupe »).
- Par défaut « Utilisateurs authentifiés » (toutes les comptes ordinateurs et utilisateurs qui ont ouvert une session) a les droits « Lire » et « Appliquer la stratégie de groupe ». Possibilité filtrage en supprimant cet entité de sécurité.



Administration des stratégies de groupe :

ORDRE APPLICATION GPO / GESTION CONFLIT :

- GPO s'appliquent dans un certains ordre : Local, Site, Domaine, unités d'organisation (OU), unités d'organisation enfant (OU)
- Si paramètres contradictoires à différents niveaux, stratégie au niveau OU qui l'emporte sauf si activation paramètres « Appliquer » (ne pas passer outre) et/ou « Bloquer l'héritage »
- Paramètre « Appliquer » : force l'application de la GPO.
- Paramètre « Bloquer l'héritage » : si ce paramètre est fixé au niveau d'une OU enfant, les GPO au niveau des sites, domaines et des OU parent ne s'appliquent pas (sauf les paramètres de sécurité).
- Le paramètre « Appliquer » prime sur le paramètre « Bloquer l'héritage ».



7. Sécuriser Windows 7

Guillaume MATHIEU – http://msreport.free.fr – La connaissance s'accroît quand on la partage

Le pare feu de Windows 7 :

PARE FEU SOUS WINDOWS SEVEN :

- Windows 7 dispose d'un pare feu entrant / sortant STATEFULL activé par défaut.
- 3 profils : domaine (machine membre du domaine), public et privé (machine en groupe de travail : l'utilisateur choisit le profil selon le réseau)
- Paramétrable par stratégie de groupe ou via la console Pare feu avec fonctionnalités avancées : <u>http://www.howtogeek.com/100409/group-policy-geek-how-to-control-the-windows-firewall-with-a-gpo/</u>
- Règles gérés dynamiquement quand on active une fonctionnalité Microsoft.
 RISQUE :
- Mauvais fonctionnement application liée à des ports bloqués. Nécessite de connaître son environnement et les prérequis des applications métiers.



L'UAC :

UAC :

- Contrôle les accès administratif au système d'exploitation Windows 7 depuis l'interface graphique ou via l'invite de commande.
- Activé par défaut sous Windows 7
- Pour exécuter une application / invite de commande sans l'UAC : faire un clic droit, exécuter en tant qu'administrateur.
- Pour configurer l'UAC : aller dans le Panneau de configuration | Comptes utilisateurs.
- Niveau de l'UAC paramétrable.
- Possibilité de configurer l'UAC par stratégie de groupe : <u>http://technet.microsoft.com/en-</u> us/library/dd835564(WS.10).aspx

PROBLEMES GENERES PAR L'UAC :

- Problème d'exécution des scripts de login.
- Problème avec des applications qui nécessitent des droits administrateurs (exécution action sur le système en arrière plan).



Change

🌏 Exécuter en tant qu'administrateur

Épingler à la barre des tâches Épingler au menu Démarrer Supprimer de cette liste

Propriétés

Pourquoi installer mises à jour Windows ?

QUELS SONT LES RISQUES POUR UNE STATION DE TRAVAIL WINDOWS 7 ?

- Virus : nécessite une action de l'utilisateur (cliquer sur fichier infecté...).
- Faille de sécurité : elle peut être exploitée sans requérir d'intervention de l'utilisateur.

COMMENT SE PREMUNIR DE CES 2 RISQUES ?

- Virus : installer un antivirus et filtrer les connexions Internet à l'aide de proxy.
- Faille de sécurité : installer les mises à jour Windows à l'aide de Windows Update ou de WSUS.

POURQUOI LES ADMINISTRATEURS HÉSITENT À INSTALLER LES MISES À JOUR ?

 Certaines mises à jour génèrent des problèmes avec les applications métiers (ralentissement ou instabilité).

COMMENT LIMITER LE RISQUE LIE A L'INSTALLATION DES MISES A JOUR ?

- Proposer aux administrateurs de valider les correctifs à déployer sur environnement de test copie conforme de la production.
- Déployer que les correctifs de sécurité critiques ou importants tous les mois
- Déployer les correctifs de sécurité moyen et faible après recette des applications.
- Déployer un serveur WSUS pour contrôler les correctifs déployés et les machines sur lesquels ils sont déployés.

Comment exploiter une faille de sécurité ?

PRÉSENTATION DE METASPLOIT :

- Outil gratuit téléchargeable depuis <u>http://www.metasploit.com/download/</u>
- Très bien documenté.
- Le TOP 10 des failles les plus dangereuses : <u>https://community.rapid7.com/community/metasploit/blog/2012/12/11/exploit-trends-new-exploits-make-the-top-10</u>
- CVE-2008-4250 / MSB-MS08-067 : prise de contrôle Windows XP SP3 : <u>http://www.metasploit.com/modules/exploit/windows/smb/ms08_067_netapi</u>
- CVE-2012-0002, MSB-MS12-020 : écran bleu machine Windows avec bureau à distance activé :

http://www.metasploit.com/modules/auxiliary/dos/windows/rdp/ms12_020_maxch annelids

 CVE-2010-0017 / MSB-MS10-006 : écran bleu sur une machine Windows 2008 R2 SP0 (nécessite accès en lecture à un partage) : <u>http://www.metasploit.com/modules/auxiliary/dos/windows/smb/ms10_006_negot</u> <u>iate_response_loop</u>

TP: Utilisation de METASPLOIT

ACTIONS 1/2 :

- Dans un environnement réseau isolé (2 machines virtuelles A, B sous Windows XP SP3 avec mise à jour pour A, sans mise à jour pour B et 1 machine virtuelle C sous Windows 2008 R2 SP1 sans mise à jour).
- Télécharger (avec Chrome) et installer l'outil METASPLOIT depuis <u>http://www.metasploit.com/download</u> sur ma machine A.
- Activer le bureau à distance sur la machine C, récupérer l'IP de la machine A et C et appliquer la procédure suivante :

http://www.metasploit.com/modules/auxiliary/dos/windows/rdp/ms12_020_maxch annelids



TP: Utilisation de METASPLOIT

ACTIONS 2/2 :

- Récupérer l'IP et désactiver le pare feu sur A et B : Il faut autoriser le déport de l'invite de commande de la machine B sur A.
- Appliquer la procédure suivante <u>http://www.metasploit.com/modules/exploit/windows/smb/ms08_067_netapi</u>
- Il est important d'avoir un déport du shell. Le service serveur plante sur B
- Taper ? pour avoir la liste des commandes puis getsystem pour récupérer les droits administrateur, clearenv pour purger les observateurs d'événements.
- Taper *getpid* pour avoir le PID du processus METADSPLOIT sur B. Valider avec Gestionnaire de tâches de B si processus existe (afficher colonne PID).
- Taper la commande ps pour lister les processus de la machine cible. Arrêter le processus à l'aide de la commande kill numéro-PID



Guillaume MATHIEU – <u>http://msreport.free.fr</u> – La connaissance s'accroît quand on la partage

APPLOCKER

COMMENT RESTREINDRE LES ACCES A UNE MACHINE WINDOWS 7:

- Paramétrage de l'interface graphique avec les stratégies de groupe.
- Utilisation d'APPLOCKER.

APPLOCKER :

- Fonctionnalités présentes sous Windows 7 et Windows 2008 R2
- Permet de bloquer l'utilisation de tous les logiciels sauf ceux autorisés.
- Pour la mise en œuvre APPLOCKER, voir : <u>http://msreport.free.fr/?p=204</u>

8. Déploiement Windows 7

Guillaume MATHIEU - http://msreport.free.fr - La connaissance s'accroît quand on la partage

Le déploiement :

A SAVOIR :

- Une machine Windows 7 a un identifiant unique (SID machine). Pour cloner une machine virtuelle, il faut auparavant exécuter SYSPREP.
- BOOT.WIM sur DVD installation Windows 7 : contient une version de Windows PE configuré pour démarrer l'installation de Windows 7.
- INSTALL.WIM sur DVD installation Windows 7 : contient l'image par défaut déployé par Microsoft.
- Possibilité de générer un fichier IMAGE.WIM personnalisé en capturant une machine Windows 7 avec IMAGEX (WAIK : <u>http://www.microsoft.com/fr-</u> <u>fr/download/details.aspx?id=5753</u>)
- Pour effectuer une installation sans assistance via fichier de réponse : installer le WAIK.
- Pour déployer les images WIM via le réseau : MDT (<u>http://www.webbedeye.com/2012/07/mdt-2012-lite-touch-deployment-step-by-step</u>), WDS, SCCM.

9. Dépannage Windows 7

Guillaume MATHIEU - http://msreport.free.fr - La connaissance s'accroît quand on la partage

Méthodologie de dépannage :

1. QUALIFIER L'INCIDENT :

- Estimer le niveau de sévérité : combien perd mon client si son outil informatique ne marche plus ? Dois-je escalader l'incident ? 3 niveaux : Sévérité A (arrêt de production), sévérité B (risque sur la production de l'entreprise), sévérité C (problème mineur).
- Utiliser un questionnaire prédéfini : relever les coordonnées du contact pour l'incident, l'architecture logicielle / matérielle, la description complète du problème, les actions qui ont effectuées avant l'apparition du problème.
- Récupérer des éléments de diagnostics : pour pouvoir reproduire l'incident sur maquette :

Exporter les journaux d'événements au format EVT.

Utiliser outil MPSREPORT (collecte journaux événements et résultats outils diagnostics).

Utilisation d'outils pour vérifier la configuration matérielle (CPUTEST, MEMTEST). Faire une trace réseau avec Wireshake.

Utiliser des Live CD pour récupérer les informations si le système d'exploitation ne démarre plus!

Méthodologie de dépannage :

2. ANALYSE ET RECHERCHE SOLUTION :

- Reproduire l'incident : pour cela, créer une copie de l'environnement de production sous forme de machines virtuelles (outils gratuits : VMware Server, Vmware ESX ou VirtualBox).
- Analyser le problème : importer les journaux d'événements sur la maquette, analyser les fichiers résultats. Configurer l'environnement de maquette comme la production et valider si le problème se produit.
- Rechercher des solutions : le but est de trouver la solution du problème que l'on a identifié. Taper les messages d'erreurs ou la source / ID des alertes dans les observateurs d'événements sous GOOGLE (exemple NETLOGON 5789).

3. VALIDATION DE LA SOLUTION ET APPLICATION :

- Tester les solutions trouvées (forum, bases de connaissance éditeur) sur l'environnement de maquette.
- Valider un plan de retour arrière en cas de problème sur la production.
- Faire une sauvegarde de l'environnement de production (pour retour arrière).
- Appliquer la solution.

La trousse à outils :

LES OUTILS :

- Logiciel de virtualisation gratuit : VMware Server / VMware ESX 5i (<u>www.vmware.com</u>), VirtualBox (<u>https://www.virtualbox.org</u>).
- Logiciel pour récupérer les logs : MPSREPORT
- Live CD Microsoft : DRD 6.5, Windows RE (démarrer sur le DVD d'installation de Windows 7 et choisir Récupérer)
- Logiciel pour générer des Live CD WINPE : <u>http://technet.microsoft.com/en-us/library/cc709665.aspx</u>
- Live CD Linux : <u>http://www.ultimatebootcd.com</u>
- Live CD BARTPE : <u>http://www.nu2.nu/pebuilder</u>)

LES ASTUCES :

- Dans Google, filtrer sur le site en tapant site:microsoft.com
- Pour les sites payants ou hors ligne, afficher le cache Google.
- Taper les Source avec ID des messages d'erreurs Microsoft.

