Sécurisation du poste client Windows Vista (Checklist)

1 Objectif

Ce document donne des recommandations pour l'installation d'un poste *Windows Vista* sécurisé.

Son utilisation doit être adaptée en fonction du contexte applicatif.

2 Installation de Windows Vista

CD utilisé pour l'installation : Windows Vista Entreprise

Lors de l'installation, la machine doit être déconnectée du réseau. En effet, il est préférable de sécuriser la machine avant de la mettre en ligne. Par contre, elle sera connectée à un *hub* afin d'activer la couche Ethernet. Cela évite de devoir redémarrer lors de changement d'adresse IP.

Préférer une installation « fraîche » plutôt qu'une mise à jour (depuis XP).

3 Sécurisation de Windows Vista

La sécurisation consiste à modifier la configuration par défaut de Windows Vista afin de minimiser les risques ; en supprimant tous les éléments ou services qui ne sont pas nécessaires et en limitant les privilèges des utilisateurs.

3.1 Installation des *Services Pack* et des *Patches*

Installer le dernier service Pack pour Vindows Vista : actuellement aucun

Installer les mises à jour pour Internet Explorer : actuellement IE7

Exécuter *Windows Update* pour installer les derniers *patches* (**Attention** : Connexion Internet nécessaire)

3.2 User Rights Assignment

Les tableaux ci-dessous illustrent les recommandations de la *NSA* pour les *User Rights Assignment* :

Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Local Policies – User Rights Assignment*** Ou ***Start – Run… – secpol.msc***

User Right	Recommended Setting
Access Credential Manager as a trusted caller	(No one)
Access this computer from network	Administrators, Users
Act as part of the operating system	(No one)
Add Workstations to domain	Administrators
Adjust memory quotas for a process	Administrators, NETWORK SERVICE, LOCAL SERVICE
Allow Log on locally	Administrators, Users
Allow logon through Terminal Services	(No one)
Back up files and directories	Administrators
Bypass traverse checking	Administrators, Users, NETWORK SERVICE, LOCAL SERVICE
Change the system time	LOCAL SERVICE, Administrators
Change the time zone	LOCAL SERVICE, Administrators, Users
Create a pagefile	Administrators
Create a token object	(No one)
Create global object	Administrators, SERVICE, NETWORK SERVICE, LOCAL SERVICE
Create permanent shared objects	(No one)
Create symbolic links	Administrators
Debug programs	(No one)
Deny access to this computer from the network	Guests
Deny logon as a batch job	Guests
Deny logon locally	Guests
Deny logon through Terminal Services	Everyone
Enable computer and user accounts to be trusted for delegation	(No one)
Force shutdown from a remote system	Administrators
Generate security audits	LOCAL SERVICE, NETWORK SERVICE

User Right	Recommended Setting
Impersonate a client after authentication	Administrators, SERVICE, NETWORK SERVICE, LOCAL SERVICE
Increase a process working set	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	(No one)
Log on as a batch job	(No one)
Log on as a service	(No one)
Manage auditing and security log	Administrators
Modify an object label	Administrators
Modify firmware environment variables	Administrators
Perform volume maintenance tasks	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators, Users
Replace a process-level token	LOCAL SERVICE, NETWORK SERVICE
Restore files and directories	Administrators
Shut down the system	Administrators, Users
Synchronize directory service data	(No one)
Take ownership of files or other objects	Administrators

3.3 Security Options

Le tableau ci-dessous illustre les recommandations de Microsoft pour les *Security Options*.

Attention : Pour ajouter les valeurs MSS (Microsoft Solutions for Security), exécuter le script *Update_SCE_with_MSS_Regkeys.vbs* fournit avec le *Security Guide* de Vista, depuis la ligne de commande exécutée avec les privilèges administrateurs (cscript *Update_SCE_with_MSS_Regkeys.vbs*).

Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Local Policies – Security Options*** Ou ***Start – Run… – secpol.msc***

Policy	Setting
Accounts: Administrator account status	Disabled
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled
Accounts: Rename administrator account	*Recommended Voir §3.8*
Accounts: Rename guest account	*Recommended Voir §3.8*
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Audit: Shut down system immediately if unable to log security audits	Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax	Not defined
Devices: Allow undock without having to log on	Disabled
Devices: Allowed to format and eject removable media	Administrators
Devices: Prevent users from installing printer drivers	Enabled
Devices: Restrict CD-ROM access to locally logged-on user only	Enabled

Policy	Setting
Devices: Restrict floppy access to locally logged-on user only	Enabled
Domain controller: Allow server operators to schedule tasks	Not defined
Domain controller: LDAP server signing requirements	Not defined
Domain controller: Refuse machine account password changes	Not defined
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Domain member: Digitally encrypt secure channel data (when possible)	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled
Domain member: Disable machine account password changes	Disabled
Domain member: Maximum machine account password age	30 days
Domain member: Require strong (Windows 2000 or later) session key	Enabled
Interactive logon: Display user information when the session is locked	Do not display user information
Interactive logon: Do not display last user name	Enabled *(voir §3.9)*
Interactive logon: Do not require CTRL+ALT+DEL	Disabled *(voir §3.10)*
Interactive logon: Message text for users attempting to log on	Disclaimer
Interactive logon: Message title for users attempting to log on	Notice To Users
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	0 logons *(voir remarques)*
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Enabled *(voir remarques)*
Interactive logon: Require Smart card	Not defined
Interactive logon: Smart card removal behavior	Lock Workstation
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Disabled
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	Disabled
MSS: (AutoShareWks) Enable Administrative Shares (not recommended except for highly secure environments)	Disabled
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Highest Protection, source routing is completely disabled
MSS: (DisableSavePassword) Prevent the dial-up passsword from being saved (recommended)	Enabled
MSS: (EnableDeadGWDetect) Allow automatic detection of dead network gateways (could lead to DoS)	Disabled
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Disabled
MSS: (Hidden) Hide Computer From the Browse List (not recommended except for highly secure environments)	Enabled
MSS: (KeepAliveTime)How often keep-alive packets are sent in milliseconds	300000 or 5 minutes
MSS: (NoDefaultExempt) Configure IPSec exemptions for various types of network traffic.	Multicast, broadcast, and ISAKMP are exempt (Best for Windows XP)
MSS: (NoDriveTypeAutoRun) Disable Autorun for all drives (recommended)	255, disable autorun for all drives
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Enabled
MSS: (NtfsDisable8dot3NameCreation) Enable the computer to stop generating 8.3 style filenames (recommended)	Enabled
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure DefaultGateway addresses (could lead to DoS)	Disabled

MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)	Enabled
Policy	**Setting**
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	0
MSS: (SynAttackProtect) Syn attack protection level (protects against DoS	Connections timeout sooner if SYN attack is detected
MSS: (TCPMaxConnectResponseRetransmissions) SYN-ACK retransmissions when a connection request is not acknowledged	3 & 6 seconds, half-open connections dropped after 21 seconds
MSS: (TCPMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	3
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	90%
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Network access: Do not allow storage of credentials or .NET Passports	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled
Network access: Shares that can be accessed anonymously	None
Network access: Sharing and security model for local accounts	Classic: local users authenticate as themselves
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Send NTLMv2 response only\refuse LM and NTLM *(voir remarques)*
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require NTLMv2 session security, Require 128-bit encryption
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require NTLMv2 session security, Require 128-bit encryption
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled
Shutdown: Clear virtual memory pagefile	Enabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Require case insensitivity for non-Windows subsystems	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled
System settings: Optional subsystems	None
System settings: Use certificate rules on Windows Executables for Software Restriction Ploicies	Not Defined
User Account Control: Admin Approval Mode for the Built-in Administrator account	Enabled
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for credentials
User Account Control: Behavior of the elevation prompt for standard users	Automatically deny elevation requests
User Account Control: Detect application installations and prompt for elevation	Enabled
User Account Control: Only elevate executables that are signed and validated	Disabled
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled

User Account Control: Run all administrators in Admin Approval Mode	Enabled
Policy	**Setting**
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled
User Account Control: Virtualize file and registry write failures to per-user locations	Enabled

Remarques :

- Pour le critère « *Interactive logon: Number of previous logons to cache (in case domain controller is not available)* » mettre la valeur à « *1 logons* » pour les portables.
- Pour le critère « *Interactive logon: Require Domain Controller authentication to unlock workstation* » mettre la valeur à « *Disabled* » pour les portables.
- Pour le critère « *Network security: LAN Manager authentication level* », l'option « *Send NTLMv2 response only\refuse LM & NTLM* » fonctionne lorsque les comptes utilisateurs sont des comptes globaux. Si l'utilisation de comptes locaux est nécessaire pour accéder à un partage, utiliser l'option « *Send LM & NTLM - use NTLMv2 session security if negotiated* »

3.4 Access Control List (ACL)

Le tableau ci-dessous donne les autorisations NTFS conseillées sur une station de travail.
Appliquer les autorisations aux répertoires parents avant d'en appliquer aux sous répertoires.
Attention à l'héritage des autorisations !

Avant d'effectuer ceci, ne pas oublier d'afficher les fichiers/dossiers masqués ainsi que les fichiers protégés du système depuis ***Control Panel – Folder Options – View.***

Répertoire ou fichiers	**Autorisations**	**Apply To**
Racine : Disque C: (partition système)	Administrators : Full Control System : Full Control Interactive : Read & Execute	This folder only
Fichiers sous la racine : Autoexec.bat Config.sys	Administrators : Full Control System : Full Control Interactive : Read & Execute	This object only (File only)
\System Volume Information\	System : Full Control	This folder, Subfolder and Files
\$Recycle.Bin\	Administrators : Full Control System : Full Control Interactive : Read & Execute, Write	This folder, Subfolder and Files Sauf Interactive = This folder only
Pour chaque profil utilisateur : \User\%user%	Administrators : Full Control System : Full Control %user% : Modify	This folder, Subfolder and Files
C:\Program Files	TrustedInstaller : Full Control Administrators : Full Control System : Full Control Interactive : Read & Execute	This folder, Subfolder and Files
Dans c:\Windows\ : Regedit.exe	TrustedInstaller : Full Control Administrators : Read & Ececute System : Read & Ececute	This object only (File only)

Dans \Windows\system32 : arp.exe at.exe attrib.exe auditpol.exe Bcdedit.exe BitlockerWizard.exe Bitsadmin.exe Bthudtask.exe cacls.exe Certmgr.exe Chkntfs.exe Cipher.exe Cliconf.exe Cmdkey.exe Colorcpl.exe Compexp.msc Compact.exe compmgmt.msc CompMgmtLaucher.exe ComputerDefaults.exe Control.exe Convert.exe Crss.exe Dcomcnfg.exe debug.exe Defrag.exe DeviceEject.exe DeviceProperties.exe devmgmt.msc Dfrgui.exe diskmgmt.msc Drvinst.exe drwatson.exe Dxdiag.exe eventcreate.exe eventvwr.msc eventvwr.exe Exe2bin.exe Finger.exe FirewallControlPanel.exe FirewallSettings.exe Forfiles.exe Format.com fsmgmt.msc Fsutil.exe Getmac.exe gpedit.msc Gpmc.msc Hdwwiz.exe Hostname.exe Icacl.exe Iexpress.exe Ipconfig.exe Iscsicli.exe Iscsicpl.exe iusrmgr.msc Label.exe Locator.exe Lodctr.exe Logman.exe Lpksetup.exe Lpremove.exe Makecab.exe Mdres.exe MdSched.exe Mem.exe mmc.exe Mountvol.exe Mrinfo.exe Msconfig.exe Msiexec.exe Msinfo32.exe	TrustedInstaller : Full Control Administrators : Read & Ececute System : Read & Ececute	This object only (File only)

Mtedit.exe Nbstat.exe Net.ext Net1.exe Netbtugc.exe Netcfg.exe Netplwiz.exe netsh.exe netstat.exe Newdev.exe Nlsfunc.exe nslookup.exe Ntprint.exe Ocsetup.exe Odbcad32.exe Odbcconf.exe Openfiles.exe OptionalFeatures.exe Pathping.exe Pcaelv.exe Perfmon.exe perfmon.msc Ping.exe PkgMgr.exe Plasrv.exe PnPutil.exe PnPUnattend.exe Powercfg.exe Printmanaggement.exe Printui.exe Qprocess.exe Query.exe Quser.exe Qwinsta.exe Raserver.exe reg.exe regedt32.exe regini.exe regsvr32.exe Relog.exe RelPost.exe route.exe RpcPing.exe Rrinstaller.exe rsop.msc Rstrui.exe sc.exe Sdbinst.exe secedit.exe secpol.msc service.msc Setupcl.exe setupSNK.exe Setupugc.exe Setver.exe Setx.exe Shrpubw.exe shutdown.exe Sllua.exe Slsvc.exe Slui.exe subst.exe Sxstrace.exe Sysedit.exe Syskey.exe systeminfo.exe SystemPropertiesAdvanced.exe SystemPropertiesComputerName.exe SystemPropertiesDataExecutionPrevention.exe SystemPropertiesHardware.exe SystemPropertiesPerformance.exe SystemPropertiesProtection.exe SystemPropertiesRemote.exe	TrustedInstaller : Full Control Administrators : Read & Ececute System : Read & Ececute	This object only (File only)

Takeown.exe Taskklii.exe Tasklist.exe Tcmsetup.exe Tcpsvcs.exe Tpm.msc TpmInit.exe Tracert.exe Tracerpt.exe Tssetup.exe Unattendedjion.exe Unlodctr.exe Unrejmp2.exe Upnpcount.exe Vds.exe Vdsldr.exe Verifier.exe Vssadmin.exe W32tm.exe Wbadmin.exe Wbengine.exe Wecutil.exe Wercon.exe WerFault.exe WerFaultSecure.exe Wermgr.exe Wevtutil.exe Wextract.exe WF.msc Whoami.exe Wininit.exe Winload.exe Winlogon.exe WinSAT.exe wmimgmt.msc Wowdeb.exe Wowexec.exe WPDShextAutoplay.exe Wscript.exe WSManHTTPConfig.exe Wuapp.exe Wusa.exe	TrustedInstaller : Full Control Administrators : Read & Ececute System : Read & Ececute	This object only (File only)
Dans \WINDOWS\system32\Boot winload.exe winresume.exe	TrustedInstaller : Full Control Administrators : Read & Ececute System : Read & Ececute	This object only (File only)
Dans \WINDOWS\system32\Com : Comrepl.exe MigRegDB.exe	TrustedInstaller : Full Control Administrators : Read & Ececute System : Read & Ececute	This object only (File only)
Disque D : (partitions pour les données utilisateur)	Administrators : Full Control System : Full Control Interactive : Modify	This folder, Subfolder and Files

Ces autorisations constituent une base à laquelle il faut ajouter les autorisations liées à certaines applications. En effet, certaines d'entre elles ont besoins d'écrire dans certains fichiers de configuration.

Attention : Si des fichiers, répertoires ou imprimantes doivent être partagés, le groupe *Interactive* doit être remplacé par *Authenticated Users* ou *Domain Users*. Ne jamais utiliser le groupe *Everyone* !

3.5 Services

Les services nécessaires au bon fonctionnement du poste dépendent de l'environnement du système. Par défaut, le système peut fonctionner sans les services listés ci-dessous.
Désactiver les services inutilisés depuis : ***Start – Settings – Control Panel – Administrative Tools – Services*** Ou ***Start – Run … – services.msc***

Note : Certains services sont protégés et ne proposent pas la possibilité de les arrêter comme par exemple le service Plug and Play. Il faut alors passer par ***Start – Run … – msconfig*** onglet Services puis décocher la croix du service désiré. Si le service Plug and Play est désactivé le système devient instable et très lent. Il n'est pas conseillé de le désactiver.

- **Application Management** si vous ne déployez aucune application via la console de stratégie de groupe [GPEDIT]
- **Background Intelligent Transfer Service** si Windows Update n'est pas utilisé
- **Certificate Propagation** désactiver le service si vous n'utilisez pas de cartes à puce
- **Computer Browser** si vous ne partagez pas de fichiers ou d'imprimantes
- **DFS Replication** désactiver le service si vous n'êtes pas en réseau
- **DHCP Client** si la configuration réseau le permet
- **Diagnostic Policy Service** si vous n'utilisez pas l'aide à la résolution des problèmes
- **Diagnostic Service Host** désactiver le service si vous n'utilisez pas l'aide à la résolution des problèmes
- **Diagnostic System Host** désactiver le service si vous n'utilisez pas l'aide à la résolution des problèmes
- **Distributed Link Tracking Client** si vous n'avez pas de liens entre les fichiers NTFS au sein d'un ordinateur ou de plusieurs ordinateurs dans un domaine de réseau
- **Distributed Transaction Coordinator**
- **DNS Client** désactive le cach DNS
- **Extensible Authentication Protocol si** l'authentification EAP n'est pas nécessaire
- **Fax** désactiver le service si vous n'en avez pas l'utilité, ou si vous n'avez pas de scanner
- **Group Policy Client** si vous ne configurez aucune action via la console de stratégie de groupe [GPEDIT]
- **Human Interface Device Access** si par ex. vous n'utilisez aucune extension ou fonction clavier étendue particulière, directement ou par logiciel
- **IKE and AuthIP IPsec Keying Modules** si par ex. vous n'utilisez pas de connexion VPN
- **IP Helper** désactiver le service si par ex. le protocole IPv6 n'est pas nécessaire
- **Link-Layer Topology Discovery Mapper** si pas de partage d'imprimante ou de fichiers
- **Microsoft iSCSI Initiator Service** si l'application iSCSI n'est pas utilisée
- **Microsoft Software Shadow Copy Provider** nécessair pour Windows Backup
- **Multimedia Class Scheduler**
- **Offline Files** désactiver le service si vous n'en avez pas l'utilité
- **Parental Controls**
- **Portable Device Enumerator Service**
- **Print Spooler** désactiver le service si vous n'utilisez pas d'imprimante
- **Problem Reports and Solutions Control Panel Support**
- **Protected Storage** si vous ne sauvegardez aucun mot de passe
- **Quality Windows Audio Video Experience** assure la QoS sur le réseau des applications AV
- **ReadyBoost** si vous n'utilisez pas de clé USB2 rapide pour mise en cache de données utilisateur
- **Remote Access Auto Connection Manager** sauf si connexion par modem
- **Remote Registry**
- **Routing and Remote Access**
- **Secondary Logon** désactiver le service en cas d'utilisateur unique de l'ordinateur
- **Security Center** désactiver le service si vous n'utilisez pas le Centre de sécurité
- **Server** si vous ne partagez pas de fichiers ou d'imprimantes
- **Shell Hardware Detection** si la fonction d'exécution automatique n'est pas utilisée
- **Smart Card** désactiver le service si vous n'en avez pas l'utilité
- **Smart Card Removal Policy** désactiver le service si vous n'en avez pas l'utilité
- **SNMP Trap** désactiver le service si vous n'êtes pas en réseau SNMP
- **SSDP Discovery** désactiver le service si vous n'utilisez pas ce type de périphérique
- **Table PC Input Service** désactiver le service si vous n'utilisez pas ce type de matériel
- **Task Scheduler** si les tâches planifiées ne sont pas utilisées
- **TCP/IP NetBIOS Helper** désactiver le service si vous n'utilisez pas le protocole NETBIOS
- **Telephony** nécessaire pour les connexions par modem et pour l'interface TAPI
- **Terminal Services** si non utilisé
- **Terminal Services Configuration** si TS non utilisé
- **Terminal Services UserMode Port Redirector**
- **Themes**
- **Volume Shadow Copy** nécessaire pour Windows Backup et System Restore
- **Windows Audio** désactive les sons
- **Windows Audio Endpoint Builder** si Windows Audio désactivé
- **Windows Backup** si vous n'utilisez pas l'outil de sauvegarde/restauration n'est pas utilisé
- **Windows Connect Now**
- **Windows Error Reporting Service** si vous n'en avez pas l'utilité
- **Windows Firewall** en cas d'utilisation d'un logiciel tiers
- **Windows Image Acquisition (WIA)** si aucun scanner ou appareils photo

- **Windows Media Center Extender Service** si vous n'utilisez pas Media Center
- **Windows Media Center Receiver Service** si vous n'utilisez pas Media Center
- **Windows Media Center Scheduler Service** si vous n'utilisez pas Media Center
- **Windows Media Center Service Launcher** si vous n'utilisez pas Media Center
- **Windows Media Player Network Sharing Service** si vous n'êtes pas en réseau ou n'utilisez pas de matériel type baladeur ou autre
- **Windows Remote Management (WS-Management)**
- **Windows Time** si aucune synchronisation de temps n'est nécessaire
- **Windows Update** si vous ne souhaitez pas l'utiliser
- **Wired AutoConfig** si l'authentification IEEE 802.1X sur les interfaces Ethernet n'est pas utilisée
- **WLAN AutoConfig** gère les interfaces sans fils

3.6 Restreindre l'exécution de programmes non autorisés

Depuis WinXP, il est possible de restreindre l'exécution de programmes non autorisés grâce aux « *Software Restriction Policies* ». Les « *Software Restriction Policies* » fournissent un mécanisme de règles qui identifie les programmes (chemin, *hash*, certificat, …) fonctionnant sur le poste. En utilisant une politique de restriction de logiciel, un administrateur peut empêcher l'exécution de code non désiré (exe, vbs, dll, virus, Trojan, …).

Pour plus d'informations sur le fonctionnement et la configuration des « *Software Restriction Policies* », voir [SoftResPol].

La configuration ci dessous autorise uniquement l'exécution de code (programmes, scripts, …) dans les répertoires suivants et leurs sous-répertoires, ainsi que l'utilisation des raccourcis :

- C:\Windows (%SystemRoot%)
- C:\Program Files

Default Security Level: Disallowed	
Apply software restriction policies to the following users:	
All users except local administrators	
Path Rules	
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Unrestricted
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%	Unrestricted
*.lnk	Unrestricted

Evidemment, les utilisateurs ne doivent pas avoir accès en écriture dans ces répertoires (§3.15). Ainsi, seules les applications installées par l'administrateur dans ces répertoires pourront être exécutées.

- Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings*** (accessible également par GPO)
- Clic droit sur ***Software Restriction Policies*** puis ***Creat New Policies***
- Double-clic sur ***Enforcement***
- Dans ***Apply software restriction policies to the following*** sélectionner ***All software files***
- Dans ***Apply software restriction policies to the following users*** sélectionner ***All users except local administrators***
- Dans ***When applying software restriction policies*** sélectionner ***Ignore certificate rules***
- ***OK***
- Double-clic sur ***Trusted Publisher***
- Sélectionner ***Define these policies settings***
- Dans ***Trusted publisher management*** sélectionner ***Allow all administrators and users to manage user's own Trusted Publishers***
- (Si les certificats sont utilisés, sélectionner également les deux cases de la partie ***Certificate verification****)*
- ***OK***
- Dans ***Security Levels*** double cliquer sur ***Disallowed*** puis ***Set as Default***
- ***OK***
- Dans ***Additional Rules***, laisser les deux règles tels quels:
  `%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%`
  `%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%`
- Clic droit sur ***Additional Rules*** puis ***New Path Rule…***
- Dans ***Path:*** entrer ****.lnk*** (Cette règle doit être ajoutée, car les raccourcis font partie des exécutables.)
- Dans ***Security level:*** entrer ***Unrestricted***
- ***OK***

Remarque : si le paramètre *Trusted publisher management* est défini avec la valeur *Allow only all administrators to manage Trusted Publishers*, il est impossible d'effectuer un Windows Update sur la machine.

3.7 Account policies

Les tableaux ci-dessous illustrent les recommandations pour les *Account Policies* :

1) Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Account Policies – Password Policy***

Policy Name	Recommended Setting
Enforce password history	24
Maximum password age	90
Minimum password age	1
Minimum password length	12
Passwords must meet complexity requirements	Enable
Store password using reversible encryption for all users in the domain	Disabled

Lorsque le paramètre *Passwords must meet complexity requirements* est activé, le mot de passé doit remplir les conditions suivantes :

- Ne doit pas contenir une partie ou tout le nom du compte utilisateur.
- Etre au minimum de six caractères
- Contenir des caractères de trois des quatre catégories suivantes :
  - Caractères majuscules (A à Z)
  - Caractères minuscules (a à z)
  - Chiffres (0 à 9)
  - Symboles (pax ex., !, $, #,%)

2) Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Account Policies – Account Lockout Policy***

Policy Name	Recommended Setting
Account lockout duration	15
Account lockout threshold	3
Reset account lockout counter after	15

3.8 Compte utilisateurs et groupes

Après une installation de Vista 3 comptes sont disponibles :
Pour les visualiser : Clic droit sur Computer – Manage - Local Users and Groups - Users

- ***Administrator*** est le compte possédant le plus de privilèges. Il fait intrinsèquement parti du système (Built-in) il n'est pas possible de la supprimer. Il fait parti du groupe Administrator. Il est désactivé par défaut.

- ***Guest*** est le compte possédant le moins de privilèges. Il fait aussi partie intégrante du système (Built-in) et n'est pas supprimable. Il est utilisé pour autoriser une personne ne possédant pas de compte sur cette machine de se loguer. Il fait partie du groupe Guests.

- ***xxxxx*** est le compte que j'ai créé à l'installation. Il fait partie du groupe Administrator tout comme le compte Built-in mais possède moins de privilège que celui-ci.

Renommer les comptes *Administrator* et *Guest*:

- Clic droit sur ***My Computer*** puis ***Manage – Local Users and Groups – Users***
- Clic droit sur ***Administrator*** puis ***Rename***

Remarque : Il est également possible de renommer le ces comptes depuis : ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Local Policies – Security Options – Accounts: Rename … account***

- Définir des mots de passe robustes, au minimum 12 caractères avec majuscules, minuscules et chiffres pour chaque utilisateur (ex : dWiht52Y8JdV)

- Créer des groupes d'utilisateurs de manière à faciliter une bonne gestion des accès aux ressources (ex : développeurs, vendeurs, secrétaires, …)

3.9 Protection de l'identité des utilisateurs lors du *logon*

Pour que le nom du dernier utilisateur ne reste pas affiché dans la fenêtre de *logon* :

- Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Local Policies – Security Options***
- Activer la police ***Interactive logon: Do not display last user name***

3.10 Ctrl-Alt-Del lors du logon

Activer la séquence « *Ctrl-Alt-Del* » pour le lancement du processus de *logon* [Q308226]. Cette séquence, appelée *Secure Attention Sequence* (*SAS*), est un dispositif de sécurité empêchant la capture du mot de passe par un programme *Trojan* qui imiterait l'écran d'ouverture Windows. En frappant cette séquence, la main et les entrées du clavier sont toujours passées au processus *Winlogon* du système.

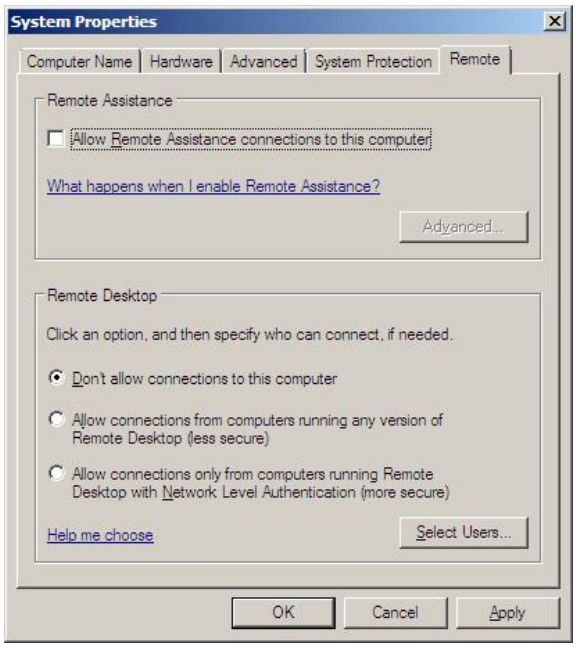
- Dans ***Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Local Policies – Security Options***
  Désactiver (*disabled*) la police ***Interactive logon: Do not require Ctrl+Alt+Del***

3.11 Désactiver Remote Assistance & Remote Desktop

Désactiver *Remote Assistance* (RA) et *Remote Desktop* (RD) :

- Clic droit sur ***Computer*** puis ***Properties – Remote settings***
- Désélectionner ***Allow Remote Assistance connections to this computer***
- Sélectionner ***Don't allow connections to this coputer***

- Dans ***Start – Settings – Control Panel – Administrative Tools – Services***
- Désactiver le service ***Terminal Services***



3.12 Event log

Configurer les événements devant être audités, suivant le tableau ci dessous, en allant dans :
Start – Settings – Control Panel – Administrative Tools – Local Security Policy – Security Settings – Local Policies – Audit Policy

Policy Name	Recommended Setting
Audit account logon events	Success & Failure
Audit account management	Success & Failure
Audit directory service access	No auditing
Audit logon events	Success & Failure
Audit object access	Failure
Audit policy change	Success & Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	Success & Failure

Les événements audités sont stockés dans le dossier suivant :

- C:\WINDOWS\system32\winevt\Logs

Vérifier que seuls les comptes *Administrator*, *System* et *Eventlog* ont des autorisations d'accès au fichiers contenus dans ce répertoire.

3.13 Afficher les extensions connues

Par défaut, Windows Vista n'affiche pas les extensions des fichiers connus (exe, txt, …). Cela permet à une personne malveillante de tromper l'utilisateur en mettant une double extension à un fichier. Par exemple, un virus nommé « photo.jpg.exe » sera affiché comme « photo.jpg » et risque d'être exécuté par l'utilisateur. Pour afficher les extensions connues :

- Dans ***Control Panel – Folder Options – View***
- Désélectionner ***Hide extensions for known file types***
- Sélectionner également la case ***Always show menus*** pour afficher le menu dans Explorer.

3.14 Cacher l'onglet sécurité des fichiers NFTS aux utilisateurs

Attention : En effectuant cet opération, l'onglet sécurité sera également masqué pour l'utilisateur créé lors de l'installation, ce dernier nécessitant une élévation de privilège pour avoir les droits admin. Pour modifier les ACL sur les fichiers/dossiers, il faudra soit exécuter explorer en administrateur (voir labo 1 : UAC), soit ouvrir une session administrateur.

Par défaut, tous les utilisateurs ont accès à l'onglet sécurité dans les propriétés des fichiers NTFS. Il est possible de limiter l'accès à cet onglet en changeant les autorisations sur le fichier ***C:\WINDOWS\Sytem32\rshx32.dll*** . Autoriser uniquement les groupes *Administrators*, *System et TrustedInstaller*.
Avant de faire cela, il faut changer le propriétaire du fichier. Remplacer *TrustedInstaller* par le groupe *Administrators*.

3.15 Désactiver les partages administratif

Les partages administratifs permettent à l'administrateur réseau d'accéder à distance aux disques durs de la machine. Mais ils peuvent aussi être utilisés par les *Hackers* pour pénétrer le système. C'est pourquoi il faut les désactiver avec ***Regedit*** (*Start – Run… - regedit*), en modifiant la clef de registre suivante :

- Dans ***HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters***
- Créer la valeur ***AutoShareWks*** à **0** (DWORD)

Ou voir §3.18, paramètre *MSS : (AutoShareWks) Enable Administrative Shares*

3.16 Services réseaux inutils

Dans la majeure partie de cas, les services réseaux suivants sont inutils :

Control Panel – Network and Sharing Center – Network – View Status – Properties

Désactiver : *File and Printer Sharing for Microsoft Networks*
QoS Packet Scheduler
Internet Protocal Version 6 (TCP/IPv6)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder

3.17 Désactiver NetBIOS

Désactiver NetBIOS sur TCP/IP (ports TCP 139 et UDP 137,138). En effet, ce protocole génère beaucoup de trafic (*broadcast*) et permet d'obtenir des informations sur une machine, ce qui n'est pas acceptable au niveau de la sécurité.
Sur un réseau Windows 2000 et XP, ce protocole n'est pas utile. Pour le désactiver, sélectionnez ***Control Panel – Network and Sharing Center – Network – View Status – Properties – IPV4 – Properties – Advanced –*** onglet ***WINS – Disable NetBIOS over TCP/IP***

Désélectionner aussi ***Enable LMHOSTS lookup***

3.18 Limiter l'accès aux informations publiques du LSA

Les informations publiques du LSA (*Local Security Authority*) permettent d'énumérer les partages disponibles et les comptes utilisateur du poste. Pour rendre cette opération impossible à des utilisateurs anonymes, modifier les critères suivant (voir §3.2) :

- *Network access: Do not allow anonymous enumeration of SAM accounts* : ***Enabled***
- *Network access: Do not allow anonymous enumeration of SAM accounts and shares* : ***Enabled***
- *Network access: Let Everyone permissions apply to anonymous users* : ***Disabled***

3.19 Autres accès anonymes

Afin d'interdire des connexions réseaux anonymes :

- Dans ***HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters*** , contrôler que la valeur ***RestrictNullSessAccess*** (DWORD) et bien à **1**.
- Dans ***HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters*** , les valeurs ***NullSessionPipes*** et ***NullSessionShares*** doivent être vides.

Remarque : Les deux dernières valeurs peuvent être modifiée directement par les ***Security Options*** (voir §3.2) , paramètres *Named Pipes that can be accessed anonymously* et *Shares that can be accessed anonymously*

Il est également possible de limiter les accès anonymes au *Named Pipes* et au partages à l'aide du paramètre *Restrict anonymous access to Named Pipes and Shares* dans les ***Security Options*** (voir §3.2) **.**

3.20 Activer le mot de passe pour l'écran de veille

Le mot de passe de l'écran de veille est un élément de sécurité simple qui n'est pas souvent employé par les utilisateurs. Pourtant, cela empêche des personnes mal intentionnées de profiter d'un poste non verrouillé.

Activer le mot de passe pour l'écran de veille dans :

Start – Settings – Control Panel – Personalization – Screen Saver – On Resume, display logon screen

Remarque : Afin de ne pas utiliser du temps CPU ou de la mémoire, utiliser des écrans de veille simples comme « Windows Logo » ou « Blank ».

3.21 Windows Features

Supprimer les composants inutils :

Start – Settings – Control Panel – Programs and Features – Turn Windows Features on or off

- ***Tablet PC Optional Components***
- ***Windows Meeting Space***

3.22 Forcer l'application des GPO avant l'ouverture d'une session

Pour gagner du temps, comme WinXP, Windows Vista n'attend pas que le réseau soit totalement initialisé avant l'ouverture de la session utilisateur. Ainsi, les GPO sont appliqués en arrière plan après l'ouverture de session. Les changements éventuels dans les GPO ne se répercuteront que lors du la prochaine ouverture de session.
Il est préférable d'appliquer les GPO avant l'ouverture de la session :

- Dans ***Start – Run…*** taper ***gpedit.msc***
- Aller dans ***Computer Configuration – Administrative Templates – System – Logon***
- Double-clic sur ***Always wait for the network at computer startup and logon***
- Sélectionner ***Enabled***
- ***OK***

3.23 SYSKEY

SYSKEY ajoute un niveau supplémentaire d'encryption aux *hashs* des *passwords* stockés dans la SAM. Par défaut, cette fonction est activée sur Windows Vista, et il n'est pas possible de la désactiver.

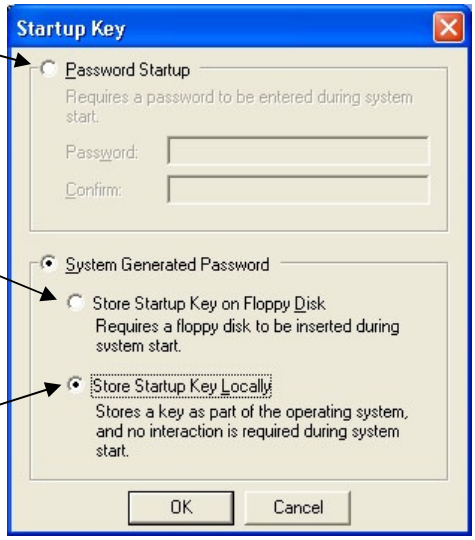
SYSKEY établit une clé de chiffrement de 128 bits. Par défaut, cette clé est stockée localement par le système. Si le système requiert un haut niveau de sécurité, il est possible de stocker la clé sur une disquette ou de la remplacer par un *password*. Cette disquette ou ce *password* est nécessaire pour *booter* la machine.

Pour modifier l'emplacement de la clé : ***Start – Run… - syskey - Update***

Si cette option est sélectionnée, la clé utilisée par SYSKEY est issue à partir d'un *password*. Ce *password* est demandé lors de chaque *boot* de la machine.

Si cette option est sélectionnée, la clé utilisée par SYSKEY est stockée sur une disquette. Cette disquette est demandée lors de chaque *boot* de la machine.

Si cette option est sélectionnée, la clé utilisée par SYSKEY est stockée sur le système (défaut).



3.24 Garder le poste à jour

Il est important de garder une machine à jour. En effet, de nouvelles mises à jour, réglant des bugs et des failles de sécurité, sont régulièrement disponibles sur le site http://www.microsoft.com.

Outils :

- Windows Update
- Hotfix Checker (Hfnetchk.exe, Q303215)

Type de mise à jour :

- Hot fixe : *Patch* non testé mis à disposition rapidement pour contrer une faille de sécurité.
- Rollup : *Package* rassemblant tous les *patches* disponibles et les installant dans le bon ordre.
- Service Pack : Mise à jour du système d'exploitation (nouvelles fonctionnalités, corrections de bugs, *patches* de sécurité).

4 Références

- **Windows Vista Security guide** [VistSecGui]
  http://www.microsoft.com/technet/windowsvista/security/guide.mspx
- **Software Restriction Policies in Windows Vista** [SoftResPol]
  http://technet.microsoft.com/en-us/windowsvista/aa940985.aspx
- **Services inutiles dans Windows Vista** [ServVista]
  http://www.informatruc.com/forum/ftopic20392.php
- **Permissions et TrustedInstaller** [TrustedInst]
  http://blogs.msdn.com/irenak/archive/2007/01/30/sysk-277-how-to-bring-back-the-trustedinstaller.aspx
  http://forums.microsoft.com/TechNet/ShowPost.aspx?PostID=921189&SiteID=17