MD-100 Chapitre 1

# Versions de Windows 10

|  |  |
| --- | --- |
| Windows 10 Home | **128GB de ram**  **Pas de contrôle sur l’update** |
| Windows 10 Pro | **2TB de ram**  **Mise à jour contrôlable par Windows Update pour Business**   * Peut joindre un domaine AD / Azure AD * Bitlocker * Mode entreprise pour Internet explorer * HyperV * Remote Server Admin Tool (RSAT) * MS Store pour entreprises * Windows Information Protection |
| Windows 10 Pro Workstation | **6TB de ram**   * SMB Direct (RDMA remote Direct Access Memory) * Resilient File System (ReFS) * Mémoire persistante * **Ultimate performance plan** |
| Windows 10 Enterprise | **Meme ram que precedent**  **Mise à jour par Windows Update for Business**  **Peut rejoindre LongTermeServicingChannel LTSC**  **Update 2-3 ans VS 6 mois**  **Skip update jusqu’à 10 ans**   * AlwaysOnVPN * DirectAccess * Windows ToGo Creator * AppLocker * BranchCache * Start Screen Control avec GPO * Managed User Expérience * Windows Defender Credential Guard * Windows Defender Device Guard * Windows Defender Advanced Threat Protection * VDI Enhancements * Virtualisation d’applications |
| Windows 10 Entreprise LTSC | **Pas de Microsoft edge, store, cortana ou apps windows** |
| Windows 10 Education | **Comme Windows 10 Enterprise**   * Sans LTSC * Seulement Academic Volume Licensing |
| Windows 10 Mobile | Obsolete |
| Windows 10 S | Mode S (stable) limité à edge, store et Azure AD.  On peut sortir du mode S mais pas y revenir |
| Windows 10 Pro + licence Windows 10 Business (365) | Windows 10 Pro mais 365 inclu |
| Windows 10 IoT Core et Enterprise | Spécial IoT |

MD-100 Chapitre 1

Toutes les éditions de Windows 10 sont compatibles 32/64bit

Passer de 32 à 64 bit = Réinstallation complète

|  |  |
| --- | --- |
| **32bit** | **64bit** |
| 4gb de ram | 128 à 6tb selon édition |
|  | Kernel Patch protection |
| Kernel mode driver signing |
| Data exécution Prevention |
| Client HyperV |
| Performance CPU meilleure |

# Fonctionnalités et matériel nécessaire

*\*TPM Trusted Plateform Module*

|  |  |
| --- | --- |
| Client HyperV | Windows 10 Pro/Enterprise  64Bit  Support SLAT  2gb de ram libre au minimum |
| Cortana | Microphone |
| Continuum | Possibilité de passer en mode tablette |
| Miracast | Moniteur adapté ou adaptater Miracast |
| Touch | Supporte Touch |
| Active Stylus | Supporte Touch |
| OneDrive | Compte MS |
| Sync your settings | Compte MS |
| BitLocker Drive Encryption | TPM 1.2 ou +  Windows 10 Pro/Enterprise |
| Device Health Attestation | TPM 2.0 |
| Secure Boot | Firmware carte mère UEFI 2.3.1 errata B  + Microsoft Windows Cert Authority |
| Multifactor authentification MFA | Finger print, ou smartphone, ou caméra (Windows hello) |
| Virtual Server Mode (Déplace des composant de l’OS dans des containers HyperV) | Windows 10 Enterprise |
| Virtual Smart Cart | TPM 1.2 |

MD-100 Chapitre 1

# Mise à jour directes

|  |  |
| --- | --- |
| Windows 7 Starter  Windows 7 Home Basic  Windows 7 Home Premium  Windows 8/8.1 | Windows 10 Home |
| Windows 7 Pro  Windows 7 Ultimate  Windows 8/8.1 Pro | Windows 10 Pro |
| Windows 7 Enterprise  Windows 8/8.1 Enterprise | Windows 10 Enterprise |
| Home = Home Pro et Ultimate = Pro Enterprise = Enterprise | |

**Obtenir Windows 10, en entreprise**

Via Volume Licencing Service Center (VLSC) qui tuilise KMS ou MAK (Multiple Activation Key)

# Méthode d’installations

|  |  |
| --- | --- |
| DVD | Obsolète, voir USB |
| USB | Télécharger le média sur site MS.  Booter par USB |
| WDS (Windows Deployment Service) | Rôle de serveur  Besoin de DHCP  PC compatiple PxE |
| Image Windows PE (Preinstallation environment) | Booter le PC en mode PE   * Ou, utiliser DISM (1) * Ou, utiliser MDT (2) * Ou, utiliser SCCM (3)  1. Deployment Image Servicing and Management 2. Microsoft Deployment Tool 3. System Center Configuration Manager |
| Network | Booter le PC en mode PE  Se connecter à un partage contenant l’image |

# Stratégies d’installations

|  |  |  |
| --- | --- | --- |
| High touch | Low touch | Zero touch |
| -100 | 100+ | 1000+ |
| DVD/USB ou network | WDS et MDT | MDT et SCCM |

MD-100 Chapitre 1

# Procédure complète d’imaging

* Choisir si on fait une réinstallation complète OU une « inplace upgrade »
* Dans les deux cas, on prépare une image

# Procédure de création d’image

Récupérer l’image par défaut de windows = **Install.wim** provenant du média d’installation

*! Pas possible d’obtenir une image Windows 10 Enterprise avec Media Creation Tool !*

1. **Utiliser Windows ADK (Widnows Assessment and Deployment Kit) qui contient DISM….**

Ligne de commande pour capturer, déployer et manager une image

1. **Utiliser Windows ICD (Imaging and Configuration Designer)**

Pour créer un package de provisionning (.ppkg) qui flash une image avec runtime et fonctonnalités

1. **Utiliser Widows System Image Manager**

Pour créer un fichier de réponse (autounattended.xml)

# Ajouter une langue à une image

Soit après install -> Paramètre, Temps et langue OU Store MS -> Module d’expérience locale

* Cherche le language pack ISO sur le site microsoft (LIPs), récupérer le ***.appx***
* Flasher l’image avec DISM

Dism /Image:"C:\mount\windows" /Add-Package /PackagePath="D:\x64\langpacks\Microsoft-Windows-Client-Language-Pack\_x64\_fr-fr.cab"

Puis :

Dism /Commit-Image /MountDir:"C:\mount\windows"

OU LPKSETUP.exe + ISO Language pack

# Migration des données utilisateur

|  |  |
| --- | --- |
| **Side by Side (Inplace upgrade)** | **Wipe and load** |
| OLD OS -> Stockage intermédiaire -> NEW OS | OLD OS -> Stockage intérmédiaire  Wipe OS + Réinstallation  Redéplacer données utilisateurs |

1. **DISM/ ScanState.exe pour capturer les données**

ScanState.exe \\Partage\MyStore /config:config.xml /i :MigDocs.xml /i:MigApps.xml /v:12 /l:scan.log

1. **DISM/ LoadState.exe pour charger les données**

LoadState.exe \\Partage\MyStore /config:config.xml /i :MigDocs.xml /i:MigApps.xml /v:12 /l:load.log

* 1. MigApp.xml, MigDocs.xml, MigUser.xml
  2. Possible de créer des fichiers customisés
  3. Config.xml pour exclusion de fichiers ou config à migrer
* Ne copie pas les applications sauf certaines applications supportées
* Ne sont pas migrés :
  + Imprimantes locales, Drivers, Mots de passes, Icones, Permissions sur les partages

MD-100 Chapitre 1

# Troubleshooting de l’upgrade et migration

**Vérifier que l’emplacement des fichiers de migration n’est pas corrompu :**

USMTUTILS /verify C :\MyStore\storename.img

**En cas de problemes durant l’upgrade :**

C:\Windows\Panther\UnattendGC\SetupAct.log

**Fail du système pendant l’upgrade**

C:\$Windows.~BT\Sources\panther\setupact.log

**Vérifier la compatibilité du système avec l’image qu’on veut déployer**

Setup.exe /Auto Upgrade /quiet /NoReboot /DynamicUpdate Disable /Compat ScanOnly

# Après l’installation - Activation

**Activer Windows**

Connaitre l’état de l’activation : slmgr -dli

|  |  |
| --- | --- |
| **Besoin d’une clé si** | **Pas besoin d’une clé d’activation si** |
| Achat en boutique (peut pas être activé par volume licensing) | Upgrade depuis windows 7/8 officiel |
| Pas de licence digitale (lié au compte MS) | Achat depuis le store MS |
| Activation par Volume Licensing | Clé inclue dans le firmware |
| Windows déjà installé | Client Windows Insider |

|  |  |  |
| --- | --- | --- |
| **KMS**  **Key Management Service** | **AD DS**  **Activation par l’AD** | **MAK**  **Multiple Activation Key** |
| Au moins 25 hosts  Ou  5 serveurs connectés en permanence | Host doit rester dans le domaine | Distribué sur l’image |
| Fonctionnalité du serveur « Volume Activation Services » | |  |

Machines virtuelles = bénéficie de l’héritage d’activation (Inherited Activation)

# Troubleshooting de l’activation

* 2h pour trigger du serveur KMS
* 180 jours pour renouveler la clé sinon elle est désactivée
* Forcer l’activation avec la commande slmgr /ato
* Obtenir le téléphone du service Windows (pas pour pro/Edu/Workstation) slui 04

MD-100 Chapitre 1

**Empêcher par GPO les utilisateurs d’utiliser leur compte Microsoft :**

|  |  |
| --- | --- |
| Computer Configuration  \Administrative Templates  \Windows Components  \Microsoft account | Block All Consumer Microsoft Account User Authentication |
| Computer Configuration  \Windows Settings  \Security Settings  \LocalPolicies  \Security Options | Accounts : Block Microsoft Accounts |

**Windows Hello**

|  |  |
| --- | --- |
| **Windows Hello** | **Windows Hello Business** |
| PIN et Facial OU Empreinte | |
| Lié à l’hote | Lié l’ Active Directory |
| PIN maximum de 127 caractères et associé à un seul compte et un seul appareil ! | |

**Dynamic Lock** = Ferme la session quand le smartphone associé en bluetooth s’éloigne.

**Windows Spotlight** = Propose des fonds d’écrans et suggère features

# Start Layout Export

* Supporté par Windows 10 1607 Enterprise / Edu
* Supporté par Windows 10 1703 Enteprirse / Edu / Pro

Full Start Layout = L’utilisateur à un menu préparé non-modifiable

Partial Start Layout = Le menu est préparé mais certaines parties peuvent être modifiées.

Export-StartLayout -path « monchemin/fichier.xml”

Pour en faire un partial, ajouter

<DefaultLayoutOverride LayoutCustomizationRestrictionType="OnlySpecifiedGroups"> au fichier

**Déploiement par :**

GPO : User/Policies/Administrative Template/Start menu/Start layout

Windows ICD, MDM

# Plans de de power

* Powercfg.exe list Affiche les plans de power
* Powercfg.exe export power.pow GUIDGUIDGUID Export un plan de power

# Windows Mobility Center

* Pour gérer les Mobiles, tablettes et laptop.
* Contient les présentation settings pour salle de réunion

MD-100 Chapitre 1

Microsoft Edge

Mis à jour chaque 2ème mardi (Tuesday) du mois

Pas de LTSC, mais IE11 oui

**Ne supporte pas :**

|  |  |
| --- | --- |
| ActiveX  Browser Helper Objects  VBScripts | Edge appellera Internet Explorer 11 pour compatibilité |

# Microsoft Edge Kiosk mode

Mode bloqué sur une ou plusieurs apps.

Configurer un kiosque, et appliquer la GPO selon le choix :

|  |  |
| --- | --- |
| Une application | Edge bloqué sur un seul site  « Affiche » – Pas besoin d’interaction (**Digital Signage**)  « Catalogue » – User peut interagir (**Interactive Signage**)  OU  Public Housing (Multi-tab limité) |
| Plusieurs apps | Edge normal  Normal = session enregistrée  Public = session privée |

MD-100 Chapitre 2

# Comptes Windows 10 par défaut :

* Administrateur
* Default (Membre des administrateur)
* Invité

# Azure AD – Joindre appareils

|  |  |
| --- | --- |
| **JOIN** | **REGISTER** |
| COPE Corporated Owned | BYOD Bring your own |
| Eilleur management des appareils | Moins d’options |

# Microsoft 365 Business / Enterprise

|  |  |
| --- | --- |
| Microsoft 365 Business | Microsoft 365 Enterprise |
| Permet d’upgrade en **Windows 10 Business** | Permet d’upgrade en Windows 10 Enterprise |

# Assistant de création de partages

Utilitaire : shrpubw

# Local Policy

* Windows 10 Home n’a pas de local policy
* Stratégie de sécurité locale : secpol.msc
* Stratégie de sécurité de groupe locale : gpedit.msc
* Résultat de stratégies : rsop.msc

Les stratégies local sont appliquées en premier, puis les GPO qui ont la priorité sur les locales.

Les stratégies locales doivent être inscrites sur chaque PC.

# Cryptage EFS

* Crptyge de dossier NTFS
* Ajouter un Data Recovery Agent dans l’AD pour bonne pratique

# BitLocker

* Pour crypter un disque entier
* Crée 2 partitions pour démarrer avant le système
* Peut être utilisé sans TPM, avec une clé USB
* Utilitaire : tpm.msc

**Si mise à jour du BIOS/UEFI | Déplacement du drive**

Mettre en pause BitLocker

Mettre à jour et réactivé après redémarrage si c’est pas déjà fait.

BitLocker to Go permet de crypter les disques amovibles et ne nécessite pas de TPM

MD-100 Chapitre 3

# Adresse IPV6 Unicast Prefixes

* IPv6 Unicast site local (Privée) = FECO ::/64
* IPv6 Unicast link local (APIPA) = FE80 ::/64

# VPN

* PPTP = Ancien protocole de VPN
* L2TP = VPN Ipsed
* SSTP = VPN SSL
* IKev2 = VPN pour mobile

# Assistance à distance et RDP

* Assistance : MSRA.exe
* Remote Desktop : MSTSC.exe

**Activer powershell à distance**

Winrm quickconfig OU PSremoting -force

MD-100 Chapitre 4

Outil en ligne de commande de sauvegarde : wbadmin.exe

* Reset this PC = Recycle
* Fresh Start = Refresh du PC
* System Image Backup (Backup & Restore) = Supprime tout
* CD de boot

1. POST
2. BootMGR
3. BCD
   1. Hiberfil.sys ?
      1. WinResume.exe
   2. Winload.exe
4. Load drivers
5. Session manager
6. Signin

BCedit.exe /enum = Liste les entrée du BCD (Boot config data)

Bootrec.exe = Reconstruit le BCD

Sigverif.exe = File Signature tool pour drivers non signés

Vérifier.exe = Driver Vérifier Manager

DriverStore = %systemroot%/system32/driverstore

PnPutil.exe = Pour ajouter des plug and play drivers

Activer sur un PC la collecte de log à distance, sur le PC qui voit les subscriptions = wecutil qc

Sur les ordis dont on va collecter les logs = winrm quickconfig

**Collector initated** : LOe serveur demande aux autres

**Source initiated** : les PC envoie au serveur directement

Printmanagement.msc

**Liste des services**

* Net start = sc start
* Net stop = sc stop
* Sc query

MD100 Labo 1

# Windows Assessment and Deployment Kit (ADK)

|  |  |
| --- | --- |
| **ACT** Application Compatibility Tool | Evalue et résout les problèmes de compatibilité des applications |
| **DISM** Deployment Image Servicing and Management | Capture, déploie, service, manage images |
| **SIM**  System Image Manager | Créé des fichiers de réponse autounattend.xml |
| **WinPE**  Windows Preinstallation Environment | Système d’exploitation basique par boot |
| **ICD**  Imaging and Configuration Designer | Pour créer des package de provisionning et « flasher » une image avec une configuration |
| **USMT**  User State Migration | Permet de déplacer les configurations user |
| **VAMT**  Volume Activation Management Tool | Automatiser l’activation |
| **MAP**  Microsoft Assessment and Planning | Liste des ordinateurs, inventaire |

# Type de déploiement

|  |  |  |
| --- | --- | --- |
| High touch | Petite organization | DVD/USB |
| Low touch | 200-500 postes | MDT + WDS |
| Zero touch | 500+ postes | MDT + SCCM |
| Provisionning package | Changer une image existante sans réinstaller | |

# Activation

|  |  |
| --- | --- |
| KMS | Minimum 25 hotes connectés |
| AD DS | Stocké directement dans l’annuaire |
| Volume Activation Services | Rôle serveur |
| MAK | Clé multiples |

VAMT = MMC pour gérer KMS et MAK

# Windows To Go

OS complet sur clé USB de 25go

# Bitlocker sans TPM

GPO, USB ou PIN = Require additional auth + Allow Bitlocker whitout TPM

MD100 Labo 2

# Virtualisation

|  |  |
| --- | --- |
| Isolated User Mode | Protection de la VM en séparant la mémoire |
| Device Guard | Bloque le périphérique pour qu’il n’utilise que des applications signées  \*Enterprise ou Education |
| Credential Guard | Bloque l’accès au mdp enregistrés dans LSA, pour empêcher les malware de passer dans le domaine |
| Device Health Attestation | TPM et Intune pour déterminer la santé des périphériques |
| VM Secure Boot | Seulement les composants validés peuvent fonctionner |
| TPM | Une VM peut utiliser Bitlocker en utilisant la carte TPM virtuelle de l’hote |
| Shielding | Empeche d’exporter une VM sur un autre hote |

# Homegroup VS Workgroup

|  |  |
| --- | --- |
| **HomeGroup** | **WorkGroup** |
| Mot de passe partagés entre utilisateurs  Partage de   * images * vidéos * documents * printers * musique | Pas de centralisation de   * Users * Groupes * GPO * Settings   Partage de fichiers et imprimantes  PC1.User1 n’est pas le même que PC2.User1 ! |

# Labo déploiement 2

RSAT = Remote Server Administration Tool, téléchargeable sur le site MS

Sigverif.exe = Pour vérifier les drivers non-signés

# Labo déploiement 3

|  |  |
| --- | --- |
| Test-Connection | Égal à Ping |
| Netsh | Pour afficher et configurer les interfaces |
| Pathping | Comme tracert mais mieux |
| Nestat-n | Liste des ports et connexions |
| NSLookup | Vérifier le DNS enregistré |
| Get-Dnsclientcache | Récupère les DNS enreigstrés et leur adresses |
| Clear-dnsclientcache | Nettoie le cache DNS |

C:\Windows\system32\drivers\etc\hosts\**hostfile**

MD100 Labo 3

# IPSEC

IPSec à deux modes :

ESP Encapsulation Security Payload

AH Authentication Header

Encrypte – Authentifie

Windows Defender : **C:\ProgramData\Microsoft\Windows Defender\Platform\<antimalware platform version>** mpcmdrun.exe

# Profils réseaux

|  |  |
| --- | --- |
| **Domaine** | Découverte du réseau active |
| Ne peut pas créer/rejoindre un Homegroup |
|  | |
| **Privé** | Découverte du réseau activé |
| Peut rejoindre un Homegroup |
|  | |
| **Public** | Découverte du réseau désactivé |
| Ne peut pas créer/rejoindre un HomeGroup |

# Modifier le parefeu avec powershell

|  |  |
| --- | --- |
| Get | Copy | Enable  Disable | New | Remove  Rename | Set | Show | NetFirewallRule |

# Divers

RDP = **mstc.exe**

Assistance = **msra.exe**

Nettoyage de disque = **Cleanmgr.exe**

Voir les partages : **net view \\localhost /all**

Work folder = Dossier local qui se synchronise avec un serveur de fichier

Pour installer package .msi = **msiexe.exe**

Gestionnaire de carte TPM : **tpm.msc**

Gestionnaire de reliability = **perfmon \rel**

Ancien panneau de configuration : **control.exe**

Gestionnaire de certificats : **certmgr.msc**

Jeu de stratégie résultant : **rsop.msc**

Compte utilisateurs : **netplwiz**

Indexing options : **control.exe srchadmin.dll**

Gérer les update manuellement : **wusa.exe**

Afficher les mise à jours installées : **wmic qfe list brief /format:table**

Ouvrir le WinPe : **shutdown /r /o**

Reset du cache de Windows Store : **WSReset.exe**

MD100 Divers

# Droits NTFS

|  |  |
| --- | --- |
| Déplacement sur le même volue | Droits conservés |
| Déplacement/Copie sur un autre volume | Droits perdus |

# Ajouter un client au domaine depuis le serveur AD

Netdom.exe

# Bitlocker

* Soit l’ordinateur à une carte TPM 1.2 minimum, qui se charge de vérifier que rien n’a été modifié sur le PC avant de booter…
* Soit on active un GPO (Require additional authentication at startup)
  + Débloque le BOOT a l’aide d’un mot de passe
  + Avec un clé USB contenant la clé de déchiffrement

# Récupération de BitLocker

* Soit on a imprimé le mot de passe de récupération de 48 caractères
* Agent de récupération Bitlocker (un certificat lié au compte AD qui se chargera de récupérer les clés)
* Un administrateur de domaine peut obtenir le mot de passe de récupération auprès d’AD DS avec GPO adéquate