2021

Windows 10 21H1

Installation et configuration

Olivier DEHECQ

Table des matières

1.1 A propos de PowerShell

L'utilisation de PowerShell s'avère indispensable dans le cadre de l'administration de Windows. Afin de ne pas être perdu avec cet interpréteur de commandes, voici un guide de survie.

`get-command` : Liste des commandes chargées (disponibles)

`get-command *dns*` : liste des commandes relatives à DNS (contenant « DNS »)

`get-command -verb get -noun dns` : liste des commandes qui ont un verbe get et un noun (nom) dns

`get-command -module DnsServer -noun *cache*` : chercher une commande pour vider le cache

`get-help nomDeLaCommande` : trouver l'aide sur la syntaxe d'une commande

`get-help clear-DnsServerCache` : trouver l'aide de la commande `clear-DnsServerCache`

`get-help new-item -examples` : afficher des exemples de la commande `new-item`

`get-date` : Afficher la date du jour (sous le format : `dimanche 11 avril 2021 09:49:35`)

`get-date | get-member` : lister toutes les propriétés contenues dans le pipe « | »

Renvoie le nombre de minutes de la date/heure du jour : 09 :

- `get-date | select minute` : renvoie la valeur sous forme de table
- `(get-date).minute` : renvoie la valeur uniquement (pratique pour stocker dans une variable)

`invoke-command` : exécuter une commande sur un poste distant

Prérequis pour `invoke-command` :

- Autoriser l'administration à distance (par défaut sous WS2012+)
  - CMD : `winrm qc`
  - PowerShell : `enable-psRemoting [-skipNetworkProfileCheck]`

    `-skipnetworkprofilecheck` (WS2012+) : pour le faire aussi sur le profil réseau « Public »

`send-mailmessage` : envoyer un mail depuis PowerShell (PS2+)

Équivalent de `ping`, renvoie true si la machine est allumée, sinon renvoie false (pratique dans un script) :

```
test-connection 192.168.10.2 -count 1 -quiet
```

`get-windowsFeature` : Lister les rôles installés (available veut dire que les sources sont disponibles dans winSxs :

Installer une fonctionnalité (en local ou à distance) :

```
install-windowsfeature [-computername leNomdeLordiSurLequelInstaller] featàInstaller
```

L'équivalent de SET en PowerShell

`Set-Item ENV:TOTO "essai"` : définir une variable d'environnement de façon temporaire

`Get-ChildItem ENV:Path` : récupérer le contenu de la variable Path

`Get-ChildItem ENV:` : récupérer l'ensemble des variables d'environnement

`setx.exe TOTO "essai" -m` : définir une variable d'environnement de façon définitive

Prérequis pour setx : exécuter la commande en tant qu'administrateur

`setx PATH "$env:path;\the\directory\to\add" -m` : ajouter un morceau à la variable place de façon définitive

Sources : http://stackoverflow.com/questions/714877/setting-windows-powershell-path-variable

1.2 Installation et mise à niveau

Configuration minimale

- Pour un particulier : pas d'utilité d'avoir la version Pro : https://www.microsoft.com/en-us/WindowsForBusiness/Compare
- Pour les entreprises : versions « Entreprise » et « Professionnel »

Configuration requise : https://www.microsoft.com/fr-fr/windows/windows-10-specifications

Installation

- Mise à jour que de Windows 7 ou Windows 8.1 vers Windows 10 avec l'assistant de mise à niveau
- WinPE = Windows Preinstallation Environment : environnement pour l'installation de Windows10, quand on met le DVD
- WinRE = Windows Reparation Environment : pour réparer l'installation existante.

Options des lecteurs avancées

- On peut charger un pilote SATA, SCSI … : typique en installation virtuelle
- Création auto d'une « partition de récupération » de 530Mo réservée pour BitLocker, WinRE, etc.

Nota : dans le cas de « Réseau public », la découverte des réseaux est désactivée

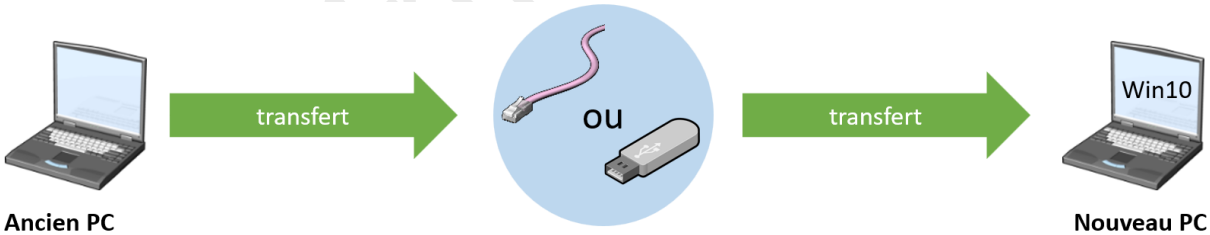
Installation par mise à niveau : à éviter

- Windows 7 ou Windows 8.1 : assistant de mise à niveau (aussi accessible via de DVD d'installation)
- Windows 8 : mettre à jour en Windows 8.1 puis mettre à niveau
- Versions inférieures à Windows 7 : nouvelle installation

Assistant de mise à niveau

Possibilité d'utiliser Windows as a Service

Migration des profils



Migration manuelle des profils

Autre solution :

Windows ADK (installation) > USMT (User Migration Tool) → pour les entreprises

Fonctionnement de USMT

Gestionnaire de Boot

Jusqu'à XP / 2003 inclus :

- NTLDR (NT Loader : chargeur d'OS orienté NT) ≈ LILO / GRUB
- NTDETECT.COM (détection du matériel)
- BOOT.INI (indique le chemin de l'OS)

Depuis Vista :

- BCD (Boot Configuration Database)

La BCD est organisée en Magasins (*store*) puis Objets (*objects*) puis Eléments (*elements*)

Exemple de chemin ARC : multi(0)disk(0)rdisk(0)partition(1)/vga

La BCD peut contenir des OS installés à différents endroits (exemple HDD(0)part(1) et C:\win7.vhd)

BCD supporte les .VHD (mais pour des images de Win7 ou ultérieur)

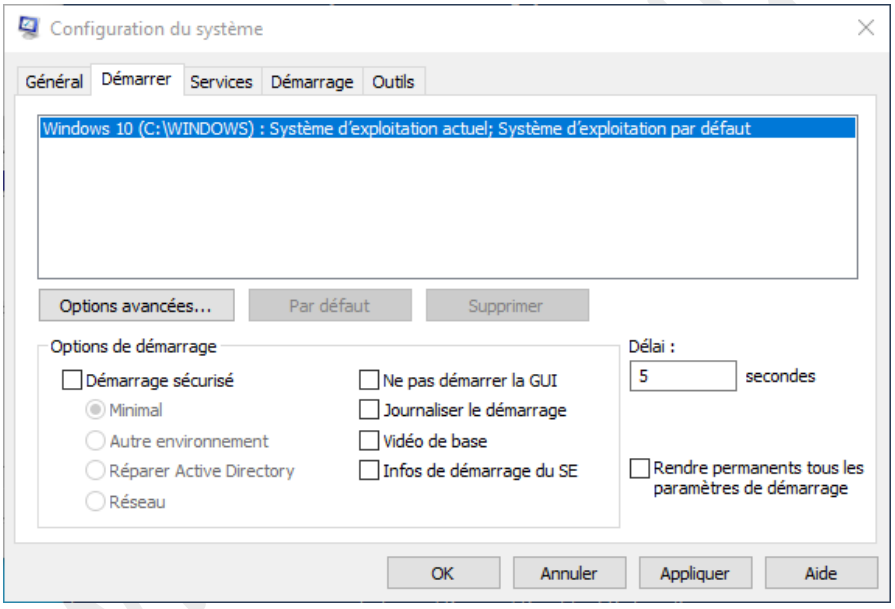
Si Win7 installé puis Win XP installé : Win7 n'est plus bootable, mais WinXP boote

Si WinXP installé puis Win7 installé : les 2 OS sont bootables

`bcdedit` : pour lancer BCD

`bcdedit –enum all` : pour lister les paramètres de BCD

`msconfig.exe` puis onglet « Démarrer » : configurer une partie des paramètres de BCD



Restaurer le boot de Windows10 :

- mettre le DVD d'installation de Windows10 puis redémarrer l'ordinateur
- Booter sur le DVD, cliquez sur « Réparer l'ordinateur » puis sur « Dépannage » et « Invite de commande »

```
cd C:
cd C:\Windows\Boot
bootsect.exe/nt60 all                          # restaure les secteurs de boot de Windows 10
```

Créer une entrée pour Windows XP dans le BCD Store :

```
bcdedit –create {ntldr} –d "Windows XP"
bcdedit –set {ntldr} path \ntldr
bcdedit /displayorder {ntldr} /addlast
```

1.3 Déploiement à partir d'images

Le déploiement à partir d'image permet d'installer rapidement une version configurée selon ses propres paramètres à plusieurs ordinateurs, de façon semi automatisée.

WIM : images de partition. Pour Windows seulement

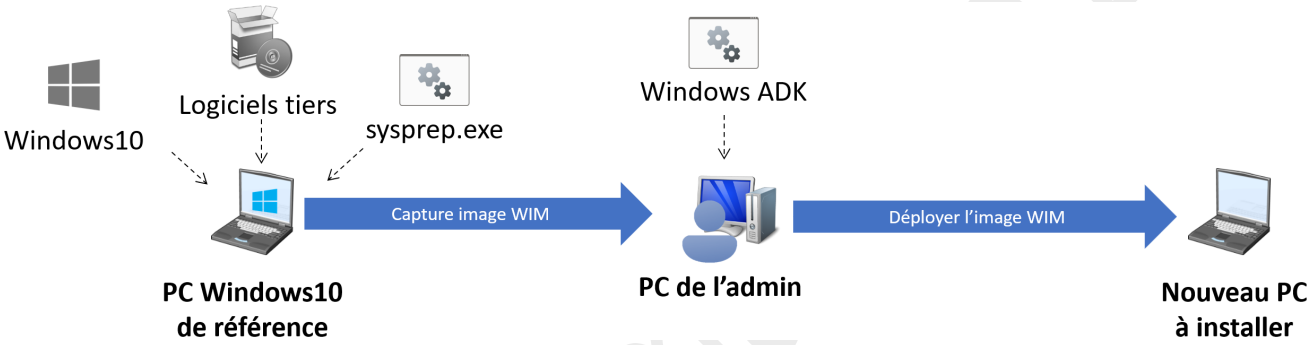
Avantages :

- Une seule image pour plusieurs configurations matérielles
- Déploiement non destructif des données existantes (prévoir de l'espace non partitionné)
- Juste besoin de WinPE pour ensuite plaquer l'image

Besoins :

- `Windows ADK` Assessment and Deployment Kit : 7,5Go contient WSIM, DISM, ImageX … : téléchargement
- `DISM` : outil de gestion et de maintenance des images de déploiement, plus complet que ImageX
- `sysprep.exe` : retire les identifiants uniques

Fichiers pour installations automatisée : unattend = fichier de réponses



Fonctionnement général du déploiement d'une image WIM

Sysprep

- Utilisé pour supprimer les données propres aux SE (systèmes d'exploitation) Windows
- Utilisé pour configurer Windows pour démarrer en mode d'Audit
- Utilisé pour configurer Windows pour lancer l'écran d'accueil (OOBE : Out Of Box Experience)
- Utilisé pour réinitialiser l'activation du produit Windows

`sysprep.exe /generalize` : Réinitialiser les identifiants de la machine

`sysprep.exe /audit` | `/oobe` : Démarrer en mode audit | oobe

`sysprep.exe /reboot` : Rebooter après sysprep (à ne pas faire, sinon l'ID machine est régénéré au reboot suivant)

ImageX

1. Utilisé pour capturer une image
2. Utilisé pour modifier une image
3. Utilisé pour déployer des images WIM
4. Utilisé pour stocker plusieurs images dans un fichier unique
5. Utilisé pour compresser les fichiers images

`imagex /capture` : capturer une image WIM à partir de la partition(0) et créer un fichier .wim

`imagex /apply` : déployer une image WIM, après avoir monté le lecteur réseau contenant le fichier .wim :

`imagex /mount`|`/mountrw`|`/unmount` : monter l'image en lecture, la monter en modification, la démonter

Création d'un disque de boot WinPE avec ImageX

Objectif : pouvoir utiliser imageX sur le pc de référence (celui qui servira pour l'image WIM de base)

Installer Windows ADK et l'environnement de déploiement et d'outils de création d'images

ouvrir Environnement de déploiement et d'outils de création d'images

`copype.cmd amd64 c:\winpe` : créer l'image boot.wim dans C:\winpe\media\sources\ (qui correspond à winpe)

`mkdir C:\winpe_x64` : créer le répertoire temporaire pour l'image winpe

`imagex /mountrw C:\winpe\media\sources\boot.wim 1 C:\winpe_x64` : monter l'image WIM dans C: \winpe_x64

optionnel : ajouter les drivers du réseau dans WinPE (dans le cas d'une image WIM copiée sur le réseau)

`copy "C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\amd64\DISM\imagex.exe" C:\winpe_x64\windows\system32` : copier l'exécutable imagex dans WinPE

`imagex /unmount c:\winpe_x64 /commit` : valider l'image et la démonter en mettant à jour le fichier boot.wim

`mkdir –P C:\isos` : créer le répertoire qui contiendra l'iso de winpe

`oscdimg.exe –n –bC:\winpe\fwfiles\efisys.bin c:\winpe\media c:\isos\winpe_imagex_BIOS–UEFI.iso` : créer l'iso (boot UEFI uniquement)

Attention : en BIOS non-UEFI : utiliser l'option `–bC:\winpe\fwfiles\etfsboot.com`

Capturer l'image WIM

Se connecter sur le pc de référence dont la partition C:\ servira de référence pour l'image WIM

Booter avec l'image iso qu'on a créé dans C:\winpe\winpe.iso

Processus d'installation

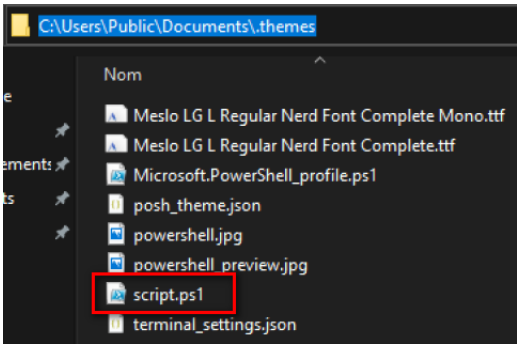
1. Générer une installation de référence (programmes, etc.) … puis …
2. `sysprep /oobe /generalize /shudown` : supprime les informations spécifiques à l'ordinateur
3. Booter sur **winpe_imagex.iso** puis capturer l'image d'installation (fichier .WIM) avec **imageX**
   `imagex /capture c: c:\win10.wim /compress fast "Windows10"` : capture de l'image dans C:\win10.wim
4. Copier l'image sur le poste de l'administrateur RSAT et la renommer en Windows10_21H1_dev.wim
5. Générer un fichier de réponses (machine de référence) avec **WSIM (Assistant Gestion d'installation)**
   a. Ajouter des composants
   b. Ajouter des packages
   c. Passer des commandes spécifiques : voir exemple chapitre suivant
6. Déployer l'image d'installation avec **WinPE + imageX**

Avantage de WIM : indépendant du matériel (indépendant de HAL), outils fournis

Exemple d'exécution de script dans WSIM :

L'objectif est d'exécuter un script PowerShell à la toute fin de l'installation de l'image

J'ai créé un petit script.ps1 dans le répertoire user public avant de capturer l'image

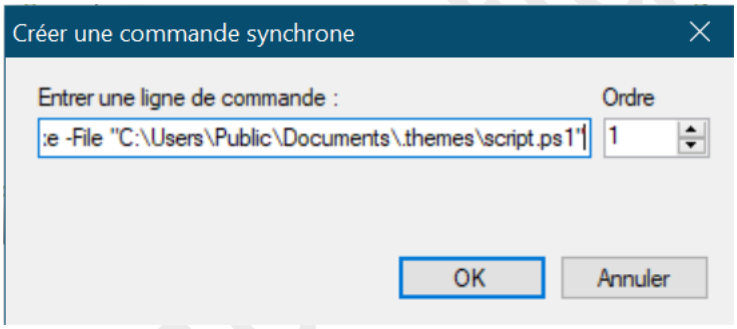


Ce script installe Windows Terminal avec Chocolatey puis applique un thème oh-my-posh :

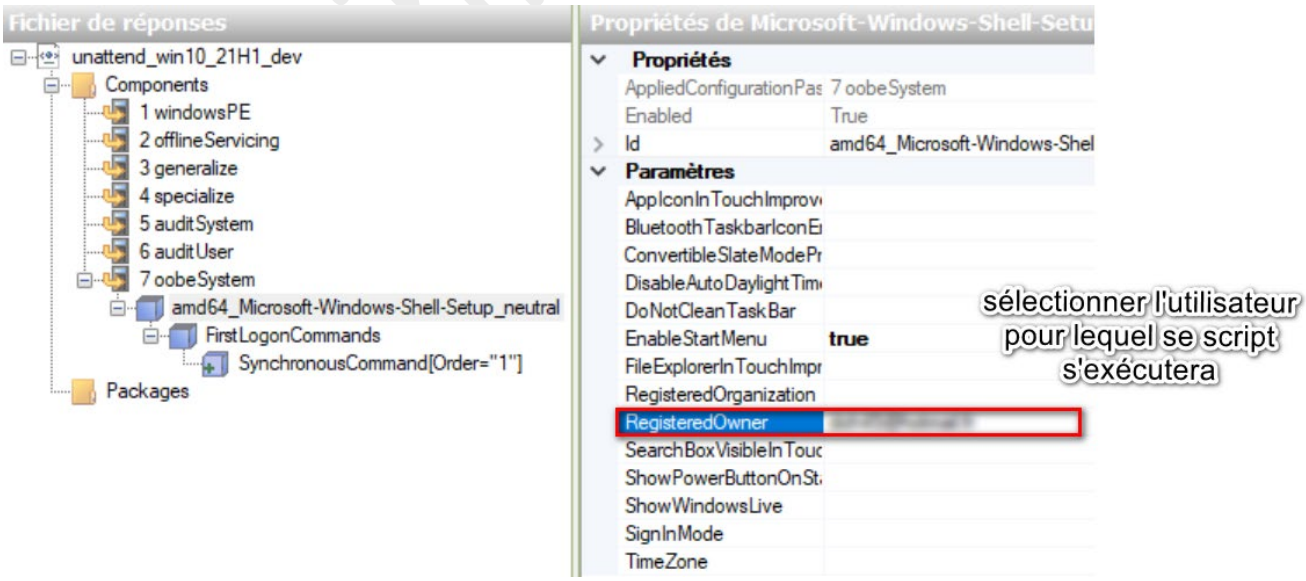
```
param([switch]$Elevated)
```

Pour exécuter ce script depuis l'invite de commande Windows, il faut exécuter :
`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe –File "C:\Users\Public\Documents\.themes\script.ps1"`

Pour ajouter cette ligne de commande dans le fichier de réponse de WSIM, il faut ouvrir WSIM, ouvrir le fichier .wim puis cliquer Insérer > Commande synchrone > 7 oobe system



Renseigner la commande à exécuter



Le script s'exécutera au premier logon

Installation personnalisée par fichier de réponses

WADK > WSIM (Windows System Image Manager) : permet de créer les fichiers de réponses

1. Création de l'image de référence, puis

```
sysprep /oobe /generalize /shutdown
```

2. Création de l'image WinPE : rendre conforme à l'architecture du poste cible (x86|x64)
3. Générer les fichiers nécessaires à l'exécution de WinPE, puis y injecter ImageX ainsi que les **drivers .inf des cartes réseau** (dans le cas d'une image .WIM sur le réseau)
4. Capturer l'image : pour ça on boot sur WinPE (avec le DVD ou en USB) puis on exécute imageX
5. Si on a rebooté en OOBE, finir la procédure puis refaire le sysprep
6. Déploiement

Il est possible de déployer des images en utilisant plusieurs méthodes :

- Avec un média WinPE
- Avec un serveur de déploiement
- Avec un HDD Virtuel

Edition d'une image WIM

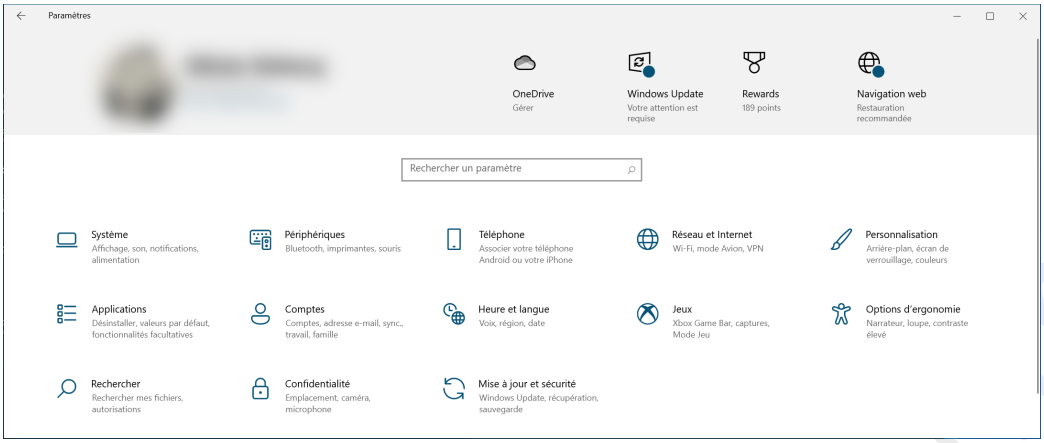
Avec DISM ou ImageX

- Maintenance hors connexion (sur un fichier)
- Maintenance en ligne (poste actuellement démarré)

1.4 Configuration du matériel et des applications

Les paramètres :

Accessible depuis Démarrer > Paramètres



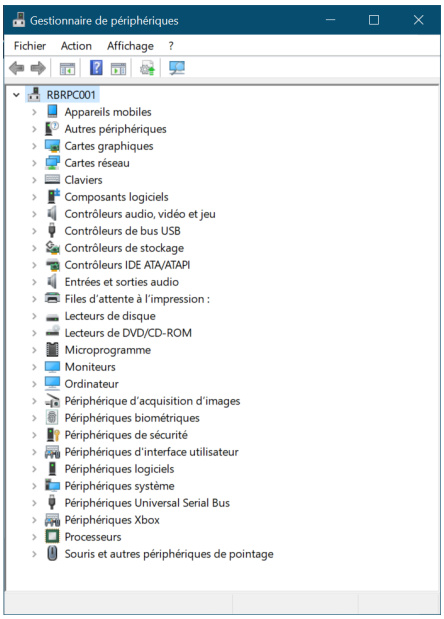
Le panneau de configuration :

Accessible depuis la barre de recherche du menu démarrer > « **Panneau de configuration** »

Aide de Windows : https://support.microsoft.com/fr-fr/windows

Gestion du matériel

Accessible depuis la 🔍 barre de recherche du menu démarrer > « **Gestionnaire de périphériques** »



Windows ReadyBoost

ReadyBoost vous permet d'utiliser un lecteur amovible, comme une clé USB, pour améliorer les performances de votre PC, sans avoir besoin d'ouvrir de l'ouvrir et d'ajouter de la mémoire (RAM). Pour utiliser ReadyBoost, il vous faut une clé USB ou une carte mémoire disposant d'au moins 500 Mo d'espace disponible et un taux de transfert de données élevé.

Pour utiliser ReadyBoost

1. Insérez la clé USB dans un port USB de votre PC.
2. Sélectionnez **Explorateur de fichiers** dans la barre des tâches.
3. Appuyez longuement (ou cliquez avec le bouton droit) sur la clé USB (ou la carte SD si vous en utilisez une) et sélectionnez **Propriétés**.
4. Sélectionnez l'onglet **ReadyBoost**, puis **Utiliser ce périphérique**.
5. Windows détermine si le périphérique peut utiliser ReadyBoost. Si ce n'est pas le cas, vous en serez informé.
6. Une fois que Windows a déterminé la quantité d'espace disponible à utiliser pour optimiser la mémoire, sélectionnez **OK** pour réserver cet espace, afin que ReadyBoost puisse l'utiliser.

Si vous examinez le contenu de la clé USB dans l'Explorateur de fichiers, vous verrez qu'un fichier nommé `ReadyBoost.sfcache` a été créé. Ce fichier affiche la quantité d'espace réservée pour ReadyBoost.

Remarque : ReadyBoost ne peut pas être utilisé si Windows est installé sur un disque SSD (Solid State Drive). Un disque SSD est déjà rapide et ReadyBoost ne pourra pas améliorer ses performances.

Aide générale sur l'amélioration de performances : ici

Configuration de la compatibilité applicative

Pour désactiver l'UAC (Contrôle d'Accès Utilisateur) : `C:\WINDOWS\System32\UserAccountControlSettings.exe` puis descendre la molette tout en bas sur « Ne jamais m'avertir »

Compatibilité des applications

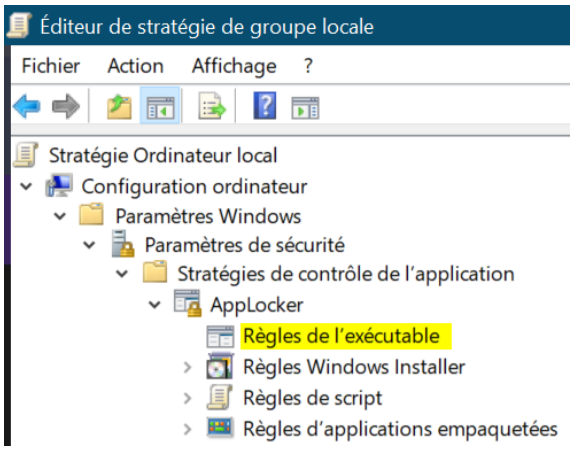
ACT (Application Compatibility Toolkit) gratuit. Inclus dans Windows ADK : téléchargement

- Standard User Analyser : permet de déterminer si l'appli a besoin d'une élévation de droits
- Compatibility administrator : liste d'applis avec les SHIM correctifs : l'aide du programme est suffisante

Configuration des restrictions d'application

AppLocker est un « pare feu » pour les applications.

`gpedit.msc` : ouvrir l'éditeur de GPO locale



Clic droit sur Règles de l'exécutable > Créer une règle pour interdire une application

Une fois AppLocker configuré, `services.msc` puis démarrer le service **Identité de l'application**

Terminer par `gpupdate /force` pour appliquer la GPO locale puis redémarrer l'ordinateur

1.5 Winget et Chocolatey – installation scriptée de programme

Historiquement, Chocolatey permet d'installer des programmes (principalement les freewares) et de les maintenir à jour de façon très simple, avec des scripts. Microsoft, conscient de son retard, a créé un outil en ligne de commande : Winget

Pour l'exemple, nous allons installer Brave browser et AdobePDF.

Winget : gestionnaire de paquets de Windows10

Attention : actuellement, winget ne permet actuellement pas de mettre à jour ni de désinstaller un package

1. Rechercher les packages brave browser et adobe PDF :

```
winget search brave
```

```
Nom                  ID                                 Version Correspondance
-------------------------------------------------------------------------------
Brave Browser        BraveSoftware.BraveBrowser         1.23.73 Moniker: Brave
Brave Browser Nightly BraveSoftware.BraveBrowser-Nightly latest  Tag: Brave
```

```
winget search adobe
```

```
Nom                           ID                                 Version          Correspondance
-------------------------------------------------------------------------------------------------
Flashpoint Infinity           bluemaxima.FlashpointInfinity      9.0              Tag: adobe
Brackets                      Adobe.Brackets                     1.14.2
AdobeDigitalEditions          Adobe.AdobeDigitalEditions         4.5.11
Adobe Acrobat Reader DC Czech Adobe.AdobeAcrobatReaderDC-Czech   19.8.20071.303822
Adobe Acrobat Reader DC       Adobe.AdobeAcrobatReaderDC         2021.001.20140
```

2. Installer les packages :

```
$packages_to_install = "BraveSoftware.BraveBrowser,Adobe.AdobeAcrobatReaderDC"
foreach ($package in $packages_to_install.split(',')) {
    winget install $package
}
```

Chocolatey : gestionnaire de paquets communautaire

Prérequis :

- Windows 7+ / Windows Server 2003+
- PowerShell v2+
- .NET Framework 4+ (the installation will attempt to install .NET 4.0 if you do not have it installed)

0. Installer chocolatey :

```
Set-ExecutionPolicy Bypass -Scope Process -Force; [System.Net.ServicePointManager]::SecurityProtocol = [System.Net.ServicePointManager]::SecurityProtocol -bor 3072; iex ((New-Object System.Net.WebClient).DownloadString('https://chocolatey.org/install.ps1'))
```

1. Rechercher les packages brave browser et adobe PDF :

Nota : il est plus pratique (visuellement parlant) d'aller rechercher des packages de Chocolatey directement sur internet, ici : https://community.chocolatey.org/packages

```
choco list brave
```

```
Chocolatey v0.10.16-beta
brave 1.23.73 [Approved]
minecraft-education 1.14.50.0 [Approved] Downloads cached for licensed users
astromenace 1.3.2 [Approved] Downloads cached for licensed users
```

```
choco list adobe reader
```

```
Chocolatey v0.10.16-beta
simnetsa-adobereader-fr 11.0.7 - Possibly broken
adobereader 2021.001.20145 [Approved]
adobereader-update 18.011.20058 [Approved] Downloads cached for licensed users - Possibly broken for FOSS users (due to original download location changes by vendor)
pdf-ifilter-64 11.0.01.20180614 [Approved] Downloads cached for licensed users
PDFXChangeViewer 2.5.317.20161116 [Approved]
PDFXchangeEditor 9.0.354.0 [Approved]
maxthon.commandline 6.1.1.1000 [Approved] Downloads cached for licensed users
```

2. Installer les packages :

`choco install -y brave adobereader` : installer les packages

`-y` permet de valider automatiquement, `-pre` : permet d'installer les version preview

3. Mettre à jour les packages :

`choco update all` ou `cup all` : mettre à jour les paquets à la dernière version disponible

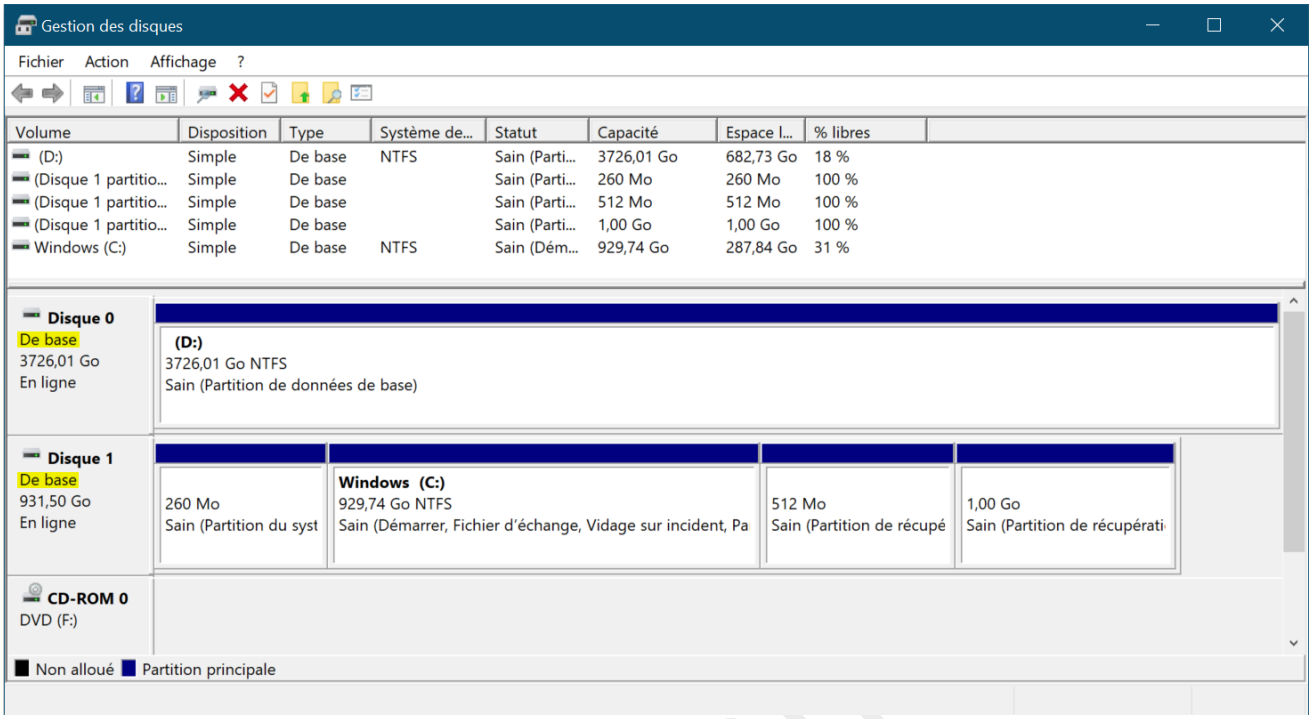
4. Desinstaller les packages :

`choco uninstall brave` : désinstaller Brave browser

1.6 Gestion des disques

Gestionnaire des disques

`diskmgmt.msc` : l'aide officielle est ici



Aussi accessible depuis ⊞ Démarrer > Gestion des disques

Disques de base (Partitions)

- MAX soit 4 partitions principales
- MAX soit 3 partitions principales étendues (lecteurs logiques)

Disques dynamiques (Volumes)

- Volumes simples (partitions principales sur disques simples)
- Volumes fractionnés (ou répartis en plusieurs disques : de 2 à 32 disques)
  - Augmente l'espace disque du lecteur
  - Aucune tolérance de pannes
  - Indissociables
- Volumes agrégés par bandes (RAID0)
  - Optimiser la lecture/écriture
  - Aucune tolérance de pannes
  - Tous les volumes font la même taille
- Volumes en miroir (RAID1)
  - Copie miroir de disque
  - Tolérance de pannes
- RAID5 (agrégat par bandes avec parité)
  - Tolérance de pannes
  - Optimiser la lecture/écriture

Gestion des disques virtuels

Créer un disque dur virtuel (fichier au format .vhd ou .vhdx présent sur un disque physique)

Ouvrir `diskmgmt.msc`

Cliquer dans Action > **Créer un disque dur virtuel**

Renseigner l'emplacement local du fichier, renseigner le format VHD ou VHDX et renseigner la taille

Initialiser le disque en faisant un clic-droit dans la zone du disque Non initialisé

Sélectionner le type de partition (GTP n'est pas reconnu par toutes les versions précédentes de Windows)

Créer vos volumes comme vous le feriez avec un disque standard.

Nota : Il est aussi possible de monter un fichier .vhd ou .vhdx existant (n'accepte pas les partitions avec des FS Linux)

Une fois terminé, clic-droit dans la zone du disque virtuel En ligne > Détacher un disque virtuel

Le disque peut ensuite être utilisé par Hyper-V, ou converti par exemple en VMDK :

Installer Virtual Box

`cd C:\temp` : emplacement de mon_disque.vhdx

`VBoxManage clonehd --format vmdk mon_disque.vhdx mon_disque.vmdk` : convertir vers C:\temp\mon_disque.vmdk

Commandes pour la gestion de disques :

- `diskmgmt.msc` : interface graphique
- `diskpart.exe` : Logiciel en ligne de commandes :

`DISKPART> commands` : Liste des commandes

`DISKPART> help fonction` : Aide sur la fonction

Créer une partition G:\ de 200Mo et la formater

`DISKPART>select disk 1` : sélectionner un disque (le rendre focus)

`DISKPART>list disk` : vérifier quel disk est focus (*)

`DISKPART>create partition primary size=200` : créer une partition de 200Mo

`DISKPART>assign letter=G` : assigner une lettre (G:)

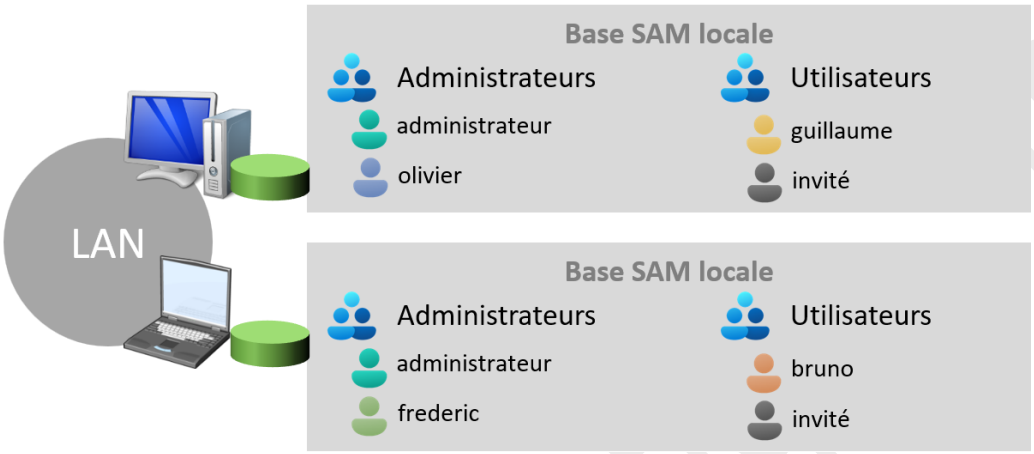
`DISKPART>format fs=NTFS label="Données"` : formater en NTFS et nommer « Données »

1.7 Gestion des groupes et des utilisateurs

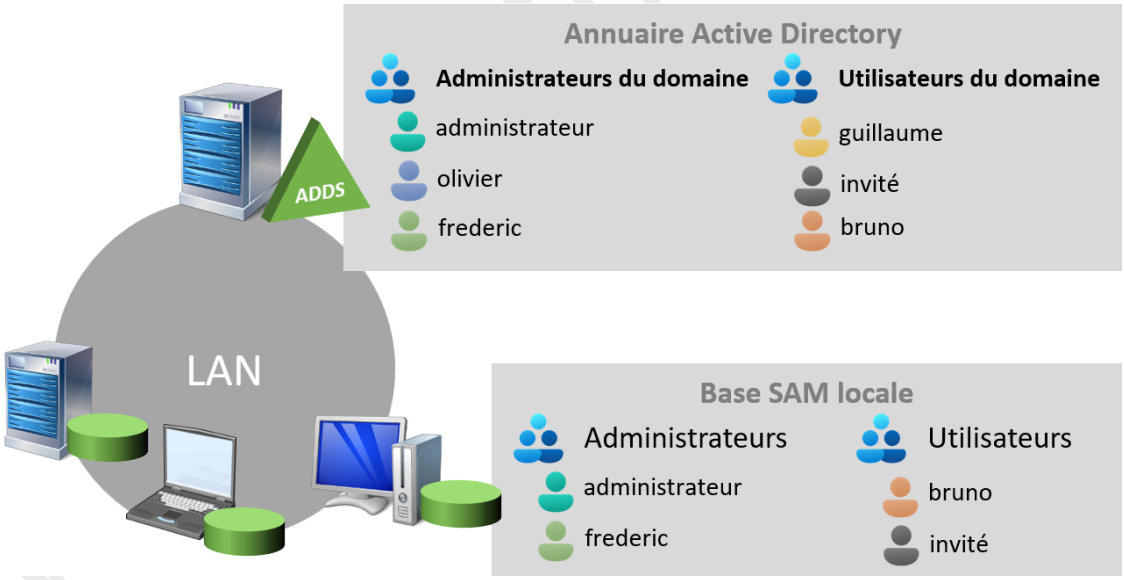
Les utilisateurs

Deux types de comptes :

- **Utilisateurs locaux** : ils ont un accès local à la machine et un accès à des ressources locale. Gestion non centralisée
- **Utilisateurs du domaine** : ressources stockées sur un serveur, authentification sur le domaine ADDS.
    - Sur un domaine, les groupes locaux de domaine sont inclus dans les groupes universels
    - Les groupes universels sont inclus dans les groupes globaux

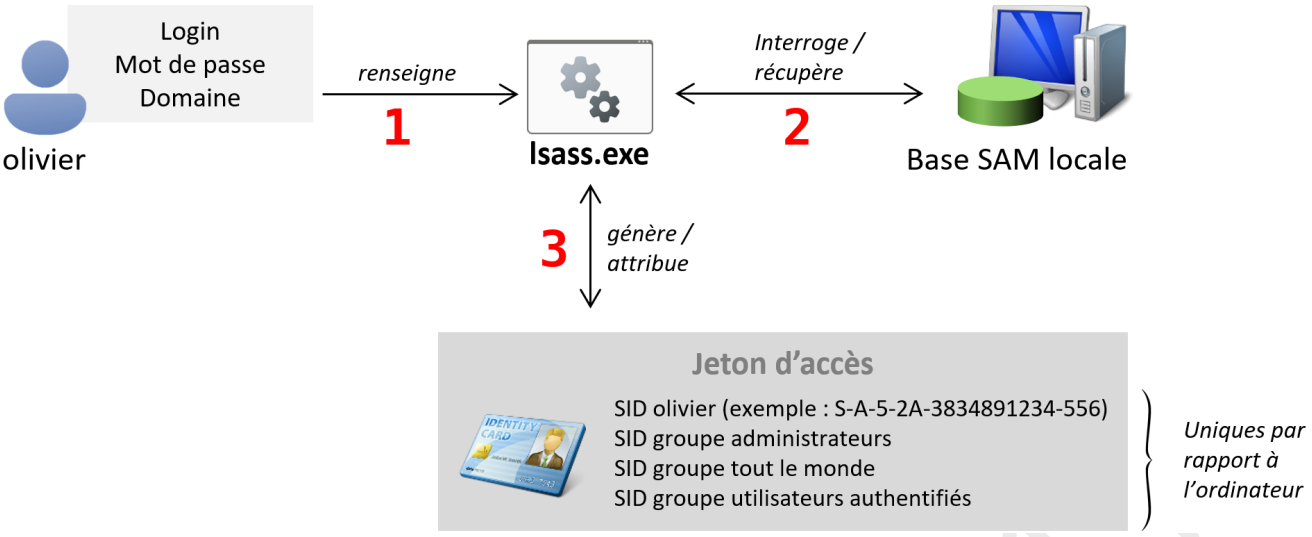


Utilisateurs locaux



Utilisateurs du domaine

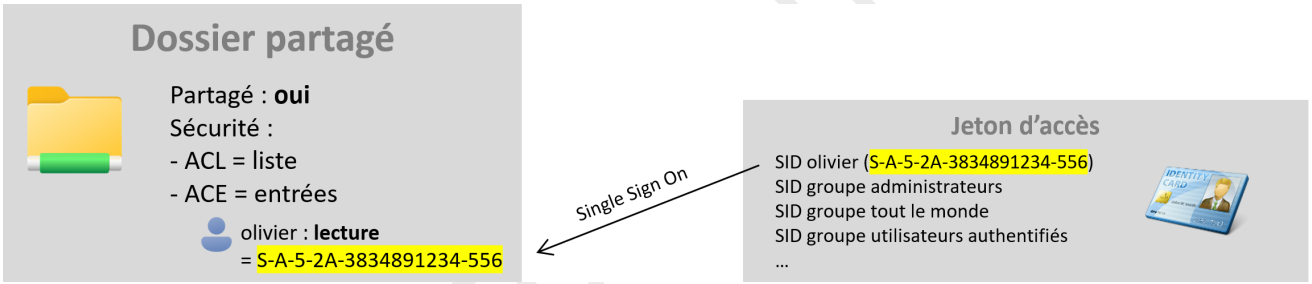
Les SID



A propos de la composition des SID utilisateurs

Vocabulaire de la sécurité sous Windows

- **Droits** : privilège (installer un pilote, modifier l'heure …)
- **Autorisation** : permissions (sur les ressources, les dossiers partagés, imp. Partagés, objets AD …)
  - Le SID sert à donner des **autorisations** d'accès aux ressources.



Méthode d'accès à un répertoire partagé

SSO (Single Sign-On) :

1. Le SID de l'utilisateur et le SID de l'ACE sont comparés
2. Si c'est ok : accès en lecture

Un jeton d'accès n'est pas dynamique : si on ajoute un utilisateur dans un groupe alors il faut redémarrer sa session pour mettre à jour les SID du jeton d'accès.

Interactions entre Partage et Sécurité

Nota : Avec un FS de type FAT, le seul moyen de sécuriser le partage est de modifier l'onglet [Partage] car [Sécurité] n'existe pas en FAT16/FAT32

Entre le partage et la sécurité, le plus restrictif des deux a le dernier mot

- Partage : olivier : modifier (RWD)
- Sécurité : olivier : lecture (R)
- Finalement, olivier ne pourra qu'écrire

Configuration idéale :

Nota : olivier et emma sont membres du groupe gg_stagiaires

Il en résulte :

- **Accès via le réseau** : olivier = lecture, emma = modifier, gg_stagiaires = modifier
- **Accès local** : olivier = lecture, emma = modifier, gg_stagiaires = modifier (on n'applique pas le filtre lié au partage)
- Avec cette méthode, l'accès via le réseau et en local ont les mêmes résultats

Un $ à la fin d'un nom de partage cache le partage. Data$ → partage caché

Partage d'imprimantes

- **Imprimer** : permet d'installer le pilote et d'imprimer sur l'imprimante partagée
- **Gérer les documents** : permet de gérer le document quand il est spoolé
- **Gérer les imprimantes** : permet de gérer les onglets de l'imprimante

Partage de dossiers en ligne de commande

`net share ?` : aide sur le partage partage de dossier | lister les partages

`net use ?` : aide sur la connexion de lecteur réseau

`New-FileShare` : créer un partage réseau (via PowerShell 5.1)

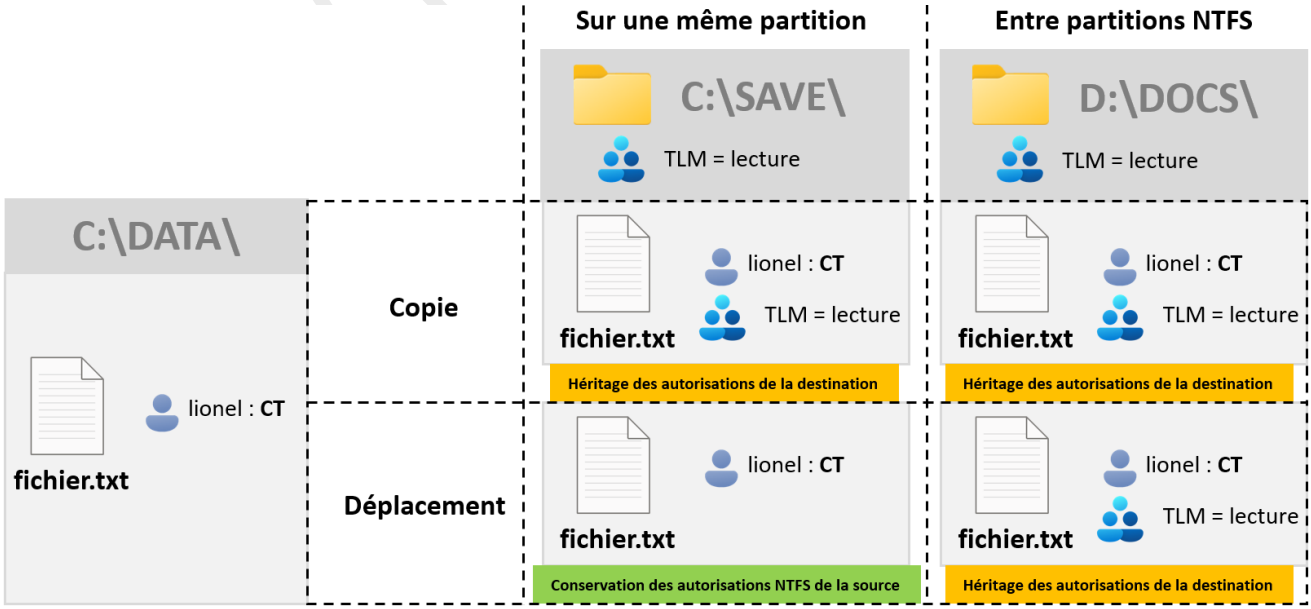
`Grant-FileShareAccess` : définir les droits sur un partage

`Get-FileShare` : lister partage réseau

`New-PSDrive` : connecter un lecteur réseau

Copies et Déplacements en NTFS

Nota : à partir de maintenant, TLM = Tout le monde / CT = Contrôle Total



Seul le déplacement sur une même partition permet de conserver les autorisations NTFS de la source

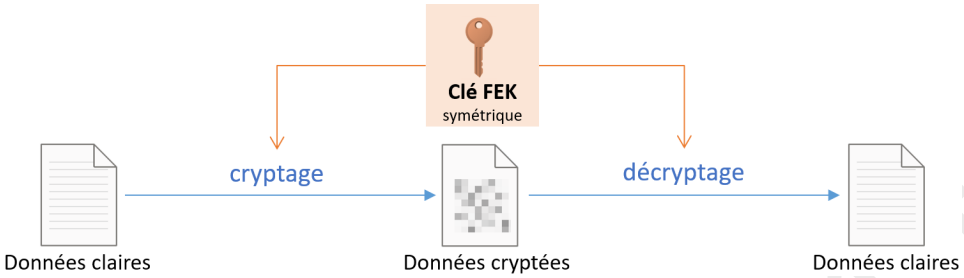
1.8 Autres fonctionnalités

EFS (Encrypting File System)

Les fichiers cryptés sont affichés avec un cadenas sur l'icône. Les droits NTFS s'appliquent aussi une fois décryptés

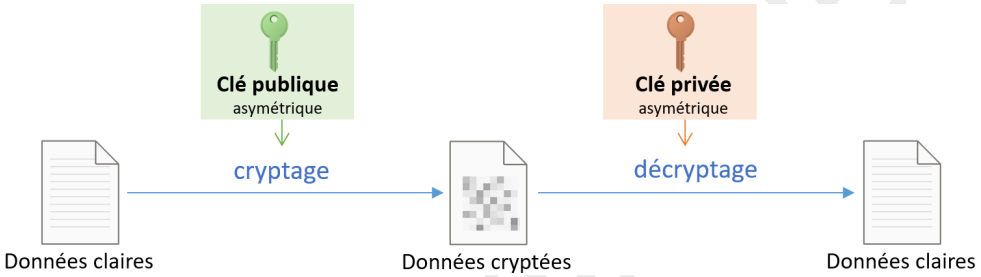
- Avantage : c'est un cryptage mominatif (propre à un compte d'utilisateur)
- Inconvénient : oubli de mot de passe de la clé EFS = perte de la clé de décruptage

Cryptage symétrique :



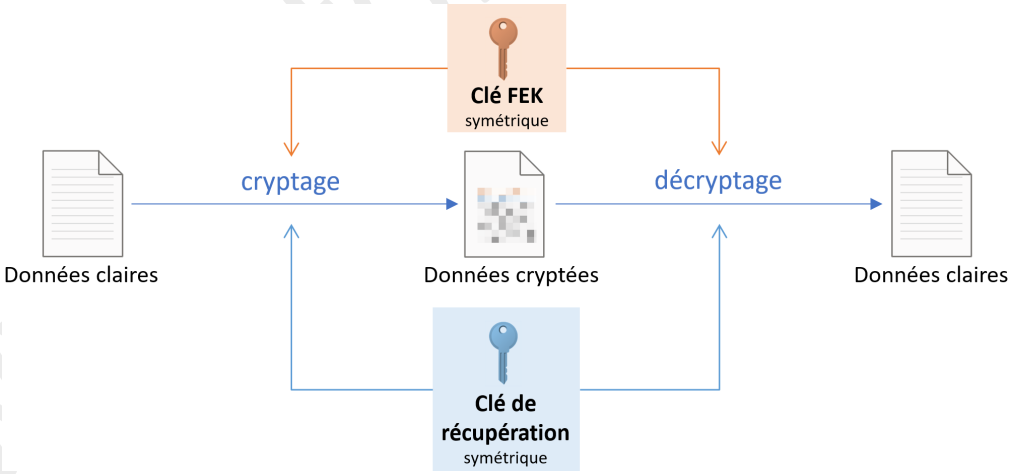
Cryptage symétrique : une seule clé pour crypter et décrypter

Cryptage asymétrique :



Cryptage asymétrique : la clé publique crypte, la clé privée décrypte

Cryptage EFS :



Crypter avec la clé FEK + la clé de récupération permet de décrypter les données en cas de perte de la clé FEK

Les données cryptées sont :

- Data Description File (DDR), encrypté par la clé FEK
- Data Recovery File (DRF), encrypté par la clé de récupération
- Données cryptées

Procédure de cryptage EFS

Attention : l'agent de récupération doit être configuré **avant** d'utiliser EFS

Créer la clé de récupération EFS :

1. `cipher /R:D:\OneDrive\Applications\PERSO\EFS\recuperation` : génère certificat.cer et certificat.pfx
2. `gpupdate /force` : forcer l'utilisation du certificat de récupération
3. Double-clic sur le certificat certificat.cer créé > Utilisateur actuel > renseigner le mot de passe > Magasin de certificat **Personnel** : permet de crypter les fichiers EFS avec la clé de récupération publique

Crypter un fichier de test :

Clic droit sur un fichier > propriétés > avancé > chiffrer le contenu pour sécuriser les données

Exporter le certificat EFS utilisateur

`rekeywiz.exe` : assistant de récupération des clés. Utiliser le certificat existant

Afficher les certificats EFS :

`mmc.exe` > ajouter un composant … > Certificat > Mon compte d'utilisateur > OK (ou bien `certmgr.msc`)

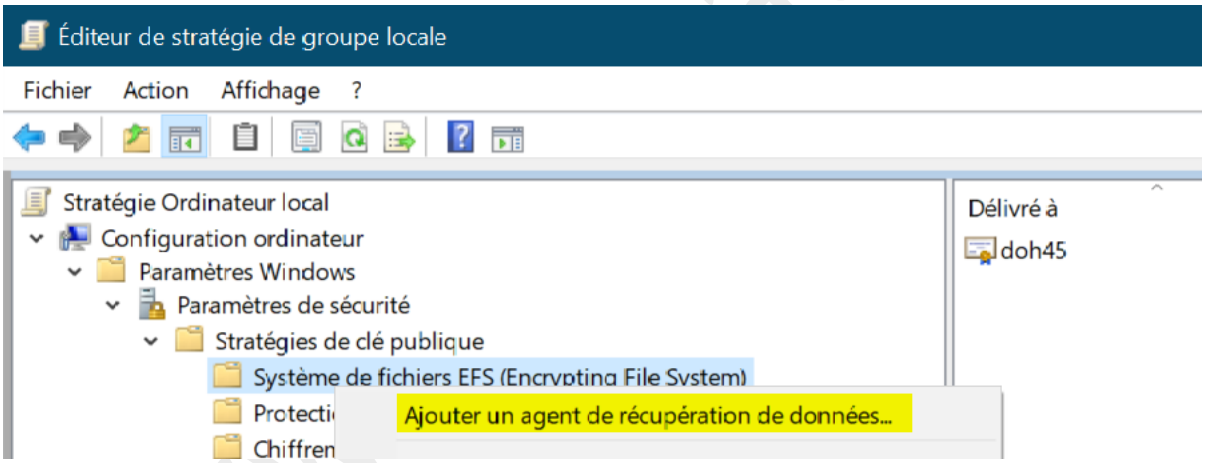
Naviguer dans Personnel > Certificats

Délivré à	Rôles prévus	Délivré par	Date d'expiration
doh45	Récupération de fichiers	doh45	18/03/2121
doh45	Système de fichiers EFS (Encrypting File System)	doh45	18/03/2121

La clé FEK a le rôle « Système de fichiers EFS », la clé publique de récupération a le rôle « Récupération de fichiers »

Définir l'agent de récupération de données :

gpedit.msc :



Le fichier certificat.cer est utilisé pour permettre de récupérer les données en cas de perte de la clé FEK

BitLocker : chiffrement de partition

Documentation en ligne

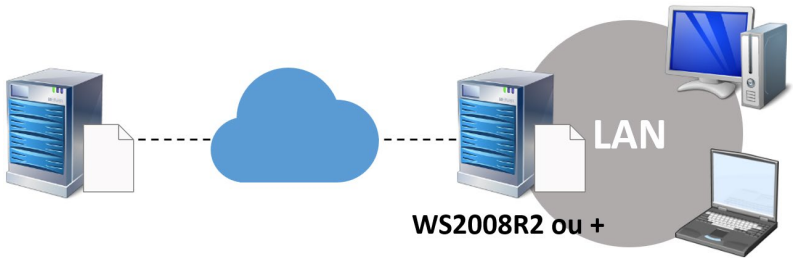
BranchCache

Mise en cache de contenu des serveurs (web et fichiers) pour économiser les liaisons entre le serveur et le LAN.

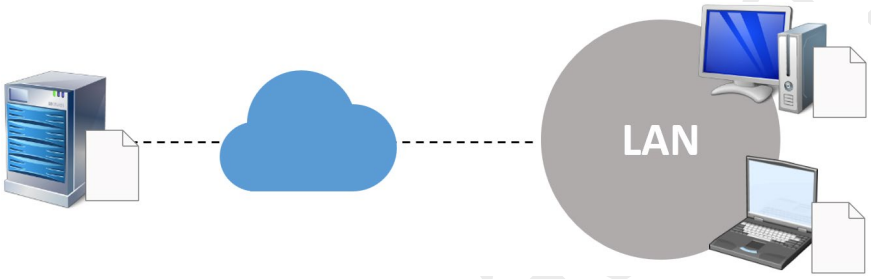
Documentation en ligne

Modes de distribution

Sur le serveur WS2008R2 ou plus récent, il faut installer le service « BranchCache » puis partage avancé avec mise en cache BranchCache.

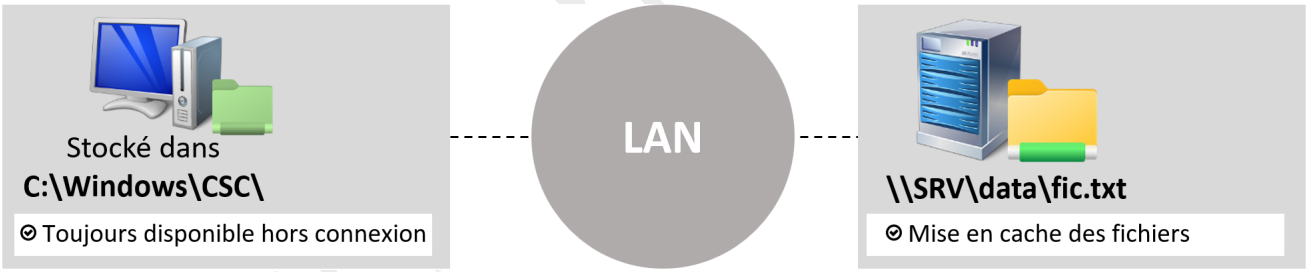


Mode hébergé



Mode distribué

Fichiers Hors connexion



L'une ou l'autre des options active les fichiers hors connexion

But : mettre en cache le(s) document(s) d'un seul utilisateur. Le fichier le plus récent écrase l'ancien.

Marche à suivre :

Sur le poste client Windows10 :

- Sur le dossier / fichier du lecteur réseau : clic droit > **Toujours disponible hors connexion**
- Centre de synchronisation : gérer la synchronisation, gérer les conflits de synchronisation

Sur le serveur de fichiers : Partage > Avancé > Mise en cache

- **Désactiver** : désactive la mise en cache
- **Activer à la demande** : autorise via le centre de synchronisation (+ BranchCache)
- **Activer toujours** : force la mise en cache des fichier

Pare Feu

⚙ Paramètres > Mise à jour et sécurité > Sécurité Windows > Pare-feu et protection du réseau

- Paramètres avancés (équivalent à `wf.msc`)
- Cliquer sur le réseau (réseau avec domaine / privé / public) pour activer / désactiver le pare-feu Windows

`netsh advfirewall firewall /?` : pare-feu en ligne de commande

Les stratégies de groupe - GPO : Group Policy Objects

- GPO de domaine : gpmc.msc
- GPO locale : gpedit.msc

`gpupdate /force` : à exécuter à chaque mise à jour des GPO pour qu'elles s'appliquent

	GPO de domaine (`gmpc.msc`)	**GPO locale** (`gpedit.msc`)
Ordinateur	S'applique à l'objet ordinateur	S'applique à tout le monde
Utilisateur	S'applique à l'objet utilisateur	S'applique à l'utilisateur connecté

Cible d'application des GPO

`mmc.exe` > ajouter un composant « Editeur d'objets de stratégies de groupes » : permet de modifier la GPO d'un utilisateur administrateur, non administrateur, spécifique ou d'un ordinateur spécifique

Attention : la partie ordinateur des GPO prime sur la partir utilisateur locale

Surveillance du système

Observateur d'évènements

Clic droit sur ⊞ Démarrer > Observateur d'évènements

Source + ID évènement : http://www.eventid.net (informations sur le souci rencontré)

`winrm quickconfig` : Gestion à distance (active également le service WinRM)

Partie de droite > Joindre une tache à cet évènement : net send|mail|programme|script …

Analyseur de performances

- [ctrl]+[shift]+[echap] : gestionnaire des taches > performances > moniteur de ressources
- `mmc.exe` : analyseur de performances
  - Ajouter des compteurs
  - Ensemble de collecteurs de données> définis par l'utilisateur : créé des rapports