Formation Windows 10/11 Pro Ent LTSC - Sr 10-11 –Système Cours

Michel Cabaré / www.cabare.net / michel@cabare.net

Windows 10-11 Système Pro Entreprise Education LTSC - 21H2 - Sr 10-11 - Cours Système V3.0 - Décembre 2021

ICPF
Certification **PRO**
Formateur Expert

CABARÉ FORMATION

Microsoft Partner

Ce Support a pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion du système Windows 10 -11 mis à jour. Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

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

Bon Travail

Michel Cabaré

Table des Matières

ASSISTANT CREATION DE PROFIL

Nouveau profil « manuel »:

Lorsque l'on crée un nouvel utilisateur, sur un poste Windows, un nouveau profil sera créé pour son environnement lors de sa première ouverture de session.

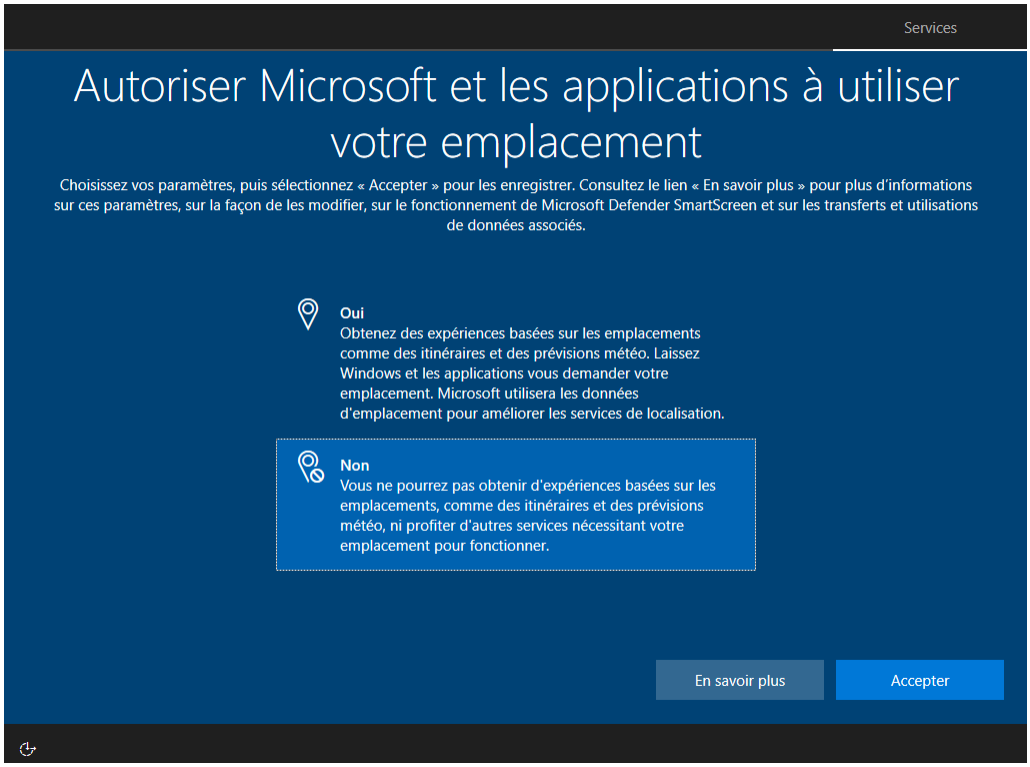
Il récupèrera des éléments éventuellement posés dans le profil par défaut mais déroulera aussi une 1° séquence découlant des obligations RGPD et des obligations de confidentialités.

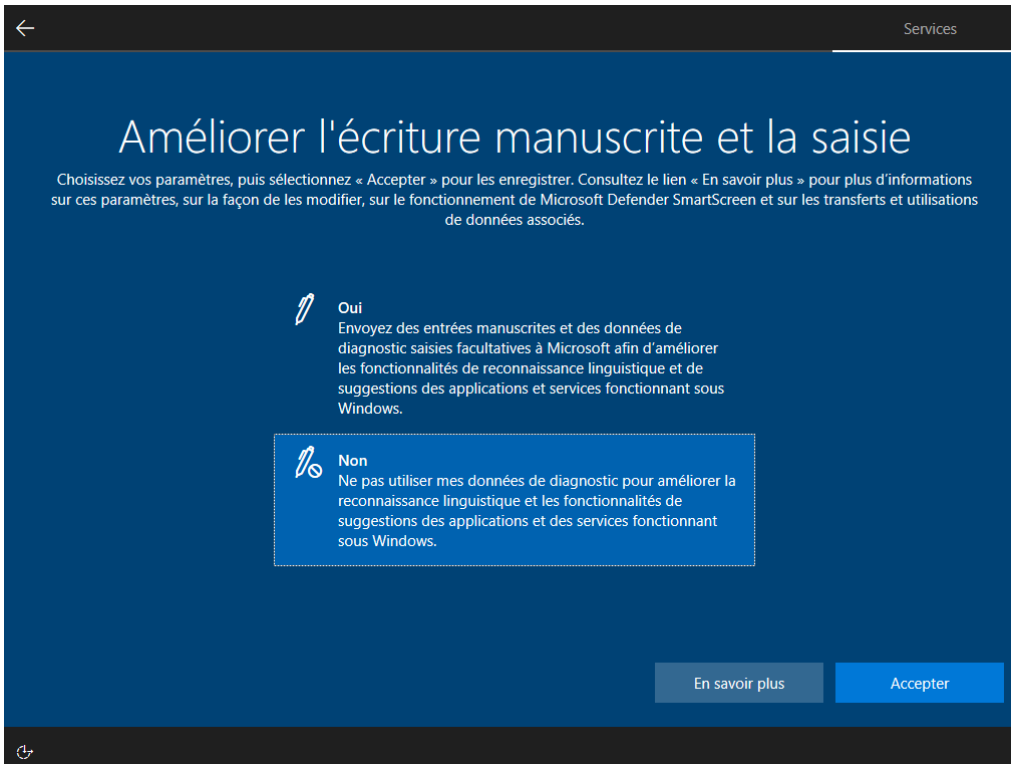
Cette séquence varie assez selon les branches. Elle peut être bien sur paramétrée par des GPO ou des réglages sur le poste, mais le déroulement « natif » permet d'avoir une idée des réglages minimum que l'on peut avoir envie de gérer

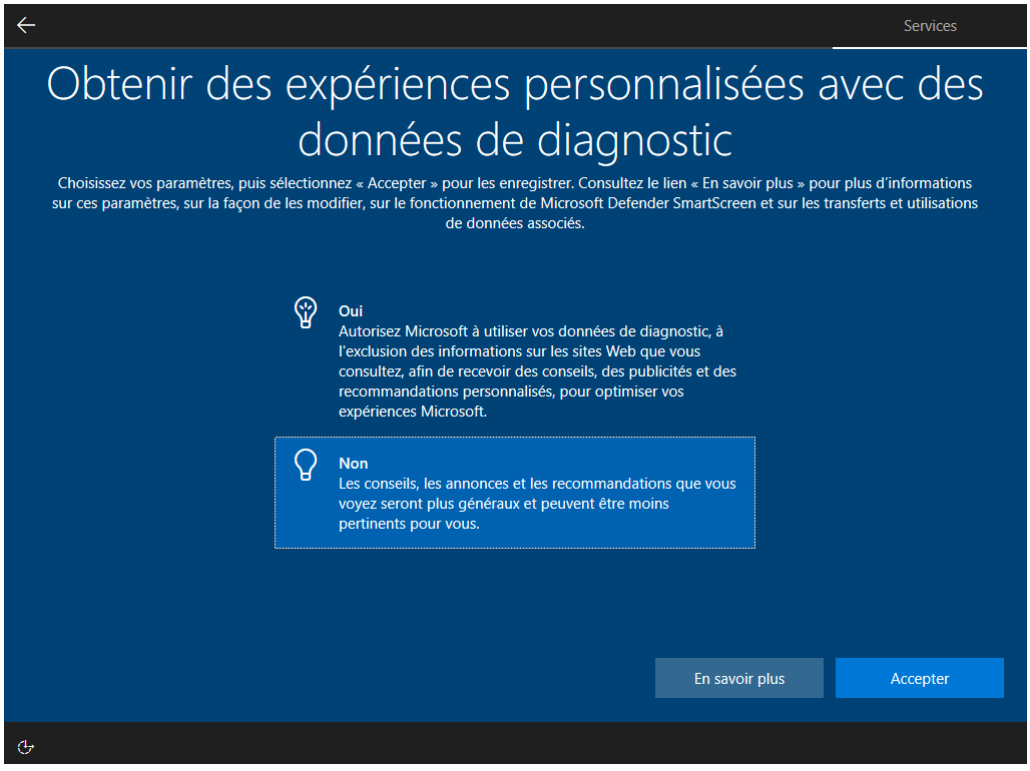
Après une 1° authentification réussie, il y a donc création du profil utilisateur

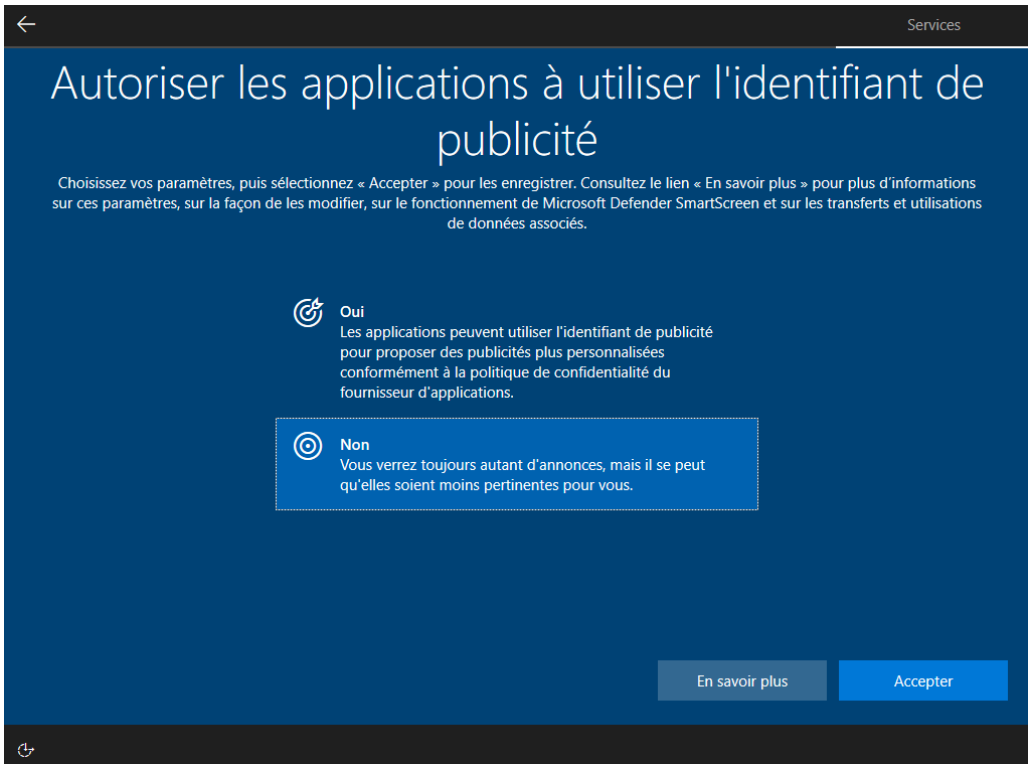
Profil sur Windows 10 pro - 21H2:

Les questions « profil » utilisateurs posées sont les suivantes :

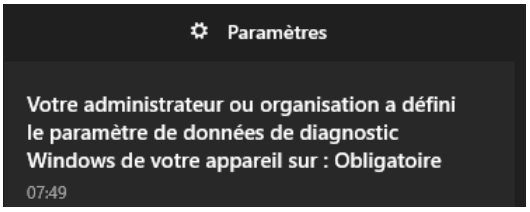



Services
Améliorer l'écriture manuscrite et la saisie
Choisissez vos paramètres, puis sélectionnez « Accepter » pour les enregistrer. Consultez le lien « En savoir plus » pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.
Oui
Envoyez des entrées manuscrites et des données de diagnostic saisies facultatives à Microsoft afin d'améliorer les fonctionnalités de reconnaissance linguistique et de suggestions des applications et services fonctionnant sous Windows.
Non
Ne pas utiliser mes données de diagnostic pour améliorer la reconnaissance linguistique et les fonctionnalités de suggestions des applications et des services fonctionnant sous Windows.
En savoir plus
Accepter


Services
Obtenir des expériences personnalisées avec des données de diagnostic
Choisissez vos paramètres, puis sélectionnez « Accepter » pour les enregistrer. Consultez le lien « En savoir plus » pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.
Oui
Autorisez Microsoft à utiliser vos données de diagnostic, à l'exclusion des informations sur les sites Web que vous consultez, afin de recevoir des conseils, des publicités et des recommandations personnalisés, pour optimiser vos expériences Microsoft.
Non
Les conseils, les annonces et les recommandations que vous voyez seront plus généraux et peuvent être moins pertinents pour vous.
En savoir plus
Accepter



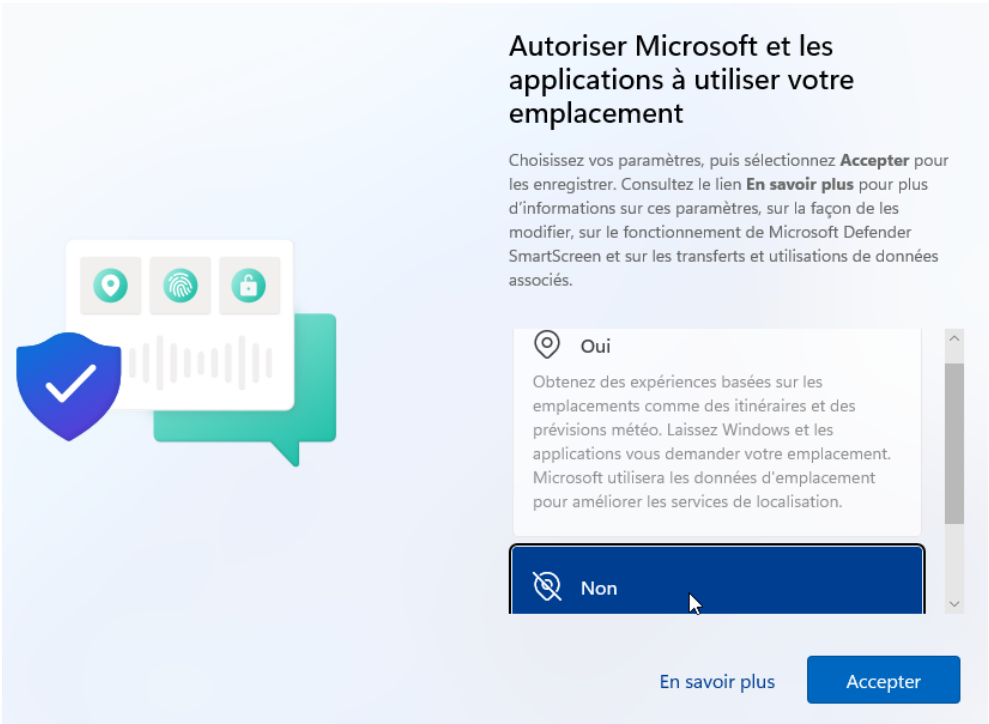
Un dernier message informatif s'affiche

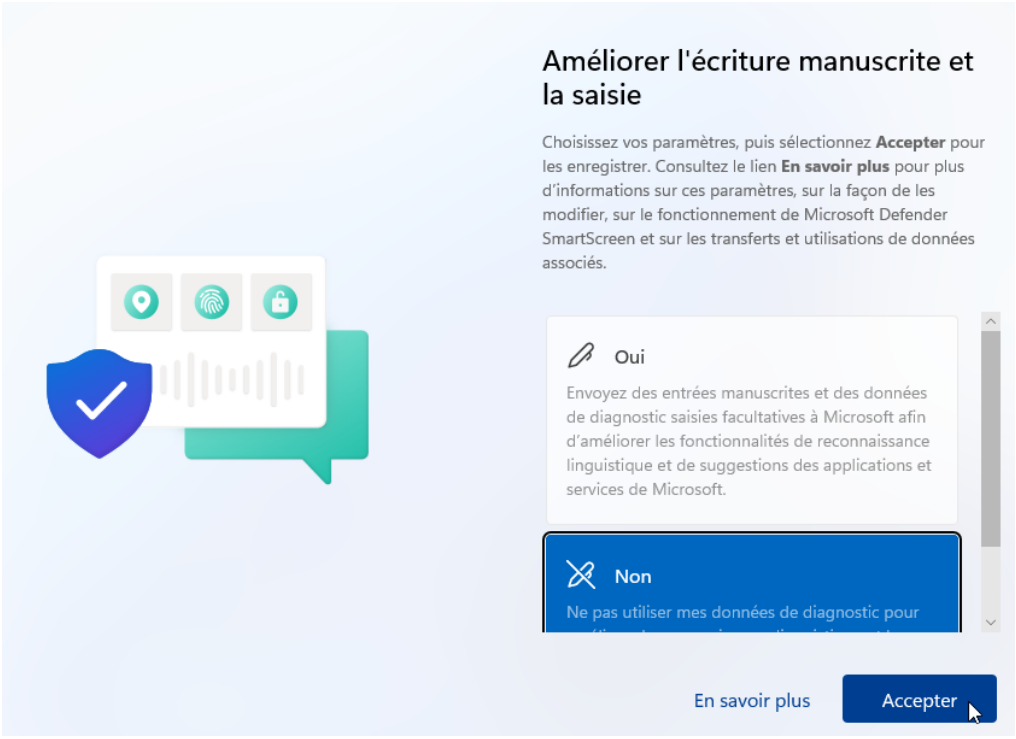


Et la session s'ouvre

Profil sur Windows 11 pro- 21H2:

Les questions « profil » utilisateurs posées sont les suivantes :




Améliorer l'écriture manuscrite et la saisie
Choisissez vos paramètres, puis sélectionnez **Accepter** pour les enregistrer. Consultez le lien **En savoir plus** pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.
Oui
Envoyez des entrées manuscrites et des données de diagnostic saisies facultatives à Microsoft afin d'améliorer les fonctionnalités de reconnaissance linguistique et de suggestions des applications et services de Microsoft.
Non
Ne pas utiliser mes données de diagnostic pour
En savoir plus
Accepter


Obtenir des expériences personnalisées avec des données de diagnostic
Choisissez vos paramètres, puis sélectionnez **Accepter** pour les enregistrer. Consultez le lien **En savoir plus** pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.
Oui
Autorisez Microsoft à utiliser vos données de diagnostic, en excluant les informations sur les sites web que vous consultez, pour vous proposer des conseils, des publicités et des recommandations personnalisés afin d'améliorer vos expériences Microsoft.
Non
En savoir plus
Accepter


Autoriser les applications à utiliser l'identifiant de publicité
Choisissez vos paramètres, puis sélectionnez Accepter pour les enregistrer. Consultez le lien En savoir plus pour plus d'informations sur ces paramètres, sur la façon de les modifier, sur le fonctionnement de Microsoft Defender SmartScreen et sur les transferts et utilisations de données associés.
Oui
Les applications peuvent utiliser l'identifiant de publicité pour proposer des publicités plus personnalisées conformément à la politique de confidentialité du fournisseur d'applications.
Non
Vous verrez toujours autant d'annonces, mais il se peut qu'elles soient moins pertinentes pour vous.
En savoir plus
Accepter

LES PROCESSUS SOUS WINDOWS

Séquence POST : Power On Self Test

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

Séquence Bootmgr depuis 10-7

3 étapes

« Séquence POST »

Bootmgr avec le magasin **\Boot\Bootstat.dat**

Winload.exe

(crée l'environnement)

(d'execution pour SEVEN)

↓

Ntoskrnel Détection hard **HAL**

(F8)

Smss.exe (gestionnaire de session)

Lance Win32 (affiche la barre de progression)

Lance les services en Boot-execute

Winlogon.exe — Gestion LSA

Screg.exe — Derniers services à démarrer

Lsass.exe **(gestion** CTRL-ALT-SUPPR)

Stratégies de groupe, Scripts de démarrage, programmes/services en

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

X:\ProgramData\Microsoft\Windows\Start Menu\Programmes\Démarrage

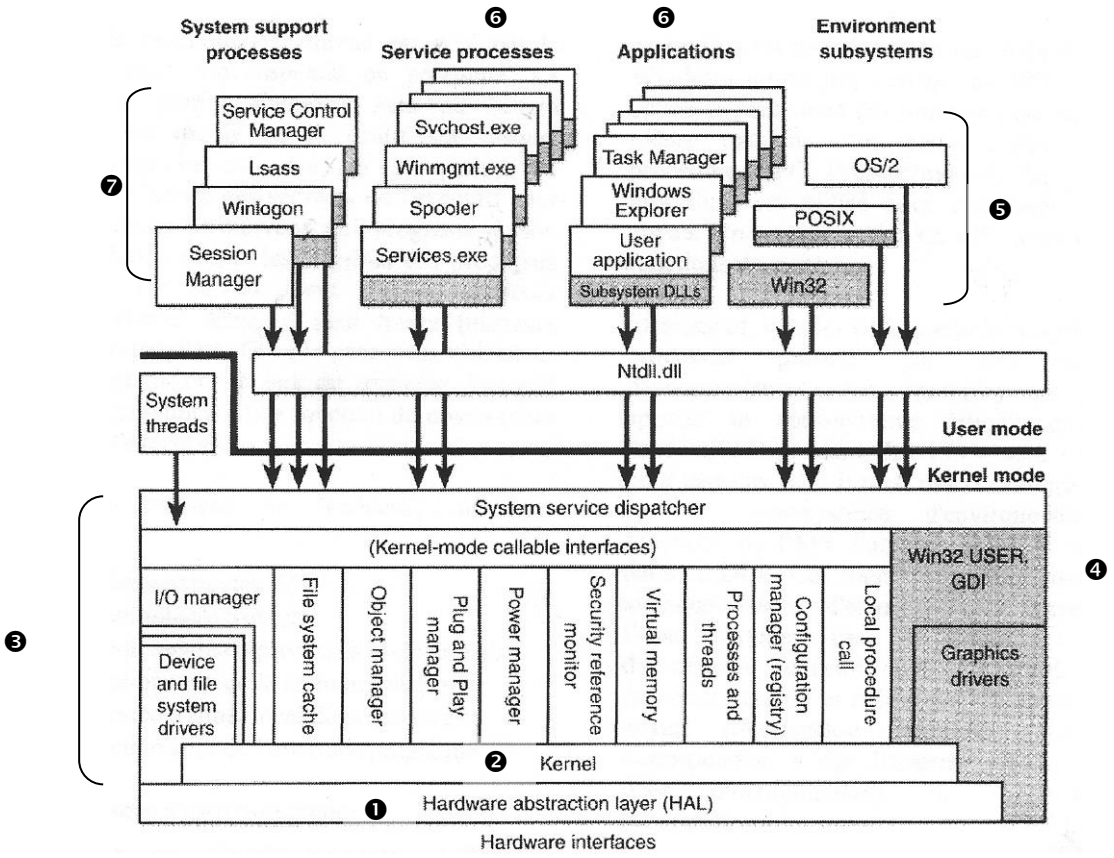
X:\User\%username%\AppData\RoamingMenu\Microsoft\Windows\ Start Menu \ Programmes\Démarrage

Msconfig permet de dire ce que l'on veut ou non

Désactivable avec **SHIFT** au moment de l'ouverture de session

Vocabulaire système sous Windows 10 :

Schématiquement on peut distinguer :



- LA **HAL** ❶ou couche d'abstraction matérielle : fournie des fonctions pour contrôler le bus système, canaux DMA, déclenchement des interruptions, horloge système… toutes ces fonctions sont utilisées dans les autres parties du noyau
- Le **Kernel** ❷ (micro kernel) : c'est le noyau toujours en mémoire, traite les interruptions, permet au CPU d'allouer du temps aux différents processus, appelé aussi **threads**.
- **L'exécutif** ❸ (serveur noyaux) : c'est l'ensemble des services système de gestion mémoire – périphériques –fichiers – appellé donc threads système. Chaque service système progresse à son propre rythme
- les **services noyaux sous systèmes environnement** ❹ : il s'agit de supporter différentes interfaces… : win32 – posix – Os2… par exemple l'executif de windows défini un ensemble de fonction nommée **API** (**Access Programming Interface**). ❺ Un programme utilisateur fait appel à des API système pour dialoguer avec l'OS.
- les **services noyaux systèmes** ❻ nécessaires comme le spool d'impression, task manager … et les **services de sécurité** associés ❼
- Certaines applications peuvent utiliser directement des **DLL Dynamic Link Library**… qui elles feront appel si nécessaire aux API système

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

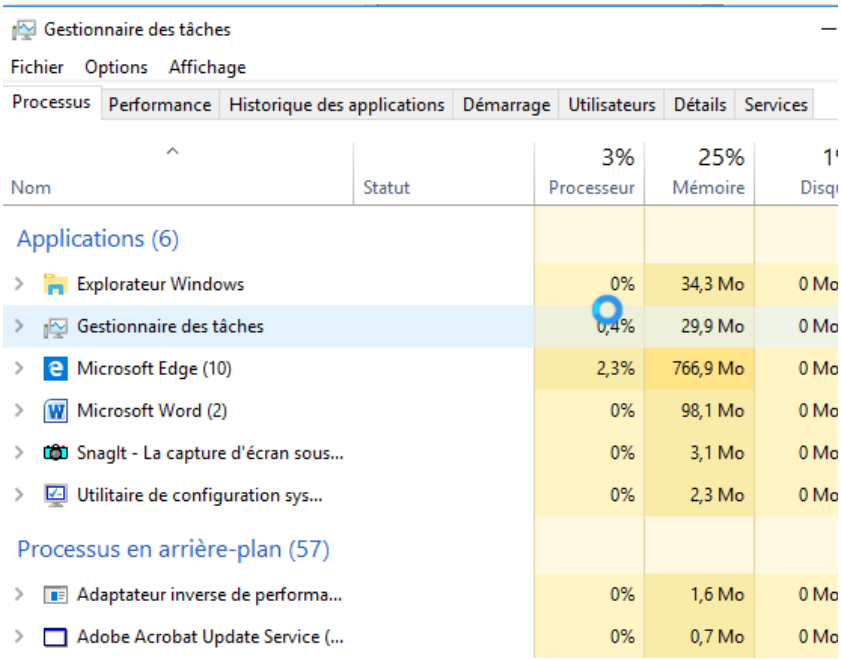
Lister les Processus – les Services :

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

Plusieurs onglets sont disponibles, l'onglet **Processus** regroupe

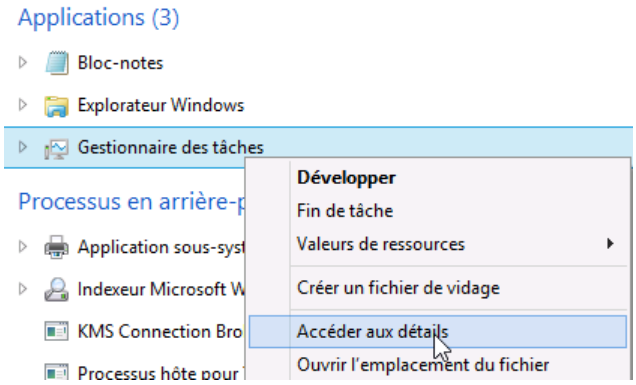
Des Application :

Programme lancé par l'utilisateur, ou lancé automatiquement au démarrage de Windows. Tourne dans une interface fenêtre, normalement sans incidence sur le fonctionnement de Windows

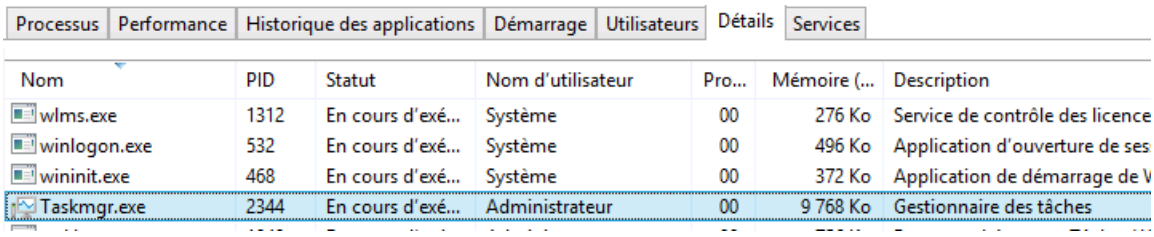


Des Processus :

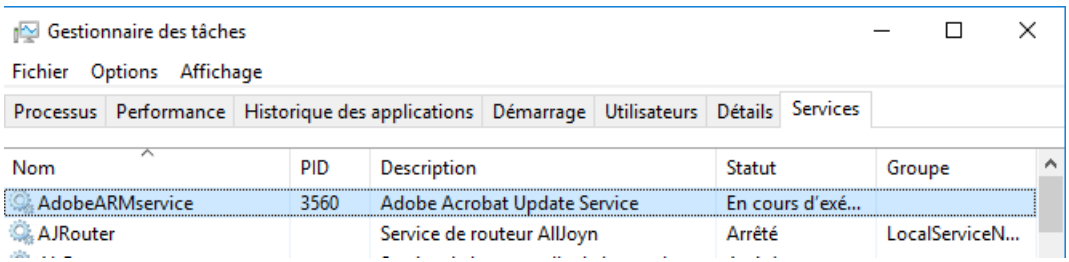
Correspond à des programmes vus par le système d'exploitation. Un processus est caractérisé par le fait qu'il a une indentification (**PID**) au niveau du système, des dépendances et une priorité d'exécution. Il peut contenir plusieurs services.



Depuis un processus on peut demander vie le menu contextuel **Accéder aux Détails** pour voir si un executable précis correspond, avec son **PID**

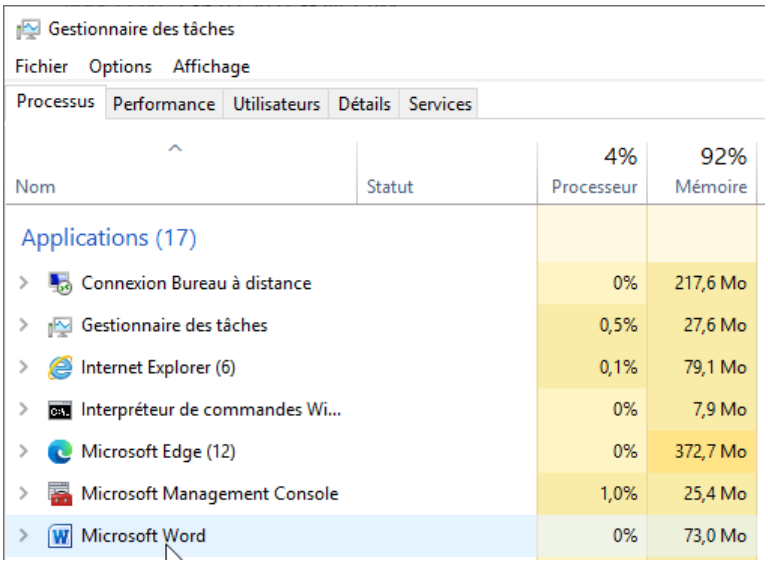


l'onglet **Services :** regroupe les programmes géré par le système d'exploitation comme "partie intégrante du système". Un service est caractérisé par le fait qu'il peut se gérer via le gestionnaire de service Windows, et est lancé dans un processus, (souvent associé avec d'autres services).

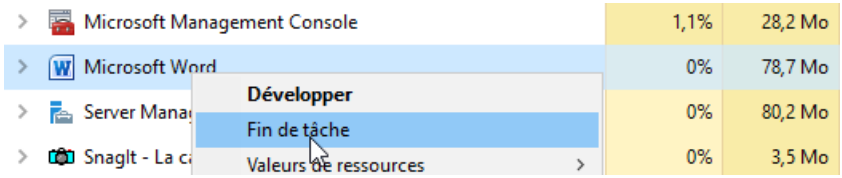


Arrêter Démarrer une Application, un Processus, un Service :

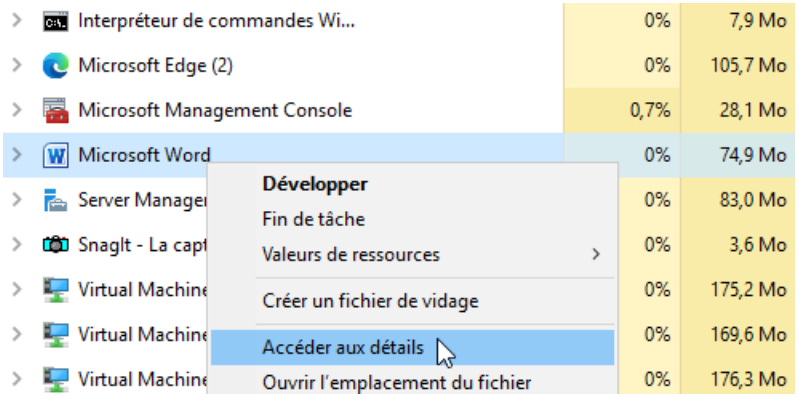
Dans le gestionnaire de tâches, on distingue Les **applications**, dont l'arrêt ne compromet pas le système, elles sont lancées en général par l'utilisateur



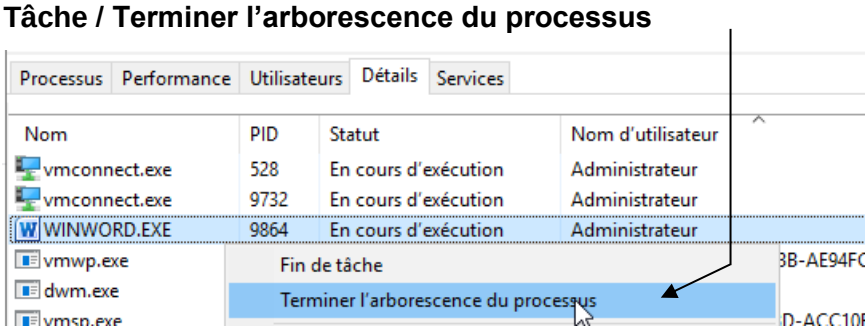
On peut demander **fin de tâche** directement depuis l'onglet **Processus**…



Si on demande d'afficher les détails via **Accéder aux détails**



Alors depuis cetonglet **Détails… c'est parfois plus efficace,** on pourra demander **Fin de Tâche / Terminer l'arborescence du processus**

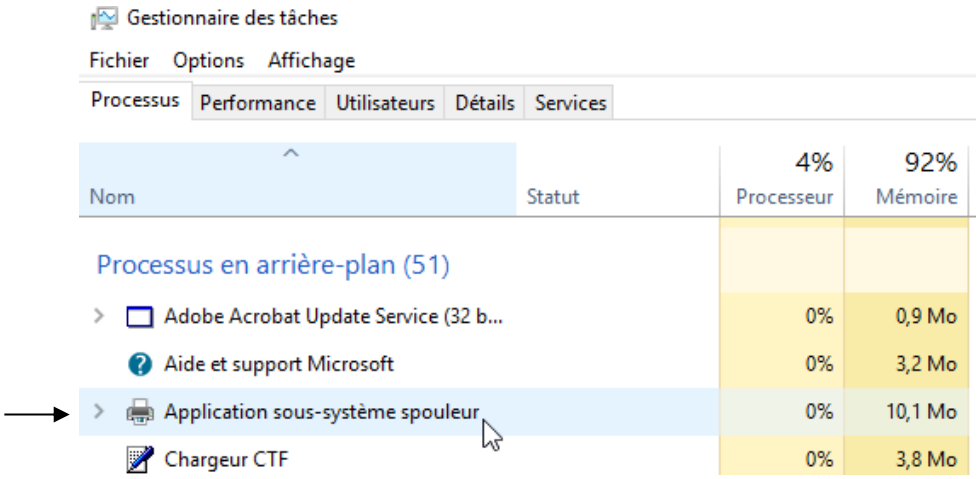


Depuis l'onglet **Détails**… on peut repérer un **PID**, il pourra être utilisé en ligne de commande (cf **taskkill** par exemple) pour forcer l'arrêt d'une application « recalcitrante »

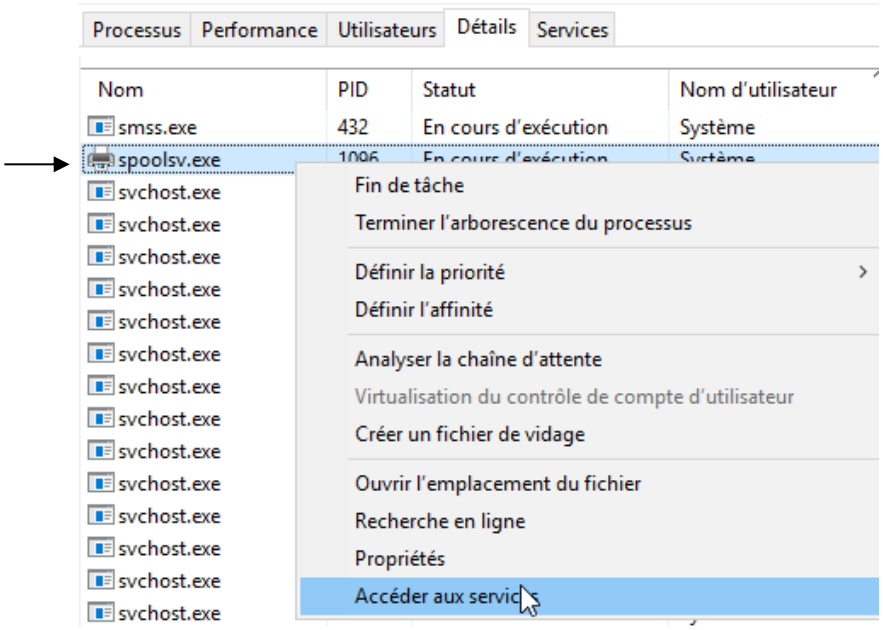
Arrêter Démarrer un Processus, un Service :

Dans le gestionnaire de tâches, on distingue Les **processus**, dont l'arrêt peut compromettre le système, elles sont lancées en général par le système lui-même ou les applications

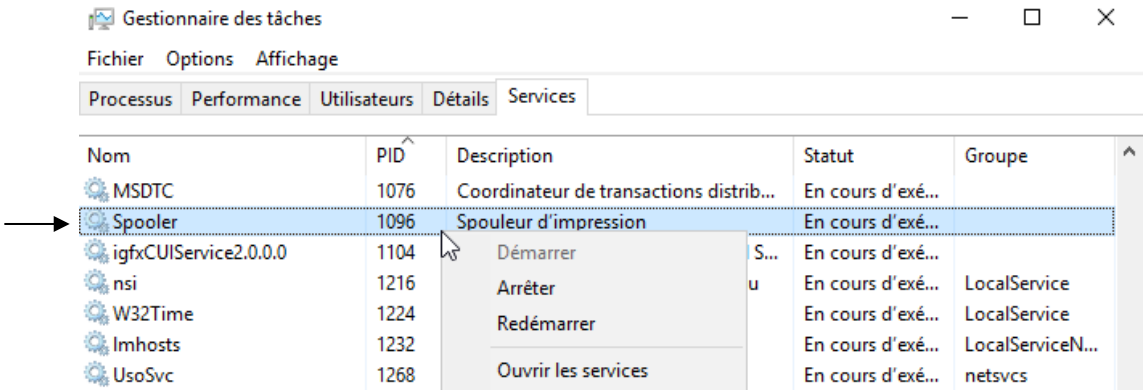
Exemple, le processus ***Application sous-système spouleur***



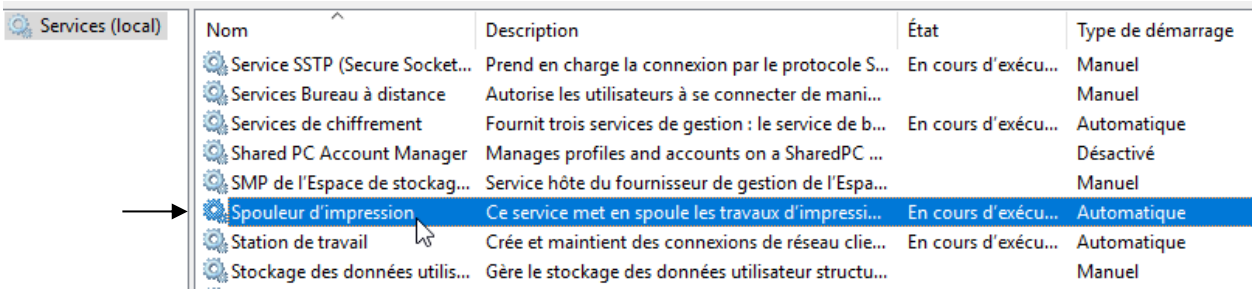
On peut demander également d'afficher les détails via **Accéder aux détails** et on voit que cela corresponds donc à l'executable ***Spoolsv.exe***



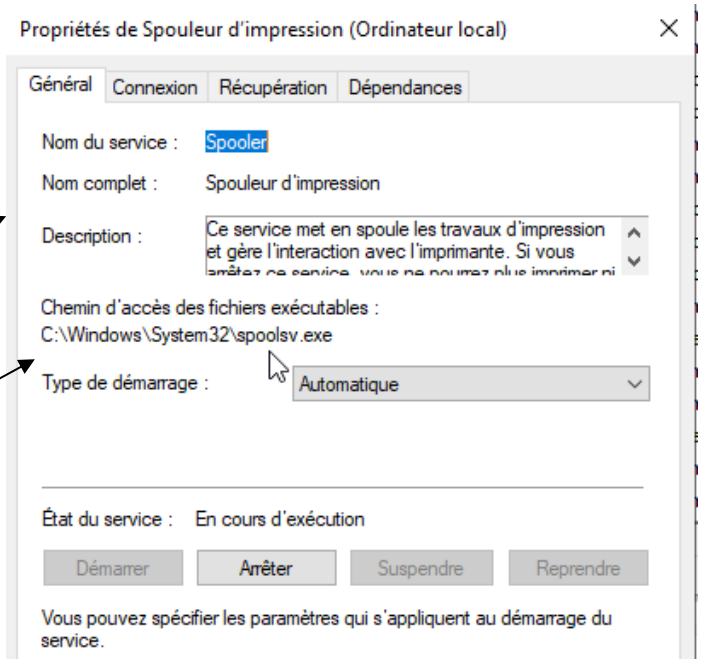
Si on veut **accéder aux services** (puisque c'est un **service**) alors une fois dans la console gestion des services (ouvris les services, par exemple)



Il va falloir comment il se nomme ! Ici **Spooler d'impression**



Et effectivement, lorsque l'on demande les propriétés de ce service, Windows nous indique bien que c'est le fichier spoolsv.exe qui en est à l'origine



Nom du service

Spooler

Nom complet

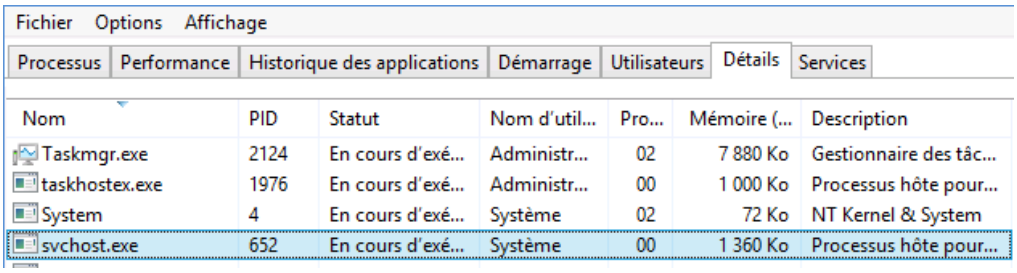
Spouleur d'impression

Nom Executable

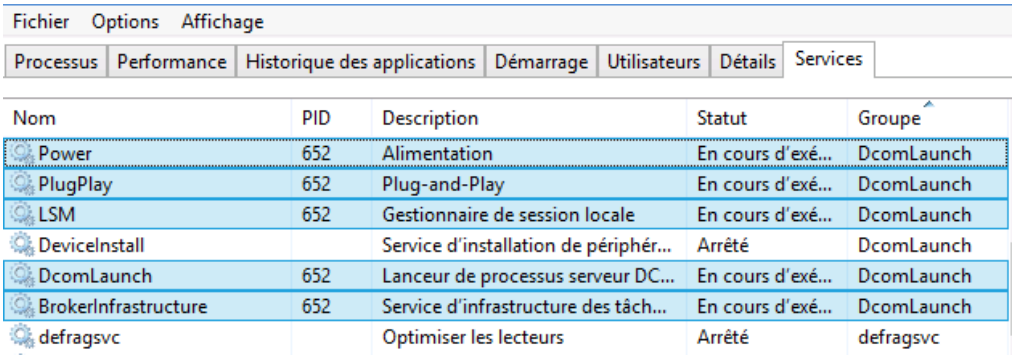
Spoolsv.exe

En résumé donc on a pas moins de 4 appellations différentes selon le niveau ou l'on se place dans le **gestionnaire de tâche**, ou le **gestionnaire de services** (si le **processus** correspond à un **service**):

Dans le **Gestionnaire des tâches**			Dans le **Gestionnaires des services**	
Onglet **Processus** (nom)	Onglet **Détail** (nom + Pid)	Onglet **Services** (nom service + Pid + Description)	Si Français (nom complet / nom long + Description)	Si US (nom complet / nom long + Description)
Application sous-système spouleur	**Spoolsv** + PID	**Spooler** + PID + Spouleur d'impression	**Spouleur d'impression** + « descriptif…. »	**Print Spooler** + « description... »

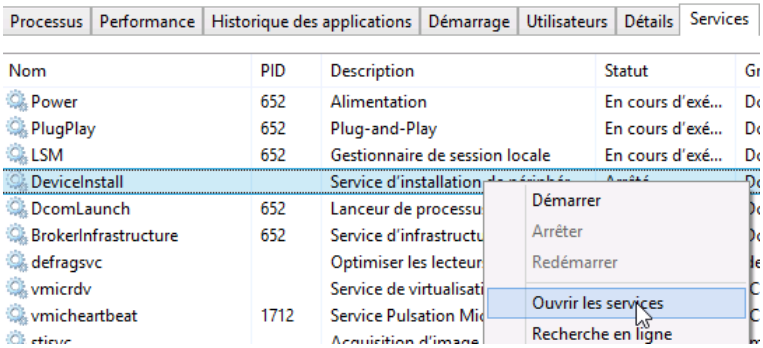


Ainsi souvent un processus générique **svchost** intègre comme son nom le laisse supposer plusieurs services – traçables avec le PID (dans l'example 652)



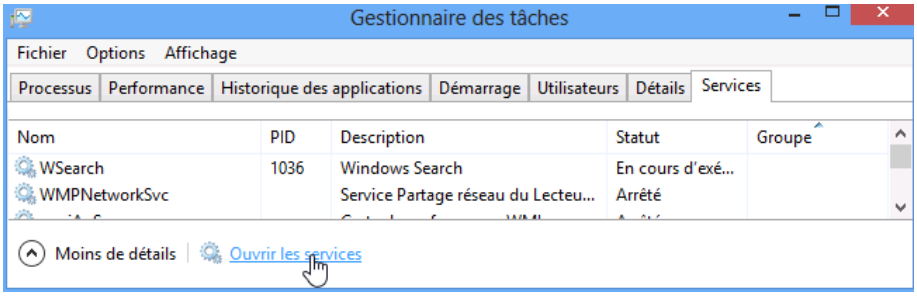
Dans l'onglet **Services** on peut

Arrêter/Démarrer/redémarrer un service: selon son état, Et accéder à la gestion des services **via Ouvrir les services…**



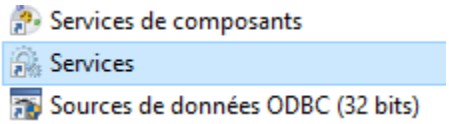
Gestionnaire de Services

Accessible via le **gestionnaire des tâches**, en bas on trouve **Ouvrir les services**



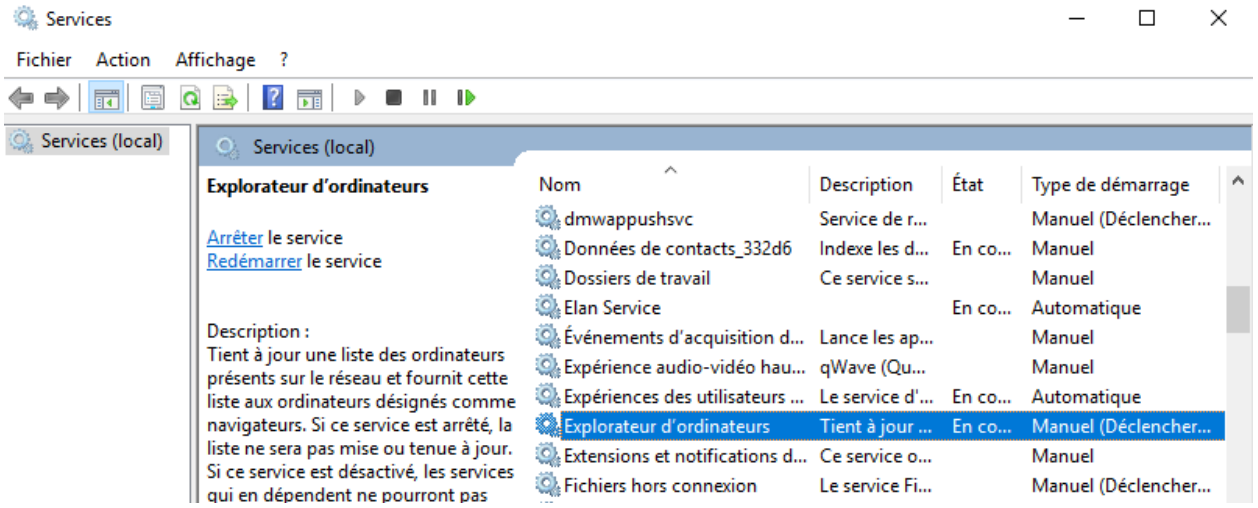
mais aussi via Clic droit – **Ce PC / Gérer / Services**

Ou **Panneau de configuration / Outils d'administration /**

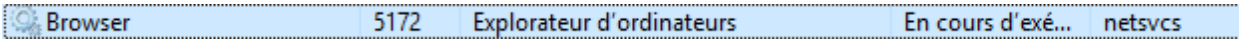


Ou en invite de commande **services.msc**

On obtient

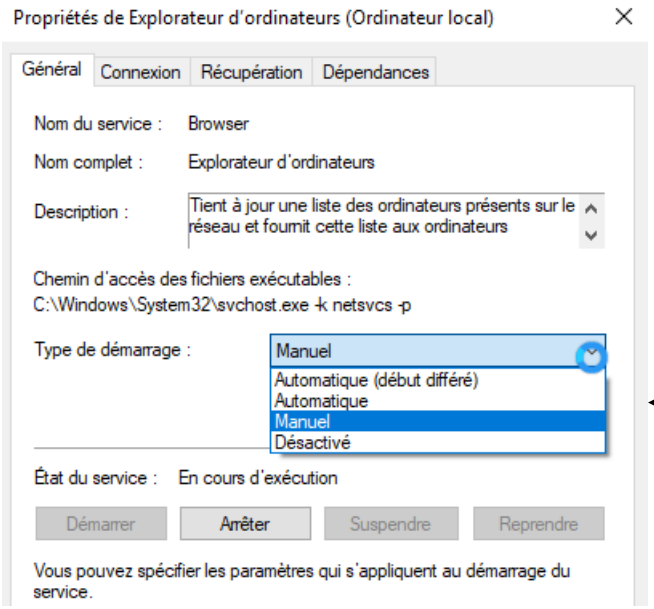


Pour un service ou une application particulière, on peut avoir son PID



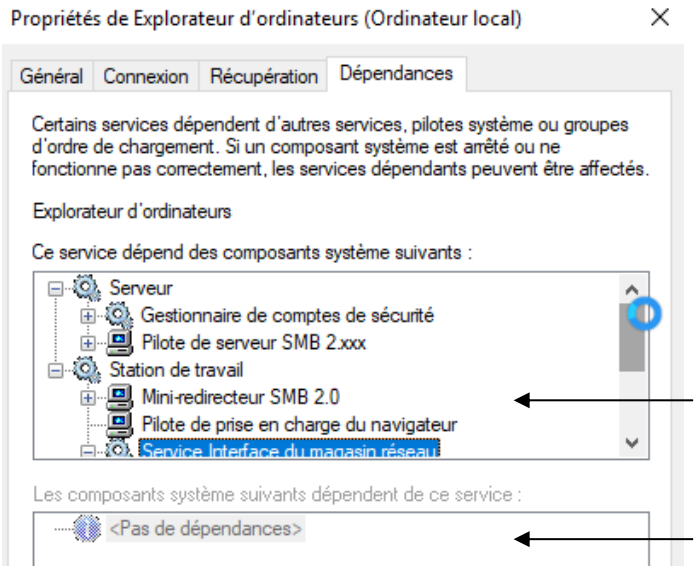
On à le nom de l'executable, le nom du service en francais, et en anglais…

on peut demander

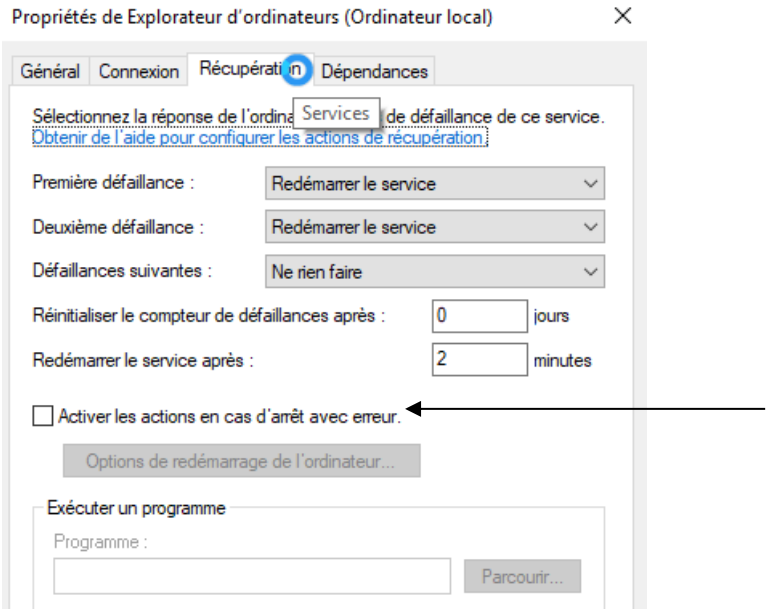


Essentiellement pour le prochain démarrage du poste

et on peut avoir une idée des dépendances…

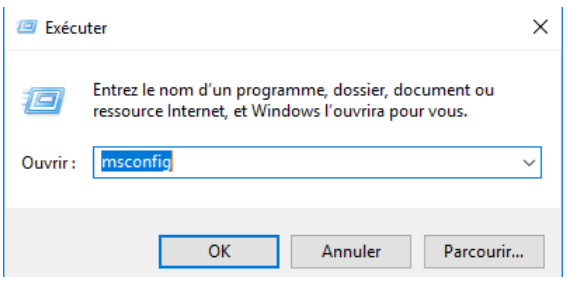


Que faire en cas de plantage



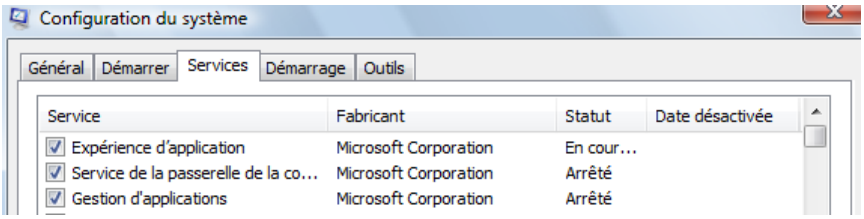
Msconfig.exe - gérer le lancement des services (temporairement):

Lançable en fenêtre d'execution par **msconfig**

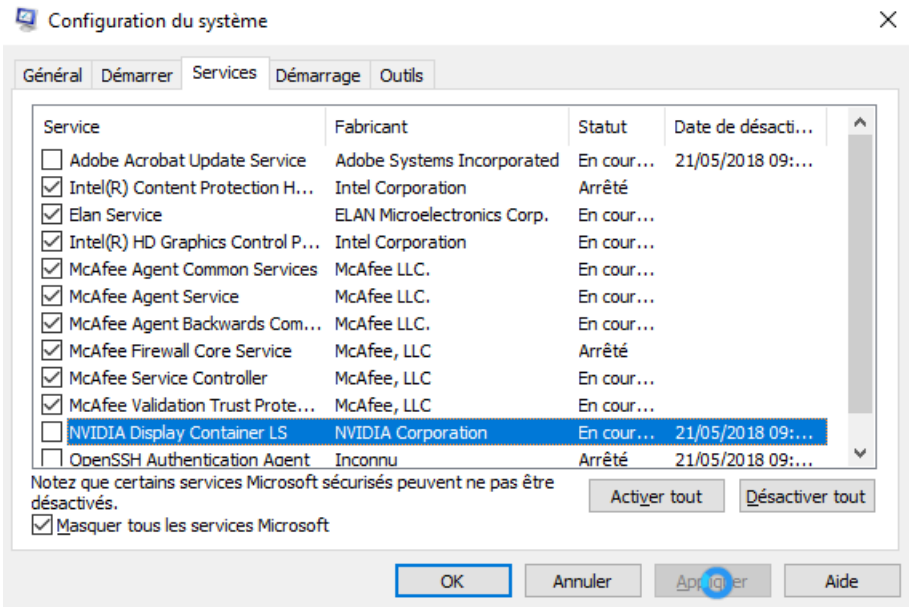


N.B : Les onglets 1-2-4 ne sont plus valables sous Windows10, on n'utilise **msconfig** maintenant uniquement avec l'onglet 3 pour choisir les **services à lancer au démarrage** :

On vient utiliser le 3°onglet **Services** :

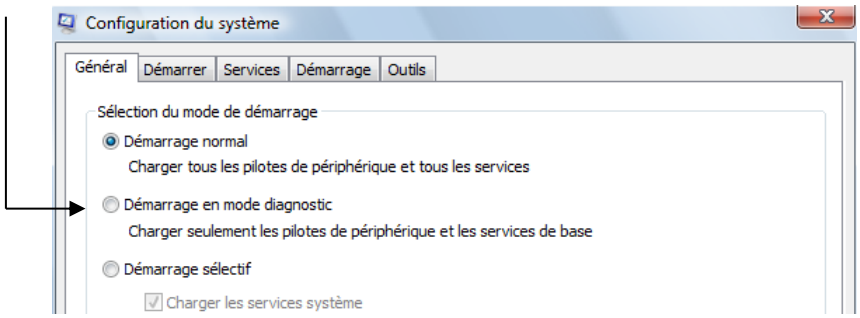


On peut demander de **Masquer services Microsoft**, et lorsque l'on décoche un service, marque pour info la date de désactivation… qui restera ainsi jusquà ce que l'on revienne annuler le changement.

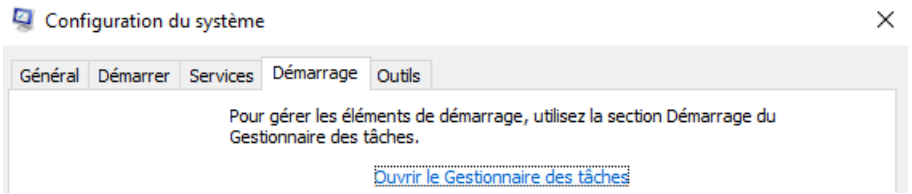


Par exemple le 1° onglet **Général** est remplacé par :

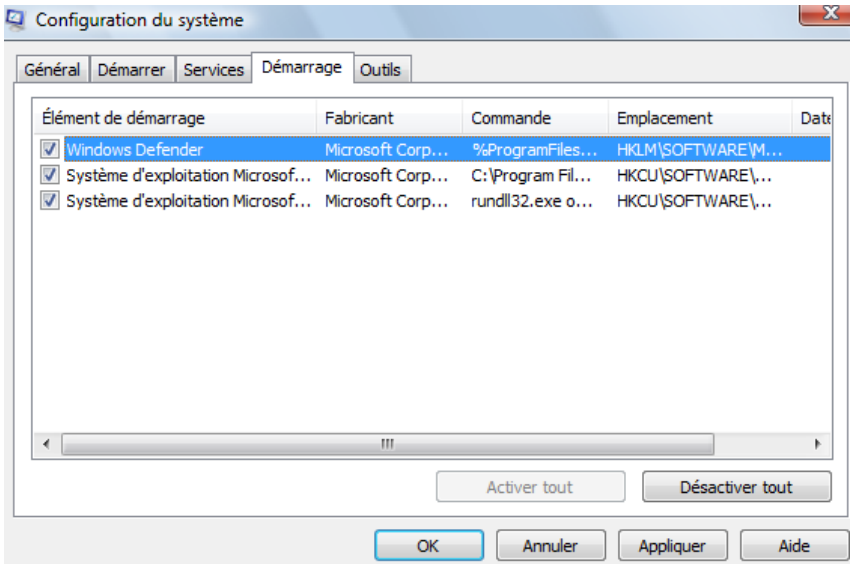
MAJ + Redémarrage Options avancées »sDiagnostic = Mode sans Echec (ex F8)



Le 4°onglet **Démarrage** de **msconfig** est remplacé par le **Gestionnaire de tâche**, dans lequel on a un onglet **Démarrage**:

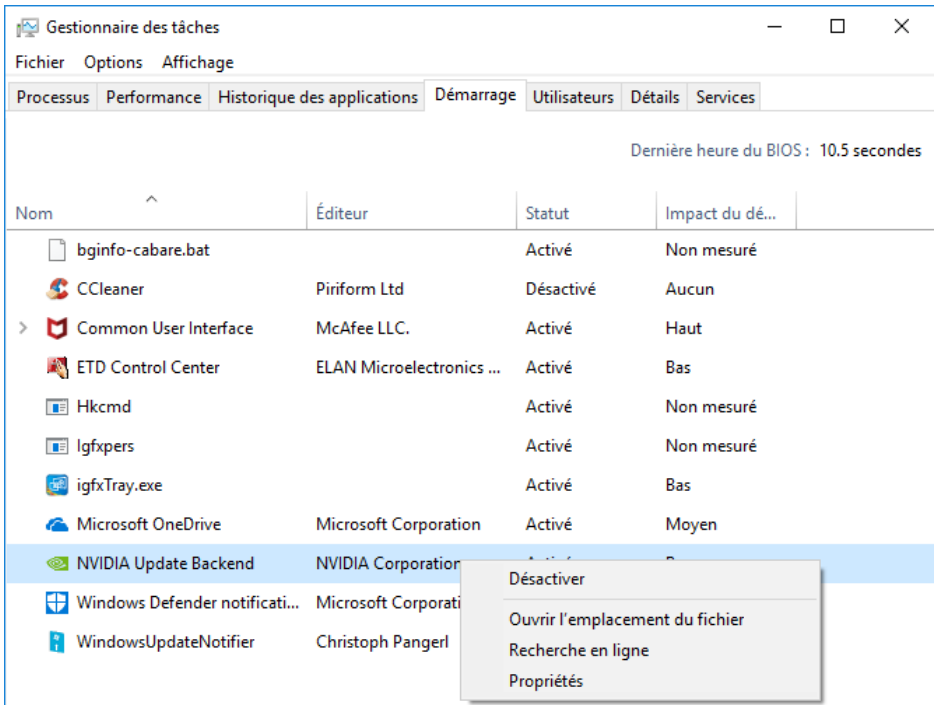


Démarrage



Gérer les programmes au Démarrage:

Appelable via **CTRL+ALT+SUPPR** ou via les propriétés de la barre des tâches, le **Gestionnaire des tâches** permet cela avec l'onglet **Démarrage**:



Rappel des emplacements utilisés

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runonce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

X:\ProgramData\Microsoft\Windows\Start Menu\Programmes\Démarrage

X:\User\%username%\AppData\RoamingMenu\Microsoft\Windows\ Start Menu \ Programmes\Démarrage

Tasklist (SEVEN - XP):

Cette commande porte pas mal de zone d'ombre…

Tasklist

```
C:\Documents and Settings\Administrateur>tasklist /?

TASKLIST [/S système [/U utilisateur [/P mot_de_passe]]]
         [/M [module] | /SVC | /V] [/FI filtre] [/FO format] [/NH]
```

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

Tasklist /SVC Tasklist /M

Taskkill (depuis SEVEN - XP):

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

Taskkill

```
C:\Documents and Settings\Administrateur>taskkill /?

TASKKILL [/S système] [/U utilisateur [/P mot_de_passe]]]
         { [/FI filtre] [/PID ID_processus | /IM image] } [/F] [/T]
```

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

Taskkill /PID x

avec

Taskkill /PID x /F

Et

Taskkill /PID x /F /T

```
C:\>taskkill /pid 940
Opération réussie : un signal de fin a été envoyé au processus de PID 940.

C:\>taskkill /pid 940 /f
Opération réussie : le processus avec PID 940 a été terminé.
```

Quelques Processus de base

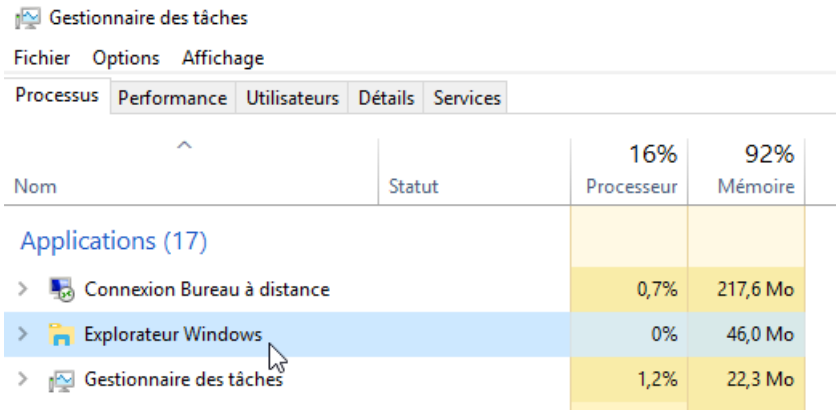
Depuis les premiers processus vitaux lancé par le système… on peut retrouver

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

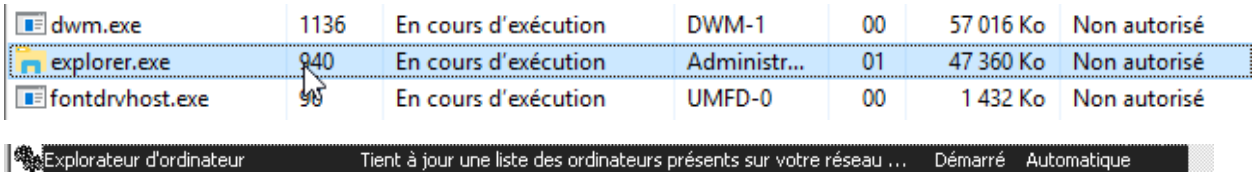
Listes les services - powershell

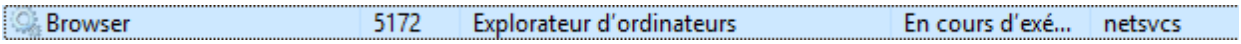
Quelques services avec leur nom français, anglais, et les noms des processus associés, en français. Pour un service particulier

Lister - Arreter les Processus (services, applications):



Correspond à





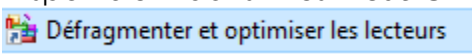
On à le nom de l'executable, le nom du service en francais, et en anglais…

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

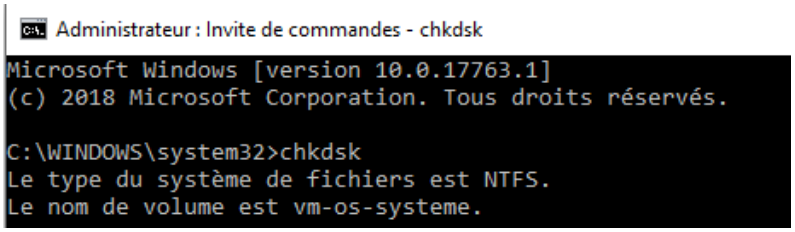
OUTILS GESTION DE DISQUE

Defragmentation chkdsk /F /R:

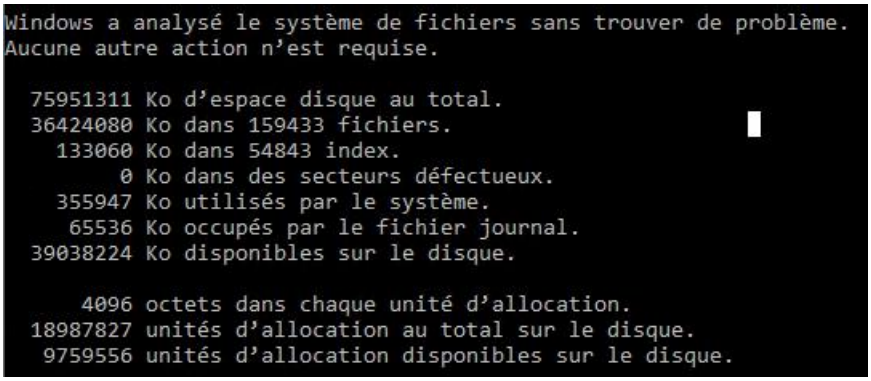
Disponible dans les **outils d'administration** en interface graphique,



Il est plus puissant et complet en invite de commande



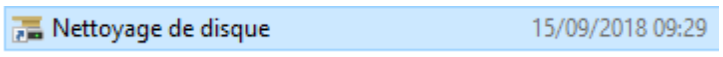
Les étapes peuvent prendre énormément de temps



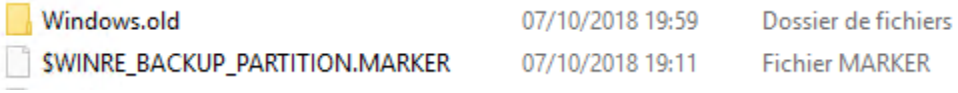
Les option **/F** et **/R** peuvent nécessiter un redémarrage de l'OS, (pour éviter un accès préemptif sur le lecteur) et nécessiter selon la taille du disque plusieurs heures

Nettoyage de disque:

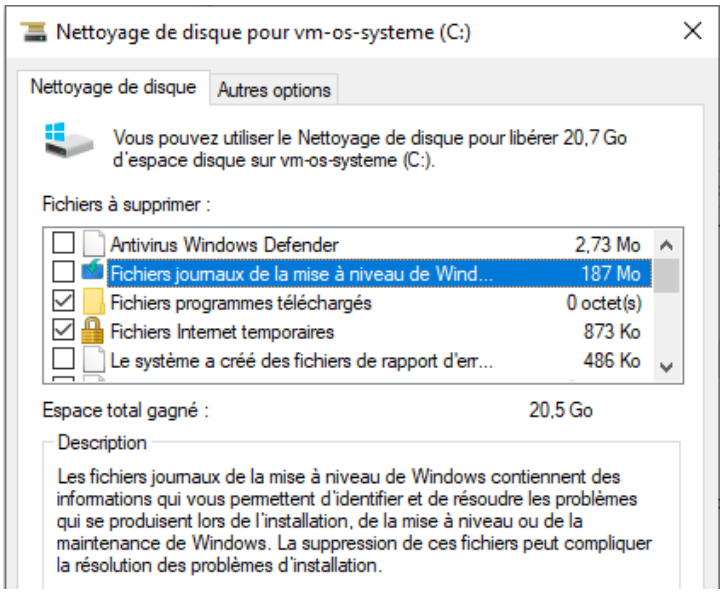
Disponible dans les **outils d'administration** en interface graphique,



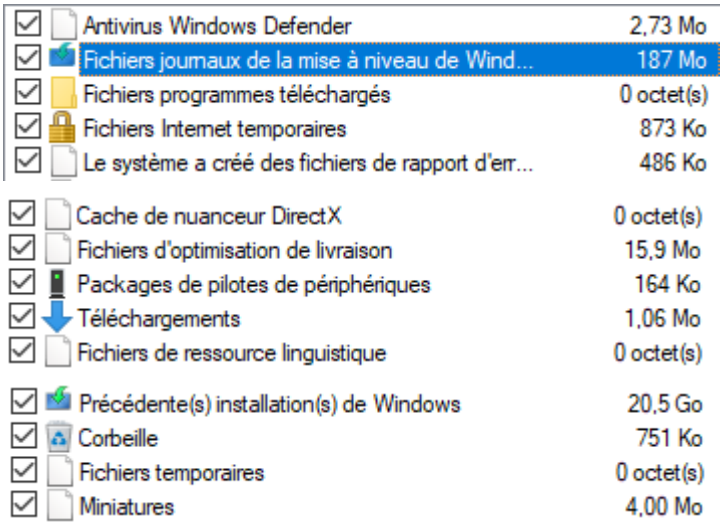
Dans une machine on peut souvent trouver des dossiers ou des fichiers et des partitions « bizarres »



Sans besoin de faire le détail,



on peut demander sur une machine stable de faire le ménage total !



les DLL (Dynamic Link Libraries) :

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

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

Des inconvénients existent :

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

Il est toujours difficile de connaître la liste des DLL nécessaires (ou plus nécessaires au bon fonctionnement d'un programme). On peut utiliser des utilitaires mais la tâche reste complexe. A cet effet, un gestionnaire d'installation, à partir de win98, travaille normalement à partir des fichiers **.msi** pour maintenir cette liste à jour. Mais les applications ne prévoient pas forcement une procédure correcte….

WRP Protection des DLL :

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

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

%systemroot%Winsxs

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

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

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

1. installation de Service Pack ou de correctifs à l'aide d'Update.exe ;
2. mises à niveau du système d'exploitation à l'aide de Winnt32.exe ;
3. Windows Update.

4. A travers une API spéciale

sfc - system file checker

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

```
C:\Users\Administrateur>sfc /help

Vérificateur de ressources Microsoft(R) Windows(R) version 6.0
Copyright (c) Microsoft Corporation. Tous droits réservés.

Analyse l'intégrité de tous les fichiers système protégés et remplace
les versions incorrectes par les versions Microsoft appropriées.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<fichier>]
    [/VERIFYFILE=<fichier>]
    [/OFFWINDIR=<répertoire Windows hors connexion>
     /OFFBOOTDIR=<répertoire Windows hors connexion>]

/SCANNOW        Analyse l'intégrité de tous les fichiers système
                protégés et répare les fichiers endommagés dès que
                possible.
/VERIFYONLY     Analyse l'intégrité de tous les fichiers système
                protégés. Aucune réparation n'est effectuée.
/SCANFILE       Analyse l'intégrité du fichier référencé et le répare
                si des problèmes ont été identifiés. Spécifiez le
                chemin d'accès complet dans <fichier>.
/VERIFYFILE     Vérifie l'intégrité du fichier ayant comme chemin
                complet <fichier>. Aucune réparation n'est effectuée.
/OFFBOOTDIR     Pour les réparations hors connexion, spécifier
                l'emplacement du répertoire de démarrage hors
                connexion.
/OFFWINDIR      Pour les réparations hors connexion, spécifier
                l'emplacement du répertoire Windows hors connexion.
```

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

UAC- USER ACCOUNT CONTROL

Objectif Visé :

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

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

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

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

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

IL – Integrity Level :

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

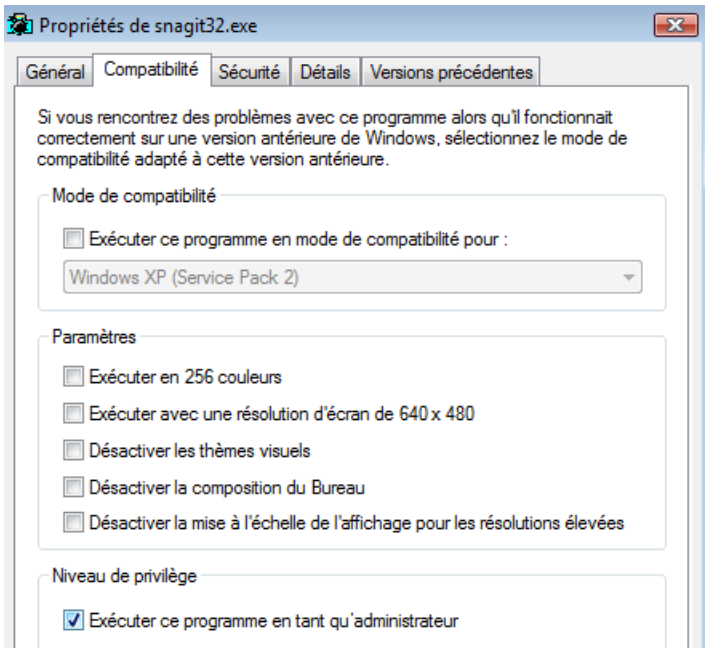
Avec Windows 8, lorsque vous ouvrez une session, **LSASS** va créer deux jetons. Un qui va contenir toutes les informations comme dans Windows XP et un autre jeton "restreint" qui ne contiendra que les privilèges d'un utilisateur standard.

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

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

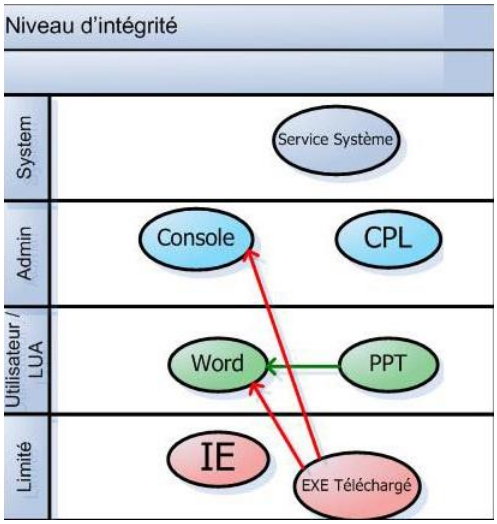
C'est donc ce deuxième jeton qui sera utilisé pour lancer les différentes applications. Pour utiliser le premier jeton, celui avec tous les privilèges, vous devrez passer par une élévation de privilège

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



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

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

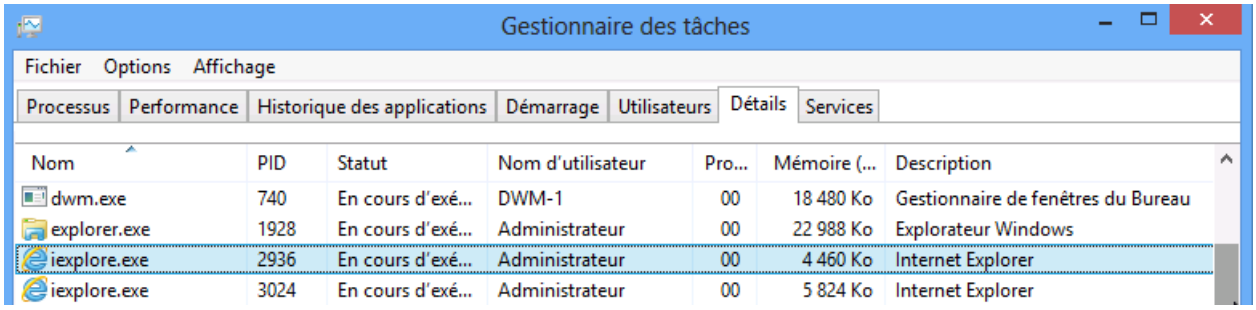


- Il faut savoir que les processus Utilisateur / LUA ne peuvent pas modifier les processus s'exécutant dans un niveau d'intégrité supérieur. (mais ils peuvent les lire pour obtenir des infos…)
- Le groupe des administrateurs à un **IL** élevé
- Pour un utilisateur, les processus qu'il lance et ses fichiers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

Dans cette optique pax exemple, lorsque l'on lance IE (par exemple) on lance en fait 2 processus, avec des niveaux IL différents…

Iexplorer : avec un **Il** d'utilisateur (pour stocker ses favoris…)

Iexplorer : avec un **Il** bas pour executer les activex et autres…



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

Gestion de l'UAC (panneau de configuration):

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

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

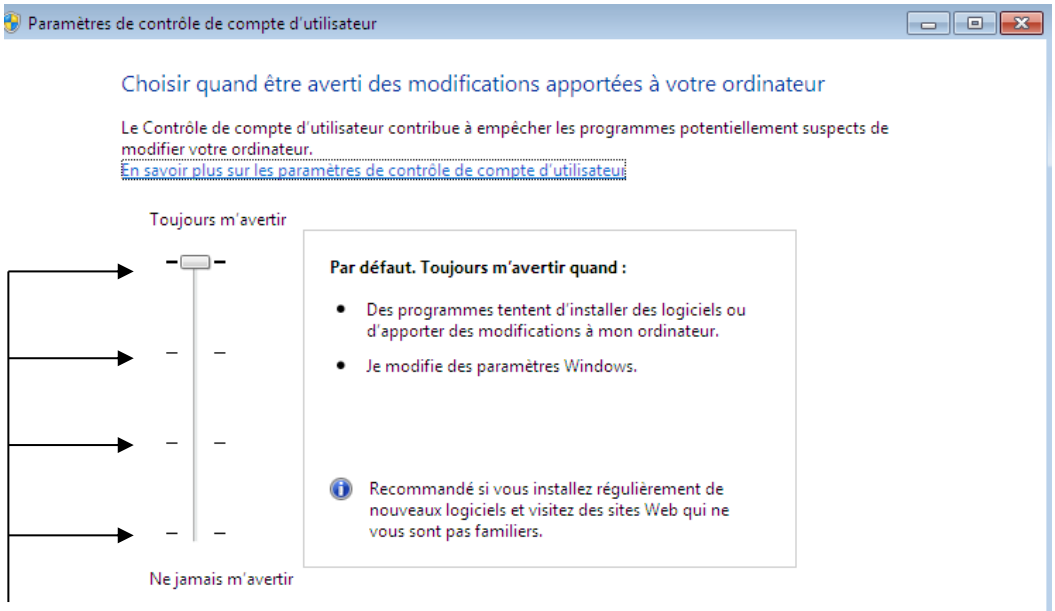
Bien que l'invite d'élévation soit la partie la plus visible du contrôle de compte d'utilisateur, celui-ci fournit également les composants sous-jacents comme :

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

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

Panneau de configuration / Comptes d'utilisateurs

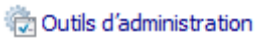
la commande **Modifier les paramètres de contrôle de compte d'utilisateur**

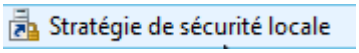


la prise en compte de cette commande peut demander un redémarrage.

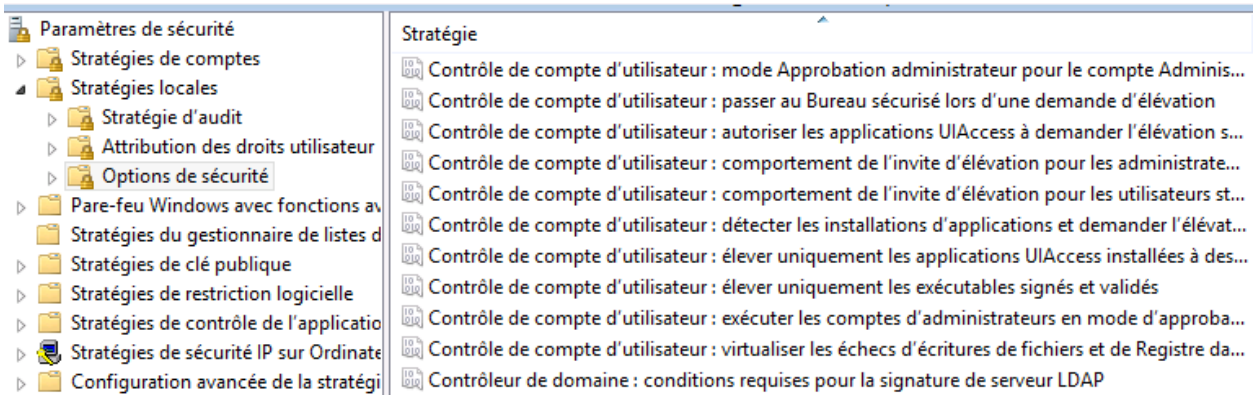
Gestion de l'UAC (stratégies locales):

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

Dans le **Panneau de Configuration / Outils d'administration /** 

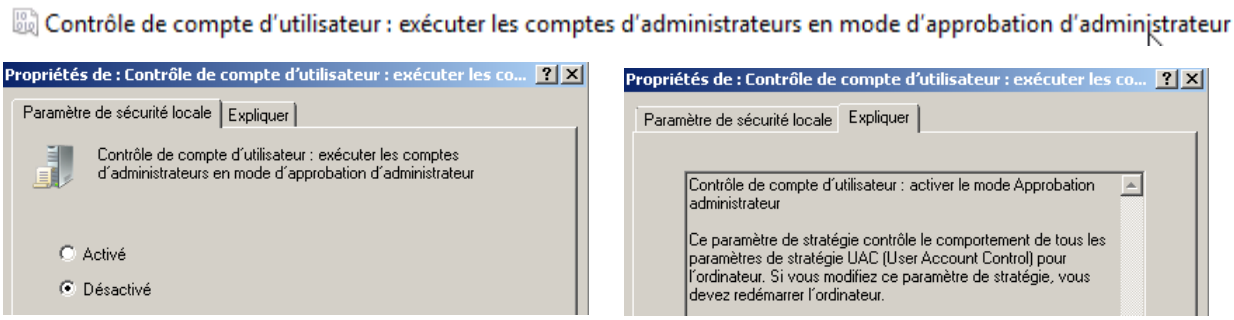
Puis **Stratégies de sécurité locales** 

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



Désactivation de l'UAC :

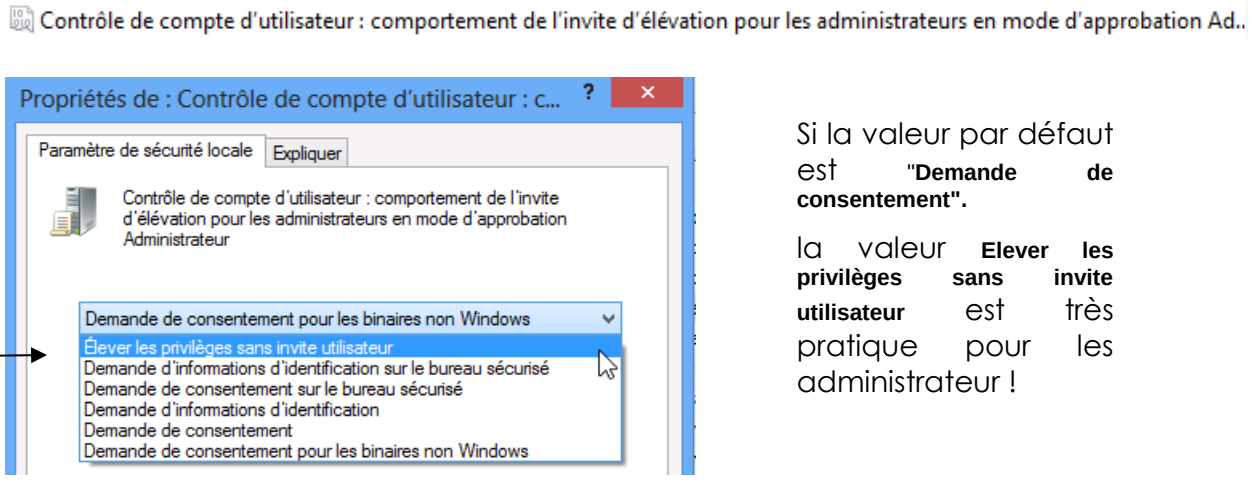
Sans doute le plus ... radical



N.B : re-démarrage du PC obligatoire

Désactivation de l'UAC pour les Administrateur :

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



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

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

Désactivation l'UAC pour les Utilisateurs :

Lorsque les logiciels anciens deviennent incompatibles

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

Activation l'UAC aussi pour le compte Administrateur Root :

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

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

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

DONC… il ne faut jamais utiliser en standard le compte Administrateur intégré pour travailler avec Windows 10, puisque un compte administrateur "autre" bénéficiera de l'effet protecteur de l'UAC sans occasionner de gêne (il suffit de demander une élévation de privilège silencieuse).

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

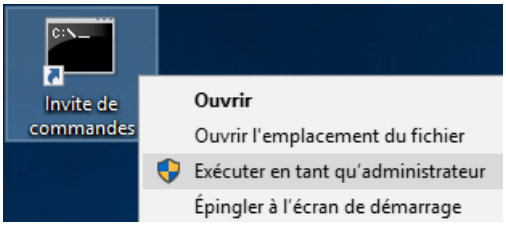
N.B : une modification des réglages de l'UAC nécessite le plus souvent un redémarrage du poste, voir la réouverture de session, pour être sûr de la prise en compte des nouveaux paramètres. Surtout celle qui active / désactive l'UAC.

Executer en mode administrateur:

Pour lancer une application / fenêtre en mode administrateur, (ce qui suppose que l'UAC soit activé) il est possible

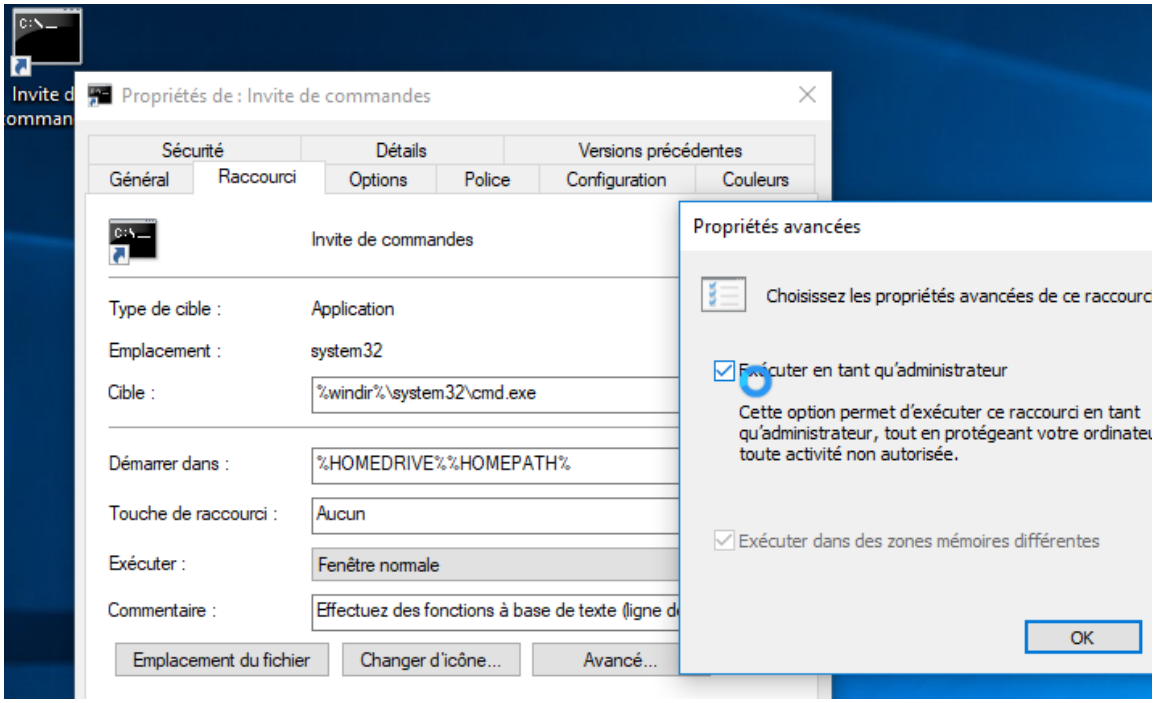
Depuis un raccourci

Si cela est possible demander **clic/droit Exécuter en tant qu'administrateur**



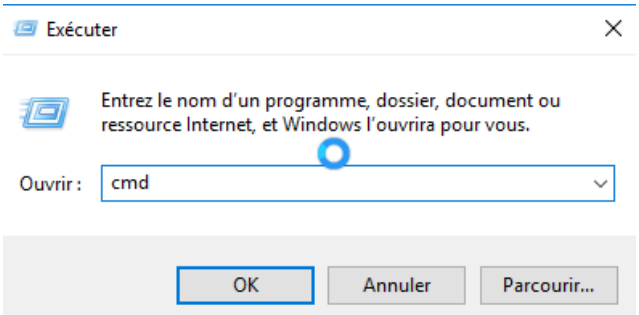
Si c'est possible on peut aussi paramétrer le raccourci pour qu'il mémorise le réglage de manière permanente.

Dans les **Propriétés** du raccourci, **Avancé**, on demande **Executer en tant qu'administrateur**



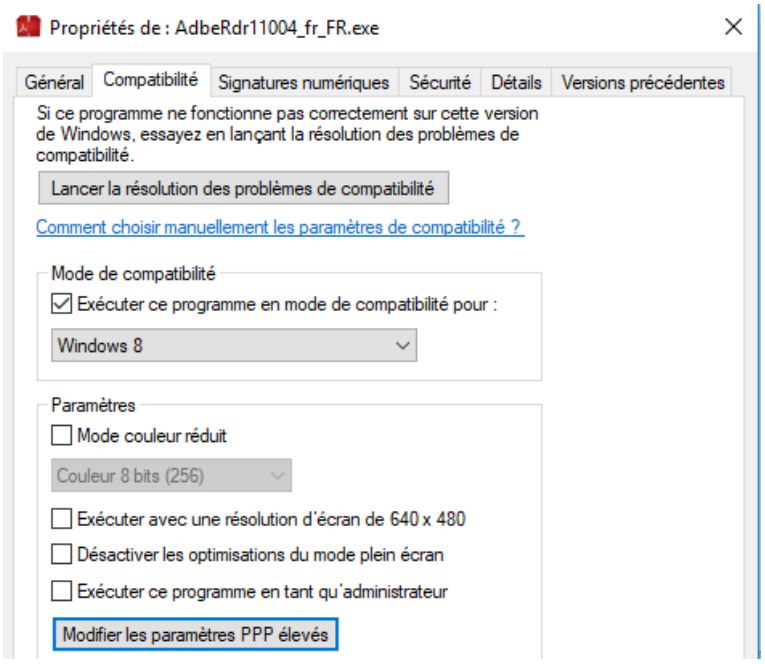
Depuis l'invite executer

Si cela est possible on valide par **CTRL+MAJ+Entrée** au lieu de **ok**



Depuis un executable

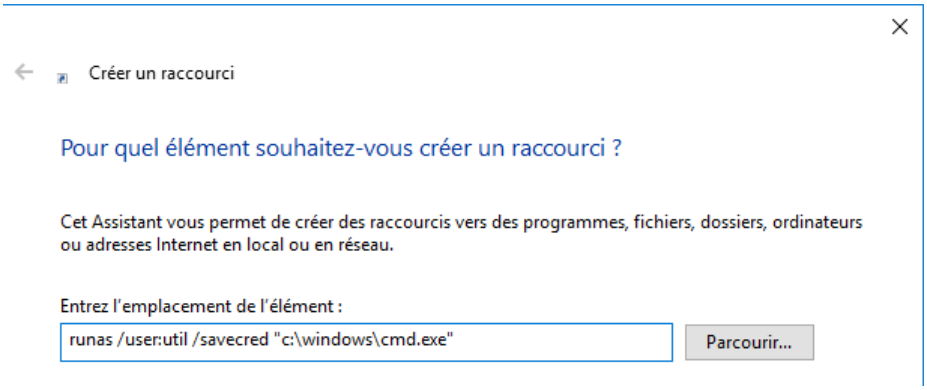
Si on pointe l'executable, par exemple 1 Acrobat reader, il faut aller dans l'onglet **compatibilité**



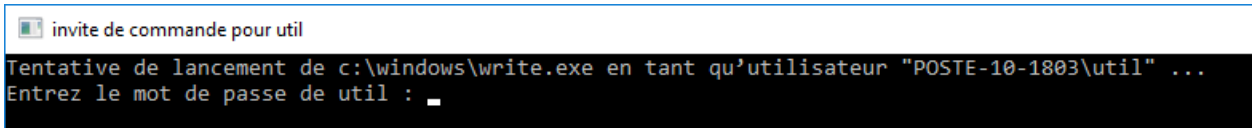
Runas changement de login (pas de gestion de l'UAC)

Si on pointe l'executable, par exemple **cmd.exe**

runas /user:util /savecred "c:\windows\system32\cmd.exe"

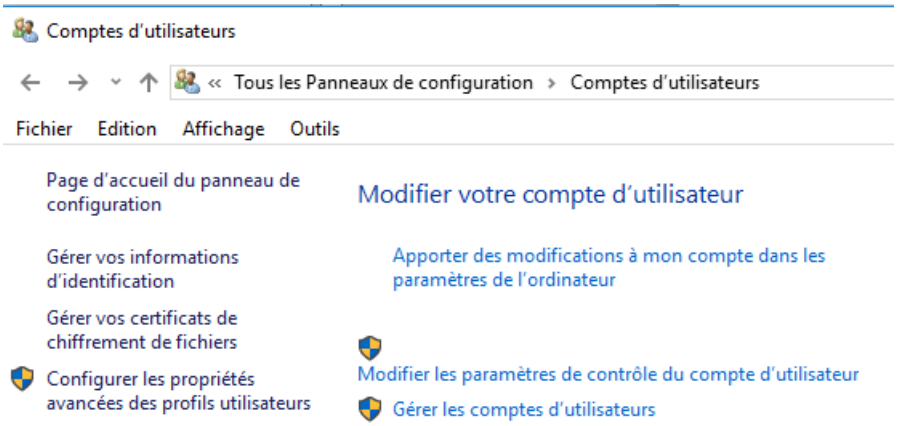


La première exécution donnera

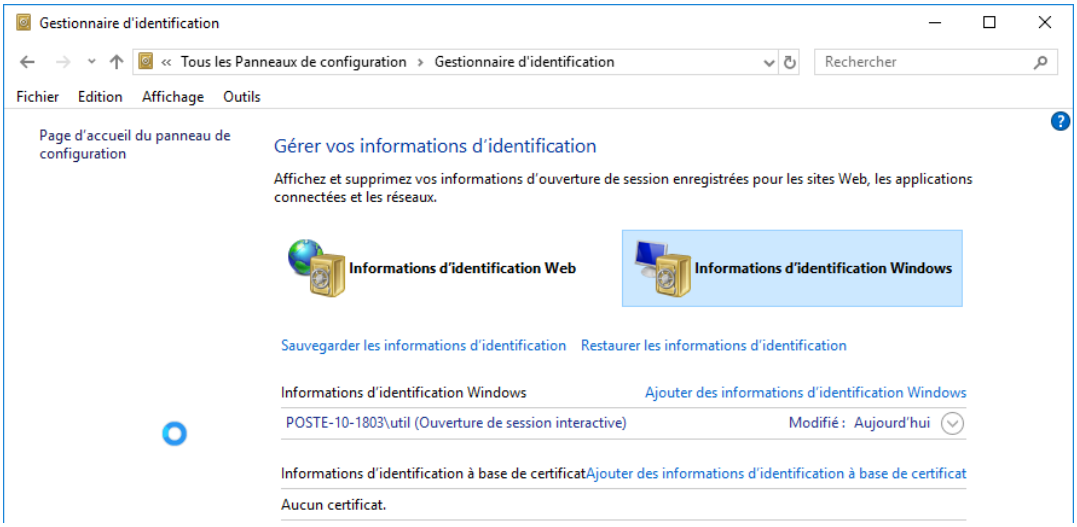


Mais ne redemanderas plus d'identification par la suite !

Les identifiants stockés via **RUNAS /savecred** peuvent être effacés via le **panneau de configuration/ comptes utilisateurs / Gérer vos informations d'identification**



Et on efface les **informations d'identification Windows**



INSTALLATIONS ET VIRTUALISATION

Préconisation microsoft :

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

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

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

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

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

Virtualisation des processus :

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

- Sous Windows XP, dans un environnement limité, vous lanciez l'installation jusqu'au moment où un fichier a besoin d'être écrit dans un espace protégé Cette opération va faire "crasher" l'installation rendant le logiciel à moitié installé et donc inutilisable
- Windows 10 déroule toute l'installation pour savoir si il a besoin d'aller écrire dans les dossiers système ou des parties réservées du registre. Si c'est le cas, et que l'installateur n'a pas les autorisations suffisantes, alors un système de dossiers virtuels est mis en place.

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

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

Lors du lancement de l'application, celle-ci ira dans un premier temps regarder dans le dossier virtuel du profil, et si elle ne trouve rien, elle chargera les

paramètres dans le Program Files réel. Grâce à ce système, près de 90% des applications non réécrites pour Windows 10 allant écrire dans **Program Files** ou dans des dossiers systèmes fonctionnent. On parle de « **programmes hérités** »

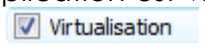
Windows 10 traite un processus comme « virtualisable » si :

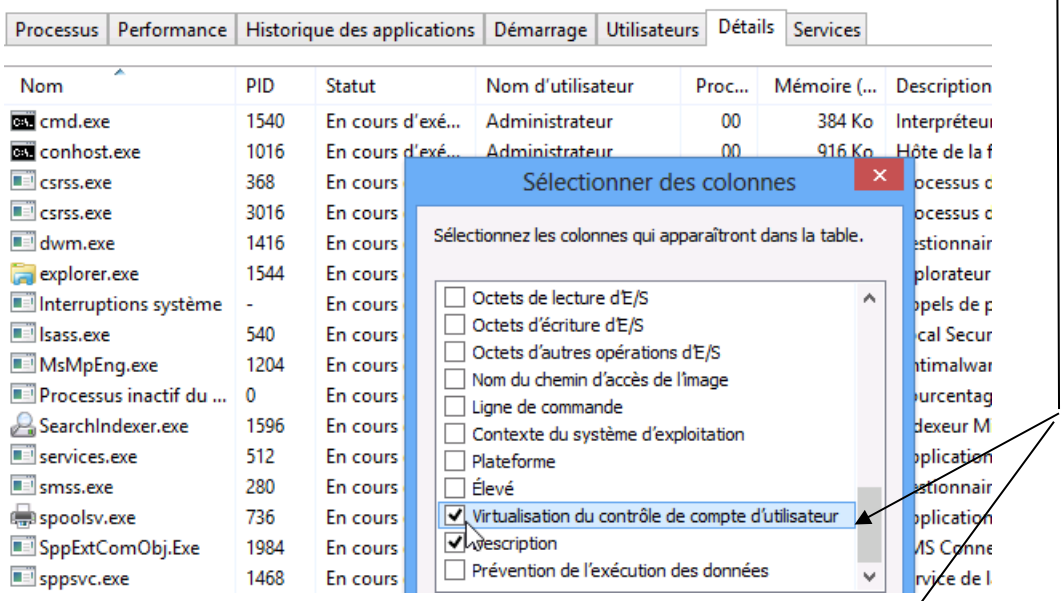
- il fait 32 bits (et non 64 bits),
- il ne s'exécute pas avec les droits administratifs,
- il n'a pas un fichier de signature spécifique pour Windows 10

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

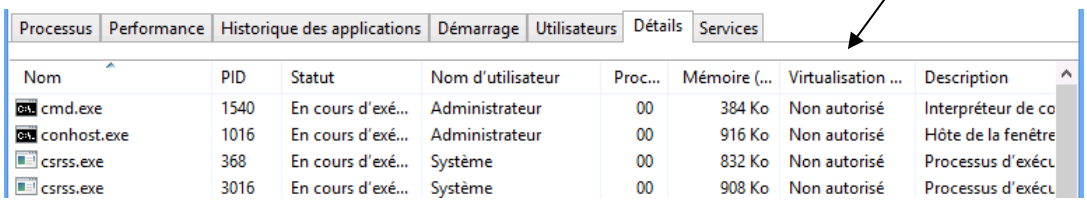
- **%ProgramFiles%**
- **%ProgramData%**
- **%SystemRoot%**

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

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



donnant

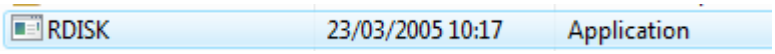


N.B : Comme les informations sont stockées dans le répertoire utilisateur, cela peut être gênant. Par exemple, pour une application qui stocke les meilleurs scores : l'utilisateur fera toujours le meilleur score !

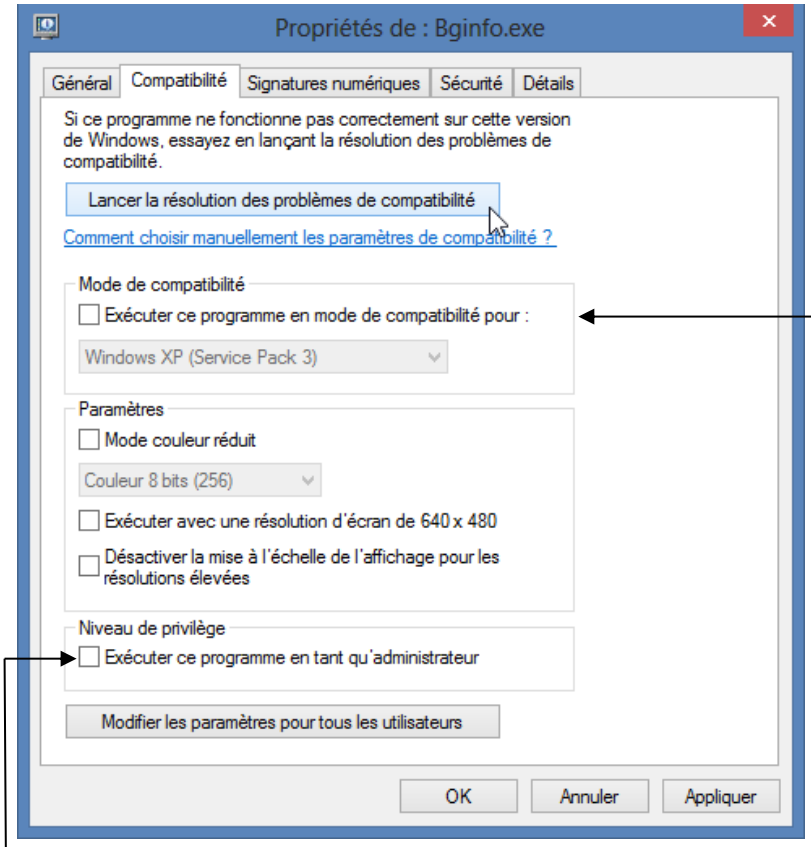
COMPATIBILITE AVANT WINDOWS 10

Exécuter en mode compatibilité:

Si un programme fonctionnait correctement sur une version antérieure à Windows 10, et que vous ne disposez pas de la version spécifique, on peut tenter de demander de l'exécuter en mode compatibilité. Par exemple

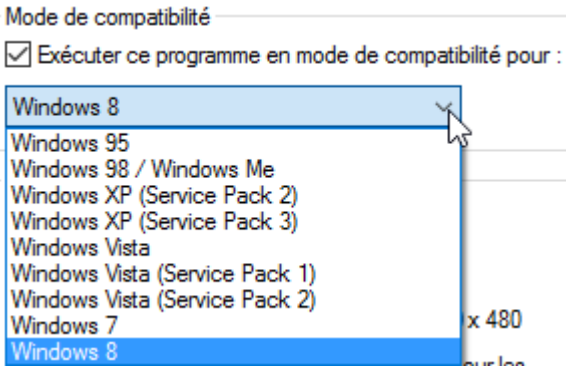


On demande clic-droit sur l'exécutable, **propriétés** onglet **Compatibilité**



On peut spécifier

- si il y a besoin d'exécuter avec un privilège d'administrateur
- On peut choisir un mode de compatibilité



Séquence possible:

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

Il se peut qu'il faille désactiver l'UAC

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

PROTECTION DEP

Principe DEP Data Execution Prevention:

Il s'agit d'une technologie développée par AMD, connue sous l'appellation **NX** (No eXecute), liée aux adressages **PAE**. (Physical Address Extension)) censée empêcher le "dépassement de mémoire tampon" (*buffer overflow*. L'objectif est donc de marquer comme non exécutable des emplacements mémoire non occupés par une application, pour éviter que des vers s'auto-répliquent dans le système. Dans XP (Sp2 mini), la fonction qui implémente NX etait baptisée **DEP**, pour **Data Execution Prevention**

Désactivation Complète de DEP :

La fonctionnalité DEP, permettant de sécuriser Windows 10 contre les virus, peut être responsable de crashs intempestifs sur votre système

bcdedit.exe /set {current} nx AlwaysOff Puis re démarrage

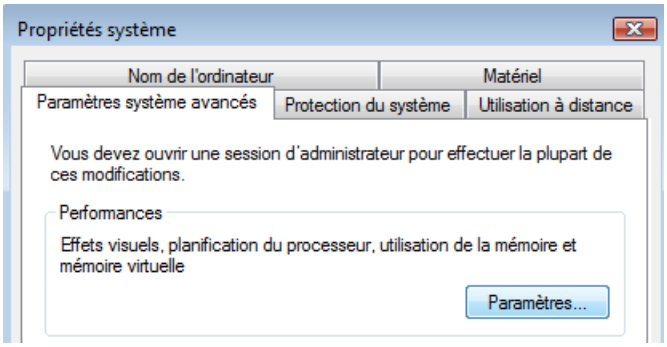
La réactivation de la protection se fait par

bcdedit.exe /set {current} nx Option (et re démarrage)

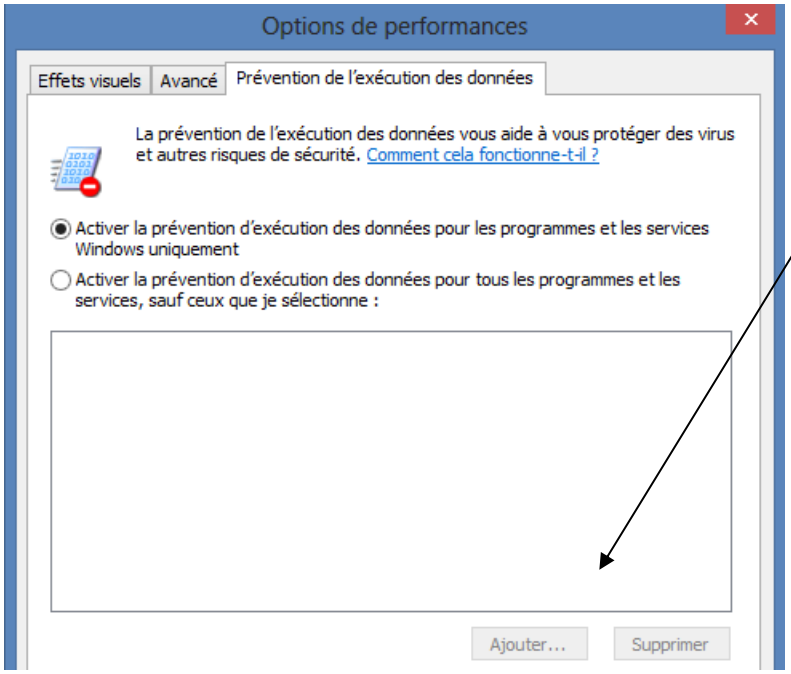
Désactivation pour une application de DEP :

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

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



onglet "**prévention de l'exécution des données**".

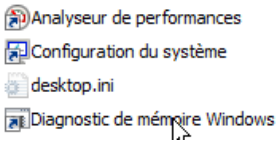


il est alors possible d'insérer dans la liste présentée les programmes ne devant pas avoir recours à la fonction DEP.

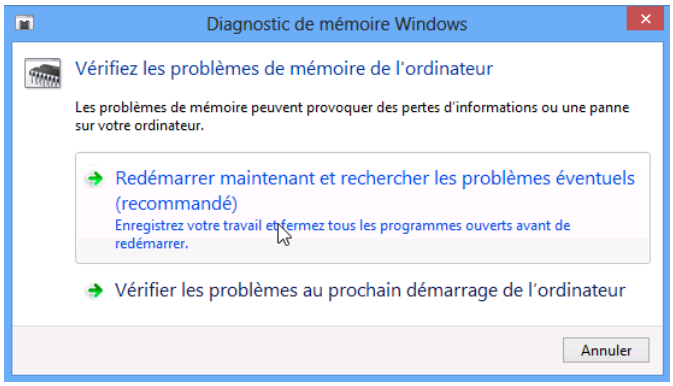
TEST MEMOIRE

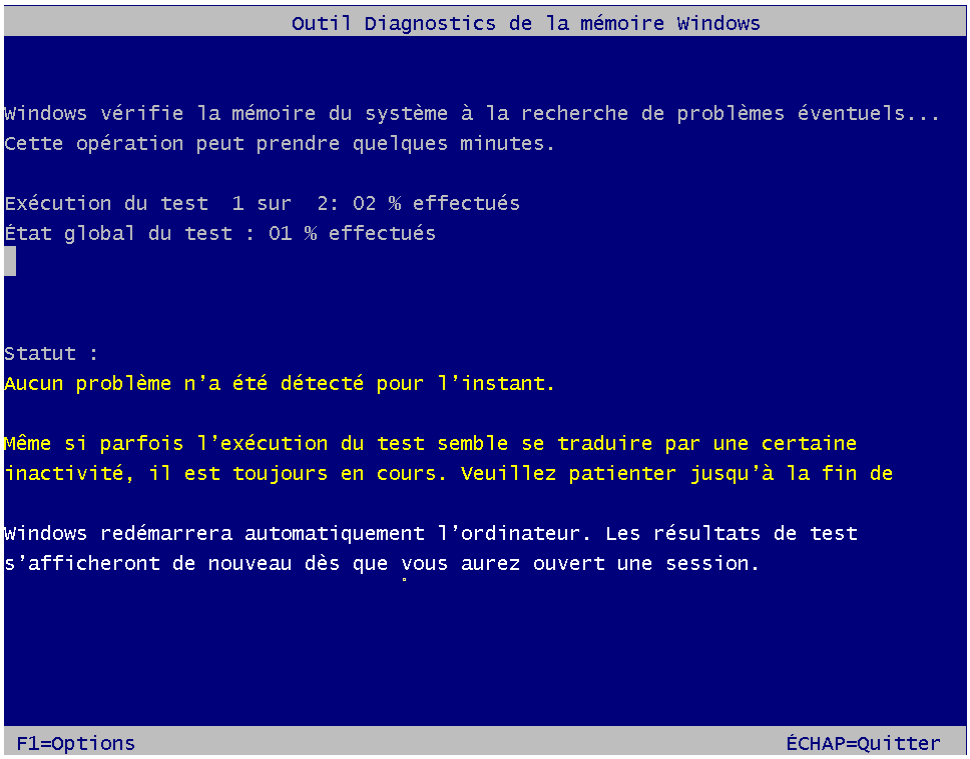
Depuis Windows 10

Via le menu **panneau de Configuration / Outils d'administration**



On demande **Diagnostic de mémoire Windows**





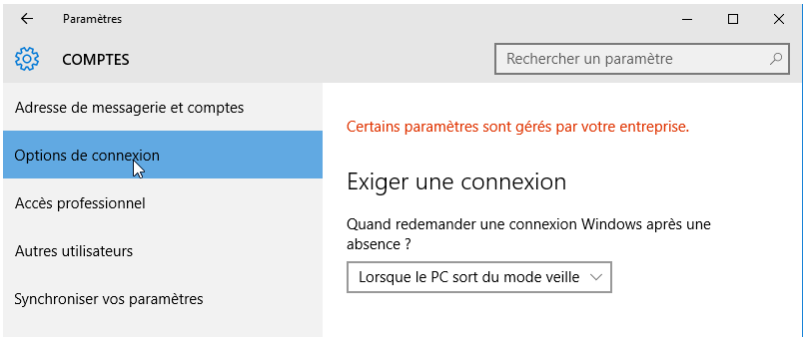
F1 permet d'executer des tests plus complets…

Correspondant à l'outil **mdsched.exe**

AUTHENTIFICATION WINDOWS 10

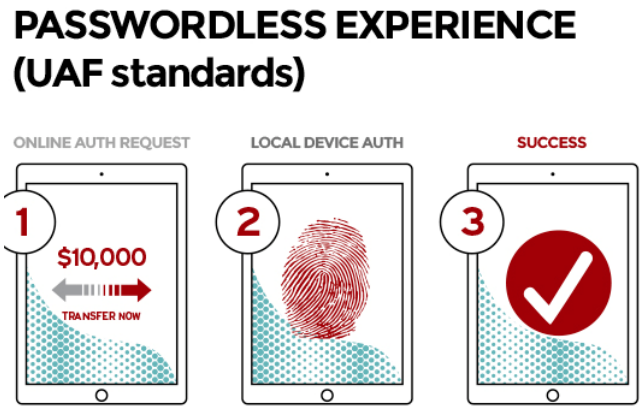
Plusieurs Mode possibles UAF - U2F:

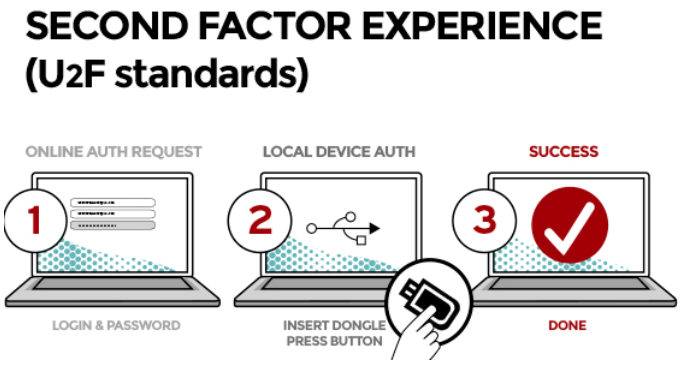
Le choix peut se faire via **Paramètres**, **Comptes** et **Options de Connexion**



- Par code PIN (4 chiffre)
- Par image (tracé sur une surface tactile)
- Par Biométrie
- Par double authentification

Microsoft, faisant partie de l'alliance FIDO définissant 2 types d'authentification . On n'y est pas encore en standard, mais c'est possible

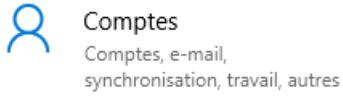


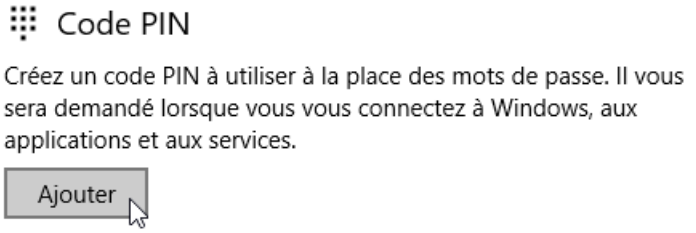


Par Code PIN :

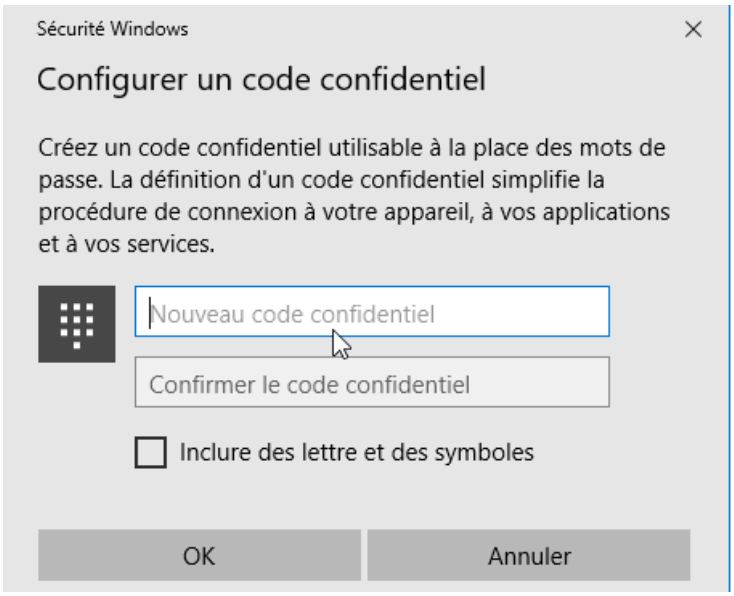
A n'utiliser que sur des tablettes et non sur des postes, mais pas systématiquement. Il est associé au périphérique sur lequel on se trouve ! (U2F)

Dans **Paramètres**, et **Comptes** on trouve **Options de connexion** on cherche **Code PIN**

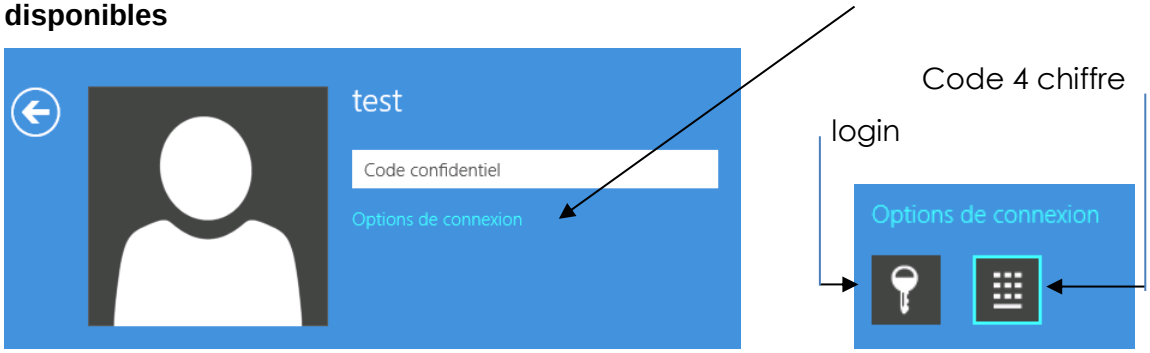




Le **code confidentiel** (ex **Code PIN** windows) doit avoir 4 caractères minimum.



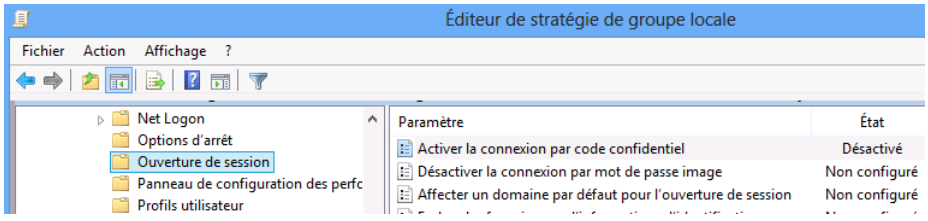
Lorsque l'utilisateur va ouvrir une session, il verra des **options de connexion disponibles**



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

C'est **Activer la connexion par code confidentiel** dans

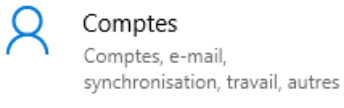
Configuration Ordinateur\Modèles d'administration\ Système\Ouverture de session



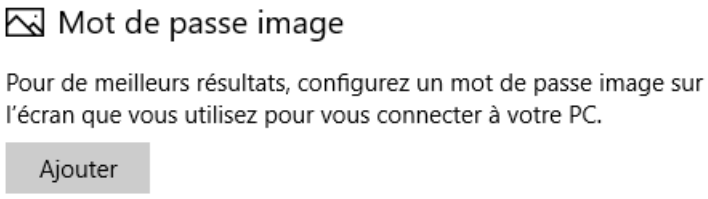
Par Tracé sur une image :

On mémorise une action à effectuer sur une image !

C'est peu sécurisé, à n'utiliser que sur des tablettes (écran tactile) ! Valable pour un compte Microsoft / et ou un compte local.

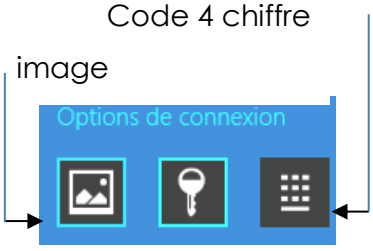


Dans **Paramètres**, et **Comptes** on trouve **Options de connexion** on cherche **Mot de passe Image**



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

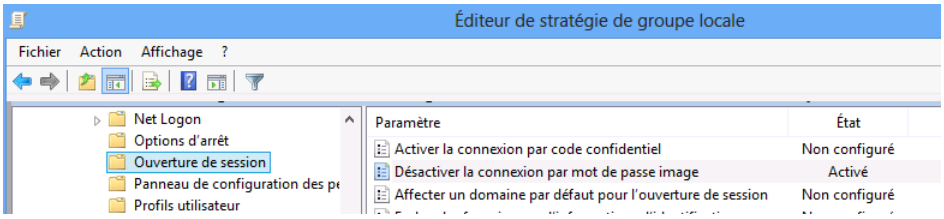
Lorsque Test va ouvrir une session, il verra des options de connexion disponibles



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

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

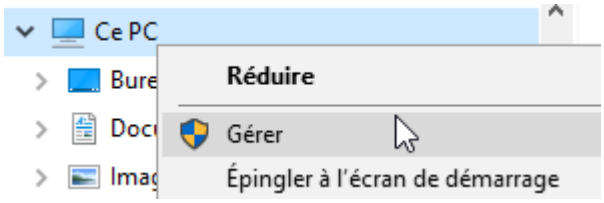
Configuration Ordinateur\Modèles d'administration\ Système\Composants Windows\ Ouverture de session

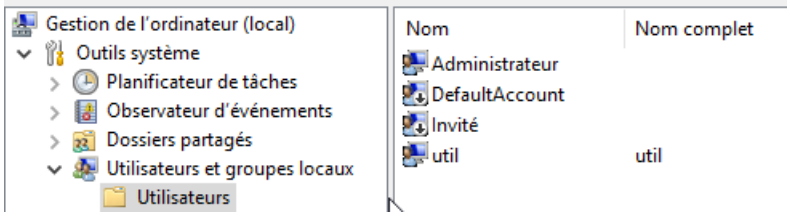


Login sur SAM ou AD :

Login Classique soit local (dans la Sam)

Il est mieux de passer par gestion des utilisateurs pour les comptes locaux





Créer un Compte Microsoft (couplé à un compte local) :

Grâce à son compte Microsoft, tel qu'un compte de messagerie Hotmail, l'utilisateur va ouvrir une session et retrouver ses propres paramètres et applications, ainsi que ses documents, depuis n'importe quel ordinateur pourvu de Windows 10. Ce service est basé sur le Cloud Computing …

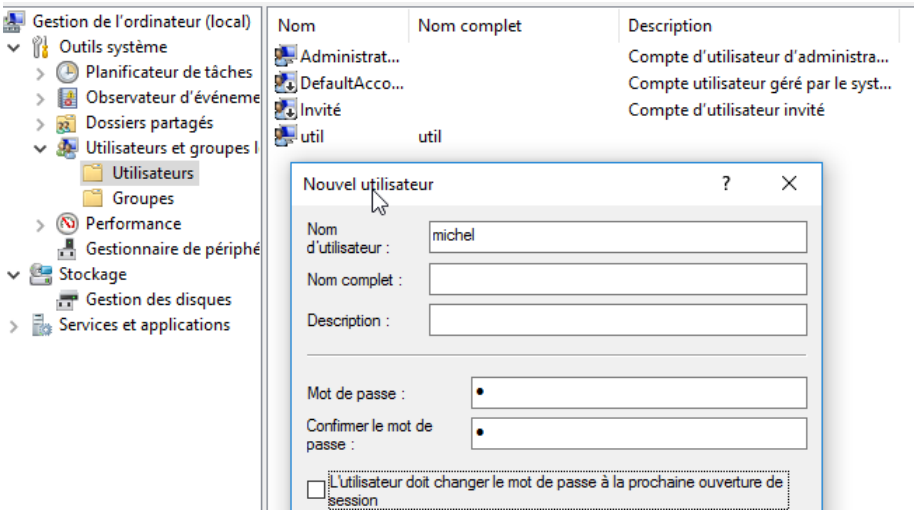
N.B : L'emplacement des données de l'utilisateur dans le nuage n'est pas connu de celui-ci.

L'authentification grâce à un compte Microsoft synchronise un certain nombre d'éléments suivants :

- Applications téléchargées depuis Windows Store.
- Favoris, thèmes, préférences linguistiques.
- Mise à jour de votre réseau social Facebook, Hotmail, Twitter…Photos et autres fichiers stockés sur des services tels que SkyDrive, Flickr…

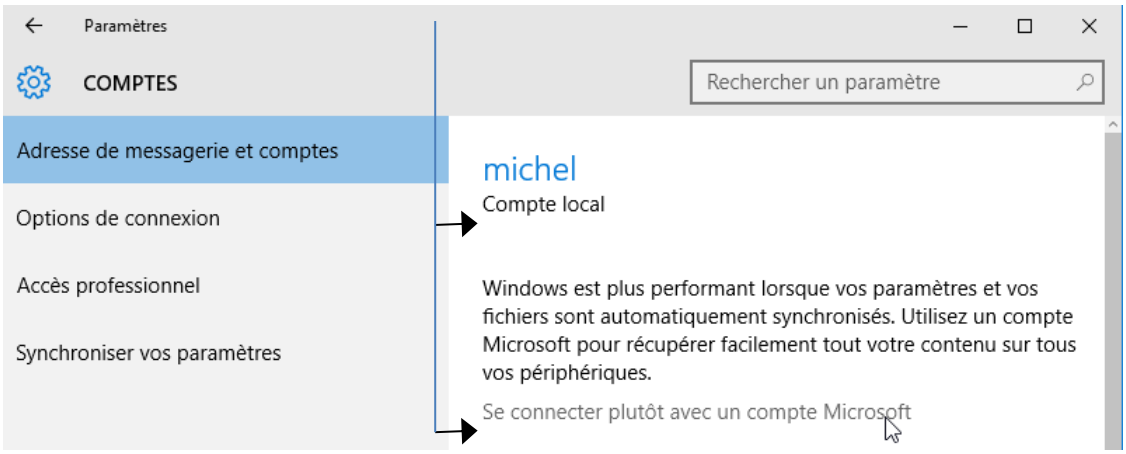
Lorsque l'on crée un compte depuis l'interface graphique, il vaut toujours mieux créer un compte local , via la **gestion de l'ordinateur**…

Par exemple ***michel***…

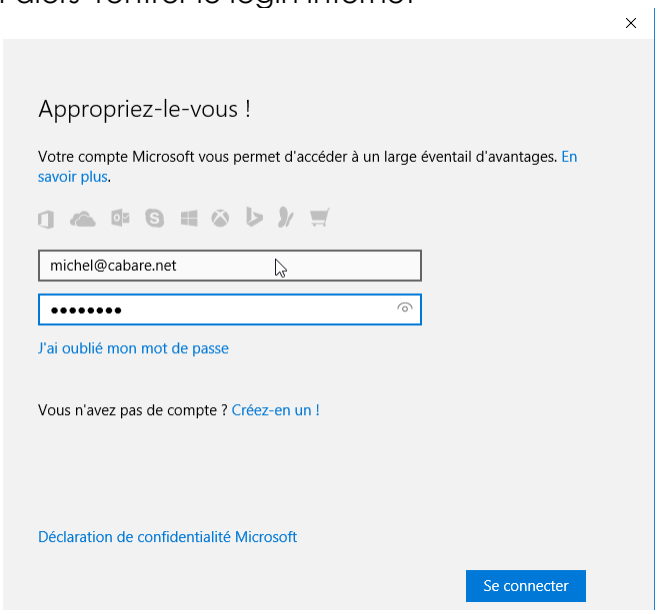


Puis se logguer avec ce compte ***michel*** …

et lui associer un identifiant microsoft en demandant de **Se connecter plutôt avec un compte Microsoft**



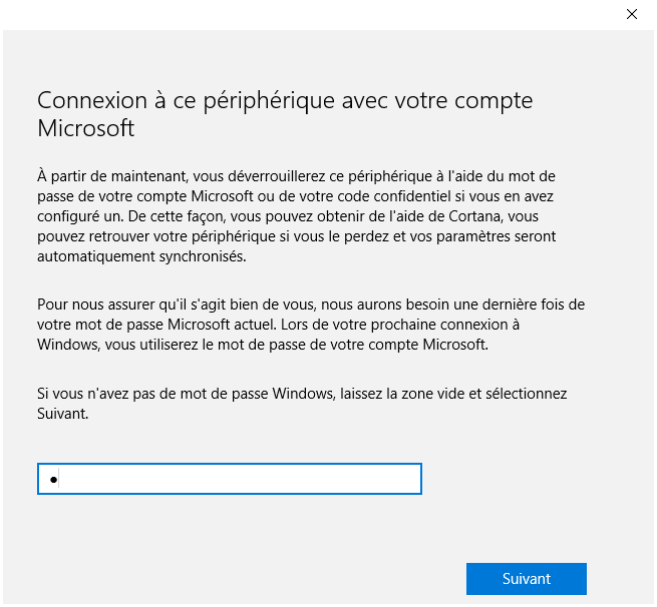
Il faut alors rentrer le login internet



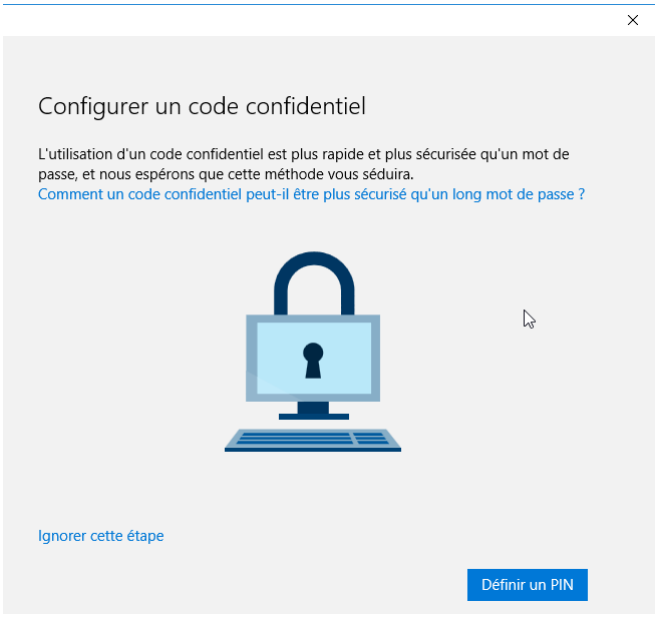
Login et MDP

Du compte microsoft à associer

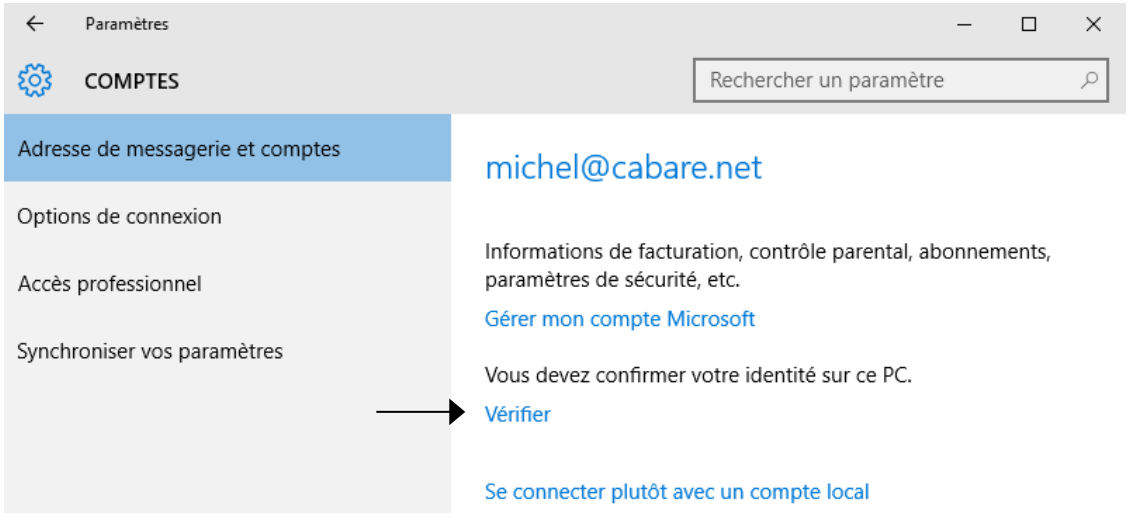
puis demande du mot de passe du compte windows local (pour confirmation), avant de lui substituer le mot de passe du login internet… c'est clair non ?



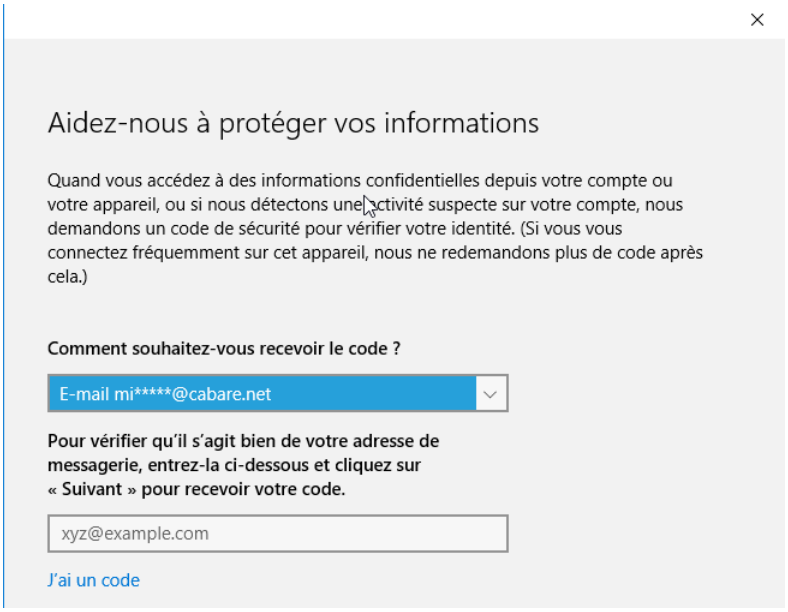
Il est possible de définir un code PIN, mais on peut **ignorer cette étape**



Et voilà !

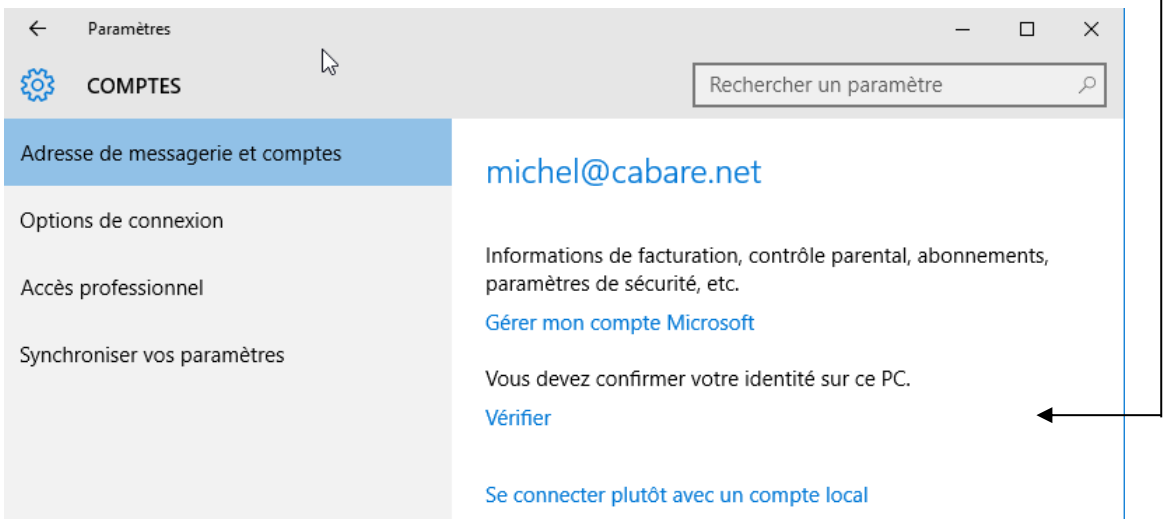


Comme l'appareil devient un élément d'authentification, il est nécessaire de confirmer son identité sur ce PC… par **Vérifier**

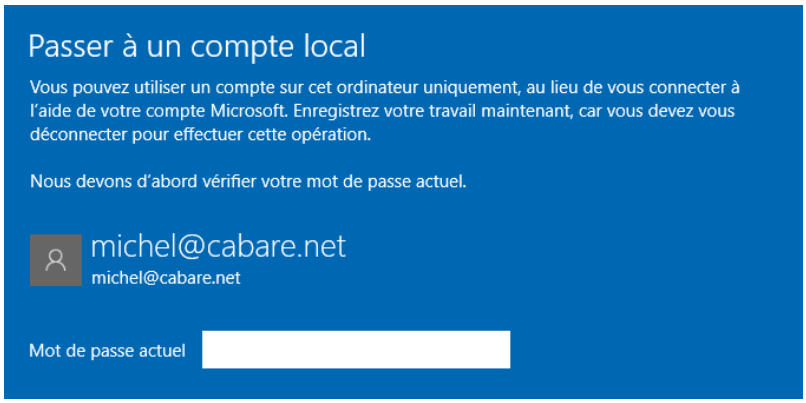


Compte Microsoft / Compte local ou AD :

Sur les anciennes versions de Windows 10, on pouvait trouver cela sur **adresse de messagerie et comptes.** Et on demande **Se connecter plutôt avec un compte local**



Il faut abandonner les identifiants du compte internet pour en recréer un jeu pour le compte local…

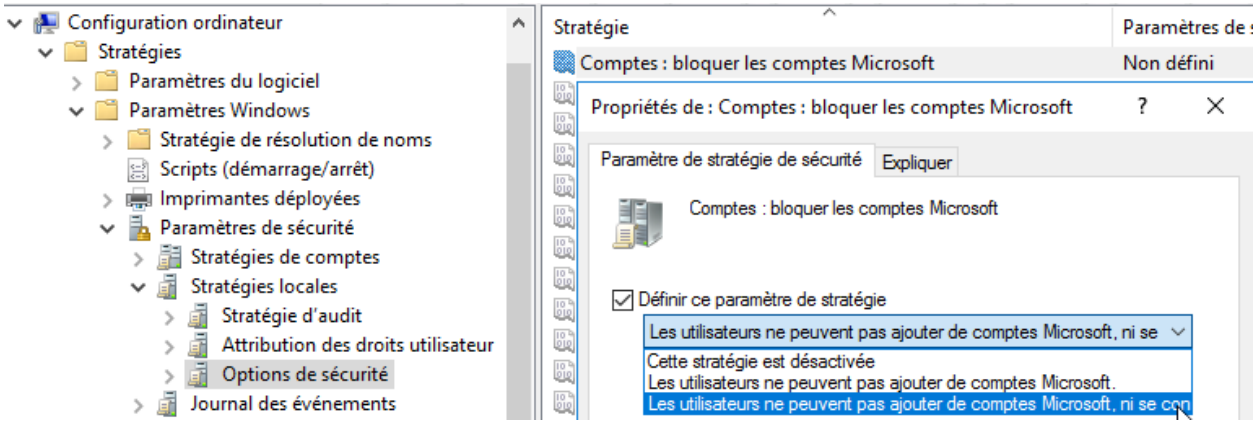


Bien sur à ne pas utiliser dans un domaine

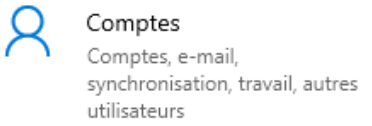
Désactivation compte Microsoft (login sur la machine)

On peut en environnement professionnel interdire l'utilisation d'un compte Microsoft. Dans les stratégies de sécurité locales, dans les **stratégies locales, / Options de sécurité**

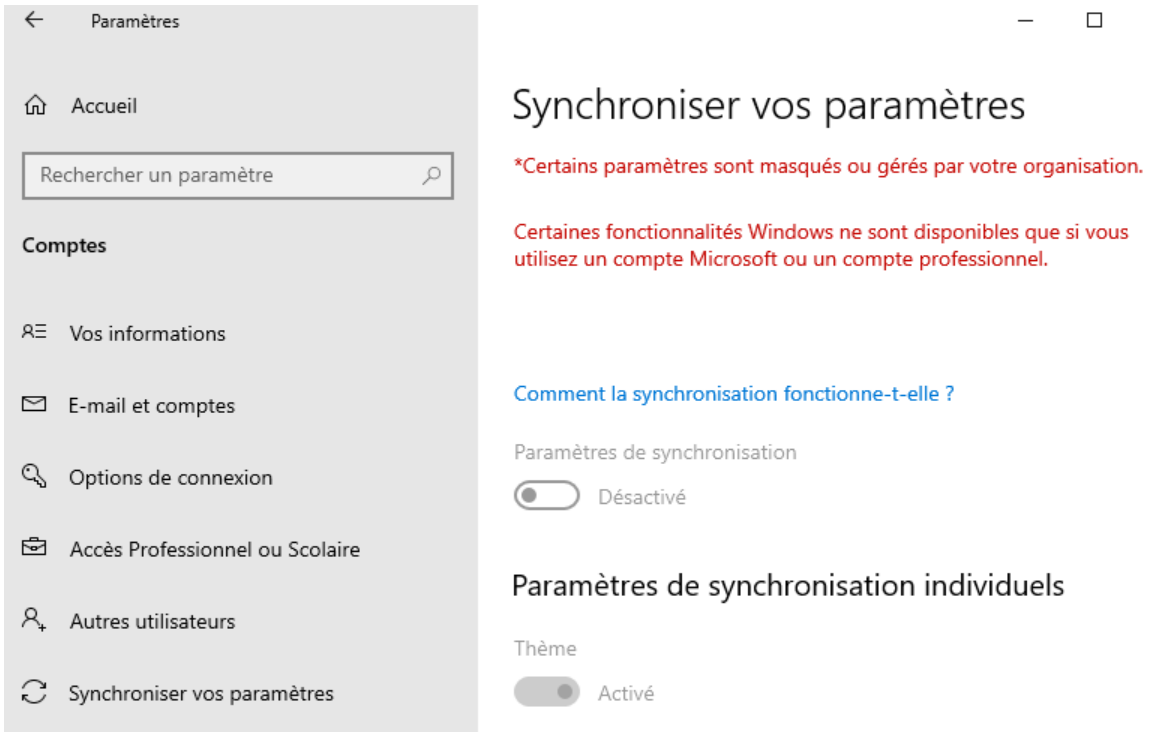
On Active le fait de **bloquer les comptes Microsoft**, (et de ne pas pouvoir se connecter avec un compte microsoft)



On pourra le vérifier par exemple via les **paramètres Windows**, / **Comptes / synchroniser vos paramètres**



dans lesquels au niveau Synchronisation par exemple on affichera l'impossibilité de mettre en oeuvre la fonction

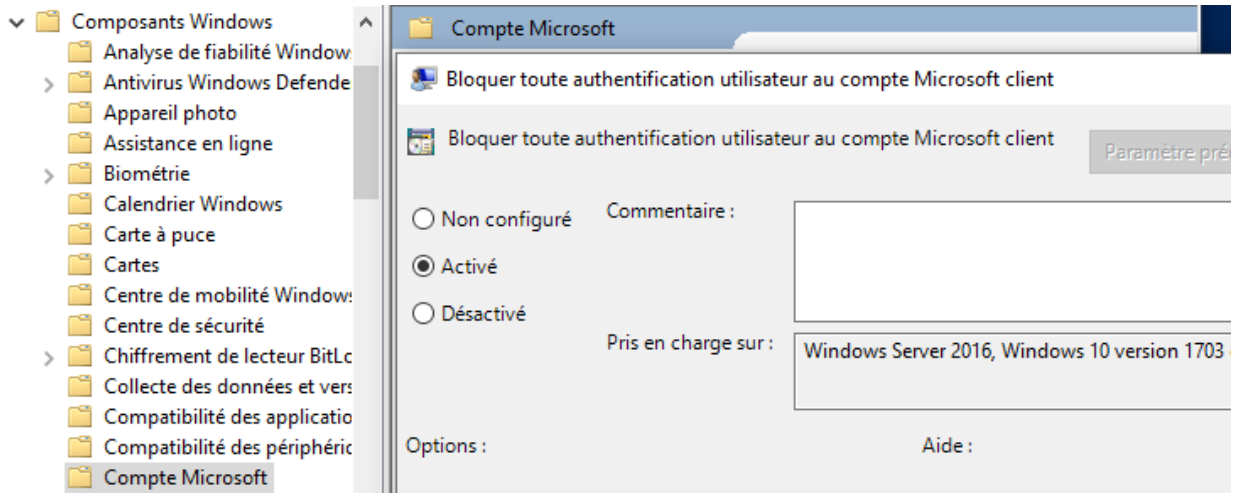


Désactivation compte Microsoft (via le Web) - msapolicy.admx

Depuis la version **1703** on a également la possibilité de demander dans

Configuration ordinateur / Modèles d'administration / Composants Windows /Compte Microsoft

De bloquer l'accès à un compte **microsoft** via le WEB



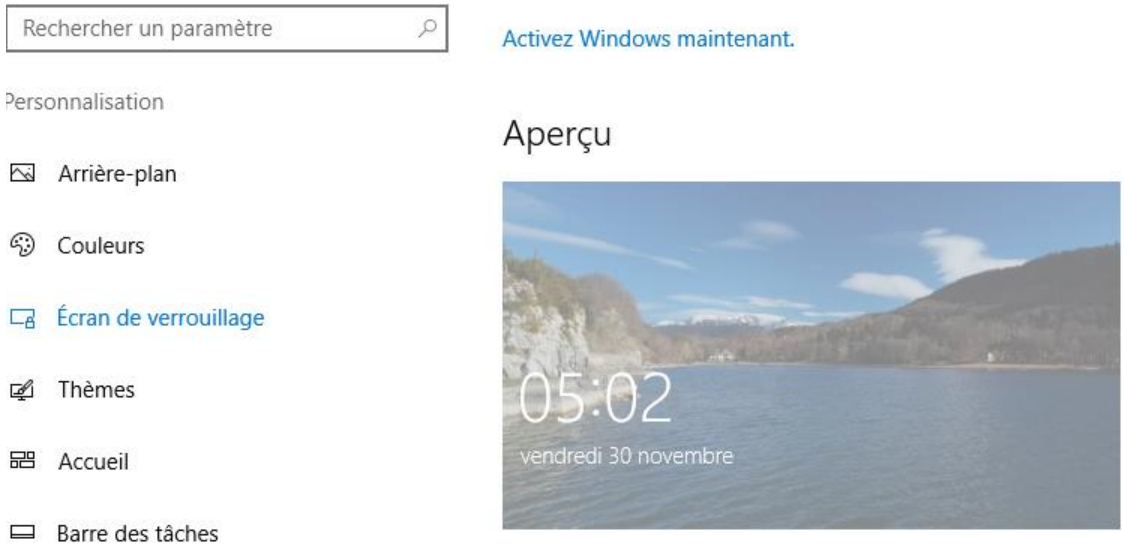
Ecran de Verrouillage – Ecran d'accueil :

L'écran de verrouillage (ou lockscreen en anglais) se présente dorénavant sous la forme d'une grande image sur laquelle il faut cliquer (ou qui nécessite l'appui sur une touche de clavier) en sortie de veille de l'ordinateur. Il apparait lorsqu'aucune session inter-active n'est ouverte.

N.B: ne faut pas confondre **l'écran de verrouillage** avec **l'écran d'accueil** qui s'affiche au démarrage du système d'exploitation, juste avant de saisir son identifiant et mot de passe. Des que l'on s'est loggué on tombe sur **le Bureau**

Il n'est pas pour l'instant possible de contourner l'écran d'accueil, mais on peut désactiver / paramétrer l'écran de verrouillage.

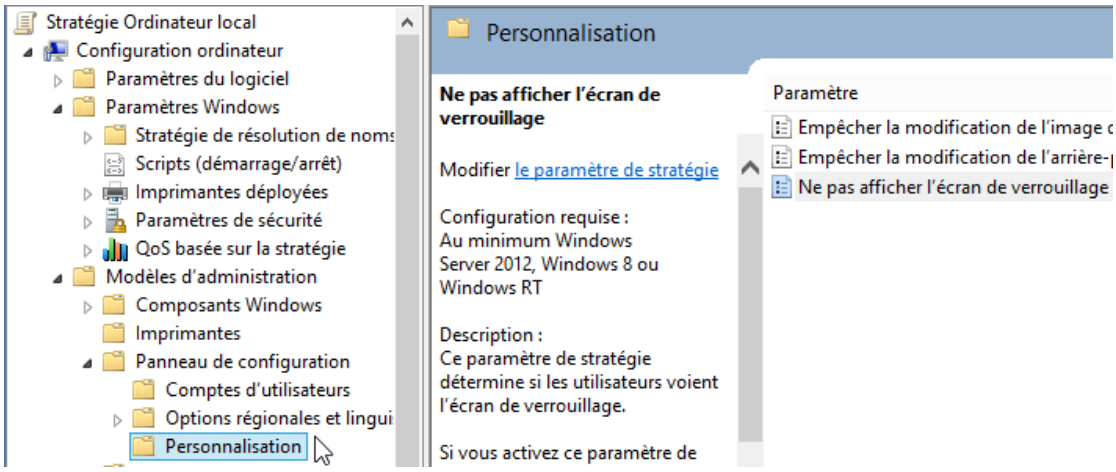
Via **Paramètres / Personnalisation / Ecran de verrouillage**



N.B : si la désactivation de l'écran de verrouillage est necessaire (car si on n'est pas sur une tablette, cela ne se justifie pas..) cela peut se gérer via les stratégies via **Gpedit.msc (**depuis **ver 1607** sur version **entreprise,** uniquement)

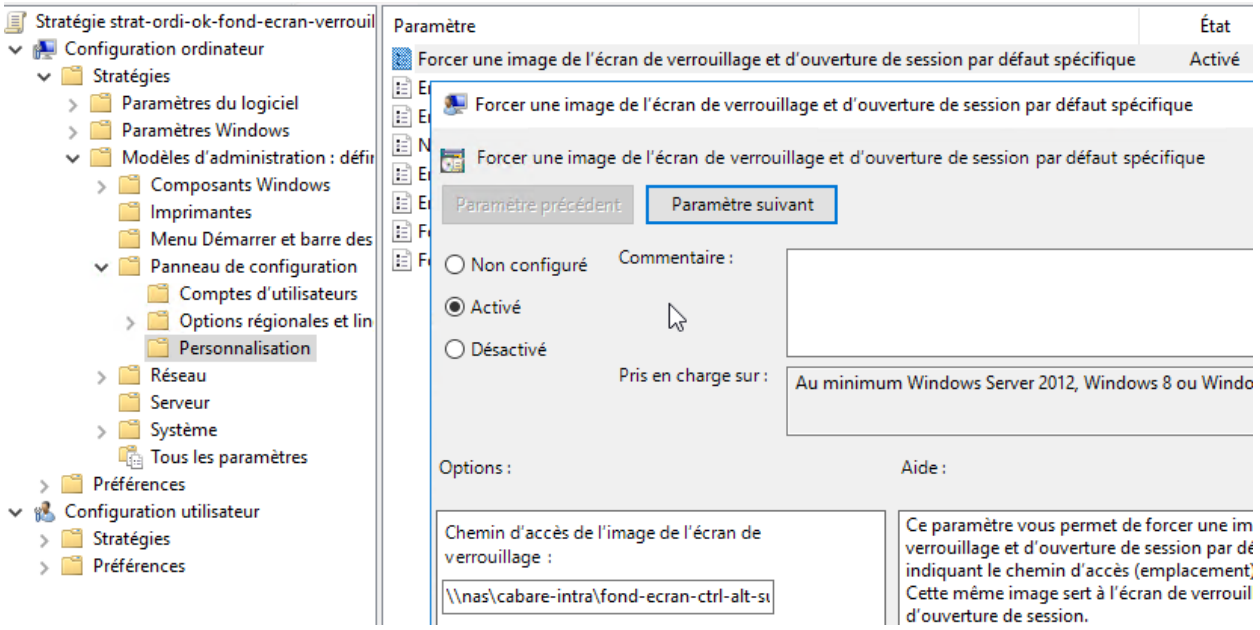
Configuration ordinateur / Modèles d'administration / Panneau de Configuration /Personnalisation

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



N.B : le choix d'une image pourl'écran de verrouillage est possible, cela peut se gérer via les stratégies via **Gpedit.msc (**depuis **ver 1803** sur version **entreprise,** uniquement)

Configuration ordinateur / Modèles d'administration / Panneau de Configuration /Forcer une image de l'écran de verrouillage et d'ouverture de session par défaut spécifique



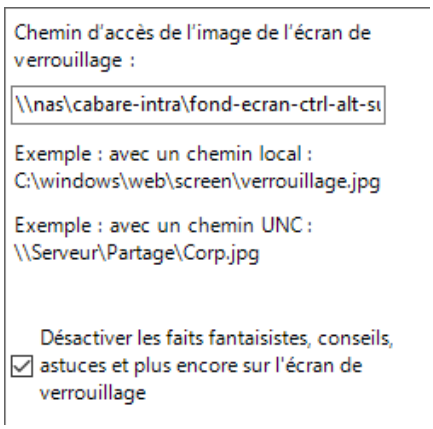
et on indique un chemin de fichier **.jgp**

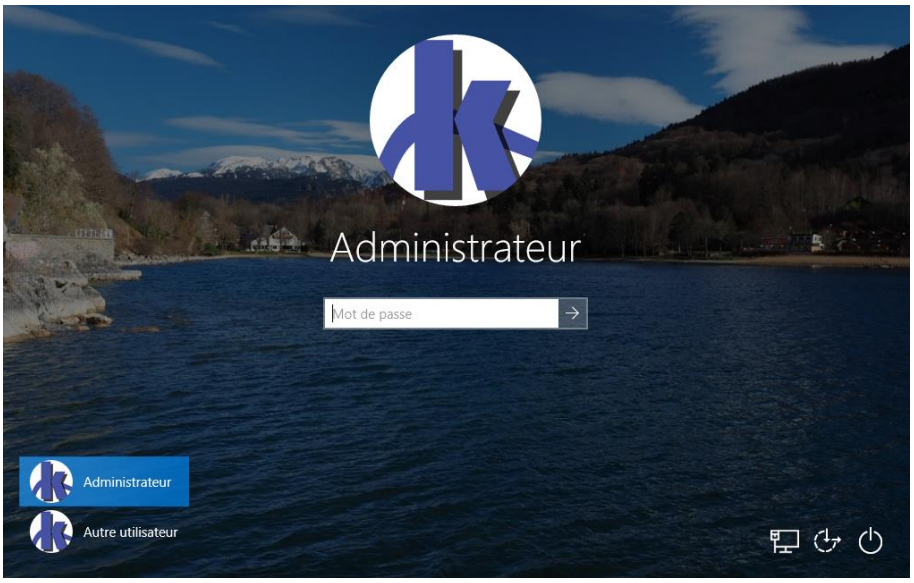
La case à cocher

Désactiver les faits fantaisistes….

empêche l'apparition de pub sur l'écran de verrouillage, et donc on peut estmier que pour ne pas avaoir de publicité, il faut avoir un version entreprise, et non pro !

il peut être necessaire de mettre à jour le modèle Admx **controlpaneldisplay.admx**



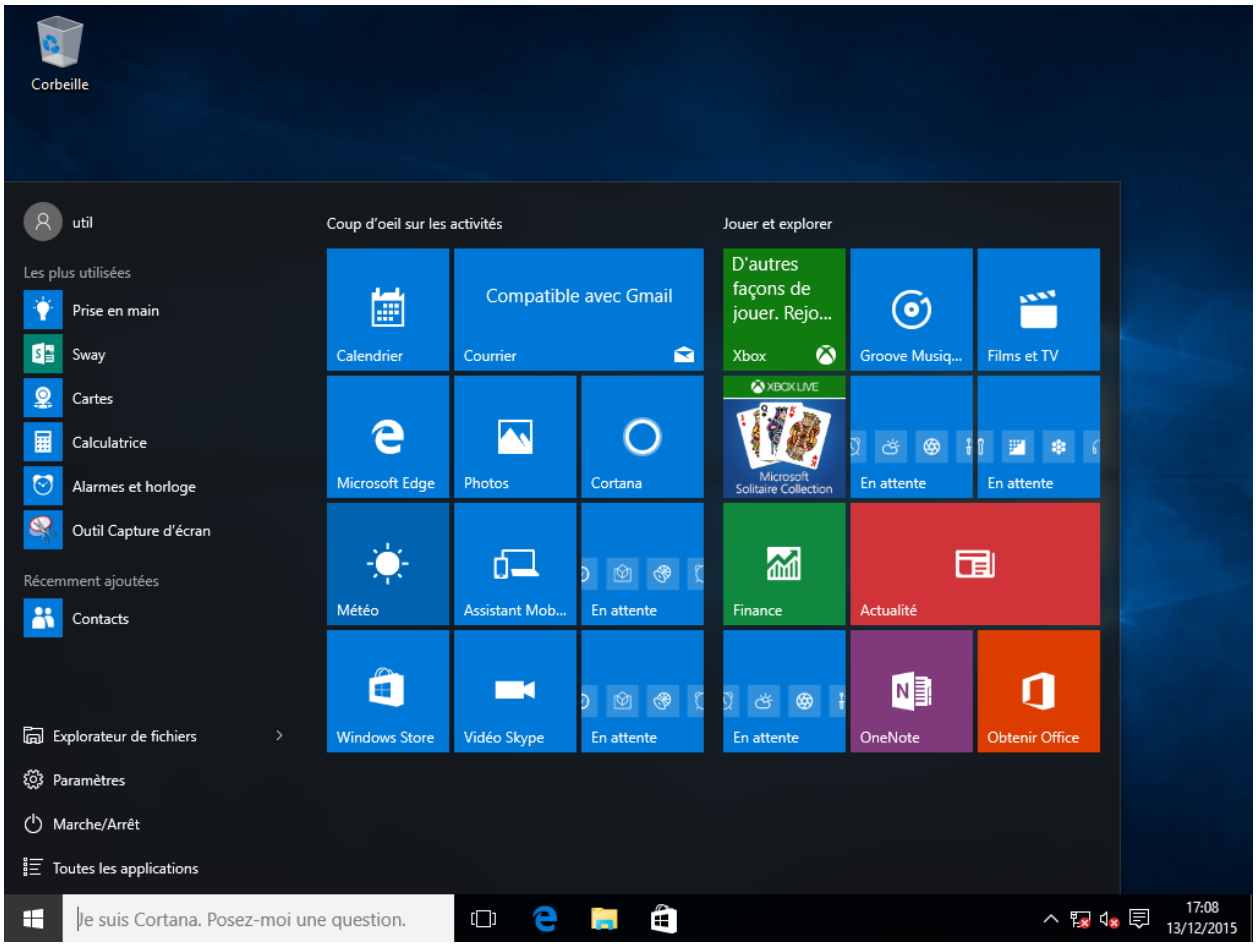


Bureau - Ecran d'accueil:

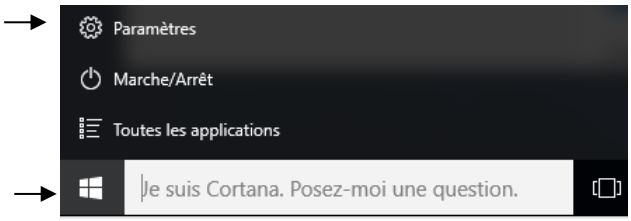
Lorsque l'on ouvre une session(après authentification) on tombe sur le bureau

Qui est personnalisable « classiquement » en modifiant l'aspect du bureau.

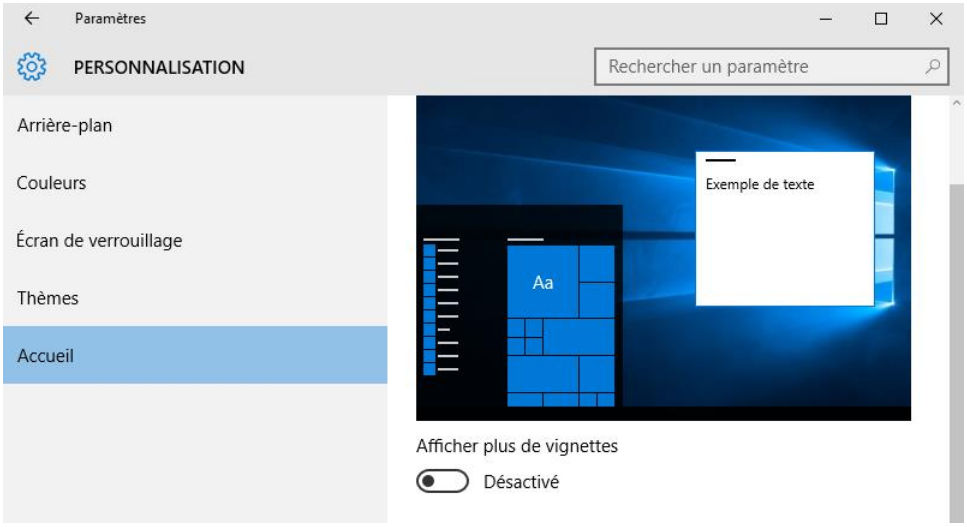
L'interface « Tuile » à laquelle on accède en cliquant en bas à gauche sur l'icône Windows se nomme l'écran d'accueil…



Son aspect est personnalisable via le menu **Windows/Démarrer**

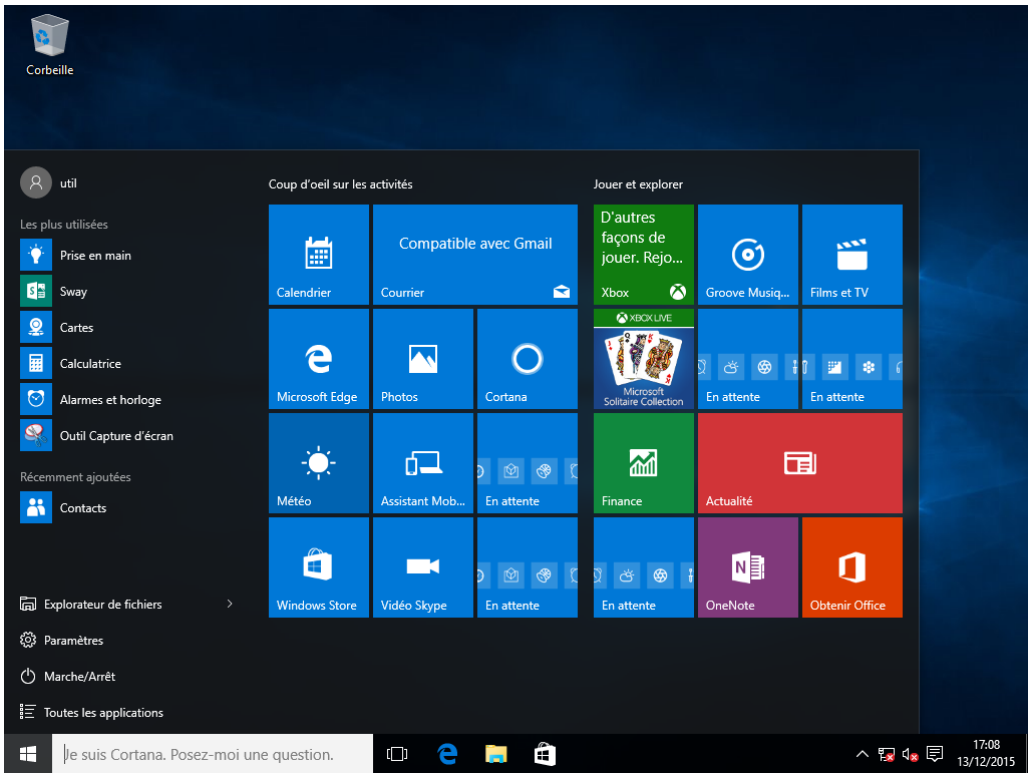


puis **Paramètres / Personnalisation / Accueil**

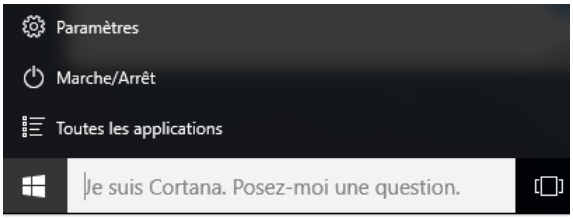


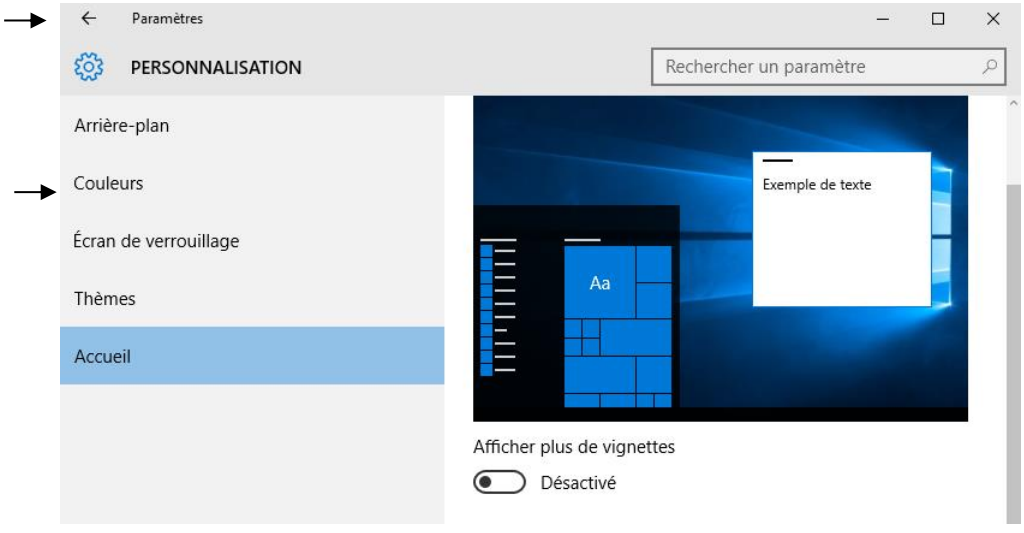
Ecran Accueil par défaut

On l'a vu, l'interface « Tuile » à laquelle on accède en cliquant en bas à gauche sur l'icône Windows se nomme **l'écran d'accueil**…



Son aspect est personnalisable via le menu **Windows /Paramètres / Personnalisation / Accueil**

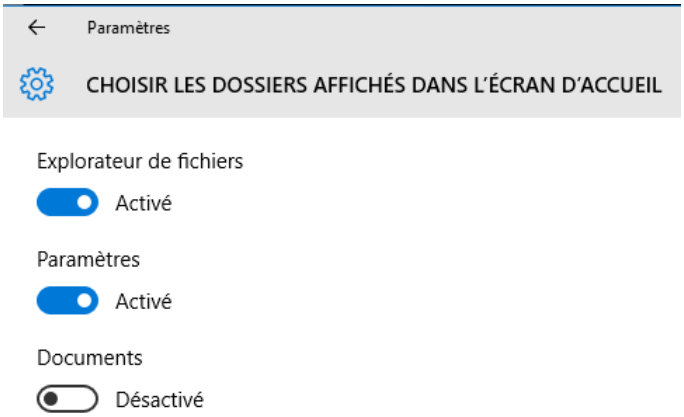


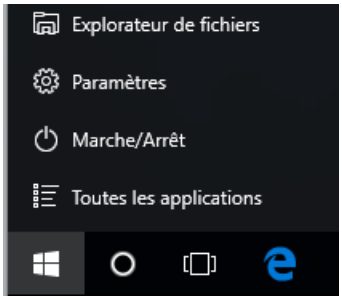


Menu Démarrer Windows

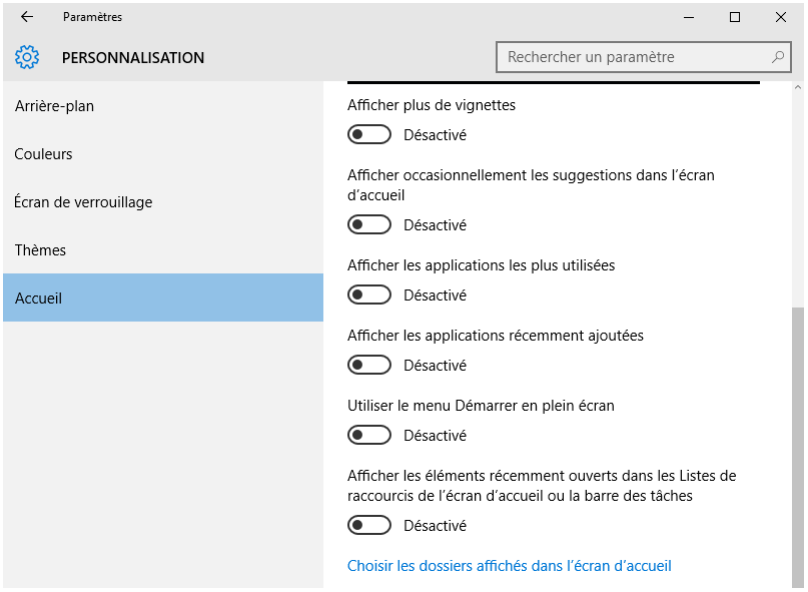
Il remplace le menu Démarrer des versions précedentes

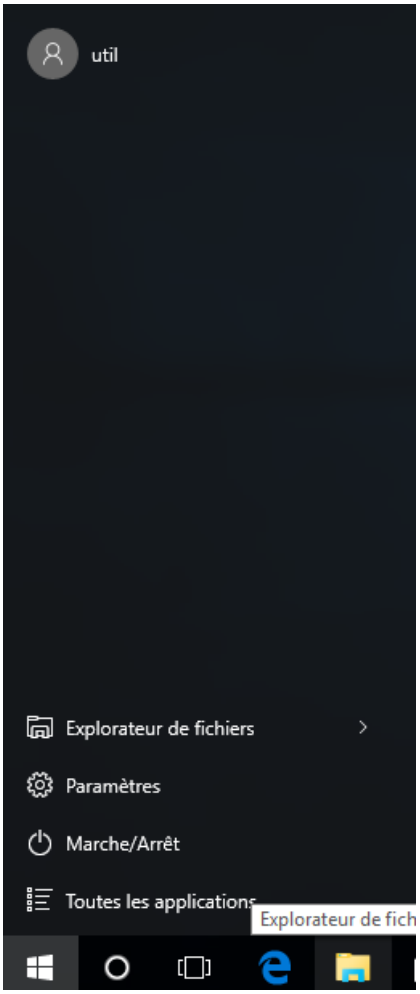
On peut Choisir les dossiers qui doivent apparaître via **Paramètres / Personnalisation / Accueil / Choisir les dossiers affichés dans l'écran d'accueil**





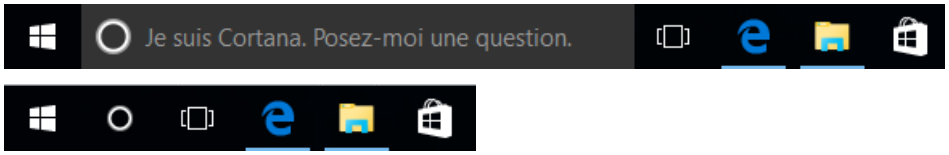
On peut aussi stopper tous les ajouts automatiques au "fil du temps" via **Paramètres / Personnalisation / Accueil**



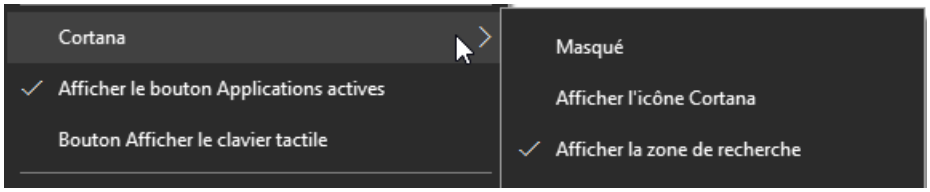


L'aspect de Cortana

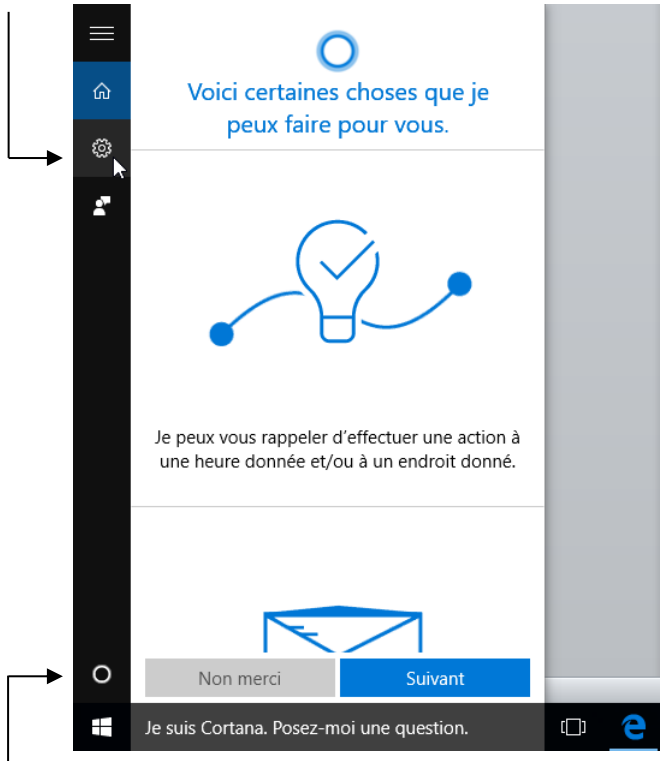
Le principe de recherche via la **Charm Bar** de **Windows 8.1** est maintenu mais refondu dans la recherche nommée maintenant **Cortana.** Cette recherche est disponible dans la barre des tâches

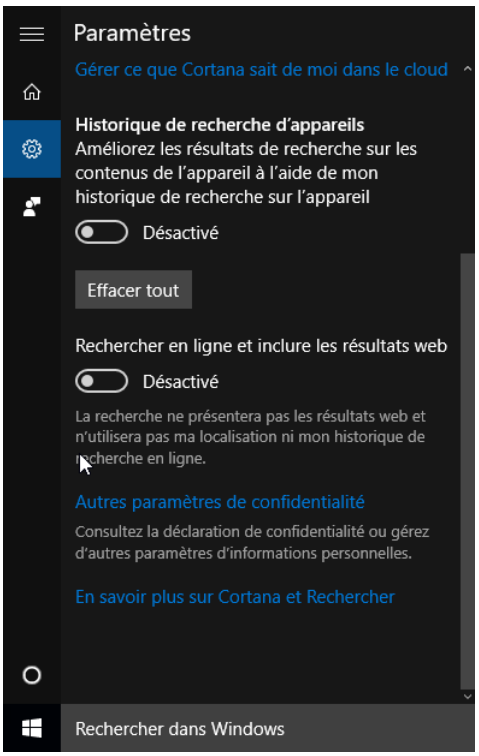


Un clic droit dessus permet un menu contextuel dans lequel on peut modifier sons aspect, et notamment la réduire en icone



Lorsque l'on clique dessus, on effectue une recherche sur la machine, et sur le web en même temps… cette recherche « vaste » et ses autres fonctions multiples se paramètre via le menu **Paramètres**





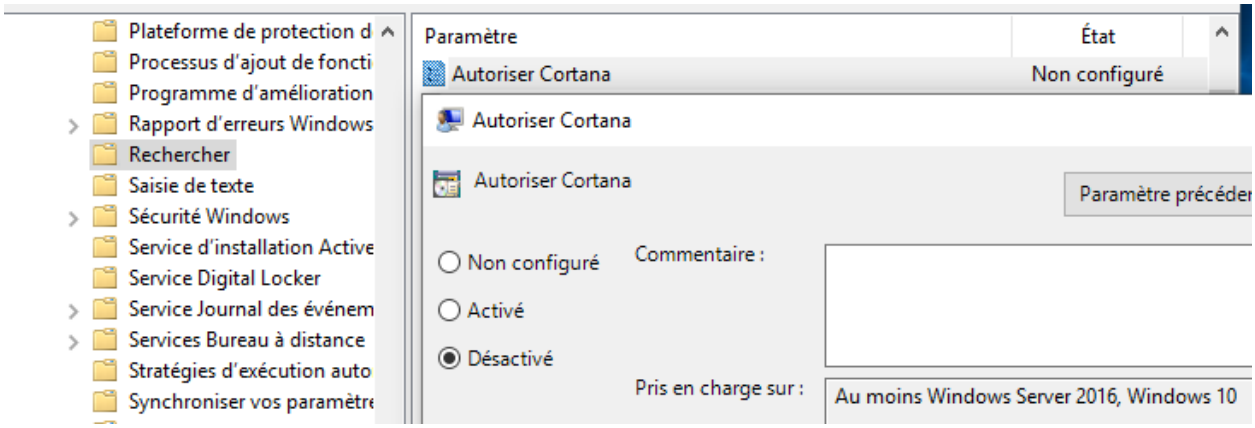
L'assistant se réactive ici

Refuser Cortana à l'installation

Cortana Gpo - désactiver – search.admx

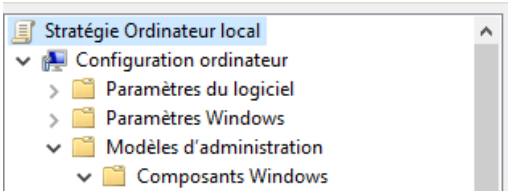
Pour limiter les remontées d'information, on doit désactiver CORTANA dans **Modèle d'administration / Composants Windows / Rechercher** on choisit

De Désactiver **Autoriser Cortana**

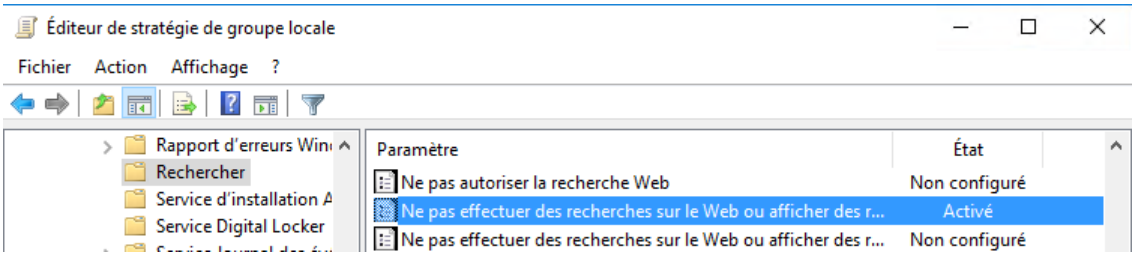


Recherche Search Windows (et Cortana) - search.admx

Mais le mieux c'est de passer par GPO, via **gpedit.msc**



Dans **Modèle d'administration / Composants Windows / Rechercher** on choisit **Ne pas effectuer des recherches sur le web ou afficher des résultats Web dans Search**



N.B: depuis la branche **1803** sur les versions **PRO** cette **GPO** ne fonctionne plus (il faut la version **entreprise** ou **EDU**). Une solution de contournement pourrait consister dans ces modifications / ajout dans le registre

Si on veut on peut faire une **préférence utilisateur** pour ces modifications

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Search

On ajoute 3 clés, respectivement :

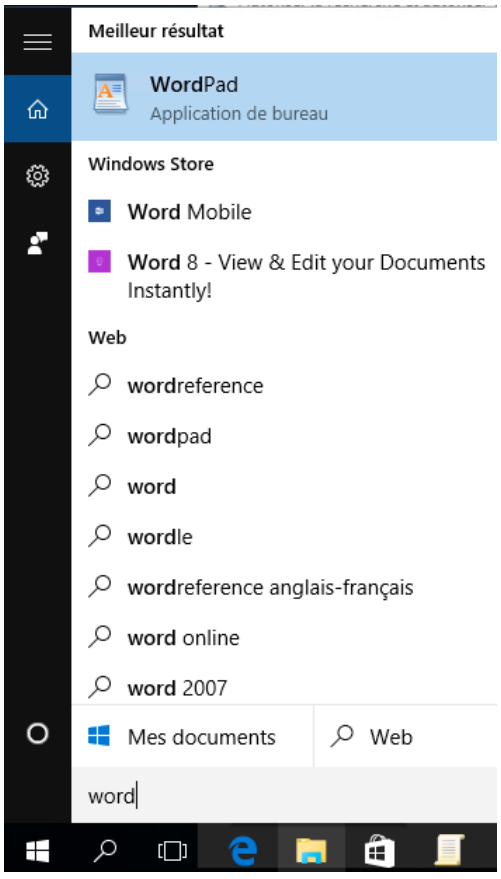
AllowSearchToUseLocation	dword	0
BingSearchEnabled	dword	0
CortanaConsent	dword	0

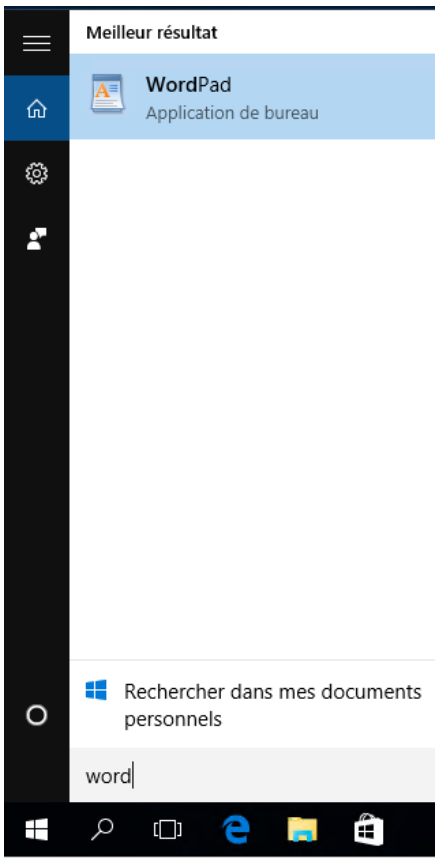
De manière optionnelle, on veut on peut aussi faire une **préférence ordinateur** pour ces modifications

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search

On ajoute 2 clés, respectivement :

AllowCortana	dword	0
ConnectedSearchUseWeb	dword	0





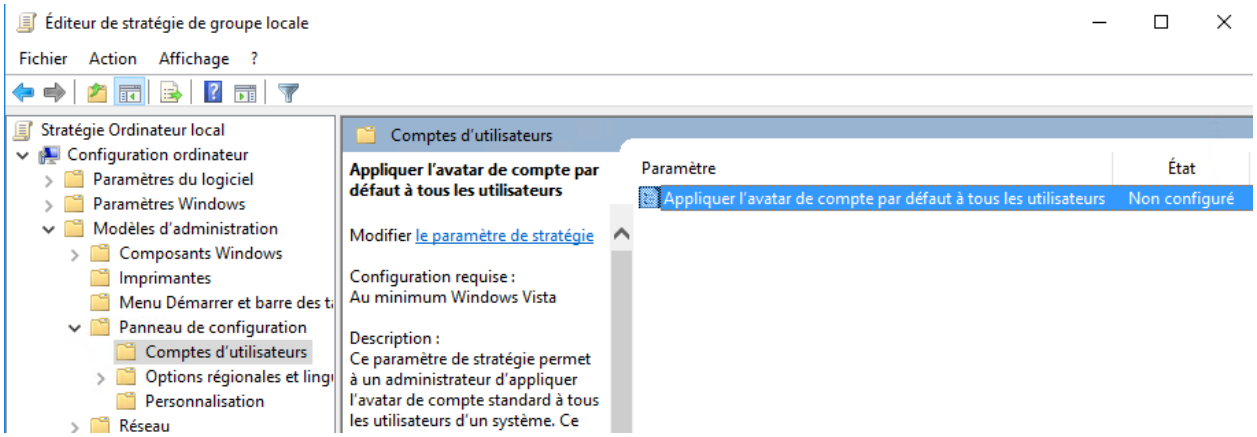
N.B: ce paramétrage affecte **CORTANA**, mais aussi l'outil **Search** de Windows (indépendamment de l'activation ou non de CORTANA **Il semblerait bon de le paramétrer systématiquement** !

AVATAR DU LOGIN

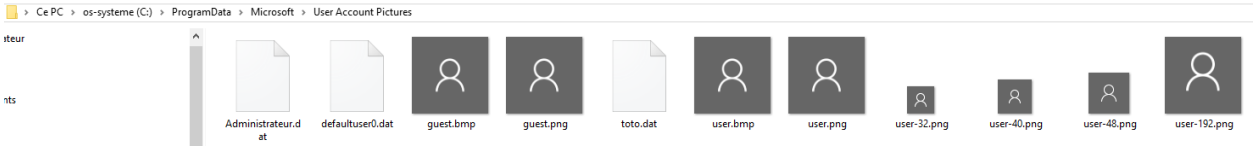
Modification de l'avatar

L'avatar associé par défaut à un compte peut être modifié par GPO via:

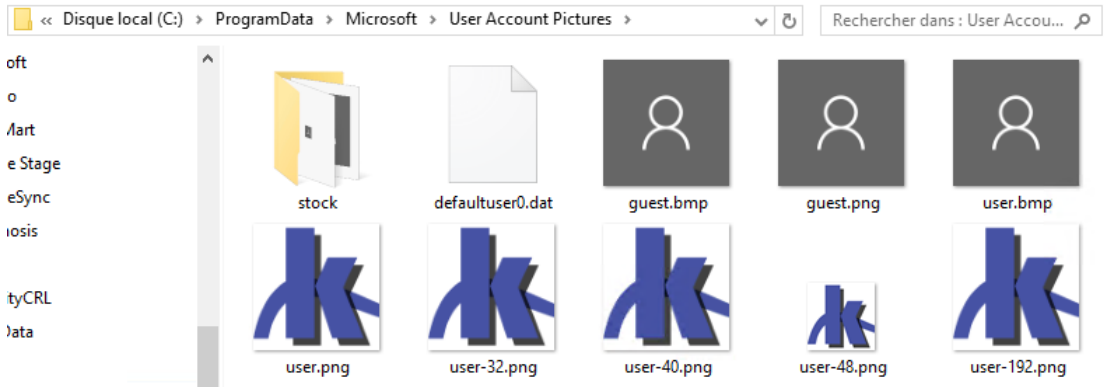
Configuration Ordinateur/ Modèle d'administration / Panneau de Configuration/ Compte d'utilisateurs / Appliquer l'avatar de compte par défaut à tous les utilisateurs



L'avatar de compte par défaut est enregistré dans le dossier **%PROGRAMDATA%\Microsoft\User Account Pictures\user.jpg.**



Que l'on peut remplacer par



L'avatar d'invité par défaut se trouve dans le dossier **%PROGRAMDATA%\Microsoft\User Account Pictures\guest.jpg.**

N.B : Si on active le paramètre de stratégie les personnalisations ne sont pas autorisées. Si vous désactivez ce paramètre de stratégie, les utilisateurs peuvent personnaliser leur avatar de compte.

LES TUILES

Tuiles par défaut

l'écran d'accueil windows 10 demande une résolution mini de 1366 x 768 px

Les 2 types d'applications suivants s'exécutent sur Windows10, nommées respectivement **Windows Apps,** et les applications traditionnelles dites **Win32**:

- **Applications dites "Apps"**: introduites à partir de Windows 8 et 10, elles sont principalement installées à partir du **Windows Store** (mais pas toutes)
- **Applications dites «Win32»**: applications Windows classiques.

Applications Apps : UWP - Applications système - Applications

Pour ces **Applications dites "Apps"**: introduites à partir de Windows 8, on peut les sub-diviser en 3 genres

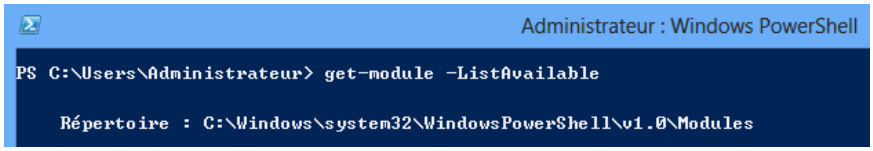
- **Applications de la plateforme Windows universelle (UWP)**: conçues pour fonctionner sur toutes les plateformes, peuvent être installées sur plusieurs plateformes, notamment le client Windows, Windows Phone et Xbox. Pn peut dire que toutes les **applications UWP** sont donc des **applications Windows**, (mais par contre toutes les **applications Windows** ne sont pas forcément des **applications UWP**)
- **Applications systèmes**: applications qui sont installées dans le répertoire **C:\Windows**. Ces applications font partie intégrante du système d'exploitation
- **Applications:** toutes les autres **applications** sont installées dans le répertoire **C:\program Files\WindowsApps.** Et on distinguera 2 classes d'applications : **Approvisionnées – Installées**
  - **Applications Approvisionnées** : elles seront installées la première fois qu'un utilisateur se connecte
  - **Applications Installées** elles sont installées en tant que partie du système d'exploitation

Gestion des Appx installées et ou Approvisionnnées en Powershell

On passe en powershell. Tache que l'on lance en mode administrateur

Si besoin **Set-ExecutionPolicy Unrestricted**

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



Si besoin, on importe juste le module appx **Import-Module appx**

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

On peut vérifier les les commandes importées par un

(Get-Module appx).exportedcommands

```
PS C:\Users\Administrateur> (get-module appx).exportedcommands

Key                     Value
---                     -----
Add-AppxPackage         Add-AppxPackage
Add-AppxVolume          Add-AppxVolume
Dismount-AppxVolume     Dismount-AppxVolume
Get-AppxDefaultVolume   Get-AppxDefaultVolume
Get-AppxPackage         Get-AppxPackage
Get-AppxPackageManifest Get-AppxPackageManifest
Get-AppxVolume          Get-AppxVolume
Mount-AppxVolume        Mount-AppxVolume
Move-AppxPackage        Move-AppxPackage
Remove-AppxPackage      Remove-AppxPackage
```

Suppression des packages utilisateur en cours (installées)

Get-AppXPackage donne la liste de tous les des packages courant,

```
PS C:\Users\Administrateur> get-appxpackage

Name                  : Microsoft.VCLibs.140.00
Publisher             : CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
Architecture          : X64
ResourceId            :
Version               : 14.0.22929.0
PackageFullName       : Microsoft.VCLibs.140.00_14.0.22929.0_x64__8wekyb3d8bbwe
InstallLocation       : C:\Program Files\WindowsApps\Microsoft.VCLibs.140.00_14.0.22929.0_x64__8wekyb3d8bbwe
IsFramework           : True
PackageFamilyName     : Microsoft.VCLibs.140.00_8wekyb3d8bbwe
PublisherId           : 8wekyb3d8bbwe
IsResourcePackage     : False
IsBundle              : False
IsDevelopmentMode     : False
```

La liste des nom de packages complets pour l'utilisateur courant s'obtient alors avec

Get-Appspackage | select packagefullname

```
PS C:\Windows\system32> Get-AppxPackage | select packagefullname

PackageFullName
---------------
Microsoft.Windows.CloudExperienceHost_10.0.17134.1_neutral_neutral_cw5n1h2txyewy
Microsoft.AAD.BrokerPlugin_1000.17134.1.0_neutral_neutral_cw5n1h2txyewy
Microsoft.Windows.ShellExperienceHost_10.0.17134.1_neutral_neutral_cw5n1h2txyewy
windows.immersivecontrolpanel_10.0.2.1000_neutral_neutral_cw5n1h2txyewy
Microsoft.Windows.Cortana_1.10.7.17134_neutral_neutral_cw5n1h2txyewy
Microsoft.MicrosoftEdge_42.17134.1.0_neutral__8wekyb3d8bbwe
Microsoft.Windows.ContentDeliveryManager_10.0.17134.1_neutral_neutral_cw5n1h2txyewy
Microsoft.VCLibs.140.00_14.0.25426.0_x64__8wekyb3d8bbwe
Microsoft.VCLibs.140.00_14.0.25426.0_x86__8wekyb3d8bbwe
Microsoft.NET.Native.Framework.1.6_1.6.24903.0_x64__8wekyb3d8bbwe
Microsoft.NET.Native.Framework.1.6_1.6.24903.0_x86__8wekyb3d8bbwe
```

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

Remove-AppxPackage *fullname*

```
PS C:\Windows\system32> remove-appxpackage Microsoft.SkypeApp_3.2.1.0_x86__kzf8qxf38zg5c
PS C:\Windows\system32> ^P_
```

Suppression des packages provisionnés

Si on veut le supprimer définitivement de la machine (et donc pour pour les autres users (a venir…) il faut supprimer le **package provisionné**

Get-appxprovisionedPackage –online donnera la liste des packages installés sur le poste dans l'image(que l'on appelle packages provisionnés)

```
PS C:\Windows\system32> Get-AppXprovisionedpackage -online


DisplayName   : Microsoft.BingWeather
Version       : 4.24.11294.0
Architecture  : neutral
ResourceId    : ~
PackageName   : Microsoft.BingWeather_4.24.11294.0_neutral_~_8wekyb3d8bbwe
Regions       :

DisplayName   : Microsoft.DesktopAppInstaller
Version       : 2018.402.2359.0
Architecture  : neutral
```

La liste des nom de packages provisionnés s'obtient alors avec

Get-AppXprovisionedpackage –online | select Displayname

```
PS C:\Windows\system32> Get-AppXprovisionedpackage -online | select displayname

DisplayName
-----------
Microsoft.BingWeather
Microsoft.DesktopAppInstaller
Microsoft.GetHelp
Microsoft.Getstarted
Microsoft.Messaging
Microsoft.Microsoft3DViewer
Microsoft.MicrosoftOfficeHub
```

La liste des nom complets de packages provisionnés s'obtient alors avec

Get-AppXprovisionedpackage –online | select packagename

```
PS C:\Windows\system32> Get-AppXprovisionedpackage -online | select packagename

PackageName
-----------
Microsoft.BingWeather_4.24.11294.0_neutral_~_8wekyb3d8bbwe
Microsoft.DesktopAppInstaller_2018.402.2359.0_neutral_~_8wekyb3d8bbwe
Microsoft.GetHelp_10.1706.10952.0_neutral_~_8wekyb3d8bbwe
Microsoft.Getstarted_6.10.10872.0_neutral_~_8wekyb3d8bbwe
Microsoft.Messaging_2018.222.2231.0_neutral_~_8wekyb3d8bbwe
Microsoft.Microsoft3DViewer_4.1804.19012.0_neutral_~_8wekyb3d8bbwe
Microsoft.MicrosoftOfficeHub_2017.1219.520.0_neutral_~_8wekyb3d8bbwe
```

Si on veut supprimer un package provisionné

Remove-AppxProvisionedPackage –PackageName:fullname **–online**

```
PS C:\Windows\system32> remove-appxprovisionedpackage -online -packagename: Microsoft.SkypeApp_3.2.1.0_neutral_~_kzf8qxf
38zg5c


Path          :
Online        : True
RestartNeeded : False
```

On peut utiliser cette commande pour s'affranchir du numero de version

Get-AppxPackage Microsoft.ZuneMusic | Select-Object -Expand PackageFullName | Remove-AppxPackage

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

N.B: **Windows 10 Enterprise LTSB** (Long Term Servicing Branch) edition, n'a aucune application pré-packagée

Supprimer tous les packages

Les commandes ci-dessous sont un peu draconniennes… puisqu'elles permettent de supprimer tous les pakages existants sur le poste

Get-AppXPackage | Remove-AppxPackage

Get-AppXProvisionedPackage -online | Remove-AppxProvisionedPackage –online

```
get-appxprovisionedpackage -online | remove-appxprovisionedpackage -online
```

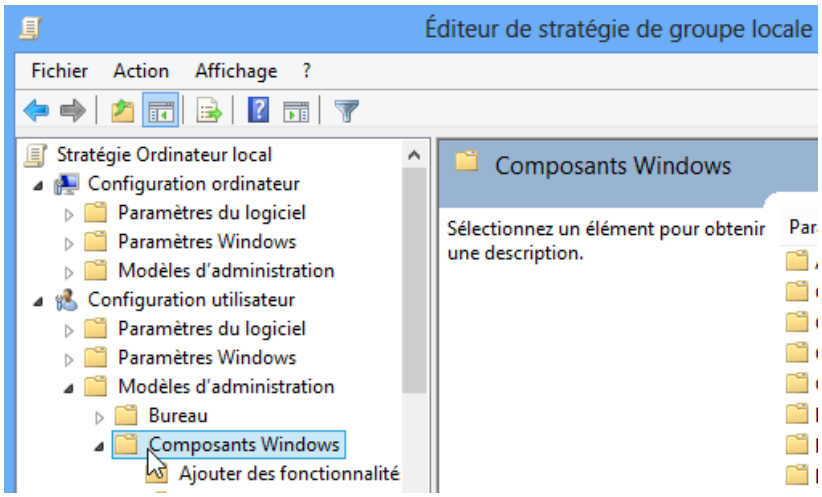
N.B: même si on demande de supprimer toutes les applications, un certains nombre de fait ne sont pas désinstallables.

Gestion Windows Store

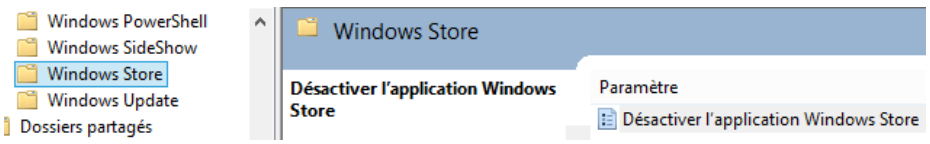
l'icone Windows Store ne peut être supprimée, mais elle peut être désactivée de manière a ce que les utilisateurs ne puissent ajouter n'importe qu'elle tuile sur leur poste.

on pourra par stratégie **gpedit.msc**

Configuration Utilisateur / Modèles d'administration / Composants Windows



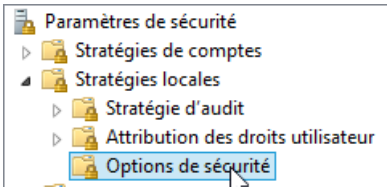
chercher l'entrée **Windows Store**



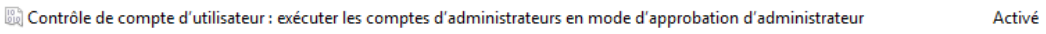
N.B : depuis **Windows 1607** la possibilité de désactiver complètement le Store est réservé aux version **education** et **entreprise**… (dans le doute on peut désactiver tous les réglages store que l'on trouvera dans la GPO…)

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

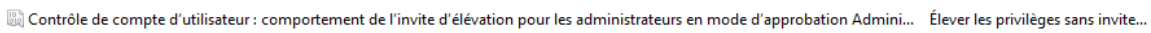
stratégies de sécurité locale /



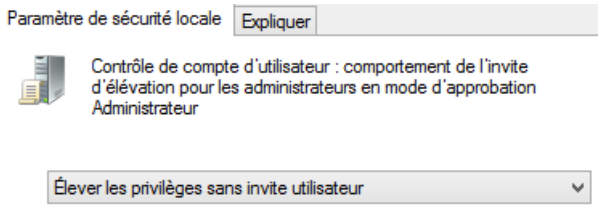
UAC actif, y compris pour les administrateur (et aussi l'admin intégré)



même si on peut demander une élévation automatique, donc



donc



CANEVAS – ECRAN D'ACCUEIL

Canevas écran d'accueil - export-startlayout

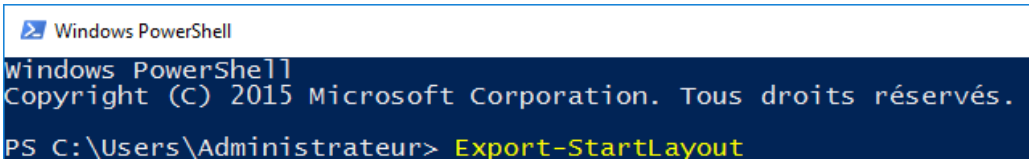
Par défaut les tuiles présentes sur le menu démarrer sont peu utiles. Cette personnalisation peut se faire via la création d'un modèle (canevas) sur un poste "maître" qui sera ensuite déployé sur les postes de travail souhaité.

Ce canevas servira de trame a appliquer sur un profil par défaut, **faire extremement attention à la Branche Version Windows 10 utilisée !!!!**

Création du canevas

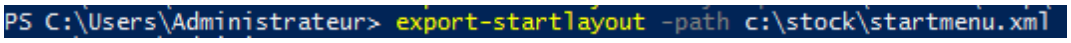
Une fois l'écran d'accueil personnalisé une capture du canevas est nécessaire.

La commande **Powershell Export-StartLayout** est utilisée

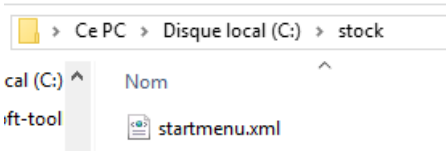


Comme dans

PS C:\> Export-StartLayout -Path "C:\stock\startmenu.xml"



le fichier XML généré contient l'ensemble des informations relatives à la position et à la taille des tuiles de l'écran d'accueil "type".



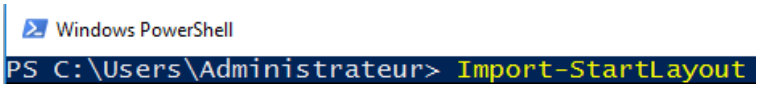
N.B : depuis **Windows 1809** la commande dot être utilisées avec un paramètre supplémentaire **UseDesktopApplicationID**

Comme dans

PS C:\> Export-StartLayout -UseDesktopApplicationID -Path "C:\stock\startmenu.xml"

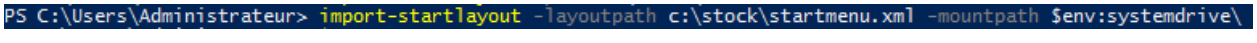
Déploiement du canevas

Par PowerShell La commande **Powershell Import-StartLayout** est utilisée

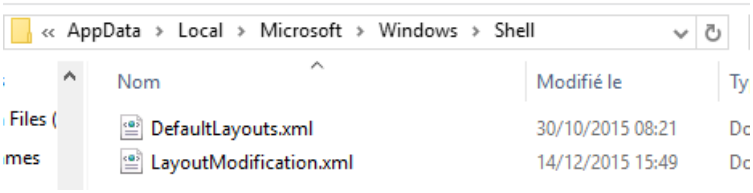


Comme dans

Import-StartLayout -LayoutPath C:\stock\canevas.xml -MountPath $env:SystemDrive



Dans le profil **Users \ default on trouve alors Appdata\Local\Microsoft\Windows\Shell**



Par GPO ***Modèle d'administration / Menu Démarrer et barre des tâches / Disposition de l'écran de démarrage***

N.B: Par GPO le déploiement d'un canevas rend les tuiles statiques, les utilisateurs ne pourront plus les modifier. On peut cependant avoir un canevas en partie fixe, et en partie modifiable, **Cf Tp** Tuiles et Startlayout.xml

COMPTES UTILISATEURS

Compte d'utilisateurs – session:

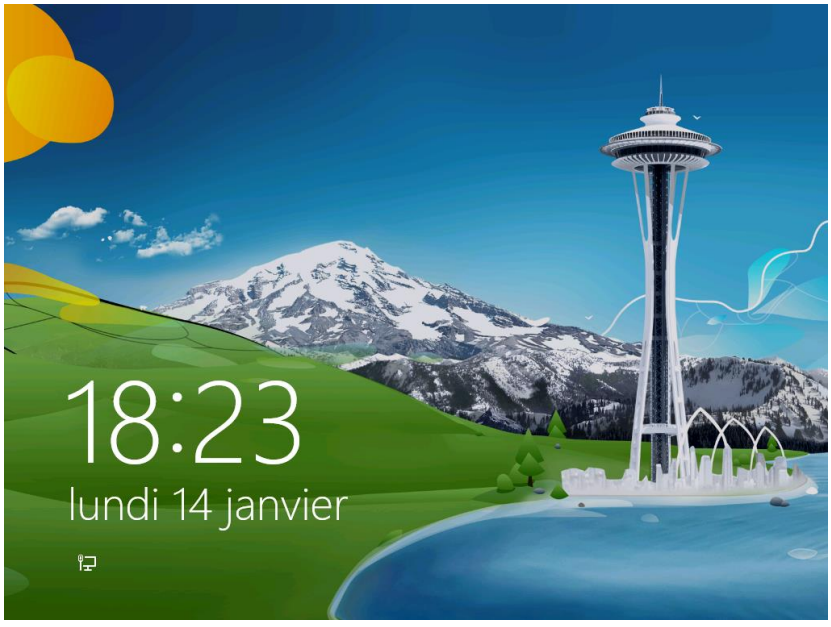
On parle de **compte utilisateur** lorsque l'on définit un individu nommément désigné, généralement par un nom d'utilisateur, et un mot de passe et des propriétés

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

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

Le nom utilisateur peut contenir jusqu'à **20 caractères**

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



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

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

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

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

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

Winlogon.exe

Ouverture de session

Séquence authentifiée 1 ↓

Fermeture de session

Ouverture de session

Séquence authentifiée 2 ↓

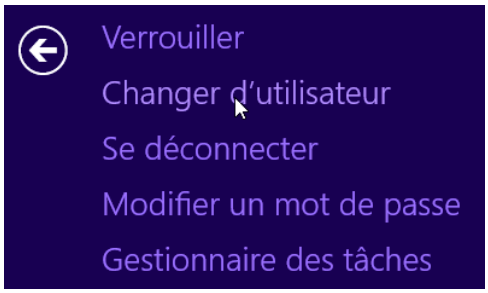
Fermeture de session

Arrêt Poste

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

Connexion multiples Utilisateur

Sur un poste Windows 10 (comme XP) il est possible de changer d'utilisateur connecté sur le poste, sans fermer sa session (les travaux et la tâches initiés continuent…) c'est-à-dire que l'on peut autoriser sur un poste plusieurs sessions en parallèle de différents utilisateurs…



- Il n'est plus nécessaire de fermer la session d'un autre utilisateur pour ouvrir sa propre session….
- Autrement dit deux utilisateurs peuvent ouvrir chacun une session et se passer la connexion sans arrêter leur travaux respectifs….

Winlogon.exe

Ouverture de session

Séquence authentifiée 1 ↓

Changer d'utilisateur (entrée stand-by)

Ouverture de session

Séquence authentifiée 2 ↓

Fermeture de session

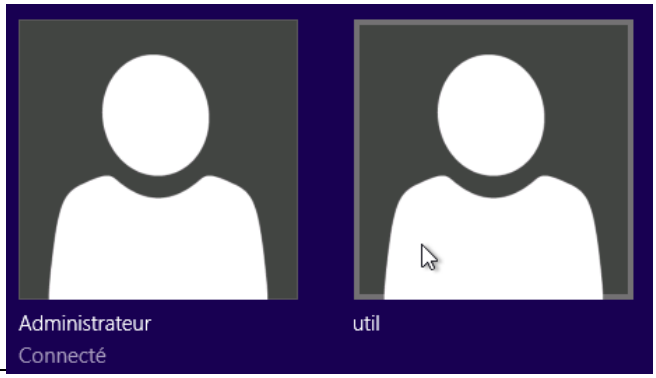
(sortie stand-by)

Séquence authentifiée 1 ↓

Fermeture de session

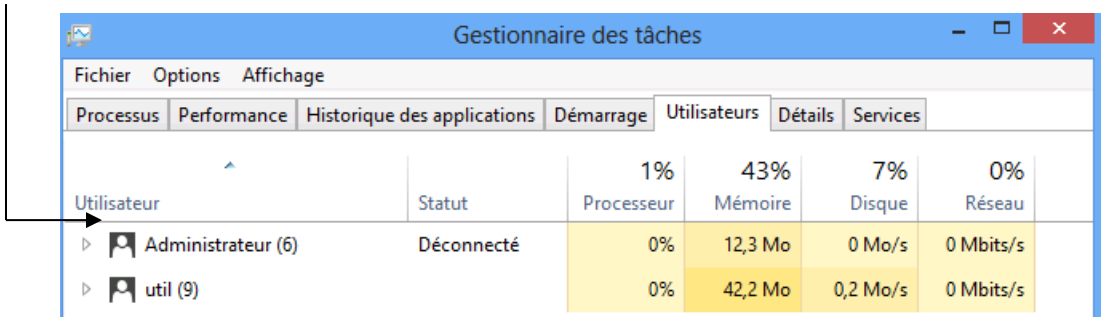
Arrêt Poste

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



Mais si l'**Administrateur** ouvre également une connexion, alors

il verra toutes les autres connections en cours

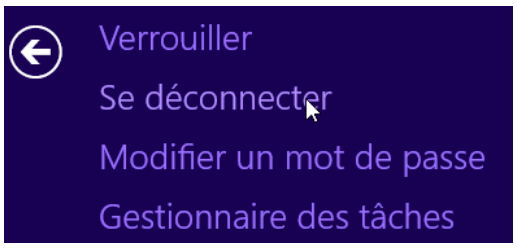


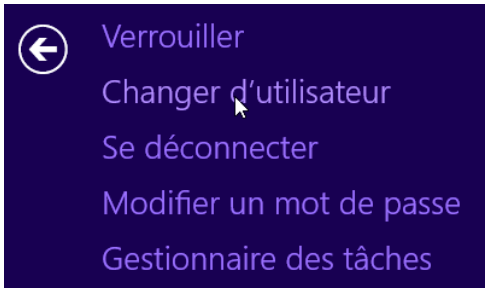
N.B: Cette fonctionnalité, extrêmement gourmande en ressource, pose certains problèmes avec des applications non spécifiquement dessinée pour **Windows 8**, et entraîne parfois des pertes de donnée …

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

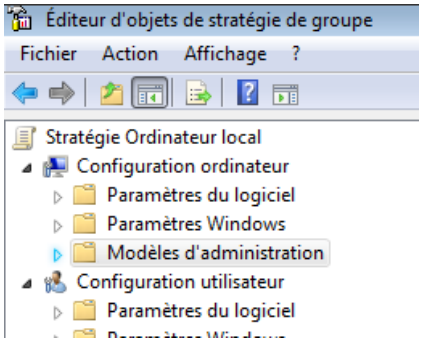
Désactiver la bascule rapide Utilisateur

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





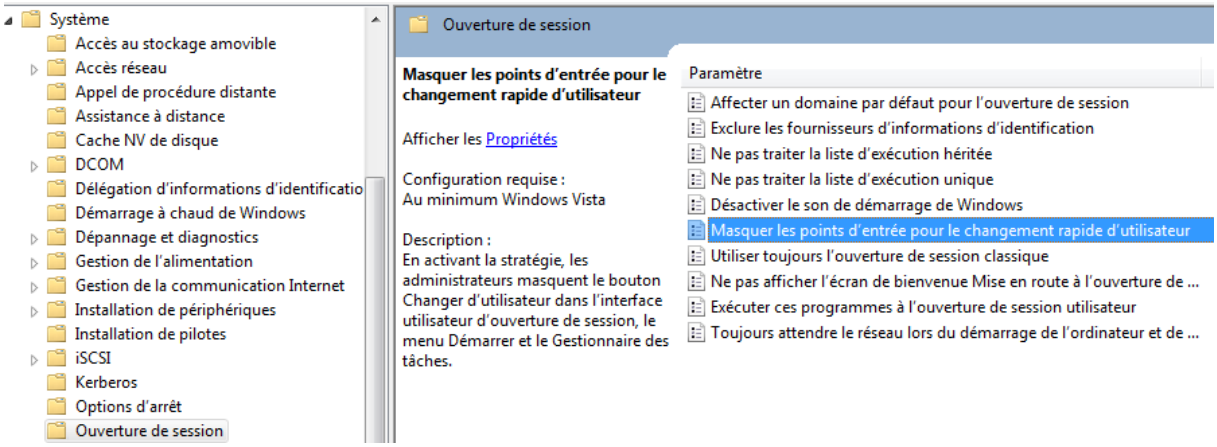
Soit on utilise **gpedit.msc**



Configuration ordinateur / Modèles d'administration

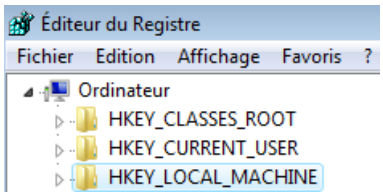
puis

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



ou alors Il faut passer par la base de registre

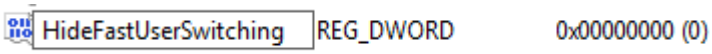
Regedt32.exe



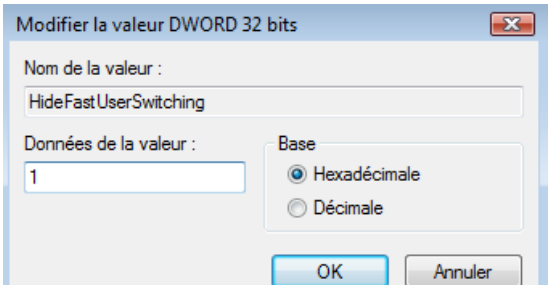
Et dans la clé

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Il faut créer la valeur DWORD : HideFastUserSwitching



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



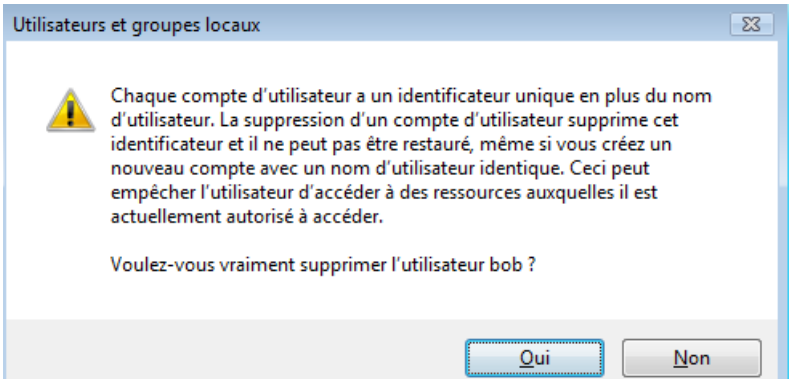
N.B : cette option est automatiquement activée si le poste fait partie d'un domaine. (par défaut la bascule entre utilisateurs locaux est activé sur un poste en workgroup)

SID Sécurity identifier :

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

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

Windows 10 se fonde sur les SID et pas sur les noms !



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

Whoami :

En tant que quoi on est logué ? **whoami (**ou **whoami /upn** ou **whoami /fqdn)**

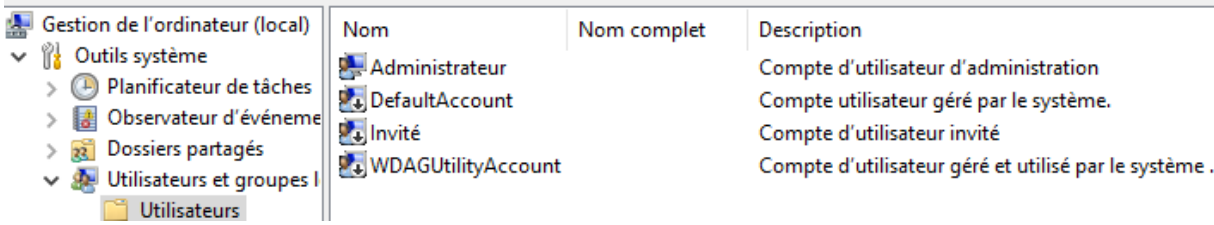
```
C:\Users\Administrateur>whoami
util-pc\administrateur
```

et le **SID** à titre d'information **whoami /user**

```
C:\Users\Administrateur>whoami /user

Informations sur l'utilisateur
------------------------

Nom d'utilisateur            SID
============================ ============================================
win-8-ent-x64\administrateur S-1-5-21-3539324183-3274001343-3598065848-500
```

Comptes Visibles pré-définis :

Il y a un changement important par rapport aux versions précédentes, seuls deux comptes sont crées. Sous **Windows 10** il existe 2 Comptes Utilisateurs prédéfinis



Le **Compte Administrateur** (celui d'origine):

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

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

Le **Compte Invité** :

Pour des utilisateurs occasionnels ayant un minimum de droits

- Ce compte par défaut est inactivé

N.B: dans la pratique, lors de l'installation d'un poste Windows 10 hors domaine, un assistant se déroule lors du premier démarrage, demandant les noms des "futurs" utilisateur du poste…. Cela a pour effet de créer des comptes utilisateur – administrateurs !

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

Comptes Invisibles système :

Il existe aussi des comptes invisibles, essentiellement

NT AUTHORITE\LocalService	Compte de service local

Un compte limité similaire au compte de service réseau mais qui se connecte au réseau en Anonyme.

NT AUTHORITE\NetworkService	Compte service réseau

Un compte de service beaucoup plus limité que le compte de Service local ou administrateurs mais qui peut accéder aux réseaux

AUTHORITE\LocalSystem ou NT AUTHORITY ou \LocalSystem	Compte système Local

Compte avec les privilèges les plus élevés sur Windows. Ce compte peut accéder aux réseaux comme n'importe quel utilisateur Windows local.

Utilisateurs locaux:

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

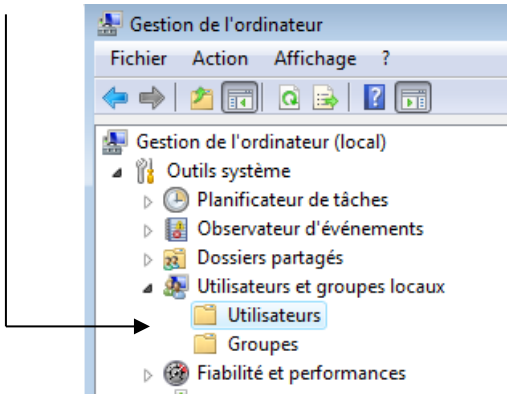
La meilleure façon pour faire cela se trouve dans le menu

Démarrer / Panneau de configuration (affichage classique)

/ Outils d'Administration/ Gestion de l'ordinateur

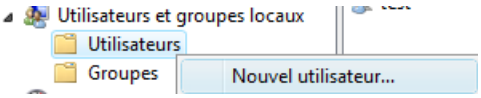
Ou plus rapidement par clic droit sur l'icône **Ordinateur** du bureau

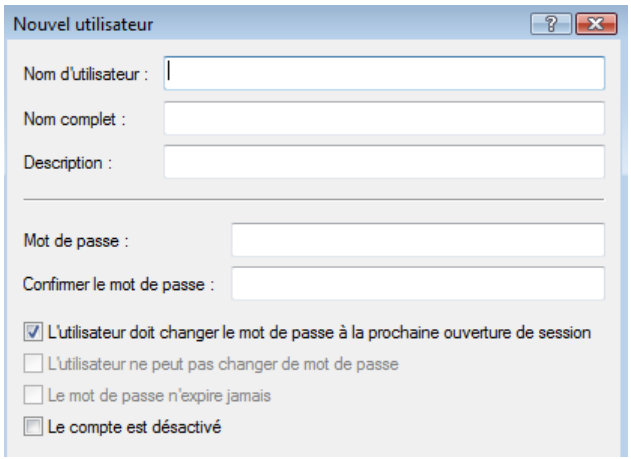
Sur l'icône **Ordinateur** du bureau on demande clic droit **gérer**



Pour créer un nouvel utilisateur il suffit de demander clic droit sur le dossier **Utilisateurs**,

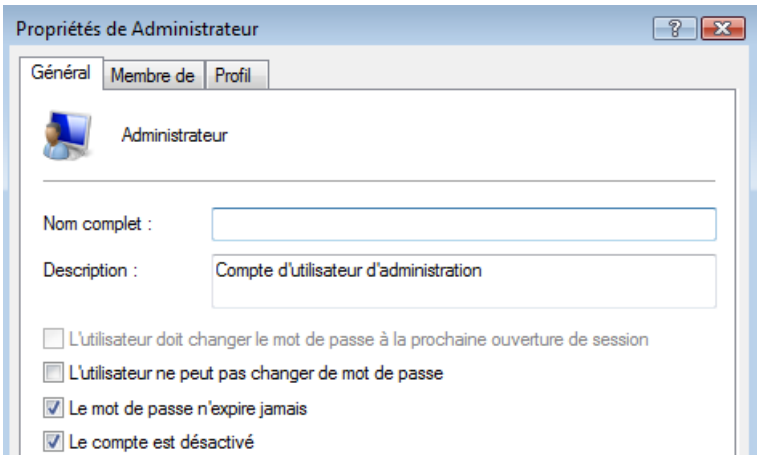
Puis **Nouvel utilisateur…**





Gestion des Comptes:

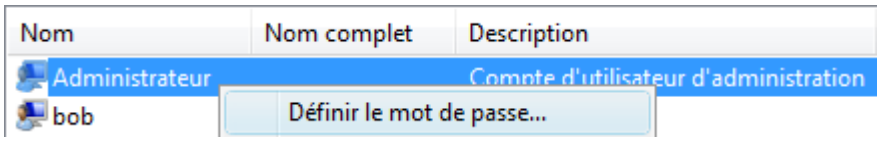
Le compte administrateur d'origine, est désactivé par défaut lors de l'installation. Comme on ne peut pas lui donner un mot de passe lors de l'installation, il faut impérativement lui en donner un lors de son activation !



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

Re-définition de mot de passe

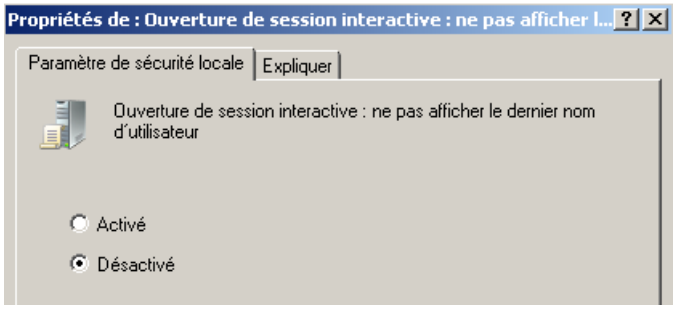
Si on en a les privilèges, on réinitialise le mot de passer d'un compte utilisateur en faisant clic-droit sur le compte à changer, puis on demande **Définir le mot de passe…**



Cacher le dernier Utilisateur

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

Stratégies de sécurité locales / Stratégies locales / Options de sécurité



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

GROUPES LOCAUX

Notions de groupes :

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

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

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

Un groupe possède un symbole qui est 

Groupes Locaux Prédéfinis :

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

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

Dans SEVEN on distingue trois types de comptes utilisateur

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

Liens Symboliques – Raccourcis – Jonctions :

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

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

Différence entre liens symboliques et raccourcis:

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

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

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

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

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

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

Objectif :

Les profils d'utilisateur présentent plusieurs avantages :

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

Les profils permettent de mémoriser notamment les paramètres suivants:

Explorateur Windows NT	Tous les paramètres définissables par l'utilisateur pour l'Explorateur Windows NT.

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

Profil Local:

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

Le profil local peut être créé à partir d'un profil local par défaut (modèle) stocké dans un dossier **Default** (depuis Windows 7) ou **Default User** (sous XP)

Emplacement Profils Locaux Seven:

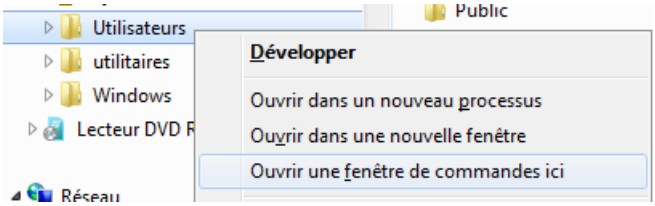
Les Profils Windows 10 ne sont pas stockés comme les profils XP:

XP (**Document and Settings**)	Windows 10 8 -7 (**Users** ou "***Utilisateurs***")

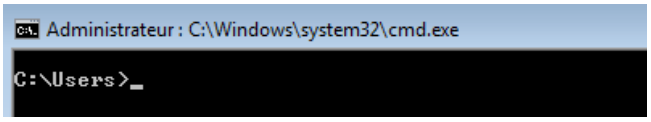
- Le dossier Racine des profils devient « visuellement » le dossier **\Utilisateurs** (selon la régionalisation française) mais se trouve être le dossier **\Users** (anciennement **\Document and Settings)**

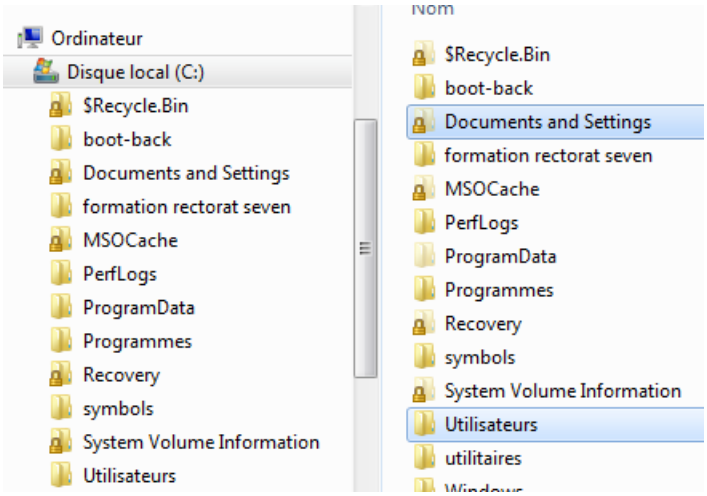
N.B : Avec la régionalisation de l'interface Windows, le dossier **Users** apparaît dans l'explorateur comme **Utilisateurs.** Mais on le retrouve en demandant

Clic-Droit / Ouvrir une fenêtre de commandes ici

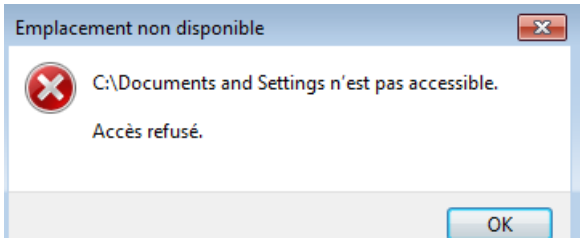


On obtiendra



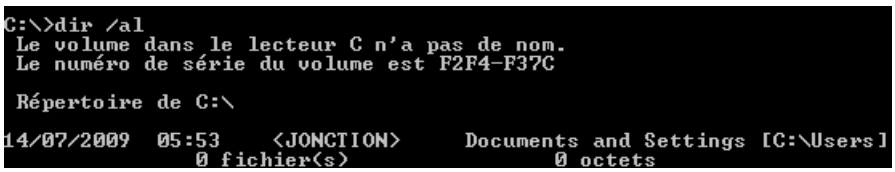


N.B : on ne peut plus « accéder » à **Documents and Settings**… ce dossier n'existe plus physiquement, c'est une "jonction" (lien) sur le dossier **user**…



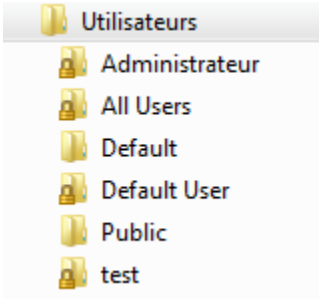
La commande en invite

dir /a ou mieux **dir /al** liste les jonctions…



Structure des Profils Windows 10 :

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



2 nouveaux dossiers système :

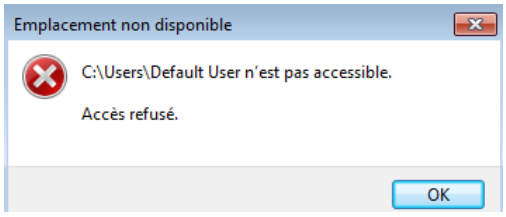
Default et **Public**

2 jonctions pour compatibilité XP-2000 :

Default User et **All Users**

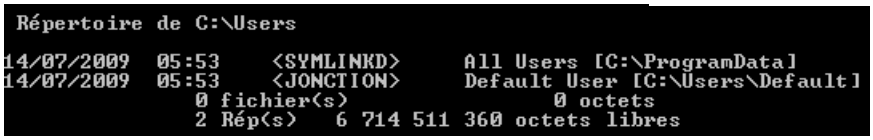
Et les dossier profils des utilisateur crées : Administrateur , test, xxxxx

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



La commande en invite

dir /a ou mieux **dir /al** liste les jonctions…

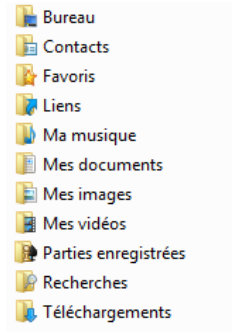


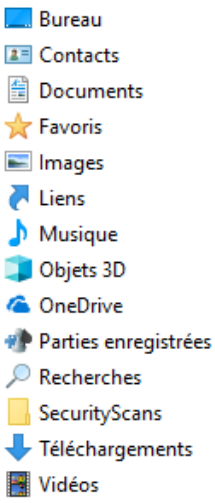
Structure d'un profil Utilisateur

Les principaux changements Windows 10-7 par rapport aux profils XP sont:

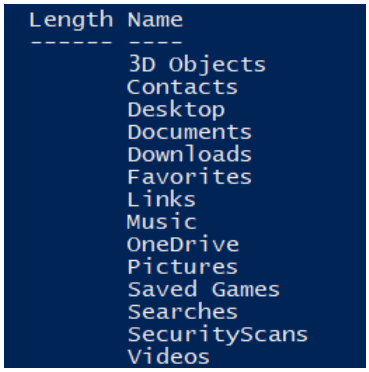
XP (**Document and Settings**)	Windows 10- 8 -7 (**Users** ou "***Utilisateurs***")
Pour un compte Donné nommé " ***Administrateur*** " Tout se trouvait dans **Document and Settings \ Administrateur**	Pour un compte Donné "***Administrateur***" désormais une partie se trouve sous **C:\Users\Administrateur** Et une autre partie se trouve dans **C:\Users\Administrateur \Appdata\Roaming\Microsoft\Windows**

- Les préfixes **mes** et **ma** sont supprimés des dossiers **document** ou **musique** (à la place de **mes document** ou **ma musique**
- Les dossiers **document** ou **musique…** ne sont plus des sous-dossiers du dossier mes documents, mais sont directement crées à la racine du dossier profils (en quelque sorte remise à plat de l'arborescence…)
- 5 nouveaux dossiers apparaissent dans le profil 10 Seven

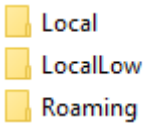




N.B : Les noms des dossiers physiques ne correspondent pas forcément. Avec la "régionalisation", on peut dire que :



Certaines entrées anciennement stockées sous XP directement dans le profil utilisateur sont maintenant depuis Windows 7 dans un sous dossier du profil utilisateur **Appdata**



\AppData\Roaming

\AppData\Local

\AppData\LocalLow

comme par exemple **AppData\Roaming\Microsoft\Windows**

Menu Démarrer **Appdata\Roaming\Microsoft\Windows\Start Menu**

Modèles **Appdata\Roaming\Microsoft\Windows\Templates**

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

Le dossier **AppData** contient 3 sous-répertoires nommés **Local, LocalLow et Roaming**, jouant chacun un rôle spécifique :

• **Roaming** : contient les données "itinérantes" de l'utilisateur, c'est-à-dire celle qui potentiellement le suivent d'une ordinateur à un autre, indépendamment de la machine utilisée.

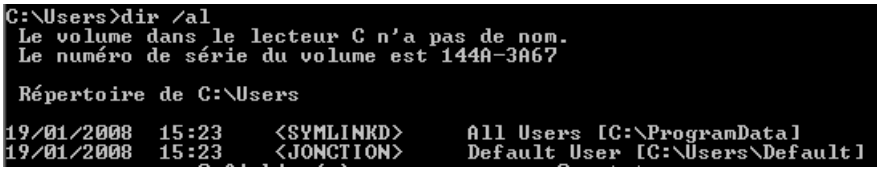
• **Local** contient les données spécifiques à un ordinateur, c'est-à-dire des données que le développeur d'une application ne souhaite pas voir synchronisées entre différentes machines. Il peut s'agir de données de cache ou des paramètres purement locaux. Notez que si votre ordinateur n'appartient pas à un domaine, il n'y a pas de différence fondamentale entre Roaming et Local.

• **LocalLow** est similaire au dossier Local si ce n'est qu'il est destiné à des applications ayant uniquement besoin d'écrire des données, mais séparément du reste des données afin qu'elles n'aient pas accès à d'autres informations. C'est le cas par exemple du mode Privé de Internet Explorer.

Profil par Défault

Les principaux changements depuis Seven par rapport aux profils XP sont :

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



Méthode Certifiée pour modifier le profil par défaut

Il n'est plus possible dans Windows 10 selon Microsoft de modifier le profil par défaut comme on le faisait dans XP ni avec windows enabled comme on pouvait encore le faire dans Seven.

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

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

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

Profil Public (ex-all users)

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

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

```
C:\Users>dir /al
 Le volume dans le lecteur C n'a pas de nom.
 Le numéro de série du volume est 144A-3A67

 Répertoire de C:\Users

19/01/2008  15:23    <SYMLINKD>     All Users [C:\ProgramData]
19/01/2008  15:23    <JONCTION>     Default User [C:\Users\Default]
```

XP (**Document & Settings**)	Windows 10 (**ProgramData** et **Users**)
All users	En partie dans **C:\ProgramData** plus exactement **C:\ProgramData\Microsoft\Windows** Et l'autre partie dans **C:\Users\Public**

Ce dossier **ProgramData** contient tous les liens pour compatibilité antérieure

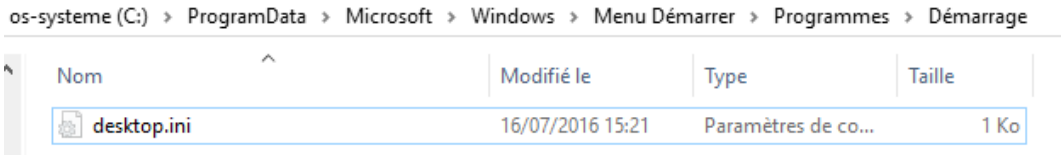
```
 Répertoire de C:\ProgramData

14/07/2009  05:53    <JONCTION>     Application Data [C:\ProgramData]
18/02/2010  09:25    <JONCTION>     Bureau [C:\Users\Public\Desktop]
14/07/2009  05:53    <JONCTION>     Desktop [C:\Users\Public\Desktop]
14/07/2009  05:53    <JONCTION>     Documents [C:\Users\Public\Documents]
18/02/2010  09:25    <JONCTION>     Favoris [C:\Users\Public\Favorites]
14/07/2009  05:53    <JONCTION>     Favorites [C:\Users\Public\Favorites]
18/02/2010  09:25    <JONCTION>     Menu Démarrer [C:\ProgramData\Microsoft\Windows\Start Menu]
18/02/2010  09:25    <JONCTION>     Modèles [C:\ProgramData\Microsoft\Windows\Templates]
14/07/2009  05:53    <JONCTION>     Start Menu [C:\ProgramData\Microsoft\Windows\Start Menu]
14/07/2009  05:53    <JONCTION>     Templates [C:\ProgramData\Microsoft\Windows\Templates]
```

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

1° partie : stockée en **ProgramData\Microsoft\Windows**

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

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



2° partie : stockée en **Users\Public**

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

- pour poser des raccourcis ou dossiers ou documents sur le Bureau de tout le monde il faut aller en **c:\Users\Public\Desktop**

N.B: les autres entrées **users\public** correspondent à des fonctionnalités de partage réseau simplifié, en environnement personnel

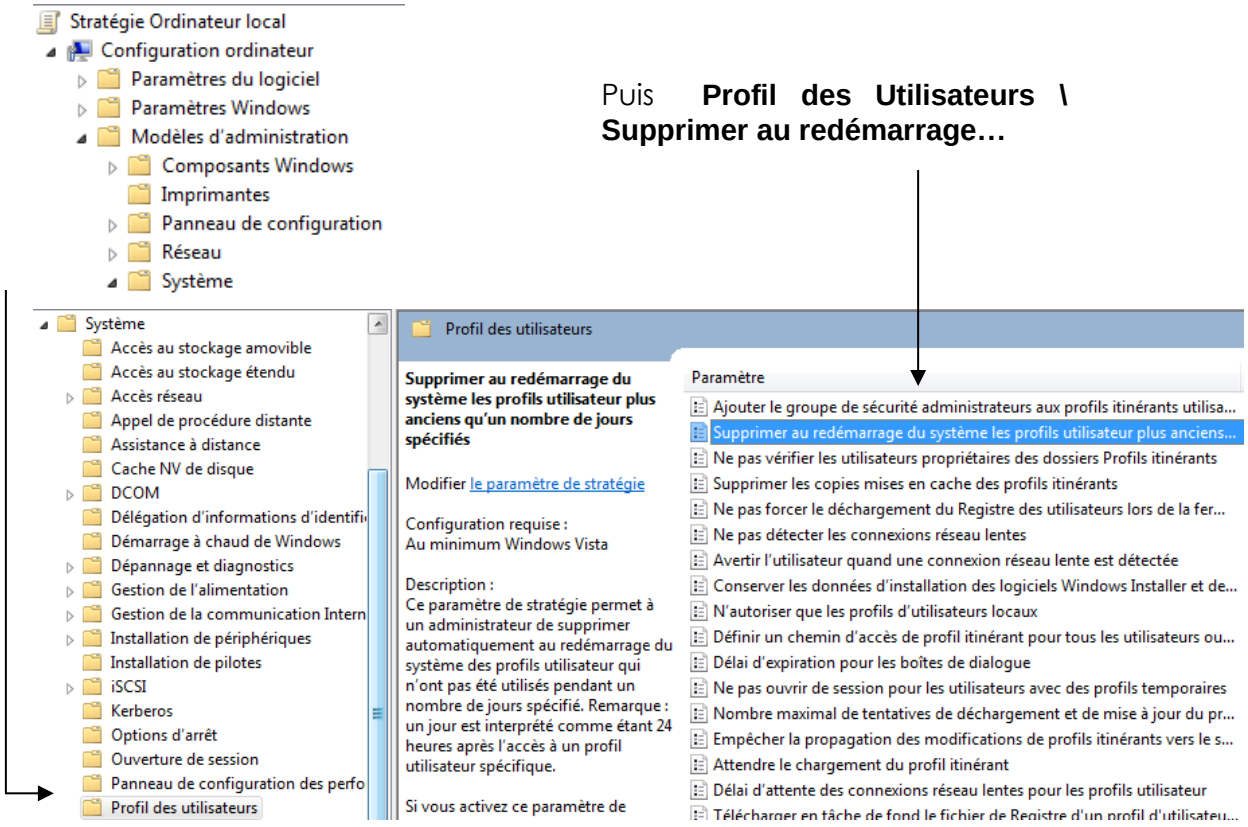
---

Supprimer tous les profils locaux Windows 10:

Par GPO

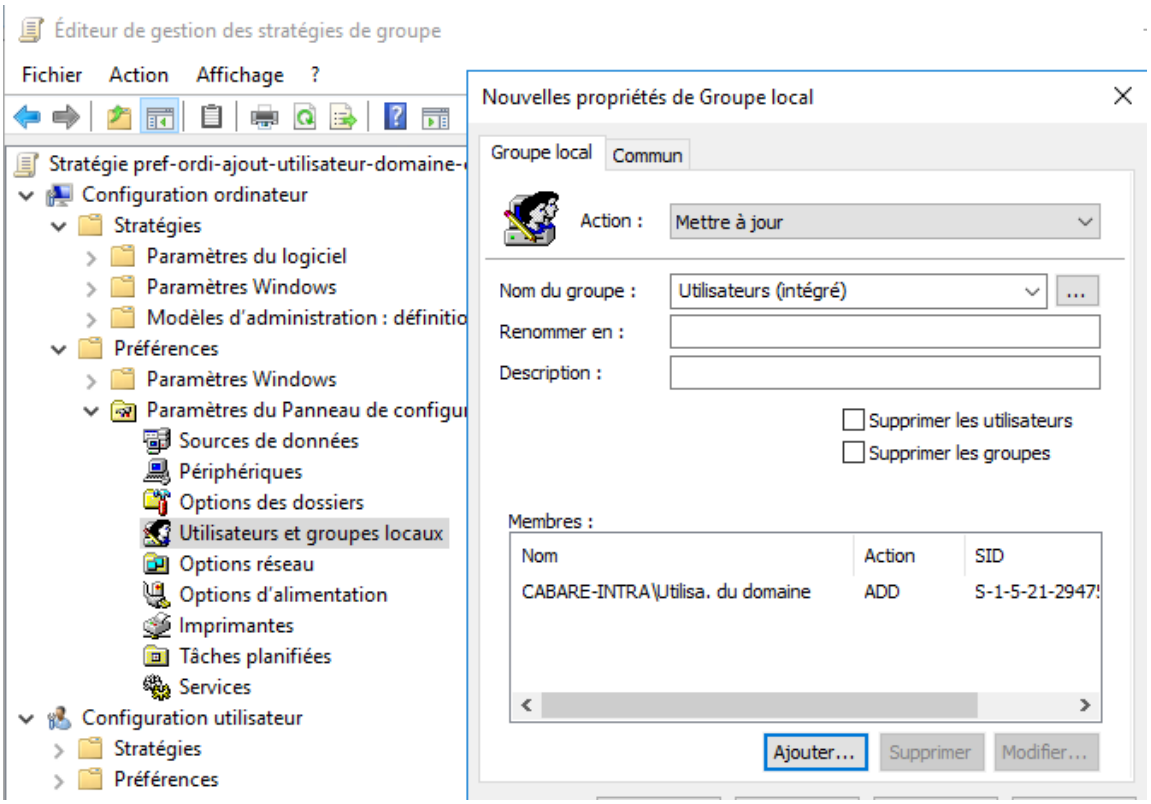
On peut passer par une GPO, ou bien **Gpedit.msc**

Configuration ordinateur \ modèles d'administration\ Système



Puis **Profil des Utilisateurs \ Supprimer au redémarrage…**

Mais il faut absolument ajouter les comptes utilisateur du domaine dans le groupe local des utilisateurs (voire invité)



Par base de registre

En effacant les entrées dans

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Profile List

Par utilitaire delprof2

Un nouvel utilitaire remplace l'ancien delprof obsolète depuis Seven

Delprof2 – User Profile Deletion Tool

Delprof2 is the unofficial successor to Microsoft's Delprof which does not work with operating systems newer than Windows XP. Here are the main facts:

```
C:\Users\Administrateur\Desktop\Delprof2 1.6.0\Delprof2 1.6.0>delprof2 /l

DelProf2 by Helge Klein (http://helgeklein.com)

Listing inactive profiles on 'PORTABLE-10'.

Ignoring profile '\\PORTABLE-10\C$\Users\Default' (reason: special profile)
Ignoring profile '\\PORTABLE-10\C$\Users\Public' (reason: special profile)
Ignoring profile '\\PORTABLE-10\C$\Users\Administrateur' (reason: in use)

The following user profiles match the deletion criteria:

\\PORTABLE-10\C$\Users\Administrateur.CABARE-INTRA
```

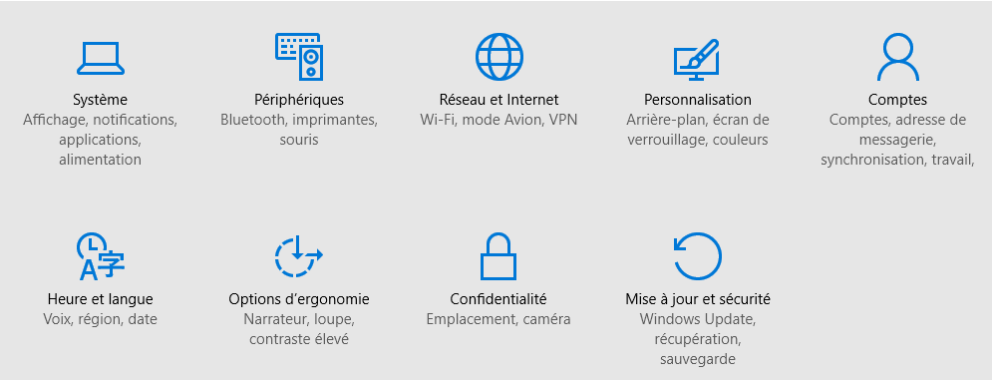
Suivit de

```
C:\Users\Administrateur\Desktop\Delprof2 1.6.0\Delprof2 1.6.0>delprof2 /q
```

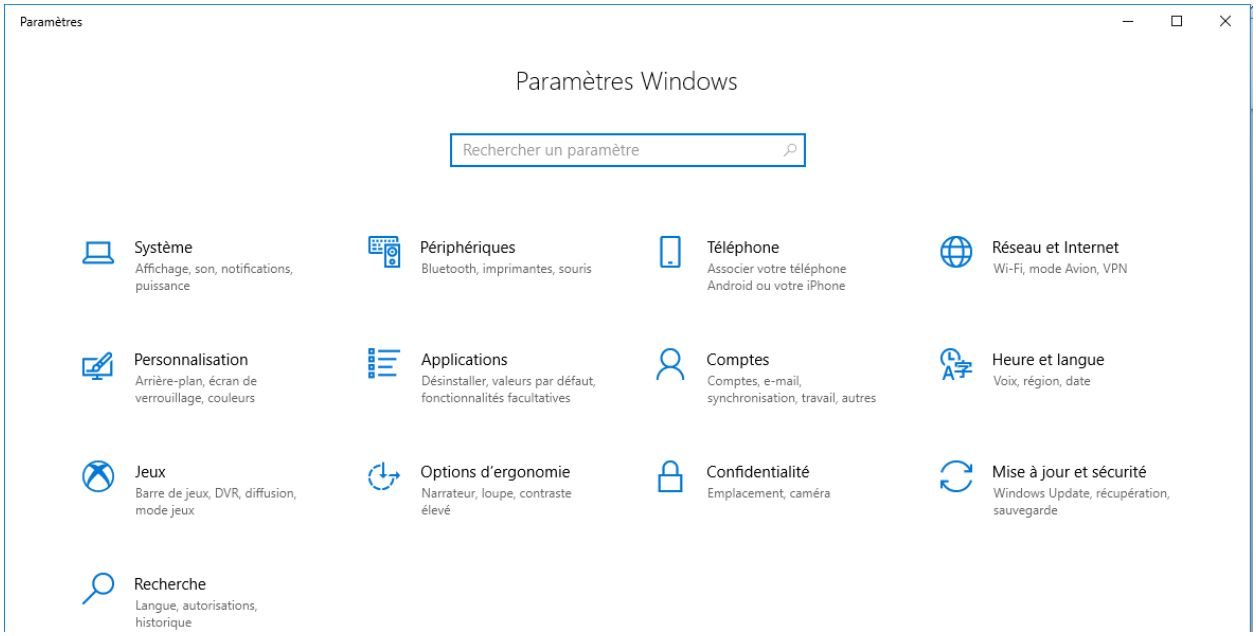
Accès Paramètres Windows 10:

Le contenu s'étoffe de build en build

Sous 1511, 9 entrées



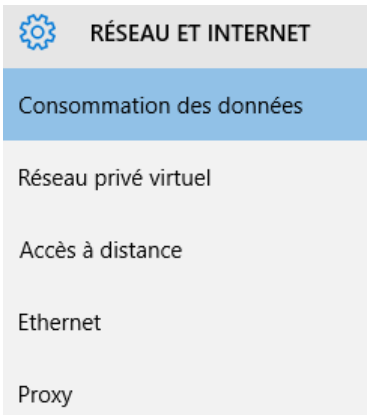
Sous 1803, 12 entrées



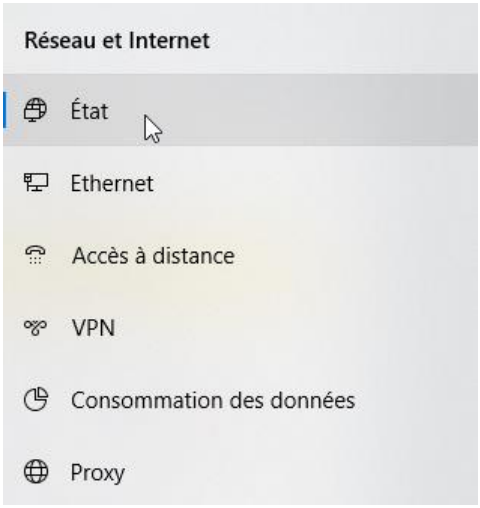
Et les entrées sont de plus en plus complètes

Réseau et internet :

1511



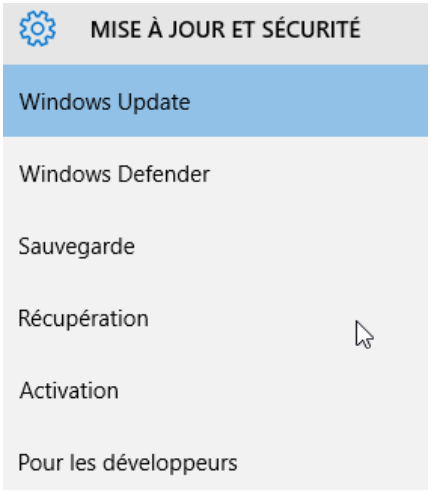
1803



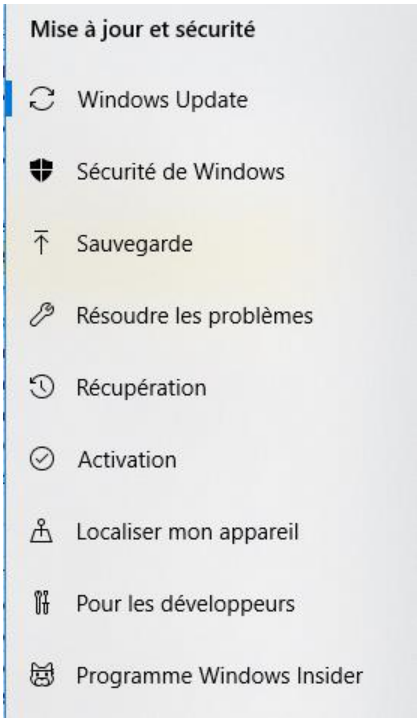
Dans **Ethernet** une réinitialisation du réseau…

Mise à Jour et Sécurité

1511



1803



Dans **Résoudre les problèmes** toute une multitude d'assistants

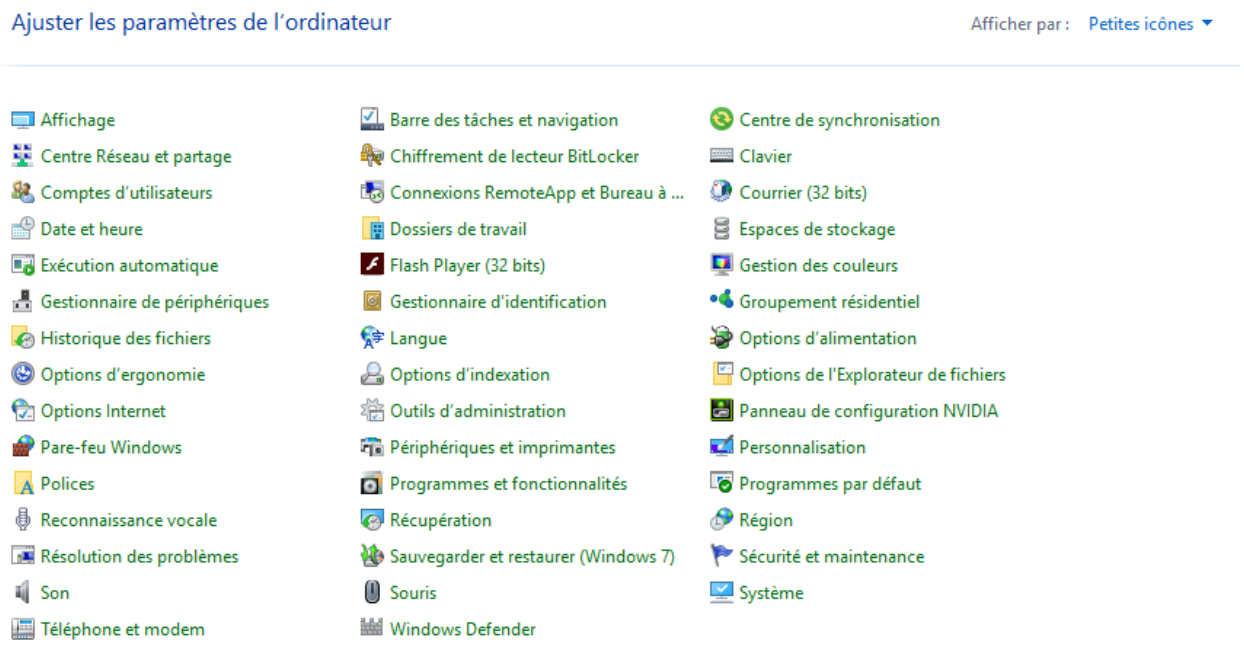
Panneau de Configuration style 7:

Microsoft veut à terme abandonner son panneau de configuration traditionnel

L'accès

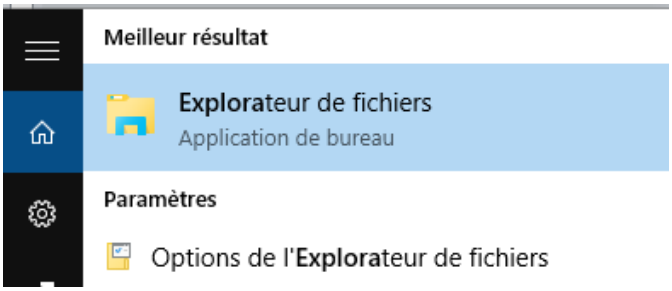
Affichage **WIndows 10** par catégories

Affichage **Windows 10** par petites icones



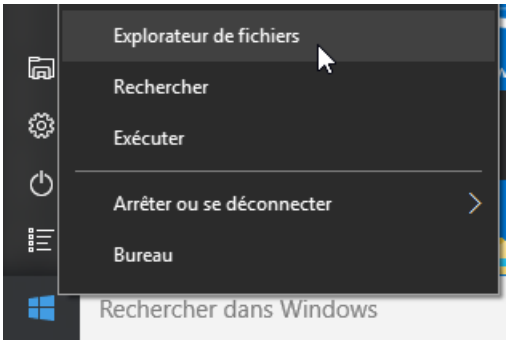
L'explorateur Windows:

On lance l'explorateur soit via la recherche **cortana**

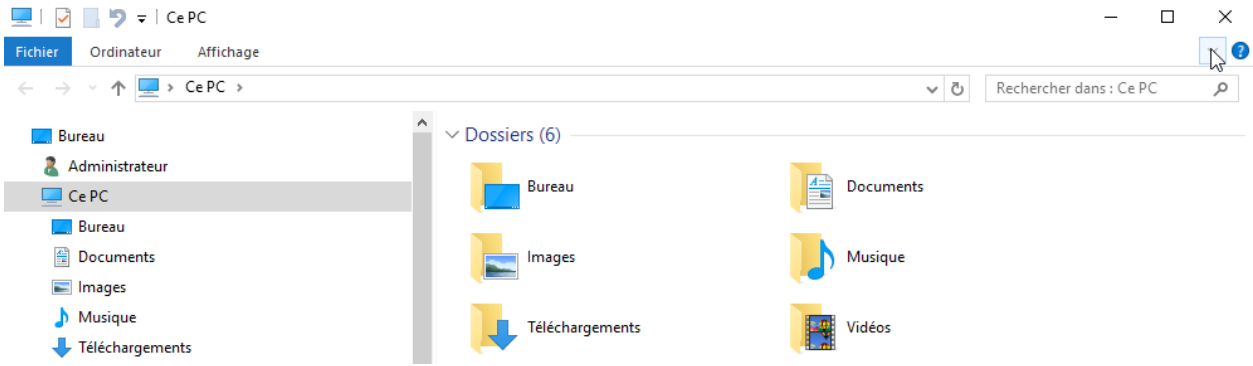


i

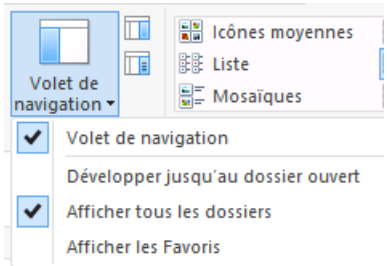
Soit clic / droit **Explorateur de fichier** dans la barre des tâches en bas à gauche sur l'icône Windows



Ce qui donne



par rapport à l'aspect par défaut de l'explorateur windows on peut modifier notamment dans **Affichage / le Volet de navigation**



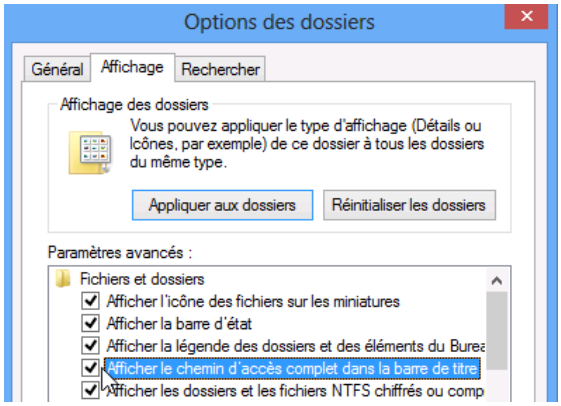
Volets de Navigation

Afficher tous les dossiers

Pas de Favoris

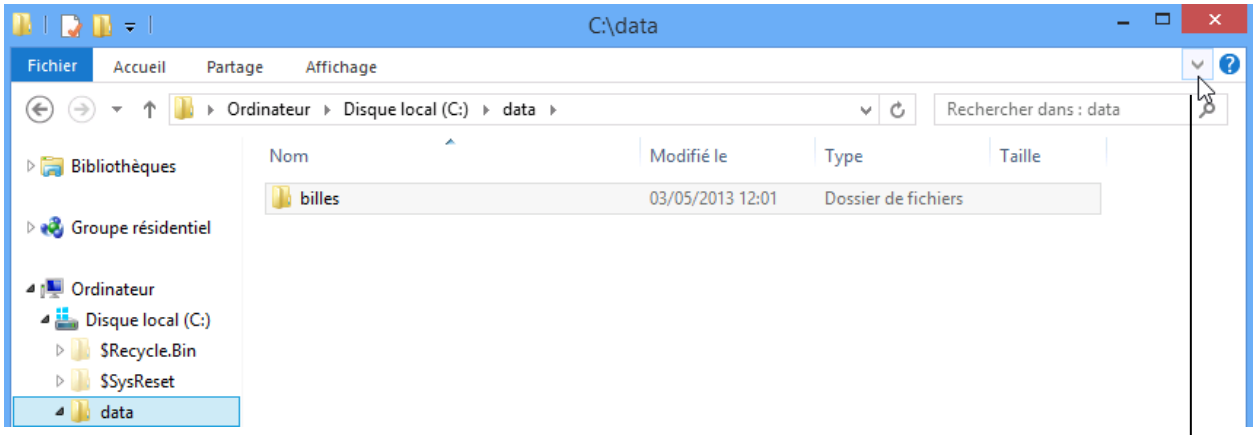
Toujours dans **Affichage / Option on demande Modifier les options des dossiers**

onglet **Affichage**

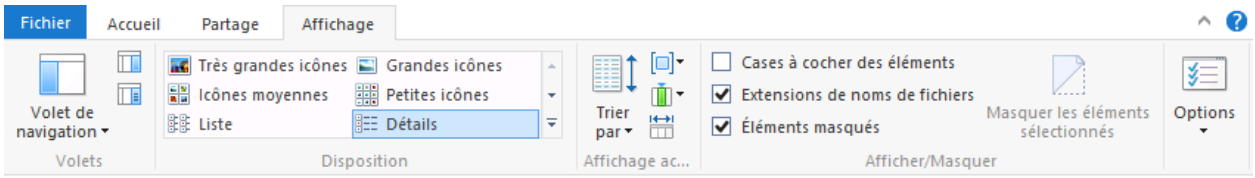


Afficher le chemin d'accès complet
Ne pas masquer les extensions
Ne pas masquer les fichiers cachés
Ne pas masquer les lecteurs vides
Ne pas masquer les fichiers systèmes
Ne pas utiliser l'assistant partage

Ensuite pour le **Ruban** c'est une affaire de choix …

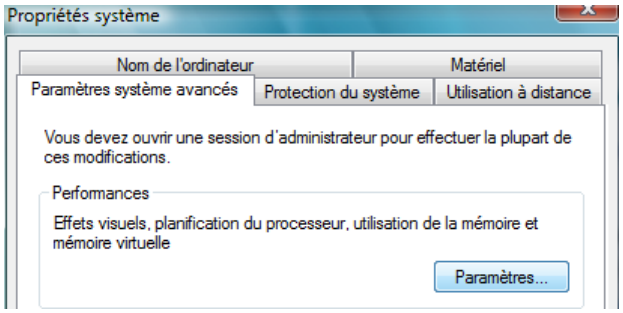


Se développe en

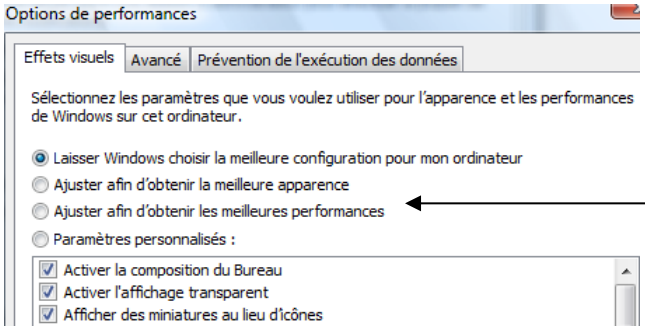


Interface Aero:

Les réglages dits « AERO » sont disponibles dans les **propriétés ordinateur**, dans **Paramètres systèmes avancés - Performances**



donnant



Pour Désactiver AERO on demande d'obtenir les meilleures performances

(Sans effet 3D à gogo…)

NB : **ALT+TAB** pour passer d'une application à l'autre gère désormais le **bureau**

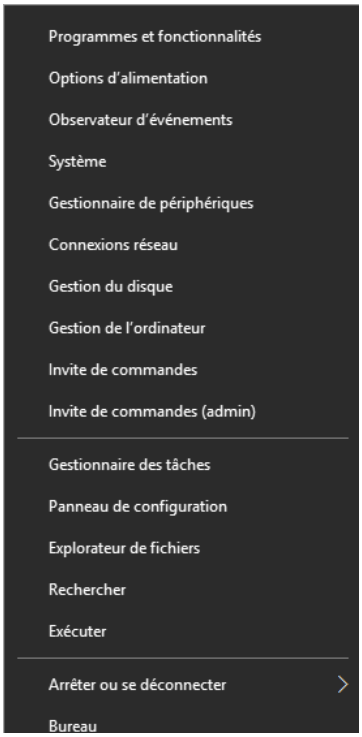
Menu Contextuel / Accueil Win+X

En bas à gauche, sur l'icône **Accueil** (lorsqu'elle apparaît)

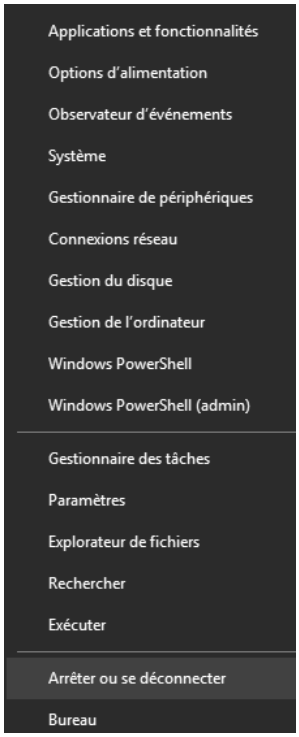
on retrouve quasiment à l'identique le menu Contextuel de l'ancien **Menu Démarrer**…

Ce Menu dit **Win+X** est modifiable selon une procédure particulière, cf chapitre suivant spécifique **Menu Win-X**

V 1511



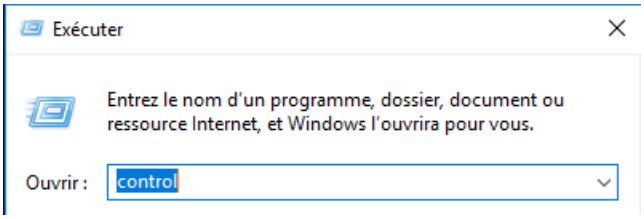
V 1803



Evolution notables :

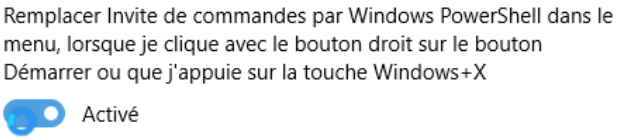
- Disparition de l'accès direct au **Panneau de configuration**

  Qui reste accessible via **executer** control



- Invite **Powershell** à la place de l'invite de commande

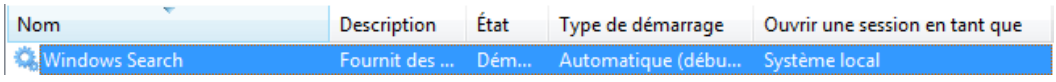
  l'invite de commande peut se redemander via **Paramètres, Personnalisation / barre des tâches** dans laquelle on va trouver

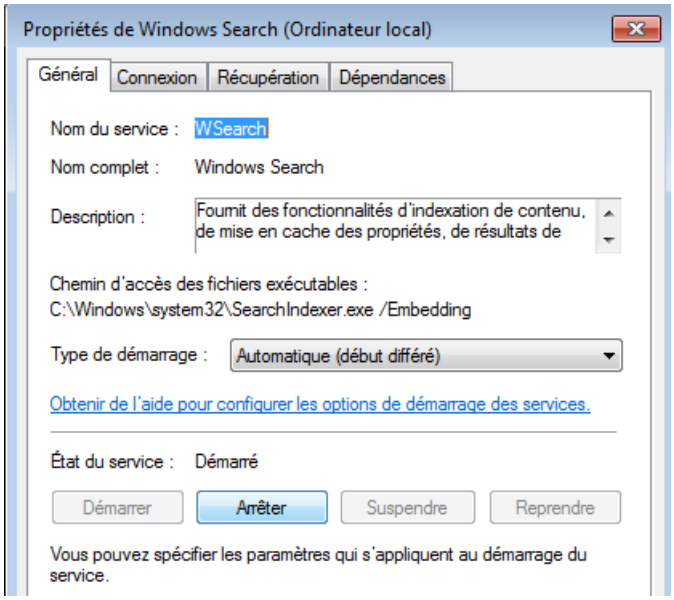


Compromis Performances – arrêt services:

Certaines fonctionnalités de Windows 10 sont « gourmandes », et par conséquent peuvent être désactivées si besoin, comme l'indexation automatique :

On peut arrêter le service : **Windows Search**



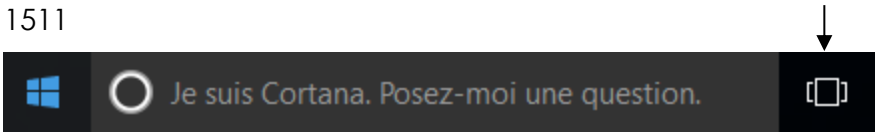


Bureaux Virtuels:

On peut disposer de plusieurs bureaux virtuels pour segmenter les environnements (perso / boulot) :

Le point d'entrée des bureaux virtuels est la 3° icone ne partant de la gauche dans la barre des tâches

Build 1511

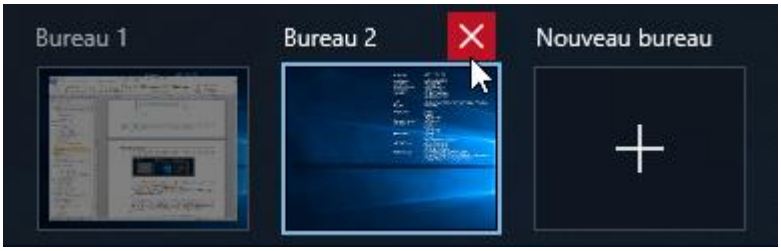


Build 1803

Cela permet de visualiser sur le haut (ou le bas) de l'écran

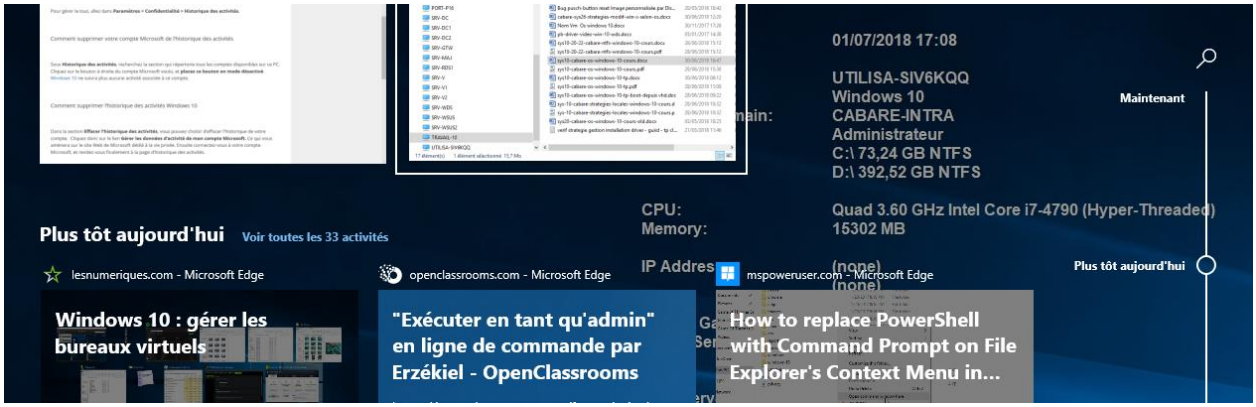
- Accéder au menu des bureaux virtuels et aux programmes en cours d'exécution : **Touche Windows + TAB**
- Créer un bureau virtuel : « **WIN + CTRL + D** »
- Passer d'un bureau virtuel à un autre très facilement : « **WIN + CTRL + flèches gauche et droite** »

N.B : Vous pouvez supprimer un poste de travail virtuel à tout moment en cliquant sur le "X" en haut à droite du bureau que vous voulez fermer. Cela transférera tous les programmes et applications sur le bureau à gauche de son emplacement dans la vue des tâches.



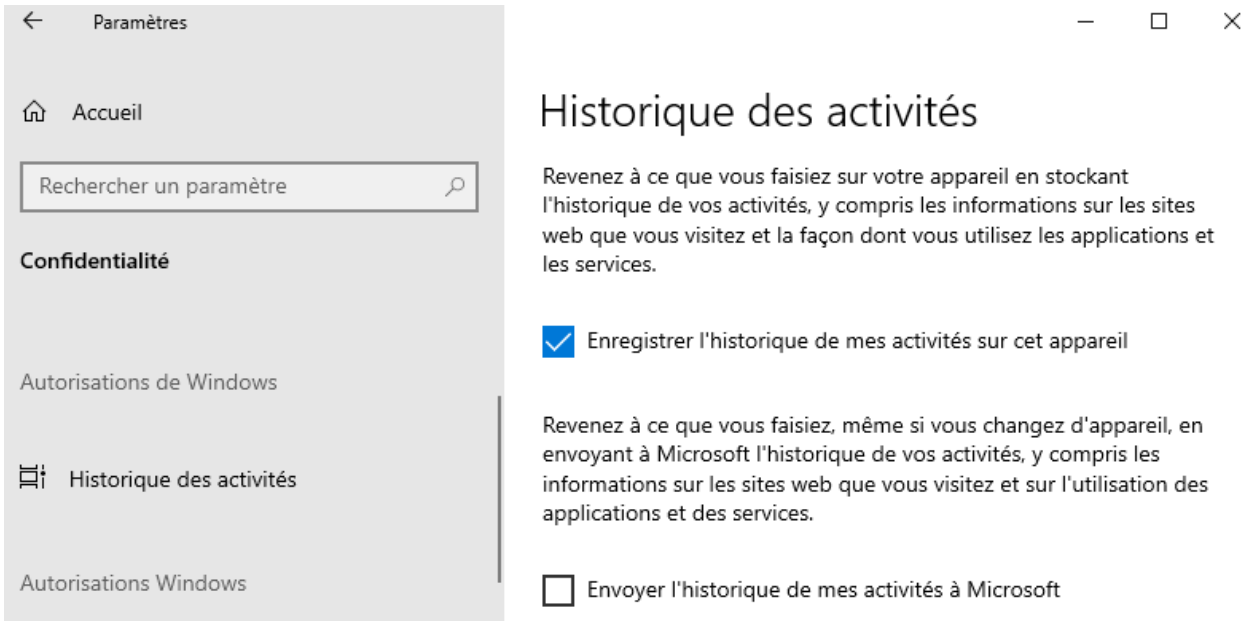
Historique des Activités – Timeline - ospolicy.admx

Windows 10 build 1803 est capable en plus de gérer un **historique des activité**



Que l'on peut effacer ou interdire via l'interface graphique dans

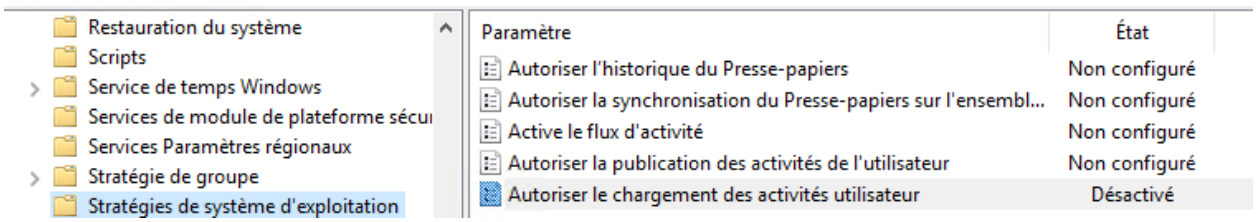
Paramètres, Confidentialité puis **Historique des activités (Historique de mes activités sur cet appareil)**



2 GPO existent

Configuration Ordinateur / Modèle d'administration / Système / stratégies de système d'exploitation

Avec respectivement **Autoriser la publication des activités de l'utilisateur** et **Autoriser le chargement des activités de l'utilisateur**



Ici on autorise la gestion de l'historique localement sur la machine, mais on s'interdit le stockage sur le Cloud Microsoft (le cas échéant)

Publication non configurée (autorisée)
Chargement désactivé (interdit)

Dans le doute, on peut désactiver les 2

Dans ce cas ne pas prêter attention au BUG d'affichage (case cochée mais grisée)

MENU WIN-X

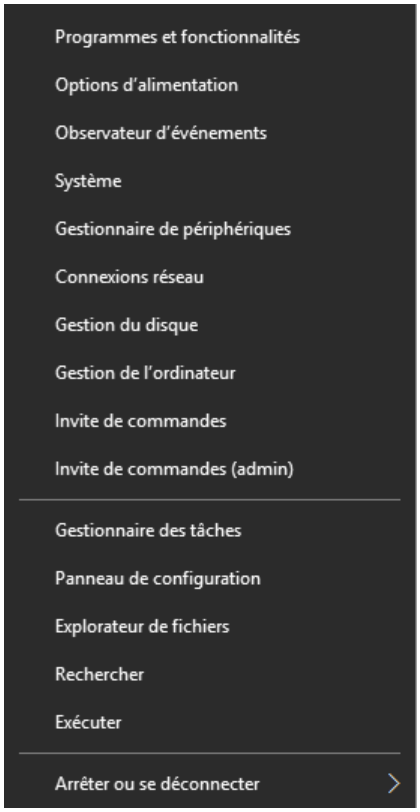
Gestion accès rapide:

Par défaut sur windows 10

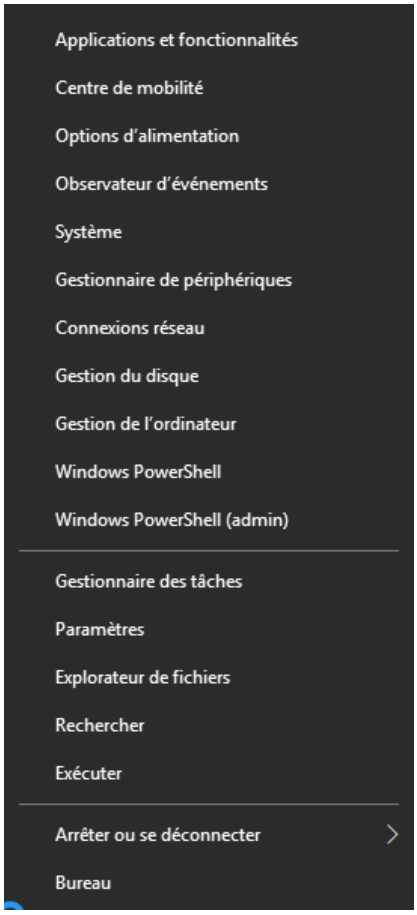
On y accède via les touches Windows + X

Ou clic bouton droit sur le menu démarrer

Menu **Win-X** sur 10-1511

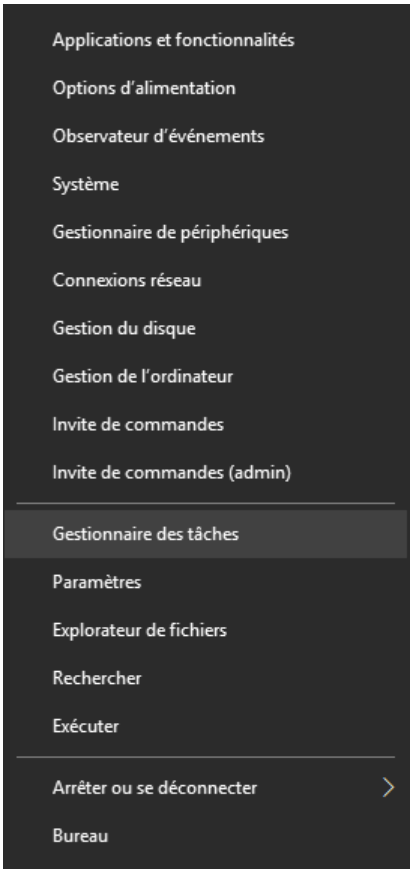


Menu **Win-X** sur 10-1709



On perd le **panneau de configuration**

Menu **Win-X** sur 10-1803



On perd le **centre de mobilité**

Choix entre **Cmd** et **Powershell**

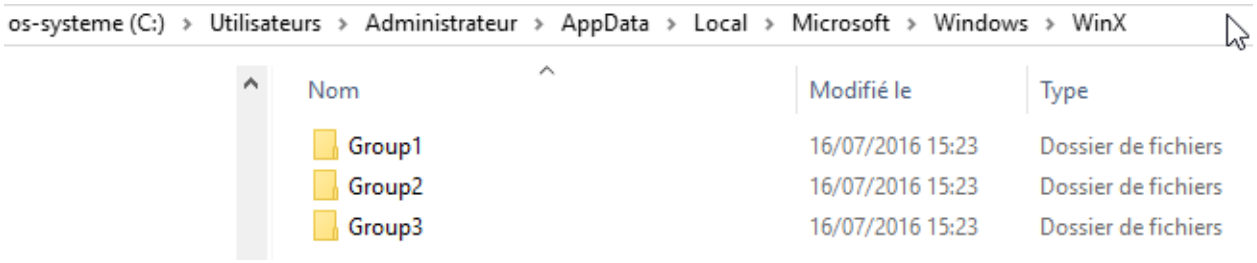
Forcément on peut avoir envie de retrouver toujours les même entrées, indépendamment des releases OS, par exemple :

- L'invite de commande(admin)
- L'accès au panneau de configuration

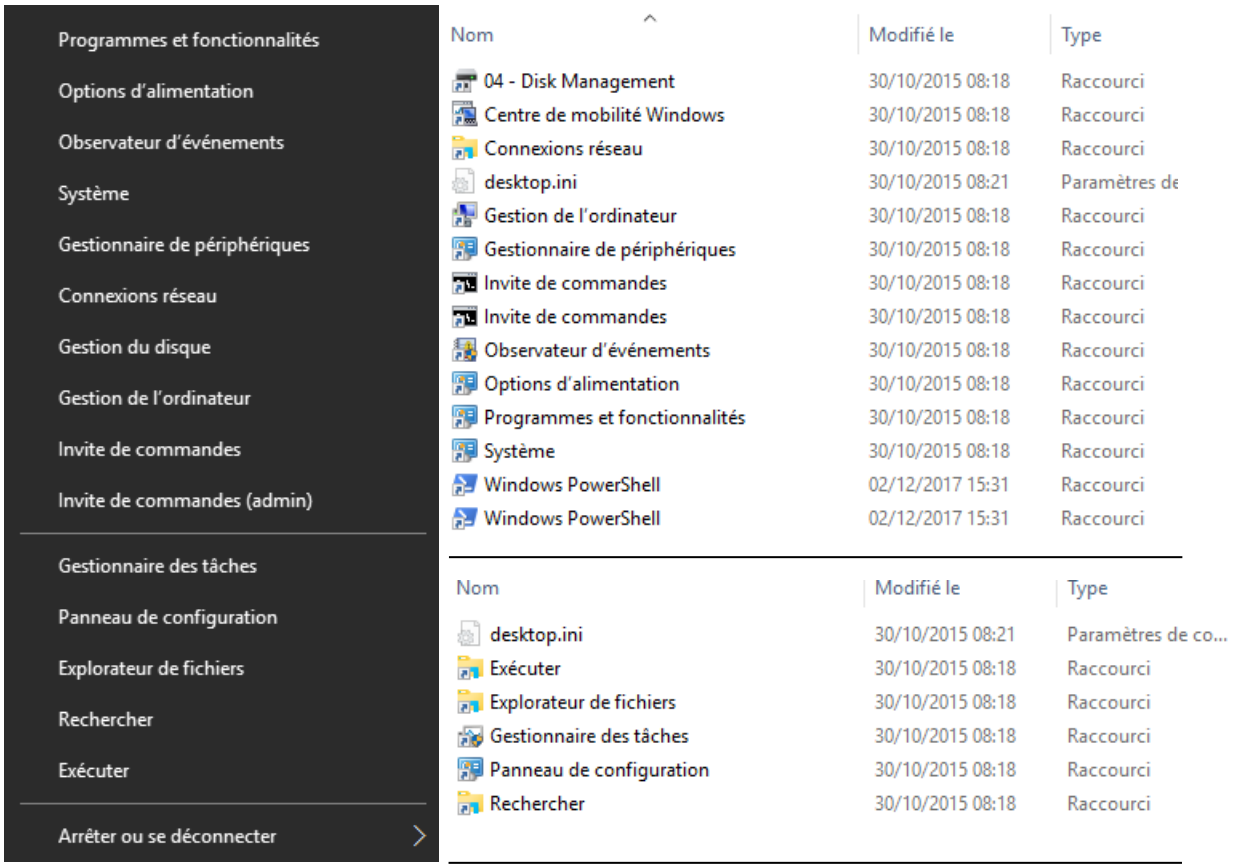
Structure Menu Windows-X

Les raccourcis sont stockés pour 1utilisateur (ici dans l'exemple Administrateur) en **C:\users\Administrateur\Appdata\Local\Microsoft\Windows\WinX**

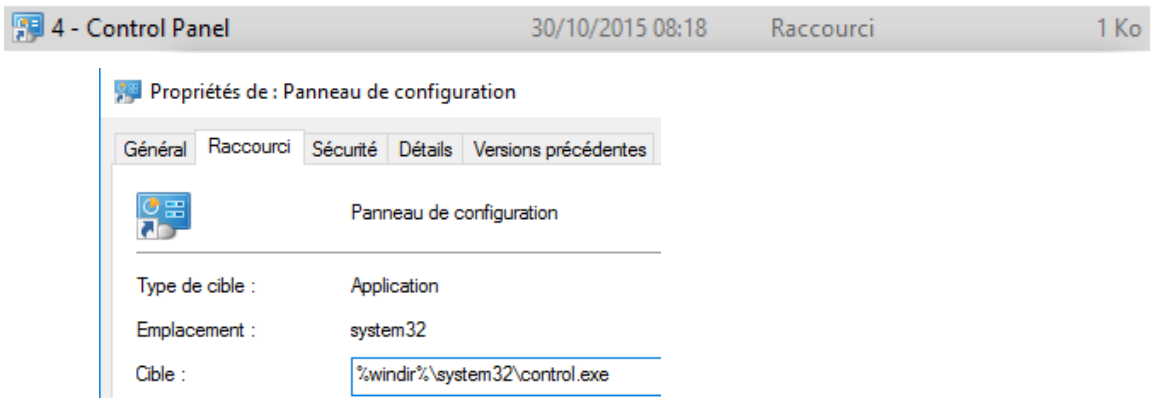
Correspondant à



les groupes contiennent des **Raccourcis + Ashcodes** (non modifiables)

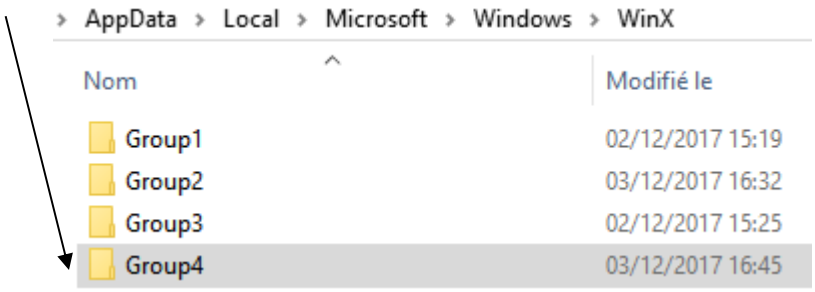


Le raccourci du panneau de configuration (récupéré sur un **menu Win-x** d'un **windows 1511** par exemple) étant le suivant

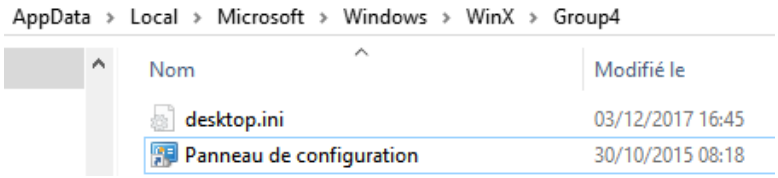


Test Modification Menu Win-X windows 10 (1709 – 1803)

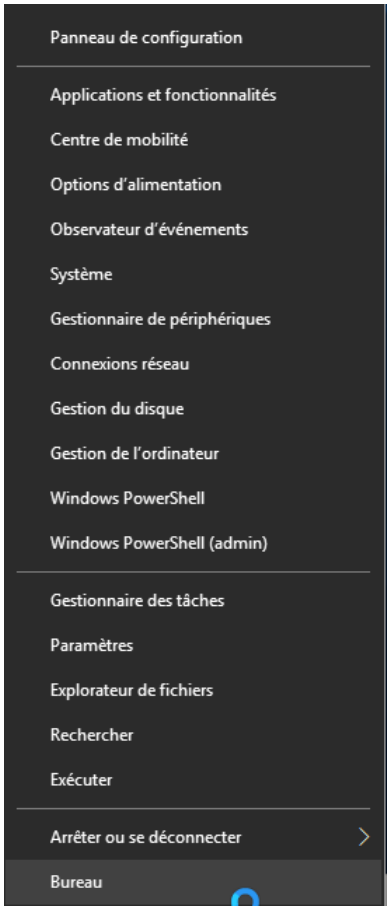
Sur un poste **Windows** pour lequel dans le **menu-X** le **panneau de configuration** à disparu (build majeur 1709-1803), on peut rajouter un 4° groupe,



Contenant le raccourci du panneau de configuration récupéré précedemment !



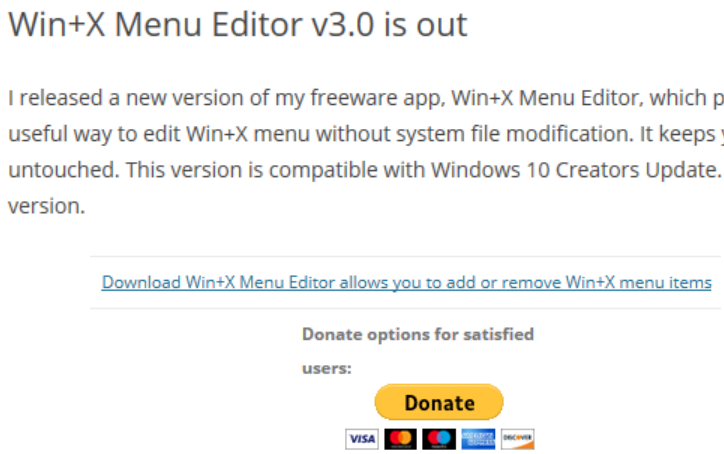
Ce qui devrait amener, après un re-démarrage, le menu **Win-X** modifié suivant



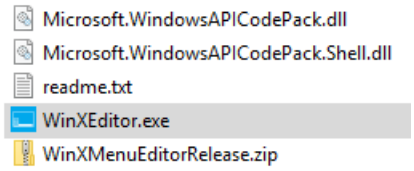
N.B : <u>on ne peut pas ajouter des raccourcis classiques</u> pour étoffer les **Win-X menu**, il faut récupérer des raccourcis spéciaux … Ceci car Microsoft à intégrer un **ahscode** sur les raccourcis de ce menu, pour que justement il ne soit pas modifiable facilement.

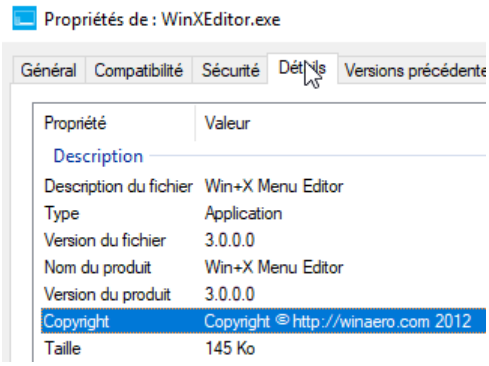
Ceci dit, maintenant que l'on a compris ou étaient stockées les entrées, on va pouvoir utiliser un petit Utilitaire **Win-X Editor** , pour générer ces raccourcis !

Récupérable sur le site de **winaero** et testé jusqu'à la version 1703



On récupère la version 3

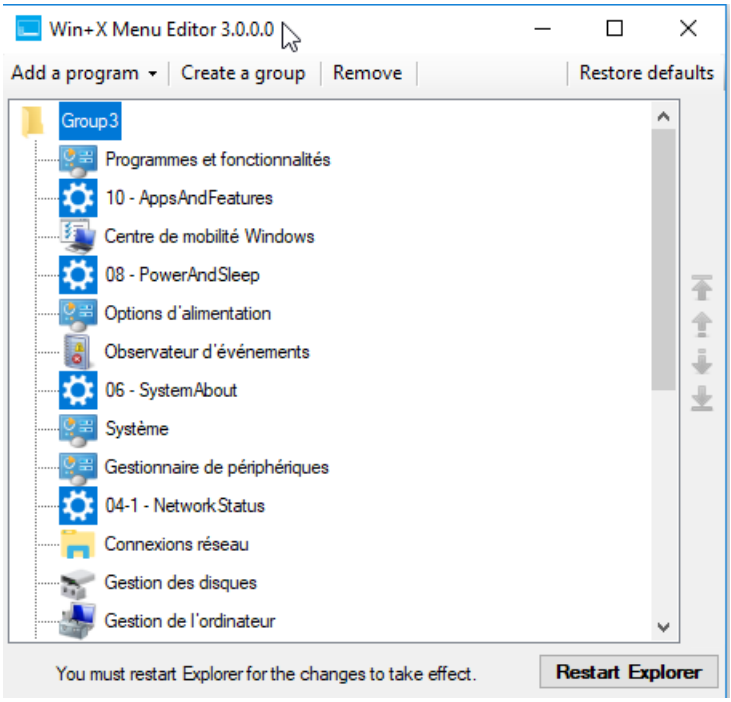




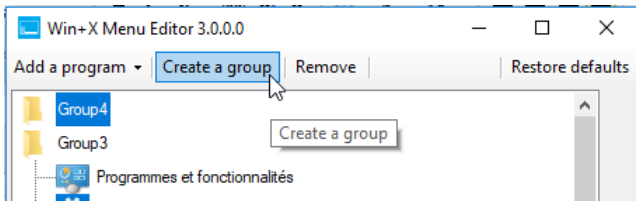
Et on le lance via l'executable **WinxEditor.exe**

Les entrées par groupe apparaissent, avec la possibilité

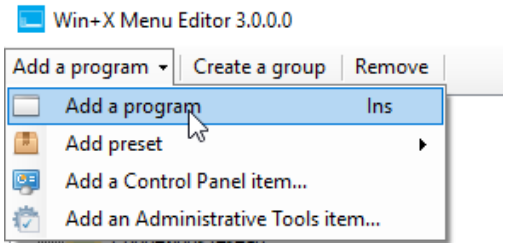
- de créer / gérer des groupes
- Ajouter un programme via un executable
- Ajouter un programme parmi ceux proposés



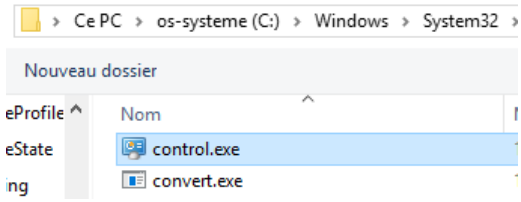
Ajouter un groupe

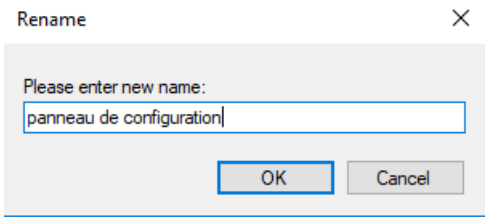


Ajouter un executable

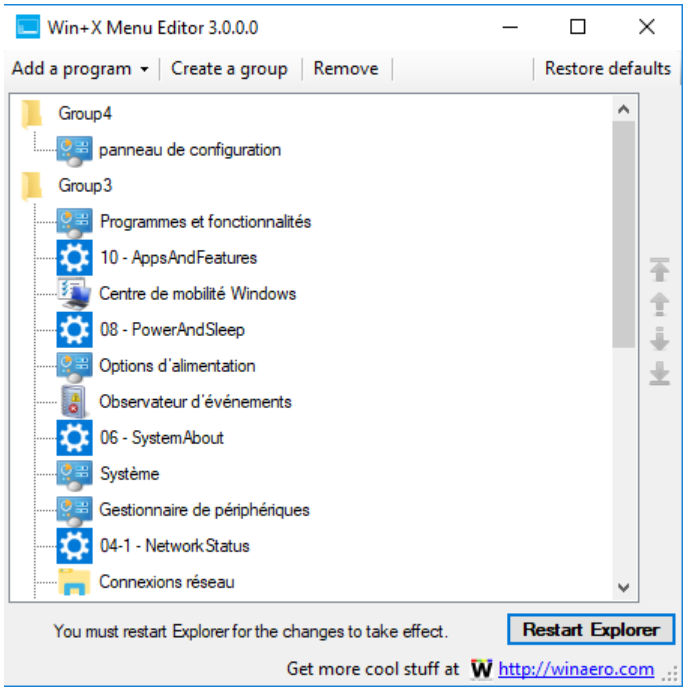


on va chercher un executable, donne un nom



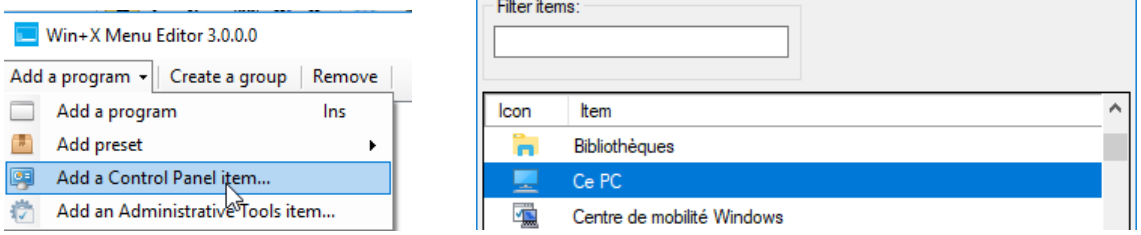


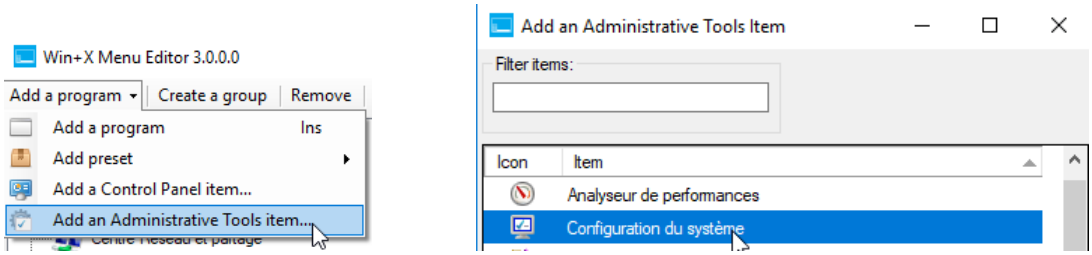
Et on obtient



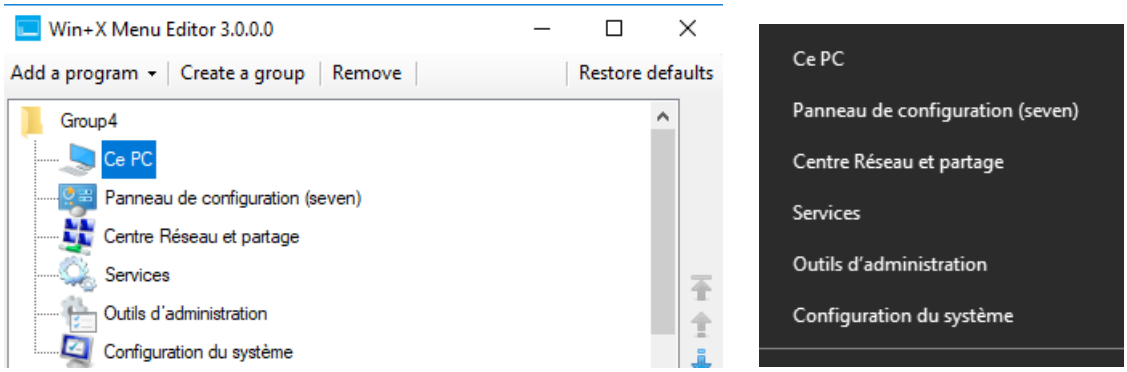
Ensuite, il n'est pas nécessaire de re-démarrer le poste pour voir les changements, il suffit de demander **restart explorer**

Ajouter un élement du panneau de configuration ou outil d'administration

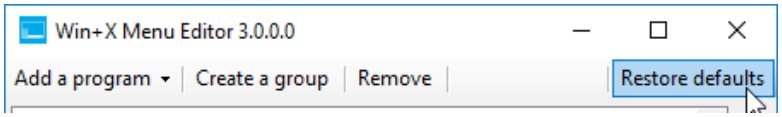




Pour obtenir au final



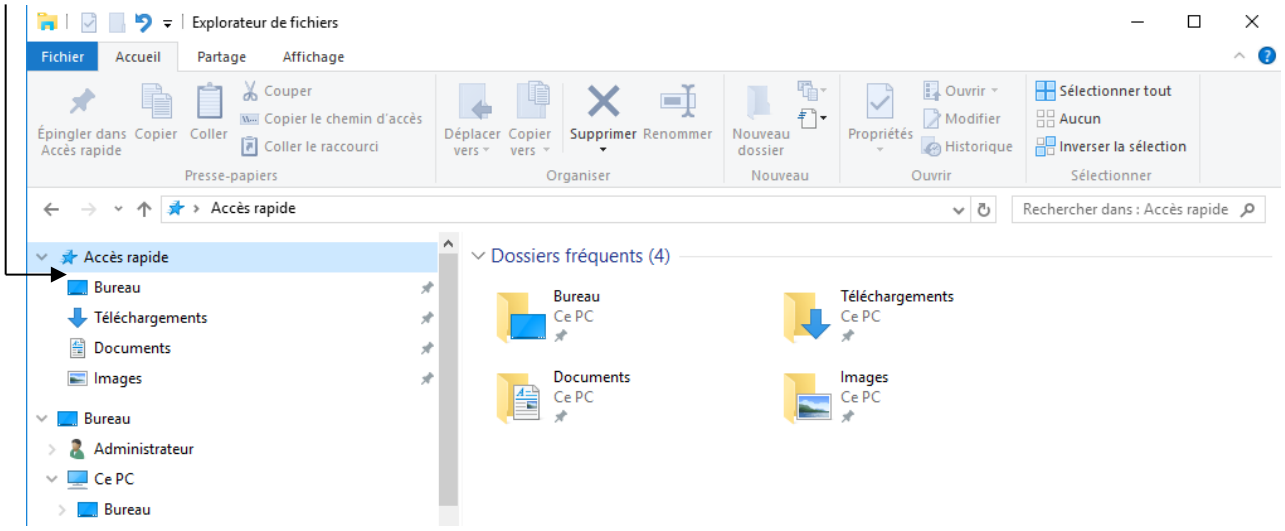
Restaurer le menu initial



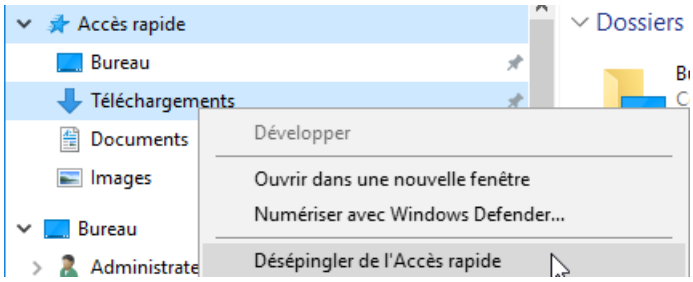
ACCES RAPIDE EXPLORATEUR

Gestion accès rapide:

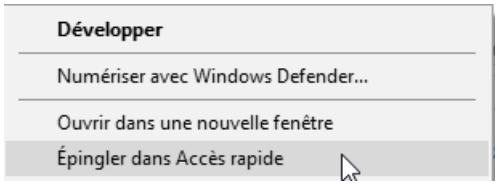
Par défaut sur windows 10… l'explorateur s'ouvre sur un accès rapide…



On peut supprimer des entrées avec le menu contextuel **désépingler de l'Accès rapide**

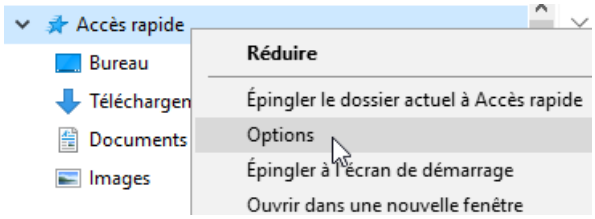


On peut ajouter une entrée avec le menu contextuel **épingler dans l'Accès rapide**



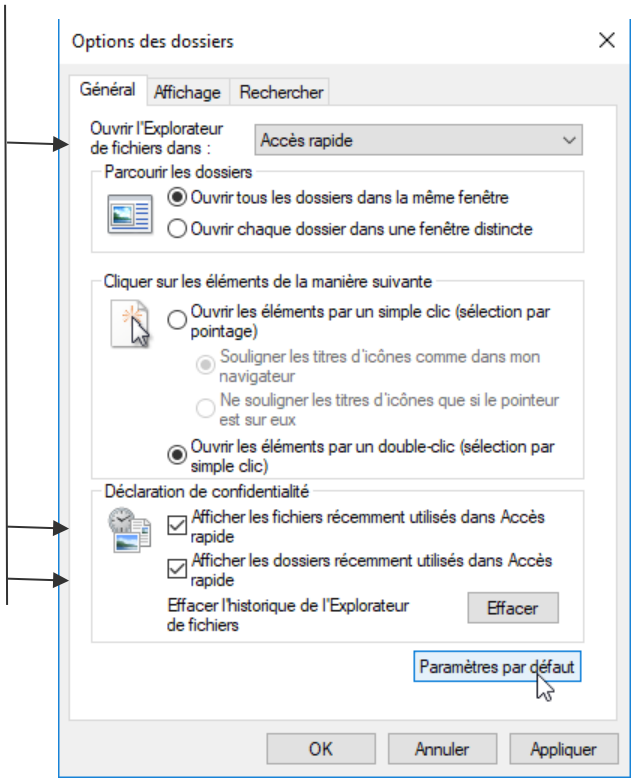
Ouverture Explorateur sur C: + pas d'accès rapide automatique

sur **l'Accès rapide** un cli droit **Options**

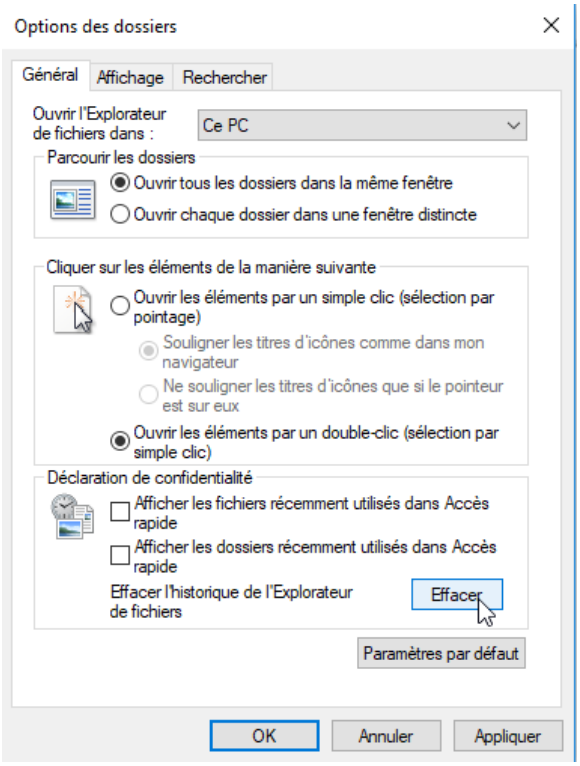


Qui amène directement à **Affichage / Option / modifier les options des dossiers et de recherche**

Par défaut on à



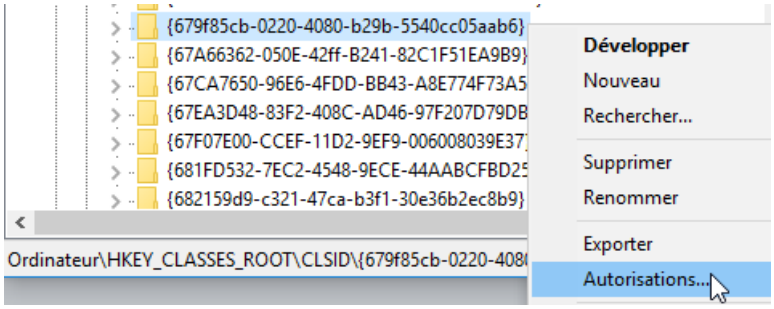
on demande **Ce Pc** et on décoche



Désinstaller l'accès rapide:

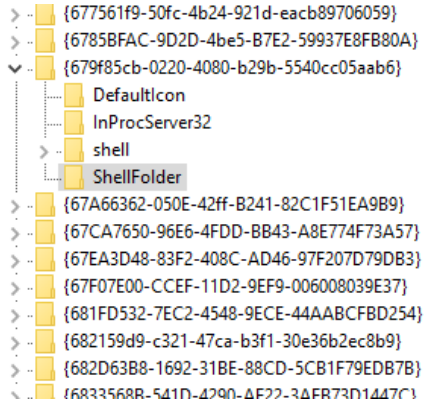
Il faut vider d'abords l'accès rapide de tout son contenu, enlever les entrées automatique, et demander à l'explorateur Windows d'ouvrir sur Ce PC (et non pas sur l'accès rapide)

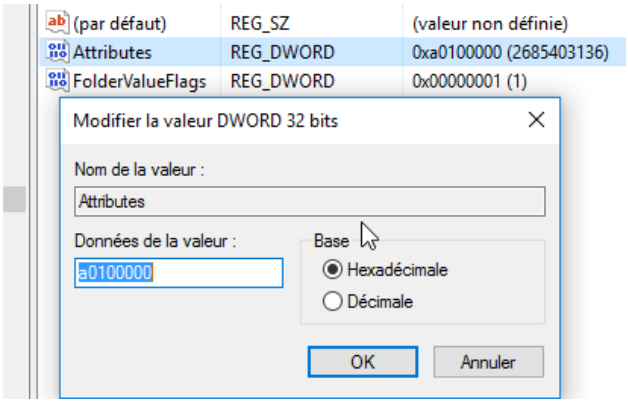
Puis Regedit, Rechercher la clé **HKEY_CLASSES_ROOT\CLSID{679f85cb-0220-4080-b29b-5540cc05aab6}** Une fois sur la clé on change ses autorisations



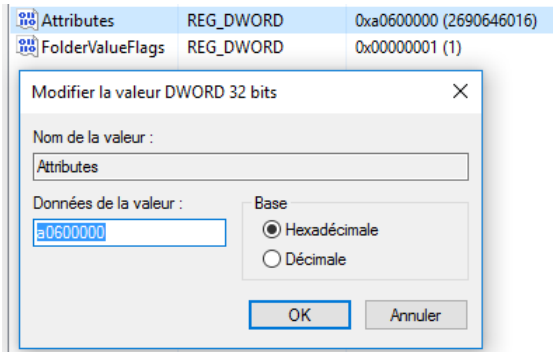
Il faut en prendre possession en se donner les droits d'accès

Du coup dans le dossier on peut demander dans "**ShellFolder**", double-click **Attributes**, et on change la clé de **a0100000** à **a0600000**, et on valide par **OK**.





Pour obtenir



Puis Il faut redémarrer windows… **N.B** : Pour retrouver l'accès rapide il suffit de redonner la valeur **a010000** à la clé…

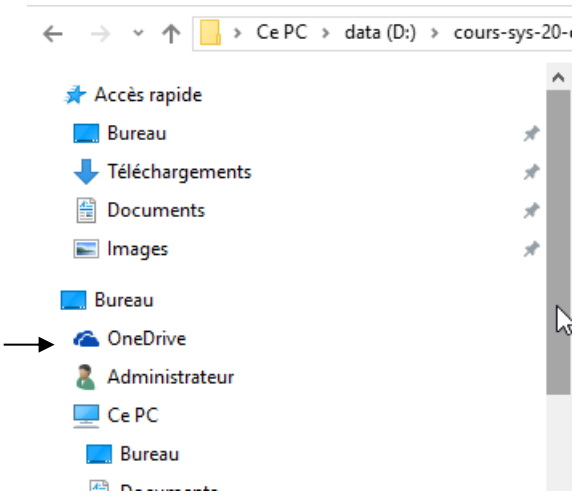
DESINSTALLER ONEDRIVE

Icones points de lancement Onedrive:

Le lancement de **Onedrive**, espace de stockage sur le cloud à l'aide d'un identifiant microsoft est présent à plusieurs endroits, notamment

- Dans la barre des tâches

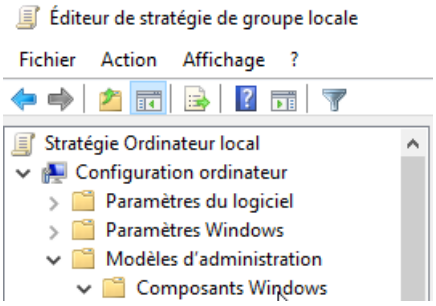
- Dans l'explorateur Windows



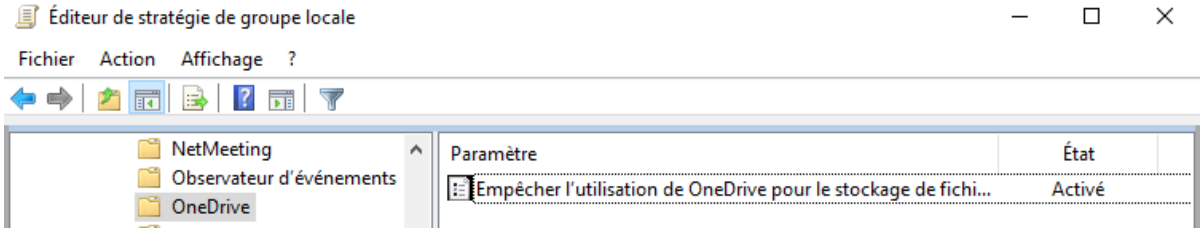
Désactivation de Onedrive:

Pour désactiver complètement **OneDrive / SkyDrive** via **gpedit.msc**

Configuration ordinateur, Modèles d'administration, Composants Windows,



Puis **OneDrive** (ou « SkyDrive » sur Windows 8)

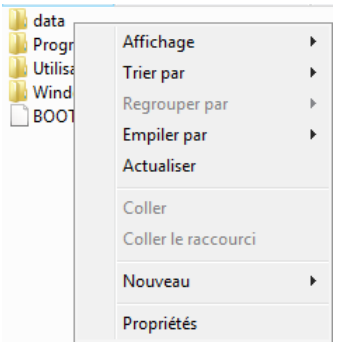


N.B : un redémarrage du poste est nécessaire !

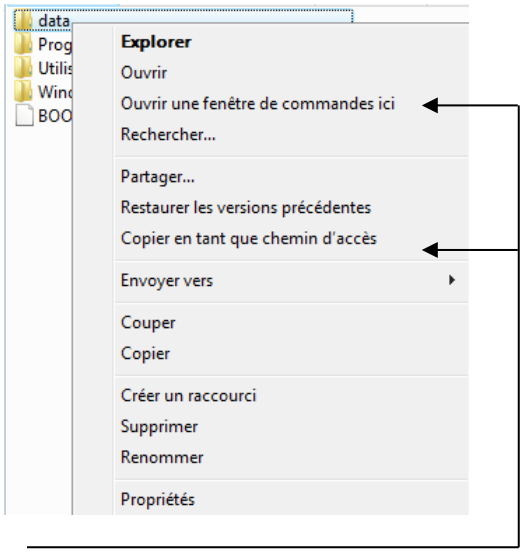
Menu étendus MAJ + clic droit:

On peut avoir des menus "contextuels" complets à l'aide de la touche **MAJ**

Menu contextuel

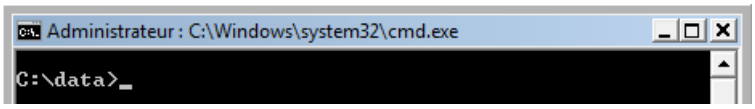


MAJ + Menu contextuel



Ouvrir une fenêtre de commande ici

Positionne le path local d'une invite de commande directement dans le dossier

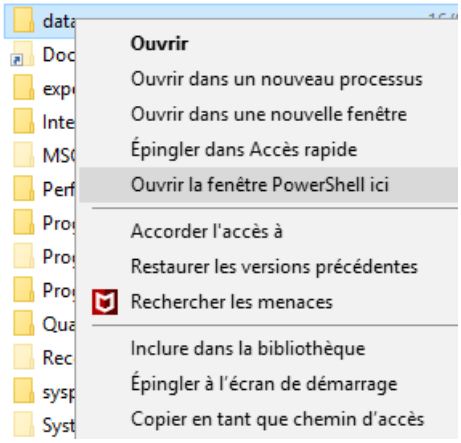


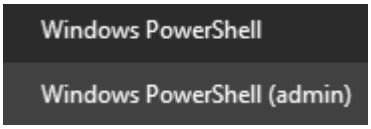
Copier en tant que chemin d'accès

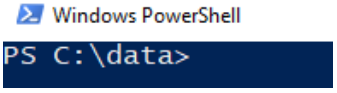
Permettant de récupérer la chaîne entre guillemet du chemin

"C:\data"

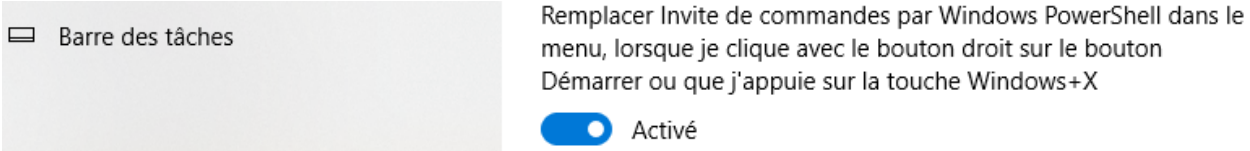
Ouvrir une fenêtre powershell ici (depuis 1803)





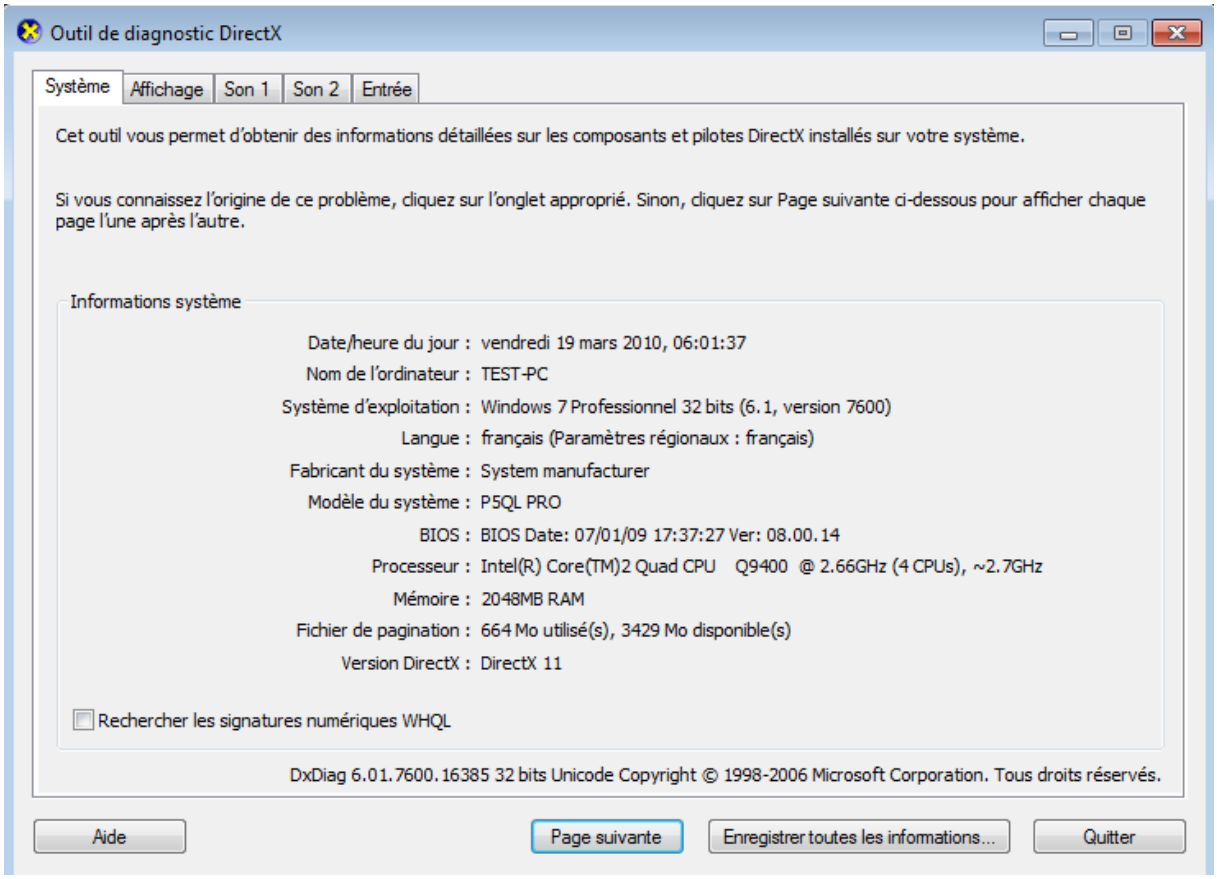


N.B : si on veut réobtenir l'invite de commande à la place de Powerschell on désactive dans **Paramètres / Personnalisation / barre des tâches**



Outils dxdiag:

Pour tester les pb directx, en ligne de commande **dxdiag**



Outils shutdown:

En ligne de commande **shutdown**

Shutdown /s /t 30	arrêt dans 30 secondes
Shutdown /ls /t 0	fermeture de session immédiate
Shutdown /m \\nomposte /t 0	arrêt du pc \\nomposte « immédiat »

N.B : Les 2 options **–r –f** semblent obligatoires avec l'option **–m**

Pour accéder au menu options de démarrage **shutdown avec l'option /r/o**

Shutdown /r /o arrêt immédiat

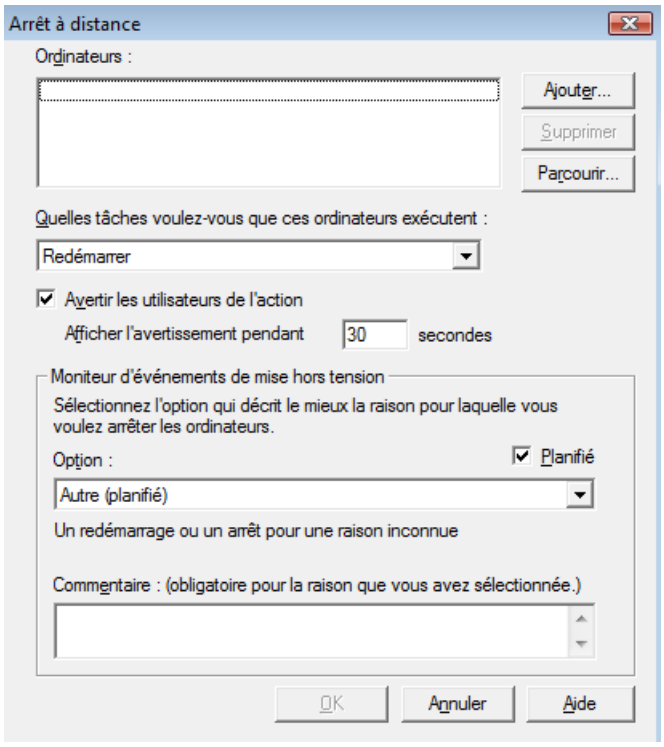
```
C:\Users\Administrateur>shutdown /r /o_
```

Ou encore mieux

Shutdown /r /o /f /t 0

Une interface graphique est également disponible

Shutdown /i



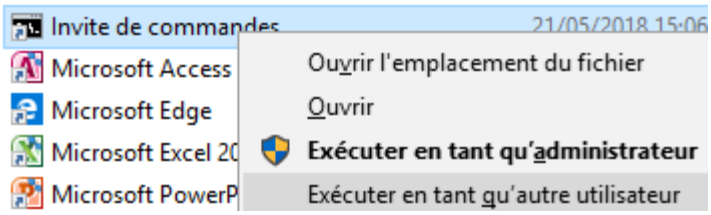
Whoami / Runas:

En ligne de commande **whoami** permet de connaître son login

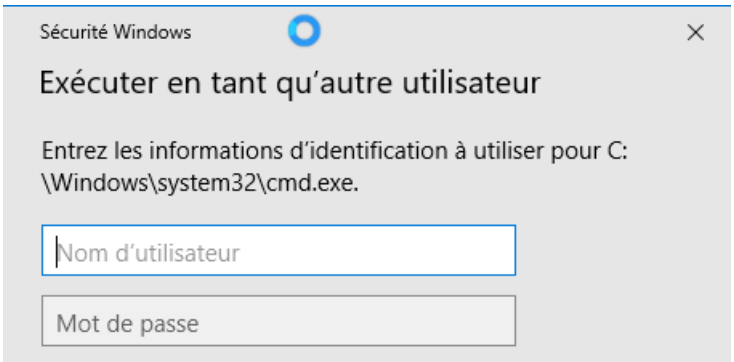
```
C:\Users\Administrateur>whoami
test-pc\administrateur
```

N.B: à ce propos on peut lancer une tache avec un autre login (équivalent de RUNAS en ligne de commande) avec **Pointer + SHIFT + Clic DROIT**

Ainsi sur un executable, parfois sur certains raccourci, on peut faire apparaître **Exécuter en tant qu'autre utilisateur**

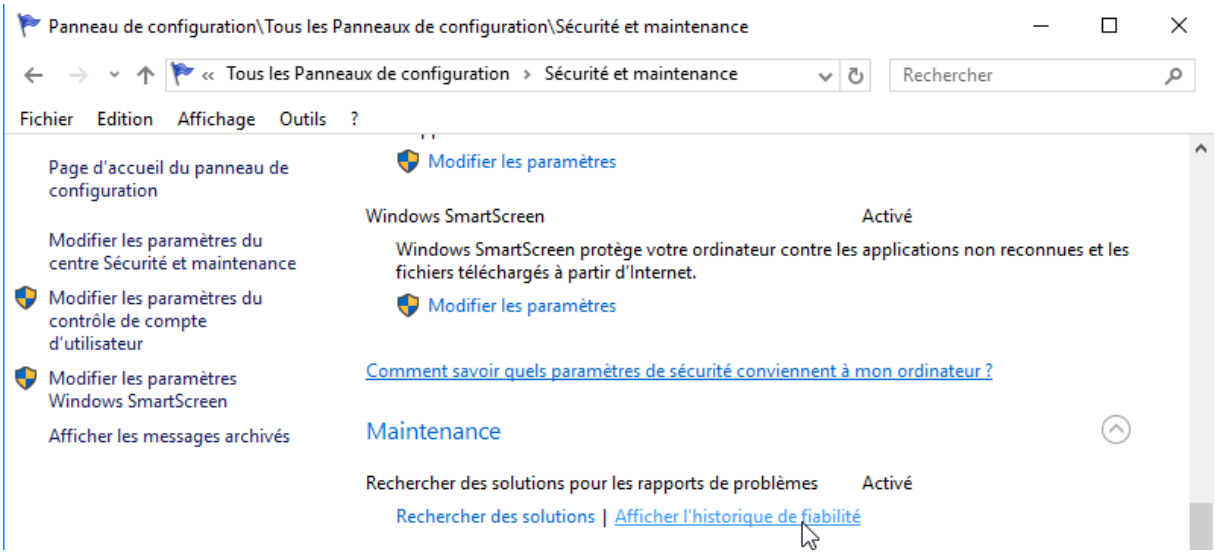


Forcément suivit de

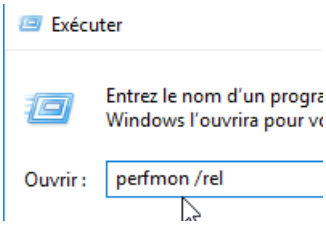


Historique de fiabilité – Perfmon /rel :

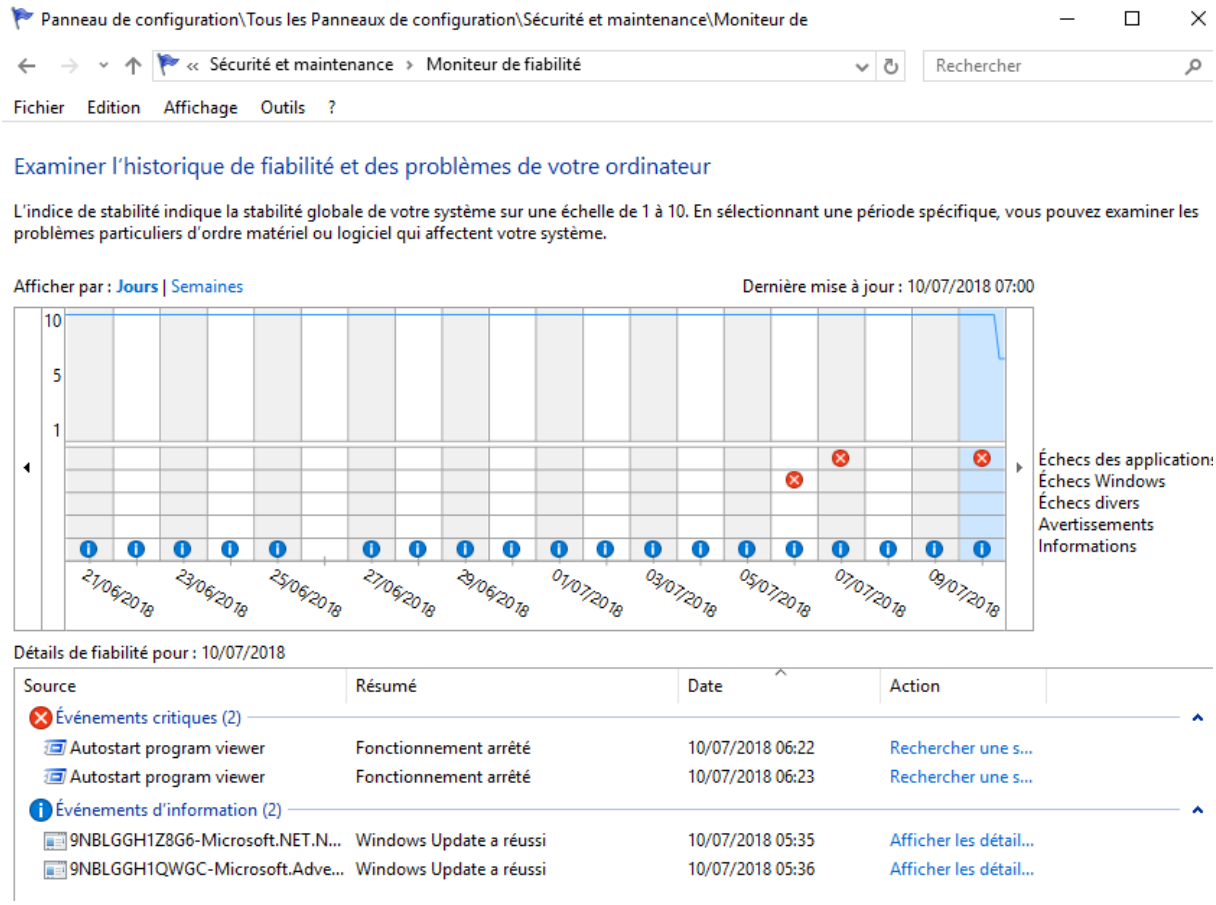
Via



Ou plus simple

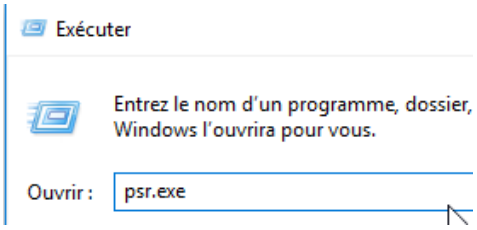


On obtient



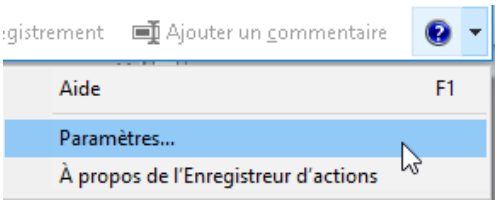
Enregistreur d'action - psr.exe:

L'outil se lance via **psr.exe**



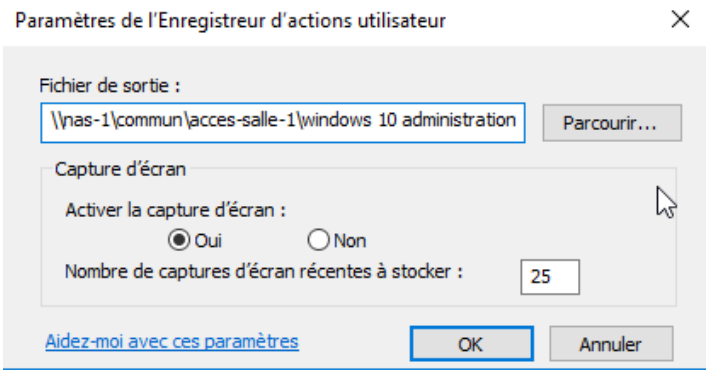
On obtient

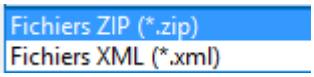
Il suffit simplement d'enregistrer l'endroit de stockage via le menu paramètres



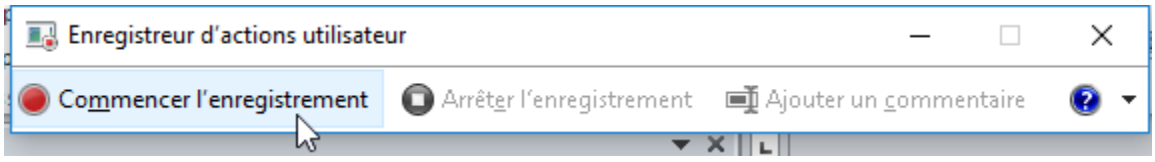
avec come choix

La localisation le format de fichier



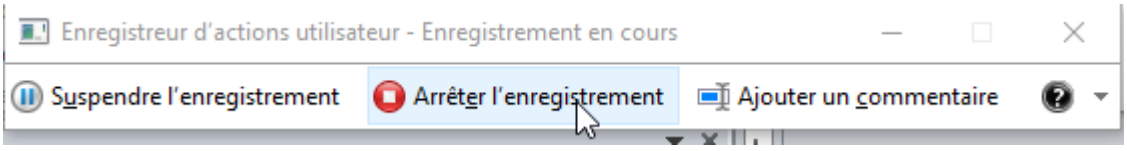


Et on démarre l'enregistrement

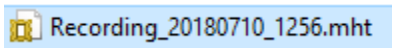


On fait ce que l'on veut,...

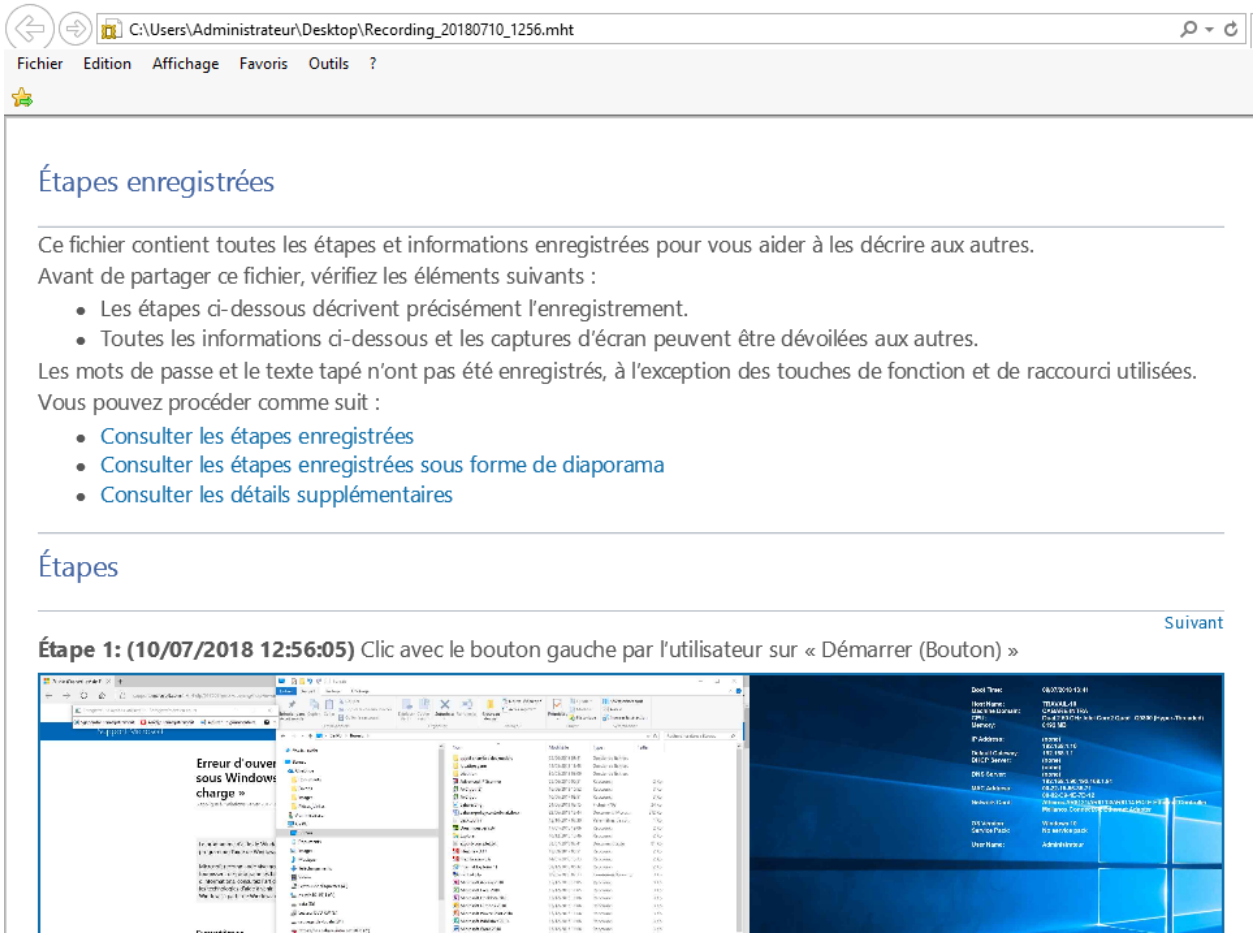
et on arrête l'enregistrement



Le résultat est un fichier ou un dossier (ZIP) que l'on désarchive en un mht



Qui est visualisable dans un navigateur:



Détails supplémentaires

La section suivante contient les détails supplémentaires enregistrés.
Ces détails facilitent l'identification précise des programmes et de l'interface utilisateur employée dans cet enregistrement.
Cette section peut contenir du texte interne aux programmes, compréhensible seulement par les utilisateurs chevronnés ou les programmeurs.
Consultez ces détails pour vérifier qu'ils ne contiennent aucune information à ne pas révéler aux autres.

```
Session d'enregistrement: 10/07/2018 12:56:04 - 12:56:16

Étapes enregistrées : 4, Actions manquées : 0, Autres erreurs : 0

Système d'exploitation: 10586.1176.amd64fre.th2_release_sec.170913-1848 10.0.0.0.2.48

Étape 1: Clic avec le bouton gauche par l'utilisateur sur « Démarrer (Bouton) »
Programme: Explorateur Windows, 10.0.10586.0 (th2_release.151029-1700), Microsoft Corporatior
Éléments d'interface: Démarrer, Start, Shell_TrayWnd

Étape 2: Clic avec le bouton gauche par l'utilisateur sur « Actualité
Macron se rend en Russie pour soutenir les Bleus (élément de liste) » dans « Début  »
Programme: Windows Shell Experience Host, 10.0.10586.1106 (th2_release.170904-1742), Microsof
Éléments d'interface: Actualité
Macron se rend en Russie pour soutenir les Bleus, TileListViewItem, en-tête de groupe Jouer e
```

CONSOLE MMC

Microsoft Management Console:

Dite plus couramment **MMC**, cette console d'administration n'est en fait qu'un coquille vide, ne faisant rien si ce n'est unifier et homogénéiser l'aspect des différents outils de gestion que l'on doit employer.

La MMC sert donc à fournir une interface commune pour tous les outils d'administrations sous Windows

Chaque MMC peut recevoir (ou on peut lui ôter) des outils d'administrations via ce que l'on appelle des « **snap-in** » ou encore des « **composant logiciels enfichables** ». Il existe un **snap-in** pour chaque outils de gestion.

Les consoles contiennent de manières générale un ou plusieurs snap-in et sont enregistrées dans des fichiers dotés de l'extension **.msc** stockés par défaut dans le dossier Outils d'Administration **Winnt\System32**

S'il est évident qu'il existe déjà un certain nombre de consoles pré-définies, il est tout aussi évident que l'on peut se créer ses propres consoles personnalisées

Si on a besoin que d'une **partie** seulement d'une console (par exemple le gestionnaire de disques), Il peut donc être **avantageux** de lancer **uniquement** la partie intéressante, en exécutant le fichier d'extension **.msc** associé

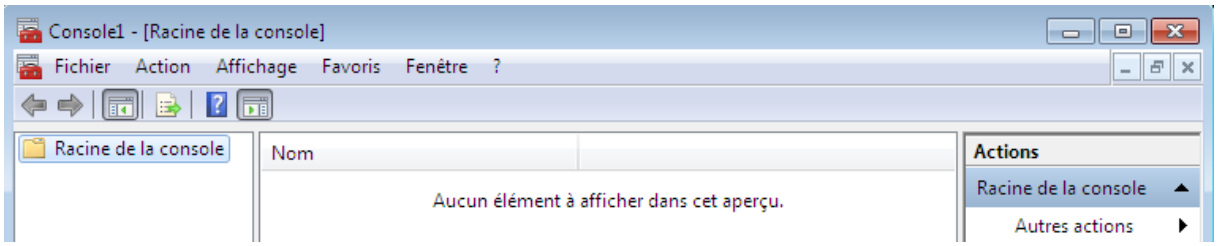
Fichier	*Rôle*
certmgr.msc	Certificats
ciadv.msc	Service d'indexation
devmgmt.msc	Gestionnaire de périphériques
dfrg.msc	Défragmenteur de disques
diskmgmt.msc	Gestion des disques
dnsmgmt.msc	Gestionnaire de DNS
eventvwr.msc	Observateur d'événements
faxserv.msc	Gestion du service de télécopie
fsmgmt.msc	Dossiers partagés
gpedit.msc	Stratégie de groupe
ias.msc	Service d'authentification Internet
lusrmgr.msc	Utilisateurs et groupes locaux
ntmsmgr.msc	Stockage amovible
ntmsoprq.msc	Demandes de l'opérateur de stockage amovible
perfmon.msc	Analyseur de performances
secpol.msc	Paramètres de sécurité locaux
services.msc	Services
wmimgmt.msc	Infrastructure de gestion Windows (WMI)
comexp.msc	Service de composants
iis.msc	Services Internet
msinfo32.msc	Informations système

Créer une console personnalisée:

Il faut demander **Executer /** Et taper **mmc**

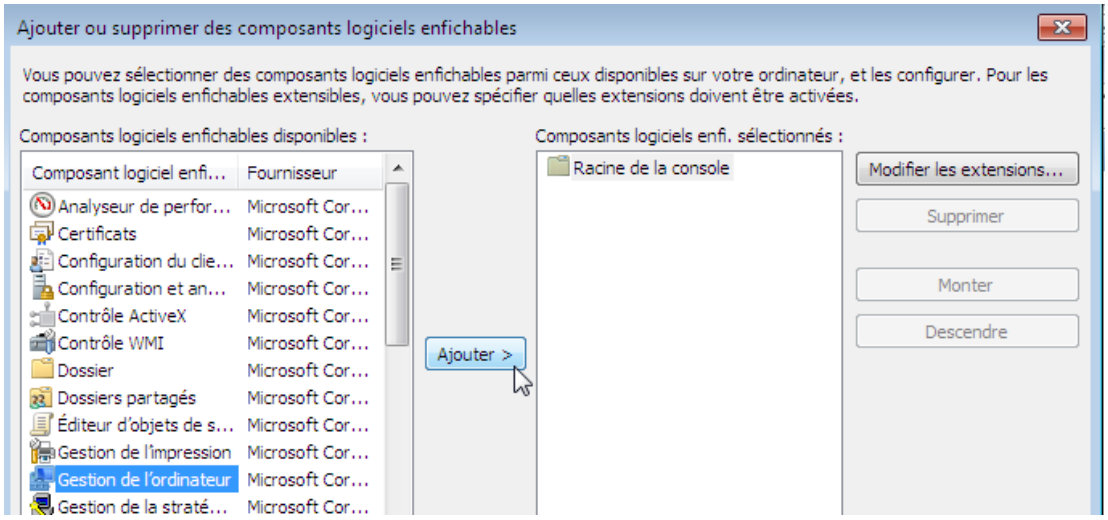
Ou rechercher MMC

On obtient une ***console1*** vide prête à être personnalisée

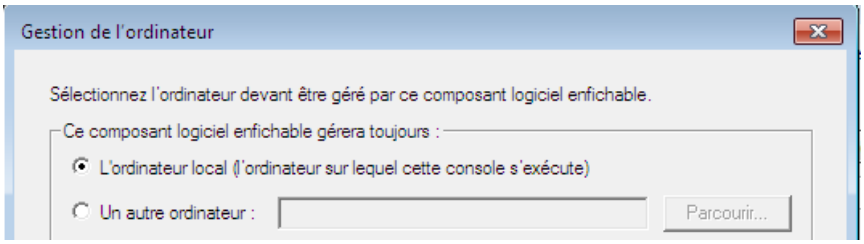


En étant placé à la racine de la console, demander dans le menu

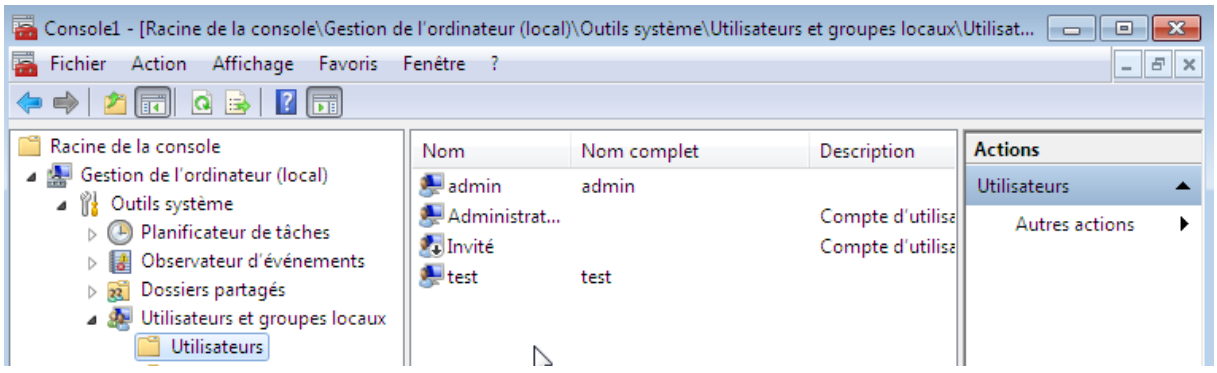
Fichier / Ajouter - Supprimer un composant logiciel enfichable



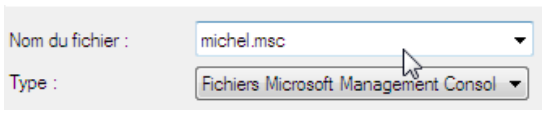
Dans la liste des snap-in choisir « **gestion de l'ordinateur** » (par exemple) et demander de gérer l'ordinateur local



Et l'on voit que notre console se personnalise !



Pour enregistrer cette console il faut demander le menu **Console / Enregistrer sous**



Et taper ici le nom de la console **mmc,** par exemple « ***michel*** »

Pour peu que l'on ait placé le fichier .msc dans le bon dossier…

N.B: on peut placer le fichier sur le bureau… ou ailleurs…

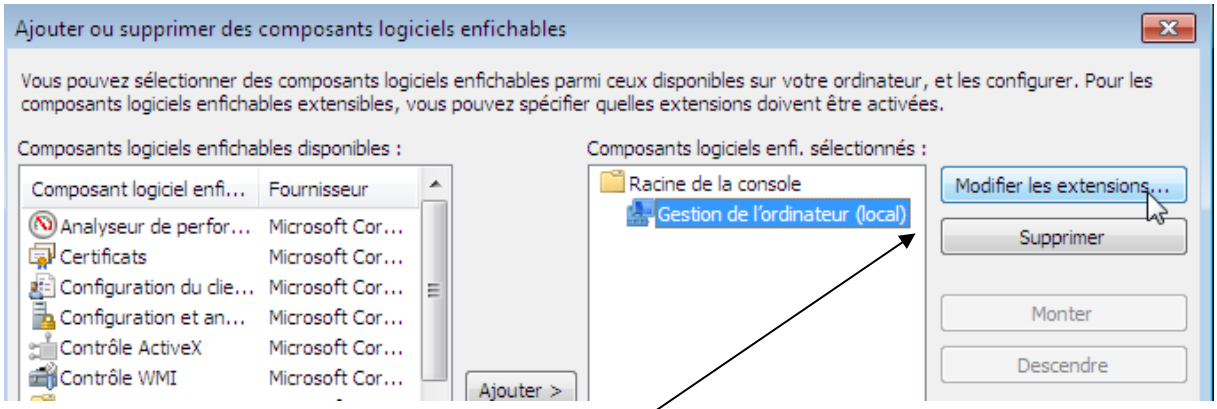
Limiter les fonctions d'un composant logiciel :

Lorsque l'on crée une console avec un composant, celui-ci peut donner accès à plein de fonctionnalités différentes. Si on veut ce composant, mais avec moins de fonctionnalités, (en quelque sorte on veut le « brider ») Il suffit de :

- désactiver certaines extensions de la console
- enregistrer la console en mode utilisateur...

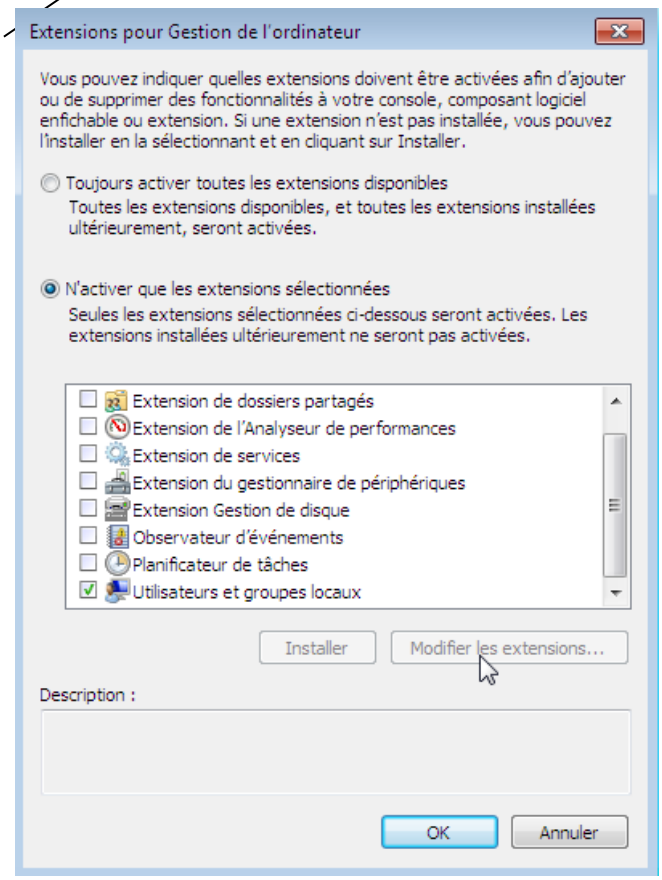
Désactiver des extensions de la console :

Au moment d'inclure le composant **gestion de l'ordinateur**



On demande **Modifier les extensions…**

pour obtenir alors

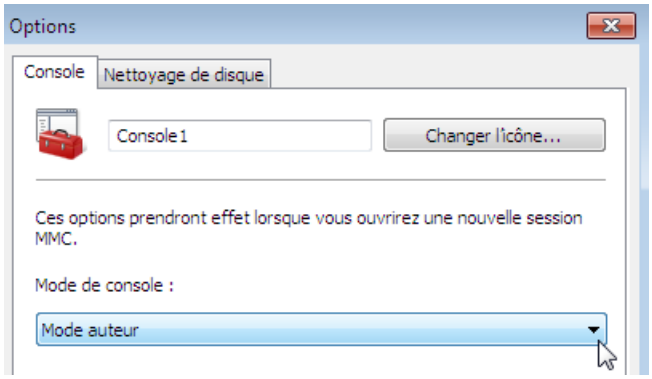


on demande de n'activer que les extensions sélectionnées

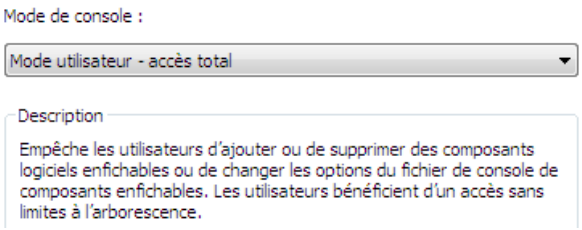
et ensuite on faite sa sélection...

Enregistrer la console utilisateur :

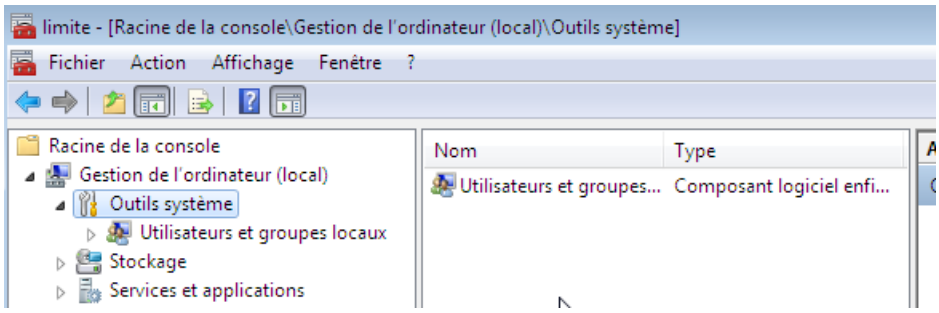
Avant d'enregistrer la console, il faut dans le menu **FIchier / Option**



Demander de passer en **Mode utilisateur**...



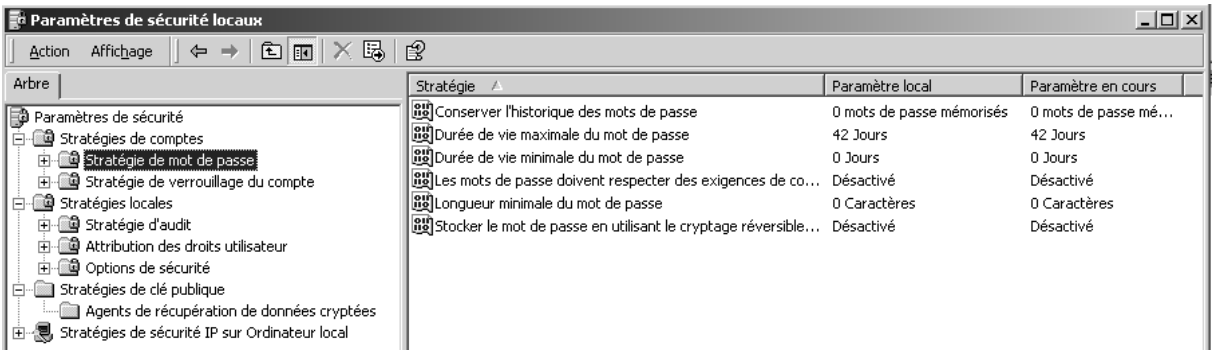
Au prochain lancement, les composants enfichables de cette console ne sont plus modifiables... et son réduit à la gestion utilisateur



Secpol.msc - Rappel stratégies locales et GPo de domaine

Les stratégies locales se lancent depuis les outils d'administration, à travers **stratégie de sécurité locale**

ce qui donne ensuite accès aux paramètres suivants :



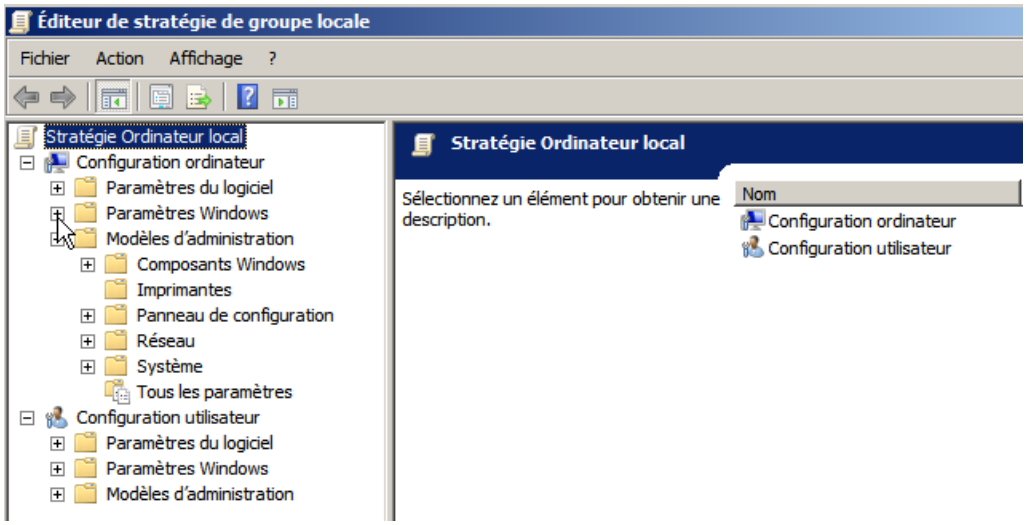
Les **GPO** ou **stratégies de domaine/réseaux** elles sont en général utilisées à travers le réseau (pour tout le domaine ou une partie à travers les UO...)

A ce stade, on ne confond plus les « réglages des stratégies locales » avec le fait de passer ces réglages localement via **secpol.msc** (ou **le panneau de configuration / stratégies locales**) ou via une **GPO** de **domaine**

Gpedit.msc - editeur de stratégie de domaine "locale" ! :

Il est cependant possible de modifier localement les stratégies d'une machine Windows avec les options normalement réservées aux stratégies de domaine /réseau, ARG !

Il faut passer par une console personnalisée **gpedit.msc** que l'on lance depuis **démarrer / executer**…



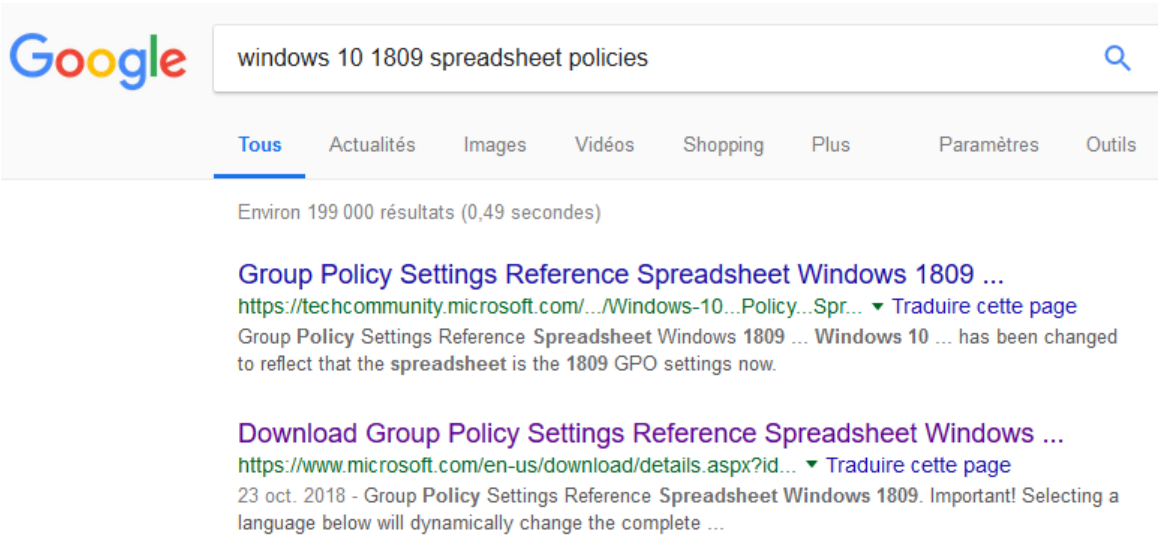
N.B: Evidemment on ne choisit pas sur qui cela s'applique…!

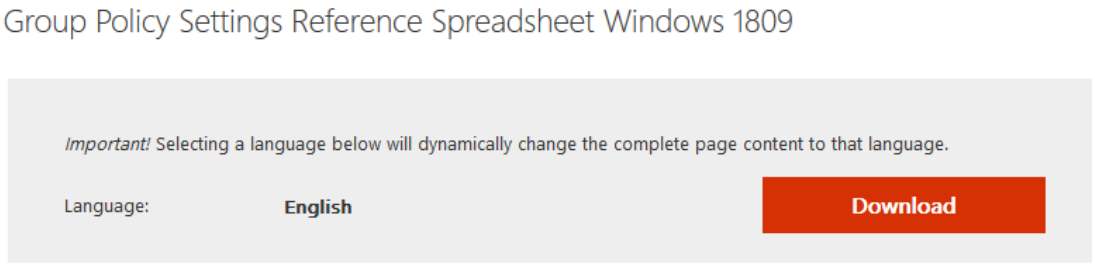
Liste de toutes les stratégies – Policysettings—1809.xls :

Microsoft publie des mises à jour dans un fichier Excel contenant le détail des paramètres de stratégies de groupe Pour les machines Windows 10. (et a chaque version, une version de ce fichier est disponible)

Windows10andWindowsServer2016PolicySettings.xlsx
Windows10andWindowsServer2016PolicySettings-1803.xlsx
Windows10andWindowsServer2019PolicySettings--21H2.xlsx
Windows10andWindowsServer2019PolicySettings--1809.xlsx
Windows11andWindowsServer2019PolicySettings--21H2.xlsx

Pour chercher la version 1809 on peut faire une recherche du genre



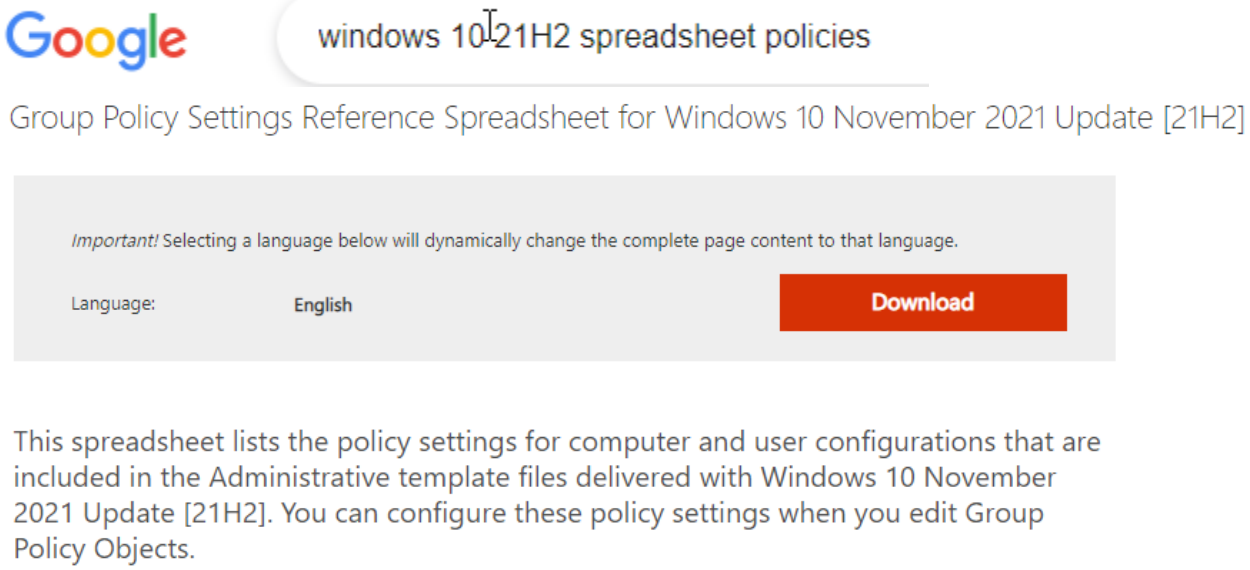


This spreadsheet lists the policy settings for computer and user configurations that are included in the Administrative template files delivered with the Windows operating systems specified. You can configure these policy settings when you edit Group Policy Objects.

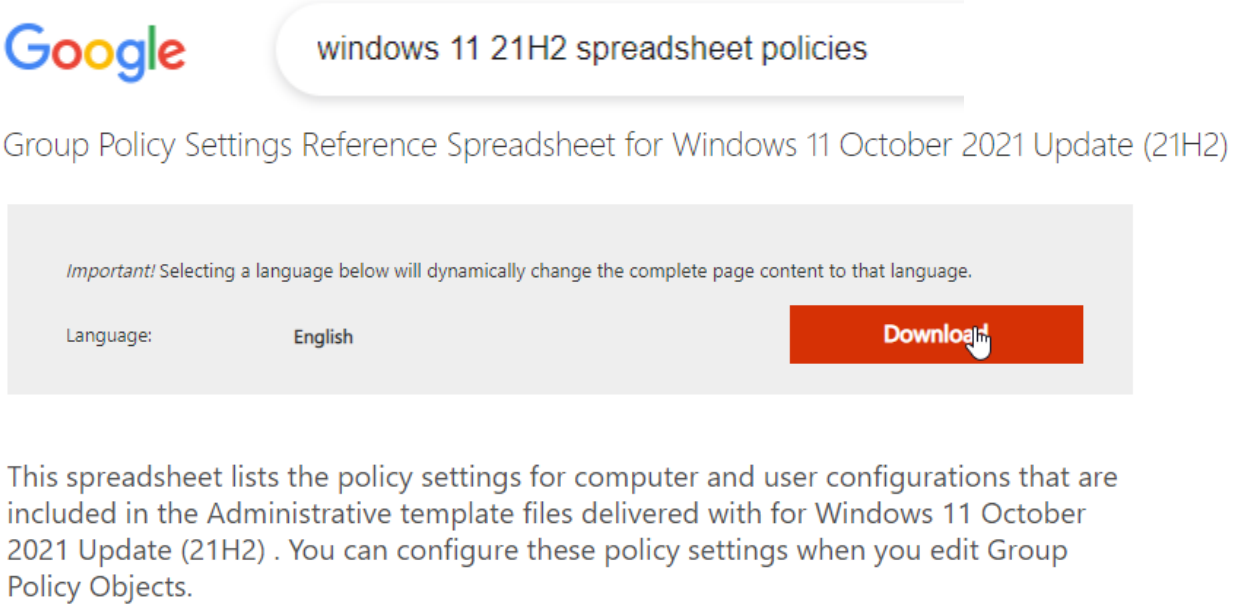
amenant

Version:	Date Published:
1809	10/23/2018
File Name:	**File Size:**
Windows10andWindowsServer2019PolicySettings--1809.xlsx	708 KB

Policysettings – 10-21H2.xls :



Policysettings – 11-21H2.xls :



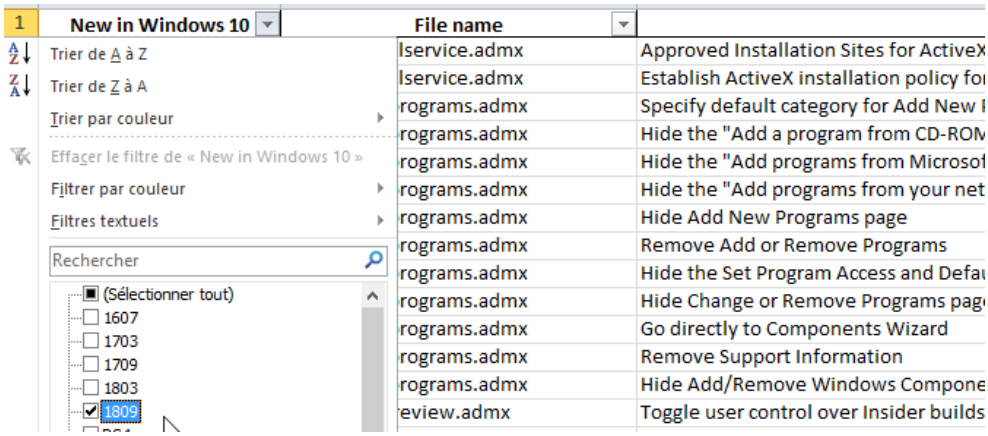
Voire les nouveautés par Branche :

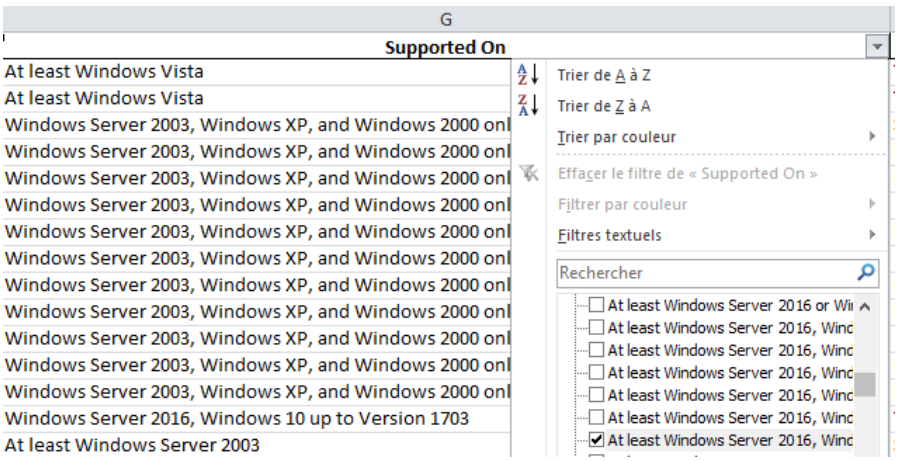
Le fichier permet de faire le lien entre les définitions des paramètres dans les GPO et les clés de registre correspondantes. On peut faire plusieurs filtres sur ce fichier excel.

Filtre simple : Si on demande juste **1809** dans la colonne **New in Windows 10** on obtiendra les 166 nouveaux réglages possibles (qui ne correspondent pas forcément à une nouvelle fonctionnalité 1809)

New in Windows 10	File name	Policy Setting Name	Scope	Policy Path	Supported On
1809	apphvsi.admx	Allow Windows Defender Application Guard to use Root Cer	Machine	Windows Components\Windows Defender Application Guar	At least Windows 10 Enterprise
1809	apphvsi.admx	Allow camera and microphone access in Windows Defender	Machine	Windows Components\Windows Defender Application Guar	At least Windows 10 Enterprise
1809	apphvsi.admx	Allow users to trust files that open in Windows Defender Ap	Machine	Windows Components\Windows Defender Application Guar	At least Windows 10 Enterprise
1809	apphvsi.admx	Configure additional sources for untrusted files in Windows	Machine	Windows Components\Windows Defender Application Guar	At least Windows 10 Enterprise
1809	controlpanel.admx	Settings Page Visibility	User	Control Panel	At least Windows Server 2016, Windows 10 Version 1703
1809	datacollection.admx	Disable deleting diagnostic data	Machine	Windows Components\Data Collection and Preview Builds	At least Windows Server 2016, Windows 10 Version 1809

Filtre multiple : si on demande ***1809*** sur la colonne **New in Windows 10** et ***at least windows server 2016 an windows 10 version 1809*** sur la colonne **Supported On**





Donc pour les nouveautés 1809 qui ne marchent que sur 1809, alors

New in Windows 10	File name	Policy Setting Name
1809	datacollection.admx	Disable deleting diagnostic data
1809	datacollection.admx	Disable diagnostic data viewer.
1809	datacollection.admx	Configure Microsoft 365 Update Readiness upload endpoint
1809	oobe.admx	Don't launch privacy settings experience on user logon
1809	oobe.admx	Don't launch privacy settings experience on user logon
1809	windowsdefender.admx	Configure low CPU priority for scheduled scans
1809	windowsdefendersecuritycenter.admx	Disable the Clear TPM button
1809	windowsdefendersecuritycenter.admx	Hide the TPM Firmware Update recommendation.
1809	windowsdefendersecuritycenter.admx	Hide Windows Security Systray
1809	windowsupdate.admx	Remove access to "Pause updates" feature

Télécharger (installer) des ADMX modèle de GPO 10-1809 (sur un Serveur)

Téléchargeons un **templates** pour **Windows 10 v1809 depuis le site de microsoft**

Administrative Templates (.admx) for Windows 10 October 2018 Update (1809)

Important! Selecting a language below will dynamically change the complete page content to that language.

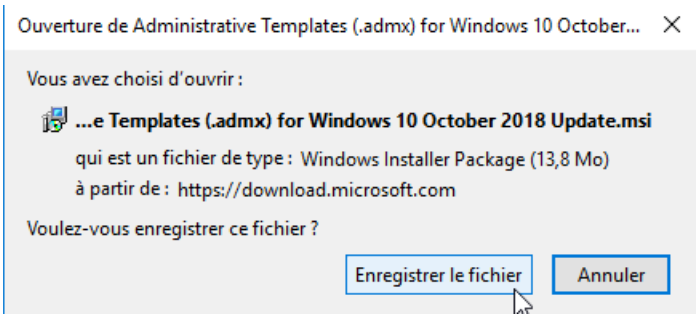
Language: **English** **Download**

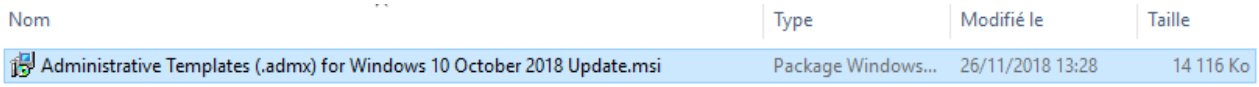
This page provides the complete set of Administrative Templates (.admx) for Windows 10 October 2018 Update (1809)

Details

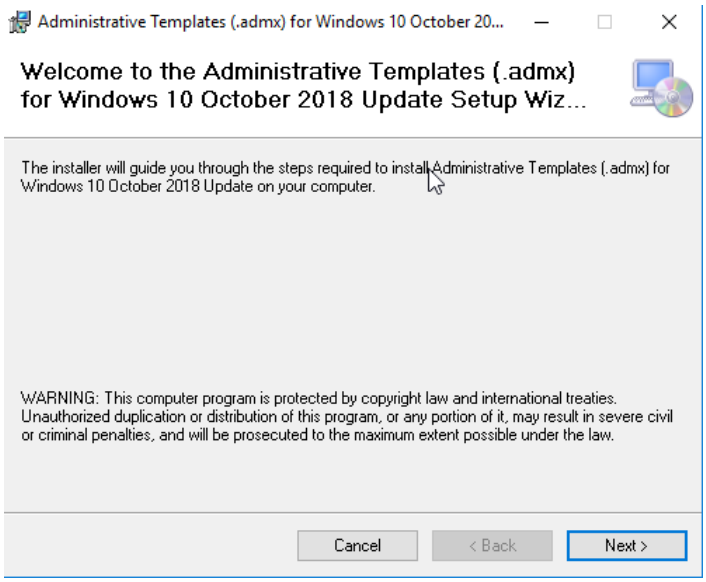
Version:	Date Published:
1.0	11/13/2018
File Name:	**File Size:**
Administrative Templates (.admx) for Windows 10 October 2018 Update .msi	13.8 MB

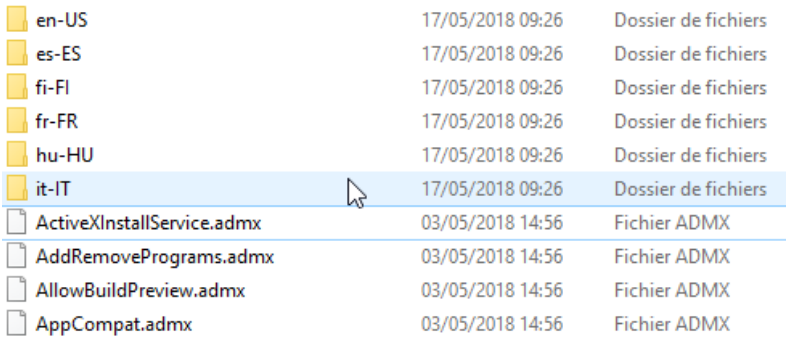
On télécharge le fichier





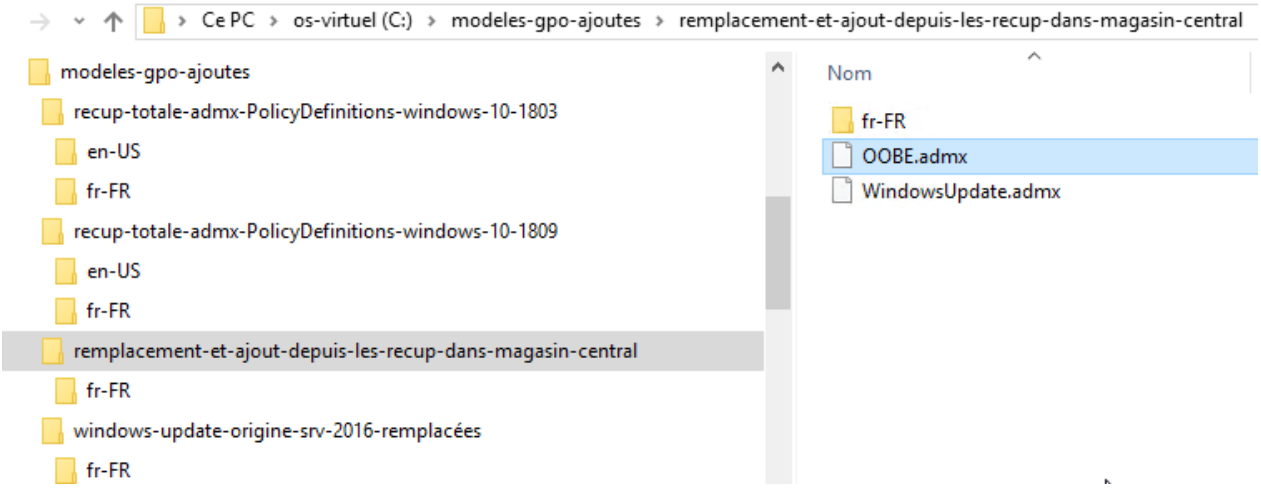
Et on l'installe





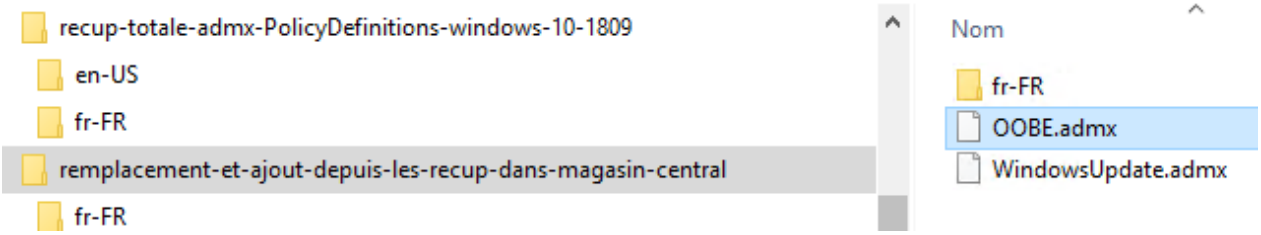
Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central**



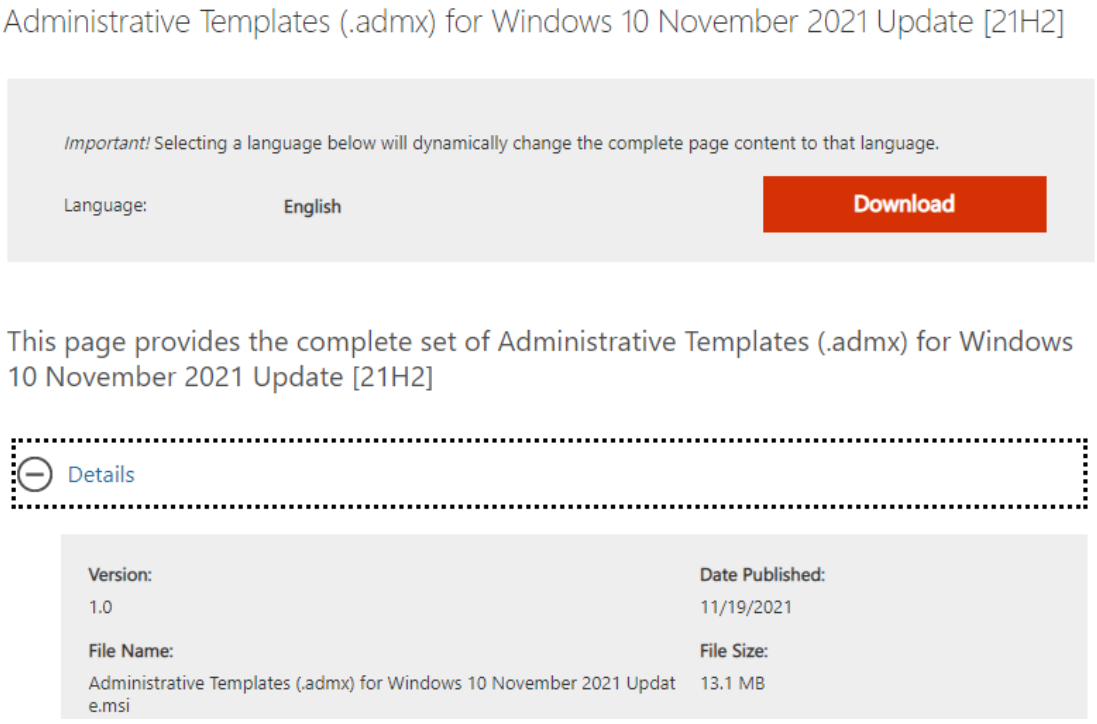
L'idée est que par rapport à un ebsemble de mises à jour disponibles, comme ici à la sortie d'une nouvelle version de l'OS windows 10 v1803, on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx…

On remplace donc juste un admx et son fichier de langue, tout en gardant l'ancien…

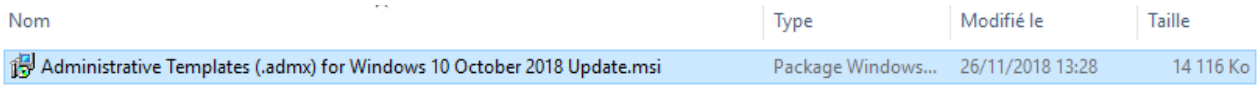


Télécharger (installer) des ADMX modèle de GPO 10-21H2 (sur un Serveur)

Téléchargeons un **templates** pour **Windows 10 v21H2 depuis le site de microsoft**



On télécharge le fichier

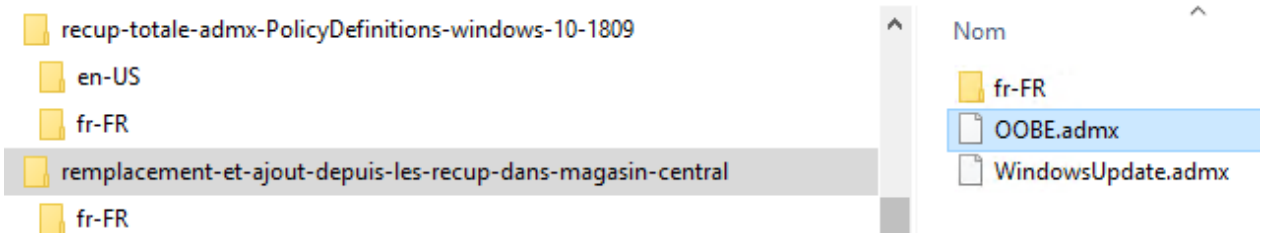


Et on l'installe

Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central.** L'idée est que on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx…

On remplace donc 1admx et son fichier de langue, tout en gardant l'ancien…



Télécharger (installer) des ADMX modèle de GPO 11-21H2 (sur un Serveur)

Téléchargeons un **templates** pour **Windows 11 v21H2 depuis le site de microsoft**

ADMX Templates for Windows 11 October 2021 Update [21H2]

Important! Selecting a language below will dynamically change the complete page content to that language.

Language: English **Download**

This page provides the complete set of Administrative Templates (.admx) for Windows 11 October 2021 Update [21H2]

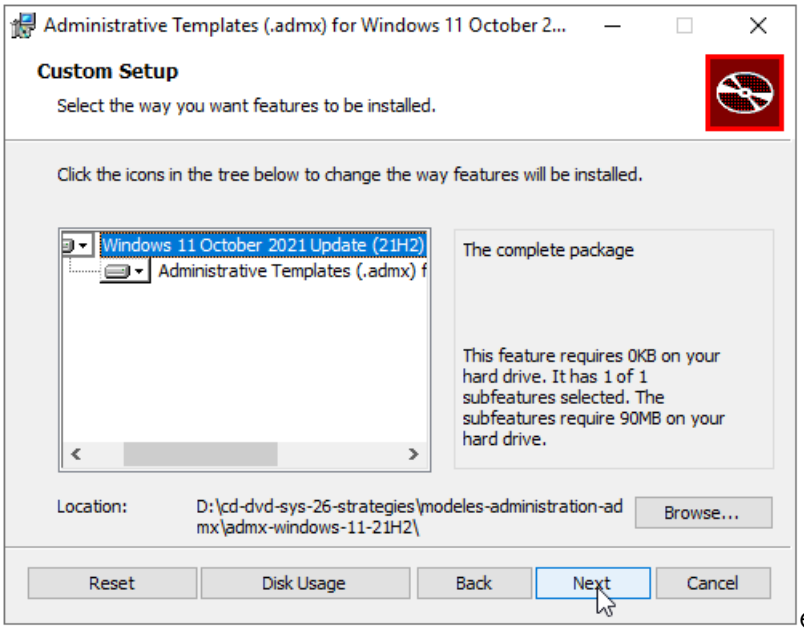
Details

Version:	Date Published:
1.0	10/6/2021
File Name:	**File Size:**
Administrative Templates (.admx) for Windows 11 October 2021 Update.msi	13.2 MB

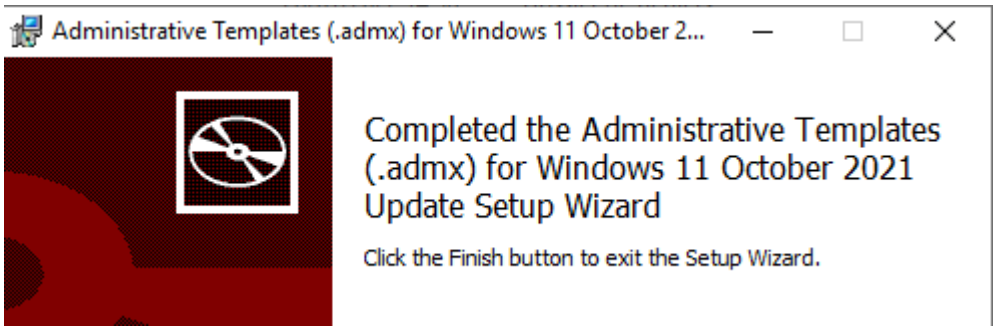
On télécharge le fichier

Nom	Modifié le	Type	Taille
Administrative Templates (.admx) for Windows 11 October 2021 Update.msi	26/01/2022 14:53	Package Windows...	13 564 Ko

Et on l'installe



et on obtient



Dans le dossier **de désarchivage** on trouve tous les modèles **admx** et les dossiers de langue (au minimum) **fr-fr** et **en-us**

Il faut copier soit tout cela, soit uniquement ce qui nous intéresse dans notre **Magasin Central.** L'idée est que on ne souhaite mettre à jour que la Windowsupdate.admx, et garder en trace de l'ancien modeles admx…

GPO Windows 10 qui disparaissent (sous Windows 11):

https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/windows-10-or-windows-11-gpo-admx-which-one-to-use-for-your/ba-p/3063322

https://4sysops.com/archives/group-policies-for-windows-11-and-10-21h2-compared/

Dans le magasin, il ne peut y avoir qu'un fichier **ADMX** avec un nom donné

Fondamentalement il y a quelques **GPO** qui n'existent que sous **Windows 10** et d'autres qui sont apparues sous **windows 11.** Apriori cela semble normal que sous **windows 11** de nouvelles **GPO** apparaissent, mais le problème c'est que quelques anciennes **GPO** de **windows 10** disparaissent !

Ce qui fait que si on remplace les **ADMX** de 10 par les **ADMX** de 11, on peut risquer de perdre la main sur ces réglages !

Heureusement la liste est courte : est l'idée pour faire simple sera la suivante : si on n'utilisa pas les rares **GPO windows 10** « qui disparaissent » dans les **ADMX** de

windows 11, on peut sans problème installer ces **ADMX**, sinon il faut s'en passer, et rester avec les **ADMX** de **windows 10**!

N.B : il existe une procédure pour faire en sorte que l'on puisse administrer le même modèle **ADMX** en version 10 et version 11 mais…. Est-ce raisonnable ?

Liste des **ADMX windows 10** dans lesquels des réglages « disparaissent »

ADMX name	Scope	Setting
DataCollection	Both	Allow Telemetry: Enhanced
DeliveryOptimization	Computer	Download Mode: Bypass
EAIME	User	Turn on Live Sticker
EAIME	User	Turn on lexicon update
InetRes	Both	Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects
InetRes	Both	Reset zoom to default for HTML dialogs in Internet Explorer mode
MicrosoftEdge	Both	Suppress the display of Edge Deprecation Notification
Printing	Computer	Limit print driver installation to Administrators
TerminalServer	Computer	Set the Remote Desktop licensing mode: AAD per User
WindowsDefender	Computer	Scan packed executables

Liste des nouveaux réglages **ADMX** qui apparaissent sous **Windows 11**

ADMX name	Scope	Setting
AppPrivacy	Computer	Let Windows apps take screenshots of various windows or displays
AppPrivacy	Computer	Let Windows apps turn off the screenshot border
AppxPackageManager	Computer	Archive infrequently used apps
AppxPackageManager	Computer	Do not allow sideloaded apps to auto-update in the background
AppxPackageManager	Computer	Do not allow sideloaded apps to auto-update in the background on a metered network
CloudContent	Computer	Turn off cloud consumer account state content
CloudContent	User	Turn off Spotlight collection on Desktop
ControlPanelDisplay	Computer	Prevent lock screen background motion
DataCollection	Computer	Limit Diagnostic Log Collection
DataCollection	Computer	Limit Dump Collection
DeliveryOptimization	Computer	Discovery Mode: Local Discovery
DnsClient	Computer	Configure DNS over HTTPS (DoH) name resolution
EAIME	User	Configure Korean IME version
FileSys	Computer	Enable NTFS non-paged pool usage
FileSys	Computer	NTFS parallel flush threshold
FileSys	Computer	NTFS parallel flush worker threads
FileSys	Computer	Configure NTFS default tier
Globalization	Both	Restrict Language Pack and Language Feature Installation
InetRes	Both	Replace JScript by loading JScript9Legacy in place of JScript via MSHTML/WebOC.
Netlogon	Computer	Use lowercase DNS host names when registering domain controller SRV records
NewsAndInterests	Computer	Allow News and Interests
Sam	Computer	Configuration settings for the Security Account Manager
Sensors	Computer	Force instant Wake
Sensors	Computer	Force instant Lock
Sensors	Computer	Configure Lock Timeout
StartMenu	Both	Locked Start Layout: Re-Apply Layout at every logon
StartMenu	Both	Show or hide "Most used" list from Start menu
TaskBar	Computer	Configure the Chat icon on the taskbar

TenantRestrictions	Computer	Configure Cloud Policy Details
TerminalServer	Computer	Enable auto-subscription
TerminalServer	Computer	Do not allow location redirection
TerminalServer	Computer	Allow UI Automation redirection
WindowsDefender	Computer	Configure scheduled task times randomization window
WindowsDefender	Computer	Define the directory path to copy support log files
WindowsDefender	Computer	Configure IP Address Exclusions
WindowsDefender	Computer	Turn on script scanning
WindowsDefender	Computer	Allow Microsoft Defender Antivirus to update and communicate over a metered connection
WindowsDefender	Computer	Configure Network Protection to be allowed to be configured into block or audit mode on Windows Server
WindowsDefender	Computer	Control datagram processing for network protection
Sandbox	Computer	Allow vGPU sharing for Windows Sandbox
Sandbox	Computer	Allow networking in Windows Sandbox
Sandbox	Computer	Allow audio input in Windows Sandbox
Sandbox	Computer	Allow video input in Windows Sandbox
Sandbox	Computer	Allow printer sharing with Windows Sandbox
Sandbox	Computer	Allow clipboard sharing with Windows Sandbox
WindowsUpdate		<Changes in folder structure>

SERVICES- NOMS LONG - COURTS

Services par noms courts

Classés par Noms courts

Noms court	LONG NAME	Noms Longs - Gestionnaire de Services
AeLookupSvc	Application Experience	Expérience d'application
ALG	Application Layer Gateway Service	Service de la passerelle de la couche Application
AppHostSvc	Application Host Helper Service	Application Host Helper Service
AppIDSvc	Application Identity	Identité de l'application
Appinfo	Application Information	Informations d'application
AppMgmt	Application Management	Gestion d'applications
aspnet_state	ASP.NET State Service	Service d'état ASP.NET
AudioEndpointBuilder	Windows Audio Endpoint Builder	Générateur de points de terminaison du service Audio Windows
AudioSrv	Windows Audio	Audio Windows
AxInstSV	ActiveX Installer (AxInstSV)	Programme d'installation ActiveX (AxInstSV)
BDESVC	BitLocker Drive Encryption Service	Service de chiffrement de lecteur BitLocker
BFE	Base Filtering Engine	Moteur de filtrage de base
BITS	Background Intelligent Transfer Service	Service de transfert intelligent en arrière-plan
Browser	Computer Browser	Explorateur d'ordinateurs
bthserv	Bluetooth Support Service	Service de prise en charge Bluetooth
CertPropSvc	Certificate Propagation	Propagation du certificat
CISVC	Indexing Service	Service d'indexation
clr_optimization_v2.0.50727	Microsoft .NET Framework NGEN v2.0.50727	Microsoft .NET Framework NGEN v2.0.x
COMSysApp	COM+ System Application	Application système COM+
CryptSvc	Cryptographic Services	Services de chiffrement
CscService	Offline Files	Fichiers hors connexion
DcomLaunch	DCOM Server Process Launcher	Lanceur de processus serveur DCOM
defragsvc	Disk Defragmenter	Défragmenteur de disque
Diagtrack	Diagnostics Tracking Service	Gestions collecte des informations de diagnostic et télémtrie

Dhcp	DHCP Client	Client DHCP
Dnscache	DNS Client	Client DNS
dot3svc	Wired AutoConfig	Configuration automatique de réseau câblé
DPS	Diagnostic Policy Service	Service de stratégie de diagnostic
EapHost	Extensible Authentication Protocol	Protocole EAP (Extensible Authentication Protocol)
EFS	Encrypting File System (EFS)	Système de fichiers EFS (Encrypting File System)
ehRecvr	Windows Media Center Receiver Service	Service de réception Windows Media Center
ehSched	Windows Media Center Scheduler Service	Service de planification Windows Media Center
EventLog	Windows Event Log	Journal d'événements Windows
EventSystem	COM+ Event System	Système d'événement COM+
Fax	Fax	Télécopie
fdPHost	Function Discovery Provider Host	Hôte du fournisseur de découverte de fonctions
FDResPub	Function Discovery Resource Publication	Publication des ressources de découverte de fonctions
FontCache	Windows Font Cache Service	Service de cache de police Windows
FontCache3.0.0.0	Windows Presentation Foundation Font Cache 3.0.0.0	Cache de police de Windows Presentation Foundation 3
fsssvc	Windows Live Family Safety	Service Windows Live Contrôle parental
ftpsvc	Microsoft FTP Service	Service FTP Microsoft
gpsvc	Group Policy Client	Client de stratégie de groupe
hidserv	Human Interface Device Access	Accès du périphérique d'interface utilisateur
hkmsvc	Health Key and Certificate Management	Gestion des clés et des certificats d'intégrité
HomeGroupListener	HomeGroup Listener	Écouteur HomeGroup
HomeGroupProvider	HomeGroup Provider	Fournisseur HomeGroup
idsvc	Windows CardSpace	Windows CardSpace
IISADMIN	IIS Admin Service	Service d'administration IIS
IKEEXT	IKE and AuthIP	Modules de génération de clés IKE et

	IPsec Keying Modules	AuthIP
IPBusEnum	PnP-X IP Bus Enumerator	Énumérateur de bus IP PnP-X
iphlpsvc	IP Helper	Assistance IP
iprip	RIP Listener	RIP Listener
KeyIso	CNG Key Isolation	Isolation de clé CNG
KtmRm	KtmRm for Distributed Transaction Coordinator	Service KtmRm pour Distributed Transaction Coordinator
LanmanServer	Server	Serveur
LanmanWorkstation	Workstation	Station de travail
lltdsvc	Link-Layer Topology Discovery Mapper	Mappage de découverte de topologie de la couche de liaison
lmhosts	TCP/IP NetBIOS Helper	Assistance NetBIOS sur TCP/IP
LPDSVC	LPD Service	Service LPD
Mcx2Svc	Media Center Extender Service	Service Media Center Extender
MMCSS	Multimedia Class Scheduler	Planificateur de classes multimédias
MpsSvc	Windows Firewall	Pare-feu Windows
MSDTC	Distributed Transaction Coordinator	Coordinateur de transactions distribuées
MSiSCSI	Microsoft iSCSI Initiator Service	Service Initiateur iSCSI de Microsoft
msiserver	Windows Installer	Windows Installer
MSMQ	Message Queuing	Message Queuing
MSMQTriggers	Message Queuing Triggers	Déclencheurs Message Queuing
napagent	Network Access Protection Agent	Agent de protection d'accès réseau
Netlogon	Netlogon	Netlogon
Netman	Network Connections	Connexions réseau
NetMsmqActivator	Net.Msmq Listener Adapter	Adaptateur d'écouteur Net.Msmq
NetPipeActivator	Net.Pipe Listener Adapter	Adaptateur d'écouteur Net.Pipe
netprofm	Network List Service	Service Liste des réseaux
NetTcpActivator	Net.Tcp Listener Adapter	Adaptateur d'écouteur Net.Tcp
NetTcpPortSharing	Net.Tcp Port Sharing Service	Service de partage de ports Net.Tcp
NfsClnt	Client for NFS	Client pour NFS
NlaSvc	Network Location Awareness	Connaissance des emplacements réseau

nsi	Network Store Interface Service	Service Interface du magasin réseau
p2pimsvc	Peer Networking Identity Manager	Gestionnaire d'identité réseau homologue
p2psvc	Peer Networking Grouping	Groupement de mise en réseau de pairs
PcaSvc	Program Compatibility Assistant Service	Service de l'Assistant Compatibilité des programmes
PeerDistSvc	BranchCache	BranchCache
pla	Performance Logs & Alerts	Journaux & alertes de performance
PlugPlay	Plug and Play	Plug-and-Play
PNRPAutoReg	PNRP Machine Name Publication Service	Service de publication des noms d'ordinateurs PNRP
PNRPsvc	Peer Name Resolution Protocol	Protocole PNRP
PolicyAgent	IPsec Policy Agent	Agent de stratégie IPsec
Power	Power	Alimentation
ProfSvc	User Profile Service	Service de profil utilisateur
ProtectedStorage	Protected Storage	Emplacement protégé
QWAVE	Quality Windows Audio Video Experience	Expérience audio-vidéo haute qualité Windows
RasAuto	Remote Access Auto Connection Manager	Gestionnaire de connexion automatique d'accès distant
RasMan	Remote Access Connection Manager	Gestionnaire de connexions d'accès distant
RemoteAccess	Routing and Remote Access	Routage et accès distant
RemoteRegistry	Remote Registry	Registre à distance
RpcEptMapper	RPC Endpoint Mapper	Mappeur de point de terminaison RPC
RpcLocator	Remote Procedure Call (RPC) Locator	Localisateur d'appels de procédure distante (RPC)
RpcSs	Remote Procedure Call (RPC)	Appel de procédure distante (RPC)
SamSs	Security Accounts Manager	Gestionnaire de comptes de sécurité
SCardSvr	Smart Card	Carte à puce
Schedule	Task Scheduler	Planificateur de tâches
SCPolicySvc	Smart Card Removal Policy	Stratégie de retrait de la carte à puce
SDRSVC	Windows Backup	Sauvegarde Windows
SeaPort	SeaPort	SeaPort
seclogon	Secondary Logon	Ouverture de session secondaire
SENS	System Event Notification	Service de notification d'événements système

	Service	
SensrSvc	Adaptive Brightness	Brillance adaptative
SessionEnv	Remote Desktop Configuration	Configuration des services Bureau à distance
SharedAccess	Internet Connection Sharing (ICS)	Partage de connexion Internet (ICS)
ShellHWDetection	Shell Hardware Detection	Détection matériel noyau
simptcp	Simple TCP/IP Services	Services TCP/IP simples
SNMP	SNMP Service	Service SNMP
SNMPTRAP	SNMP Trap	Interruption SNMP
Spooler	Print Spooler	Spouleur d'impression
sppsvc	Software Protection	Protection logicielle
sppuinotify	SPP Notification Service	Service de notification SPP
SSDPSRV	SSDP Discovery	Découverte SSDP
SstpSvc	Secure Socket Tunneling Protocol Service	Service SSTP (Secure Socket Tunneling Protocol)
StiSvc	Windows Image Acquisition (WIA)	Acquisition d'image Windows (WIA)
StorSvc	Storage Service	Service de stockage
swprv	Microsoft Software Shadow Copy Provider	Fournisseur de cliché instantané de logiciel Microsoft
SysMain	Superfetch	Superfetch
TabletInputService	Tablet PC Input Service	Service Panneau de saisie Tablet PC
TapiSrv	Telephony	Téléphonie
TBS	TPM Base Services	Services de base de module de plateforme sécurisée
TermService	Remote Desktop Services	Services Bureau à distance
Themes	Themes	Thèmes
THREADORDER	Thread Ordering Server	Serveur de priorités des threads
TlntSvr	Telnet	Telnet
TrkWks	Distributed Link Tracking Client	Client de suivi de lien distribué
TrustedInstaller	Windows Modules Installer	Programme d'installation pour les modules Windows
UI0Detect	Interactive Services Detection	Détection de services interactifs
UmRdpService	Remote Desktop Services UserMode Port Redirector	Redirecteur de port du mode utilisateur des services Bureau à distance
upnphost	UPnP Device Host	Hôte de périphérique UPnP

UxSms	Desktop Window Manager Session Manager	Gestionnaire de sessions du Gestionnaire de fenêtrage
VaultSvc	Credential Manager	Gestionnaire d'informations d'identification
vds	Virtual Disk	Disque virtuel
VSS	Volume Shadow Copy	Cliché instantané des volumes
W32Time	Windows Time	Temps Windows
W3SVC	World Wide Web Publishing Service	Service de publication World Wide Web
WAS	Windows Process Activation Service	Service d'activation des processus Windows
wbengine	Block Level Backup Engine Service	Service de moteur de sauvegarde en mode bloc
WbioSrvc	Windows Biometric Service	Service de biométrie Windows
wcncsvc	Windows Connect Now - Config Registrar	Windows Connect Now - Registre de configuration
WcsPlugInService	Windows Color System	Système de couleurs Windows
WdiServiceHost	Diagnostic Service Host	Service hôte WDIServiceHost
WdiSystemHost	Diagnostic System Host	Hôte système de diagnostics
WebClient	WebClient	WebClient
Wecsvc	Windows Event Collector	Collecteur d'événements de Windows
wercplsupport	Problem Reports and Solutions Control Panel Support	Prise en charge de l'application Rapports et solutions aux problèmes du Panneau de configuration
WerSvc	Windows Error Reporting Service	Service de rapport d'erreurs Windows
WinDefend	Windows Defender	Windows Defender
WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service	Service de découverte automatique de Proxy Web pour les services HTTP Windows
Winmgmt	Windows Management Instrumentation	Infrastructure de gestion Windows
WinRM	Windows Remote Management (WS-Management)	Gestion à distance de Windows (Gestion WSM)
Wlansvc	WLAN AutoConfig	Service de configuration automatique WLAN
wmiApSrv	WMI Performance Adapter	Carte de performance WMI
WMPNetworkSvc	Windows Media Player Network	Service Partage réseau du Lecteur Windows Media

	Sharing Service	
WMSVC	Web Management Service	Service de gestion Web
WPCSvc	Parental Controls	Parental Controls
WPDBusEnum	Portable Device Enumerator Service	Service Énumérateur d'appareil mobile
wscsvc	Security Center	Centre de sécurité
WSearch	Windows Search	Windows Search
wuauserv	Windows Update	Windows Update
wudfsvc	Windows Driver Foundation - User-mode Driver Framework	Windows Driver Foundation - Infrastructure de pilote mode-utilisateur
WwanSvc	WWAN AutoConfig	Service de configuration automatique WWAN

Services par noms longs - fr

Classés par Noms longs français

Noms Longs - Gestionnaire de Services	**Nom court**	**LONG NAME**
Accès du périphérique d'interface utilisateur	hidserv	Human Interface Device Access
Acquisition d'image Windows (WIA)	StiSvc	Windows Image Acquisition (WIA)
Adaptateur d'écouteur Net.Msmq	NetMsmqActivator	Net.Msmq Listener Adapter
Adaptateur d'écouteur Net.Pipe	NetPipeActivator	Net.Pipe Listener Adapter
Adaptateur d'écouteur Net.Tcp	NetTcpActivator	Net.Tcp Listener Adapter
Agent de protection d'accès réseau	napagent	Network Access Protection Agent
Agent de stratégie IPsec	PolicyAgent	IPsec Policy Agent
Alimentation	Power	Power
Appel de procédure distante (RPC)	RpcSs	Remote Procedure Call (RPC)
Application Host Helper Service	AppHostSvc	Application Host Helper Service
Application système COM+	COMSysApp	COM+ System Application
Assistance IP	iphlpsvc	IP Helper
Assistance NetBIOS sur TCP/IP	lmhosts	TCP/IP NetBIOS Helper
Audio Windows	AudioSrv	Windows Audio
BranchCache	PeerDistSvc	BranchCache
Brillance adaptative	SensrSvc	Adaptive Brightness
Cache de police de Windows Presentation Foundation 3	FontCache 3.0.0.0	Windows Presentation Foundation Font Cache 3.0.0.0
Carte à puce	SCardSvr	Smart Card

Carte de performance WMI	wmiApSrv	WMI Performance Adapter
Centre de sécurité	wscsvc	Security Center
Cliché instantané des volumes	VSS	Volume Shadow Copy
Client de stratégie de groupe	gpsvc	Group Policy Client
Client de suivi de lien distribué	TrkWks	Distributed Link Tracking Client
Client DHCP	Dhcp	DHCP Client
Client DNS	Dnscache	DNS Client
Client pour NFS	NfsClnt	Client for NFS
Collecteur d'événements de Windows	Wecsvc	Windows Event Collector
Configuration automatique de réseau câblé	dot3svc	Wired AutoConfig
Configuration des services Bureau à distance	SessionEnv	Remote Desktop Configuration
Connaissance des emplacements réseau	NlaSvc	Network Location Awareness
Connexions réseau	Netman	Network Connections
Coordinateur de transactions distribuées	MSDTC	Distributed Transaction Coordinator
Déclencheurs Message Queuing	MSMQTriggers	Message Queuing Triggers
Découverte SSDP	SSDPSRV	SSDP Discovery
Défragmenteur de disque	defragsvc	Disk Defragmenter
Détection de services interactifs	UI0Detect	Interactive Services Detection
Détection matériel noyau	ShellHWDetection	Shell Hardware Detection
Disque virtuel	vds	Virtual Disk
Écouteur HomeGroup	HomeGroupListener	HomeGroup Listener
Emplacement protégé	ProtectedStorage	Protected Storage
Énumérateur de bus IP PnP-X	IPBusEnum	PnP-X IP Bus Enumerator
Expérience audio-vidéo haute qualité Windows	QWAVE	Quality Windows Audio Video Experience
Expérience d'application	AeLookupSvc	Application Experience
Explorateur d'ordinateurs	Browser	Computer Browser
Expérience des utilisateurs connectés et télémétrie	DiagTrack	Diagnostics Tracking Service
Fichiers hors connexion	CscService	Offline Files
Fournisseur de cliché instantané de logiciel Microsoft	swprv	Microsoft Software Shadow Copy Provider
Fournisseur HomeGroup	HomeGroupProvider	HomeGroup Provider
Générateur de points de terminaison du service Audio Windows	AudioEndpointBuilder	Windows Audio Endpoint Builder
Gestion à distance de Windows (Gestion WSM)	WinRM	Windows Remote Management (WS-Management)
Gestion d'applications	AppMgmt	Application Management
Gestion des clés et des certificats d'intégrité	hkmsvc	Health Key and Certificate

		Management
Gestionnaire d'identité réseau homologue	p2pimsvc	Peer Networking Identity Manager
Gestionnaire d'informations d'identification	VaultSvc	Credential Manager
Gestionnaire de comptes de sécurité	SamSs	Security Accounts Manager
Gestionnaire de connexion automatique d'accès distant	RasAuto	Remote Access Auto Connection Manager
Gestionnaire de connexions d'accès distant	RasMan	Remote Access Connection Manager
Gestionnaire de sessions du Gestionnaire de fenêtrage	UxSms	Desktop Window Manager Session Manager
Groupement de mise en réseau de pairs	p2psvc	Peer Networking Grouping
Hôte de périphérique UPnP	upnphost	UPnP Device Host
Hôte du fournisseur de découverte de fonctions	fdPHost	Function Discovery Provider Host
Hôte système de diagnostics	WdiSystem Host	Diagnostic System Host
Identité de l'application	AppIDSvc	Application Identity
Informations d'application	Appinfo	Application Information
Infrastructure de gestion Windows	Winmgmt	Windows Management Instrumentation
Interruption SNMP	SNMPTRAP	SNMP Trap
Isolation de clé CNG	KeyIso	CNG Key Isolation
Journal d'événements Windows	EventLog	Windows Event Log
Journaux & alertes de performance	pla	Performance Logs & Alerts
Lanceur de processus serveur DCOM	DcomLaunch	DCOM Server Process Launcher
Localisateur d'appels de procédure distante (RPC)	RpcLocator	Remote Procedure Call (RPC) Locator
Mappage de découverte de topologie de la couche de liaison	lltdsvc	Link-Layer Topology Discovery Mapper
Mappeur de point de terminaison RPC	RpcEptMapper	RPC Endpoint Mapper
Message Queuing	MSMQ	Message Queuing
Microsoft .NET Framework NGEN v2.0.x	clr_optimization_v2.0.50727	Microsoft .NET Framework NGEN v2.0.50727
Modules de génération de clés IKE et AuthIP	IKEEXT	IKE and AuthIP IPsec Keying Modules
Moteur de filtrage de base	BFE	Base Filtering Engine
Netlogon	Netlogon	Netlogon
Ouverture de session secondaire	seclogon	Secondary Logon
Pare-feu Windows	MpsSvc	Windows Firewall
Parental Controls	WPCSvc	Parental Controls
Partage de connexion Internet (ICS)	SharedAccess	Internet Connection Sharing (ICS)
Planificateur de classes multimédias	MMCSS	Multimedia Class Scheduler
Planificateur de tâches	Schedule	Task Scheduler

Plug-and-Play	PlugPlay	Plug and Play
Prise en charge de l'application Rapports et solutions aux problèmes du Panneau de configuration	wercplsupport	Problem Reports and Solutions Control Panel Support
Programme d'installation ActiveX (AxInstSV)	AxInstSV	ActiveX Installer (AxInstSV)
Programme d'installation pour les modules Windows	TrustedInstaller	Windows Modules Installer
Propagation du certificat	CertPropSvc	Certificate Propagation
Protection logicielle	sppsvc	Software Protection
Protocole EAP (Extensible Authentication Protocol)	EapHost	Extensible Authentication Protocol
Protocole PNRP	PNRPsvc	Peer Name Resolution Protocol
Publication des ressources de découverte de fonctions	FDResPub	Function Discovery Resource Publication
Redirecteur de port du mode utilisateur des services Bureau à distance	UmRdpService	Remote Desktop Services UserMode Port Redirector
Registre à distance	RemoteRegistry	Remote Registry
RIP Listener	iprip	RIP Listener
Routage et accès distant	RemoteAccess	Routing and Remote Access
Sauvegarde Windows	SDRSVC	Windows Backup
SeaPort	SeaPort	SeaPort
Serveur	LanmanServer	Server
Serveur de priorités des threads	THREADORDER	Thread Ordering Server
Service d'activation des processus Windows	WAS	Windows Process Activation Service
Service d'administration IIS	IISADMIN	IIS Admin Service
Service de biométrie Windows	WbioSrvc	Windows Biometric Service
Service de cache de police Windows	FontCache	Windows Font Cache Service
Service de chiffrement de lecteur BitLocker	BDESVC	BitLocker Drive Encryption Service
Service de configuration automatique WLAN	Wlansvc	WLAN AutoConfig
Service de configuration automatique WWAN	WwanSvc	WWAN AutoConfig
Service de découverte automatique de Proxy Web pour les services HTTP Windows	WinHttpAutoProxySvc	WinHTTP Web Proxy Auto-Discovery Service
Service de gestion Web	WMSVC	Web Management Service
Service de l'Assistant Compatibilité des programmes	PcaSvc	Program Compatibility Assistant Service
Service de la passerelle de la couche Application	ALG	Application Layer Gateway Service
Service de moteur de sauvegarde en mode bloc	wbengine	Block Level Backup Engine Service

Service de notification d'événements système	SENS	System Event Notification Service
Service de notification SPP	sppuinotify	SPP Notification Service
Service de partage de ports Net.Tcp	NetTcpPortSharing	Net.Tcp Port Sharing Service
Service de planification Windows Media Center	ehSched	Windows Media Center Scheduler Service
Service de prise en charge Bluetooth	bthserv	Bluetooth Support Service
Service de profil utilisateur	ProfSvc	User Profile Service
Service de publication des noms d'ordinateurs PNRP	PNRPAutoReg	PNRP Machine Name Publication Service
Service de publication World Wide Web	W3SVC	World Wide Web Publishing Service
Service de rapport d'erreurs Windows	WerSvc	Windows Error Reporting Service
Service de réception Windows Media Center	ehRecvr	Windows Media Center Receiver Service
Service de stockage	StorSvc	Storage Service
Service de stratégie de diagnostic	DPS	Diagnostic Policy Service
Service de transfert intelligent en arrière-plan	BITS	Background Intelligent Transfer Service
Service d'état ASP.NET	aspnet_state	ASP.NET State Service
Service d'indexation	CISVC	Indexing Service
Service Énumérateur d'appareil mobile	WPDBusEnum	Portable Device Enumerator Service
Service FTP Microsoft	ftpsvc	Microsoft FTP Service
Service hôte WDIServiceHost	WdiServiceHost	Diagnostic Service Host
Service Initiateur iSCSI de Microsoft	MSiSCSI	Microsoft iSCSI Initiator Service
Service Interface du magasin réseau	nsi	Network Store Interface Service
Service KtmRm pour Distributed Transaction Coordinator	KtmRm	KtmRm for Distributed Transaction Coordinator
Service Liste des réseaux	netprofm	Network List Service
Service LPD	LPDSVC	LPD Service
Service Media Center Extender	Mcx2Svc	Media Center Extender Service
Service Panneau de saisie Tablet PC	TabletInputService	Tablet PC Input Service
Service Partage réseau du Lecteur Windows Media	WMPNetworkSvc	Windows Media Player Network Sharing Service
Service SNMP	SNMP	SNMP Service
Service SSTP (Secure Socket Tunneling Protocol)	SstpSvc	Secure Socket Tunneling Protocol Service
Service Windows Live Contrôle parental	fsssvc	Windows Live Family Safety
Services Bureau à distance	TermService	Remote Desktop Services
Services de base de module de plateforme sécurisée	TBS	TPM Base Services

Services de chiffrement	CryptSvc	Cryptographic Services
Services TCP/IP simples	simptcp	Simple TCP/IP Services
Spouleur d'impression	Spooler	Print Spooler
Station de travail	LanmanWorkstation	Workstation
Stratégie de retrait de la carte à puce	SCPolicySvc	Smart Card Removal Policy
Superfetch	SysMain	Superfetch
Système d'événement COM+	EventSystem	COM+ Event System
Système de couleurs Windows	WcsPlugInService	Windows Color System
Système de fichiers EFS (Encrypting File System)	EFS	Encrypting File System (EFS)
Télécopie	Fax	Fax
Téléphonie	TapiSrv	Telephony
Telnet	TlntSvr	Telnet
Temps Windows	W32Time	Windows Time
Thèmes	Themes	Themes
WebClient	WebClient	WebClient
Windows CardSpace	idsvc	Windows CardSpace
Windows Connect Now - Registre de configuration	wcncsvc	Windows Connect Now - Config Registrar
Windows Defender	WinDefend	Windows Defender
Windows Driver Foundation - Infrastructure de pilote mode-utilisateur	wudfsvc	Windows Driver Foundation - User-mode Driver Framework
Windows Installer	msiserver	Windows Installer
Windows Search	WSearch	Windows Search
Windows Update	wuauserv	Windows Update