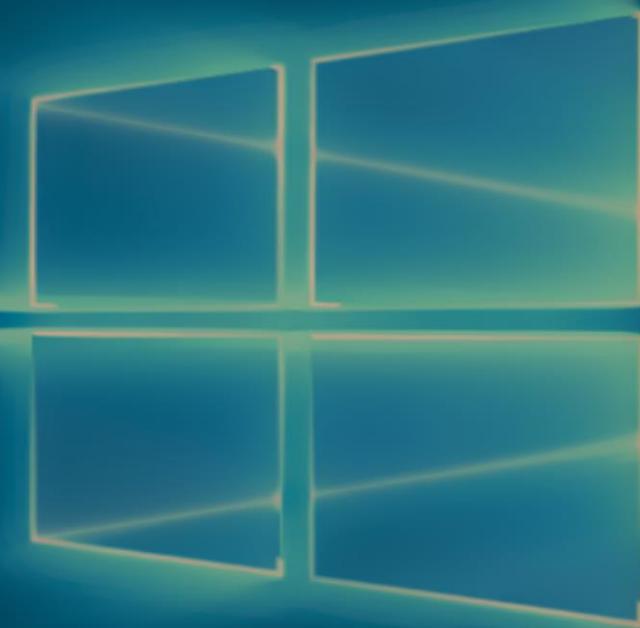


Windows 10



Windows 10 Création

Monter l'ISO Windows 10 (Ici l'ISO = E:\)

Monter VHDX vierge initialisé avec Volume Simple (Ici VHDX = Z:\)

Ouvrir un CMD en administrateur

Se positionner sur l'ISO

E:

cd sources

Dism /apply-image /imagefile:install.wim /index:1 /applydir:Z:\

bcdedit /copy {current} /d "Windows Formation"

bcdedit /set {{ID}} device vhd=[C:]\\Chemin\\fichier.vhdx

bcdedit /set {{ID}} osdevice vhd=[C:]\\Chemin\\fichier.vhdx

bcdedit /set {{ID}} detecthal on

shutdown -r -t 0



Versions Windows



Licensing

Features	Home	Pro	Enterprise	Education
Device Encryption ⁶	✓	✓	✓	✓
Domain Join		✓	✓	✓
Group Policy Management		✓	✓	✓
BitLocker ²		✓	✓	✓
Enterprise Mode Internet Explorer (EMIE)		✓	✓	✓
Assigned Access 8.1		✓	✓	✓
Remote Desktop		✓	✓	✓
Direct Access			✓	✓
Windows To Go Creator			✓	✓
AppLocker			✓	✓
BranchCache			✓	✓
Start Screen Control with Group Policy			✓	✓

Méthode d'installation

1. Installation depuis un DVD

Cette méthode d'installation est manuelle et introduit certains concepts de personnalisation qui seront détaillés dans la suite de ce chapitre.

L'installation de Windows depuis un DVD est la méthode d'installation la plus utilisée par le grand public. Cette méthode d'installation requiert un DVD soit provenant d'un achat de Windows 8.1, soit issu de la gravure d'une image téléchargée sur les sites de téléchargements Microsoft.

Cette méthode convient pour l'installation standard de Windows mais les possibilités de personnalisation sont limitées, notamment par la taille maximale du média.

Il est possible de personnaliser la configuration de l'exécution de l'installation via l'utilisation d'un fichier de réponses placé sur une clé USB ou à la racine d'un des lecteurs.

Méthodes d'installation

L'installation de Windows depuis une clé USB ou depuis un périphérique amovible est réalisable sous deux conditions :

- Le poste de travail doit être capable de démarrer sur le média.
- Le média doit disposer de suffisamment d'espace libre pour accueillir les fichiers d'installation.

Cette méthode d'installation est similaire à l'installation depuis un DVD. L'utilisation d'une clé USB offre cependant de multiples avantages :

- Capacité de personnalisation de l'image limitée à l'espace disponible sur la clé USB et personnalisations réalisables directement sur la clé USB.
- Rapidité d'installation induite par les performances accrues des clés USB comparativement aux lecteurs de DVD.

Méthodes d'installation

Autres outils orientés système :

- Windows Deployment Service
- Microsoft Deployment Toolkit
- System Center

Multi Boot

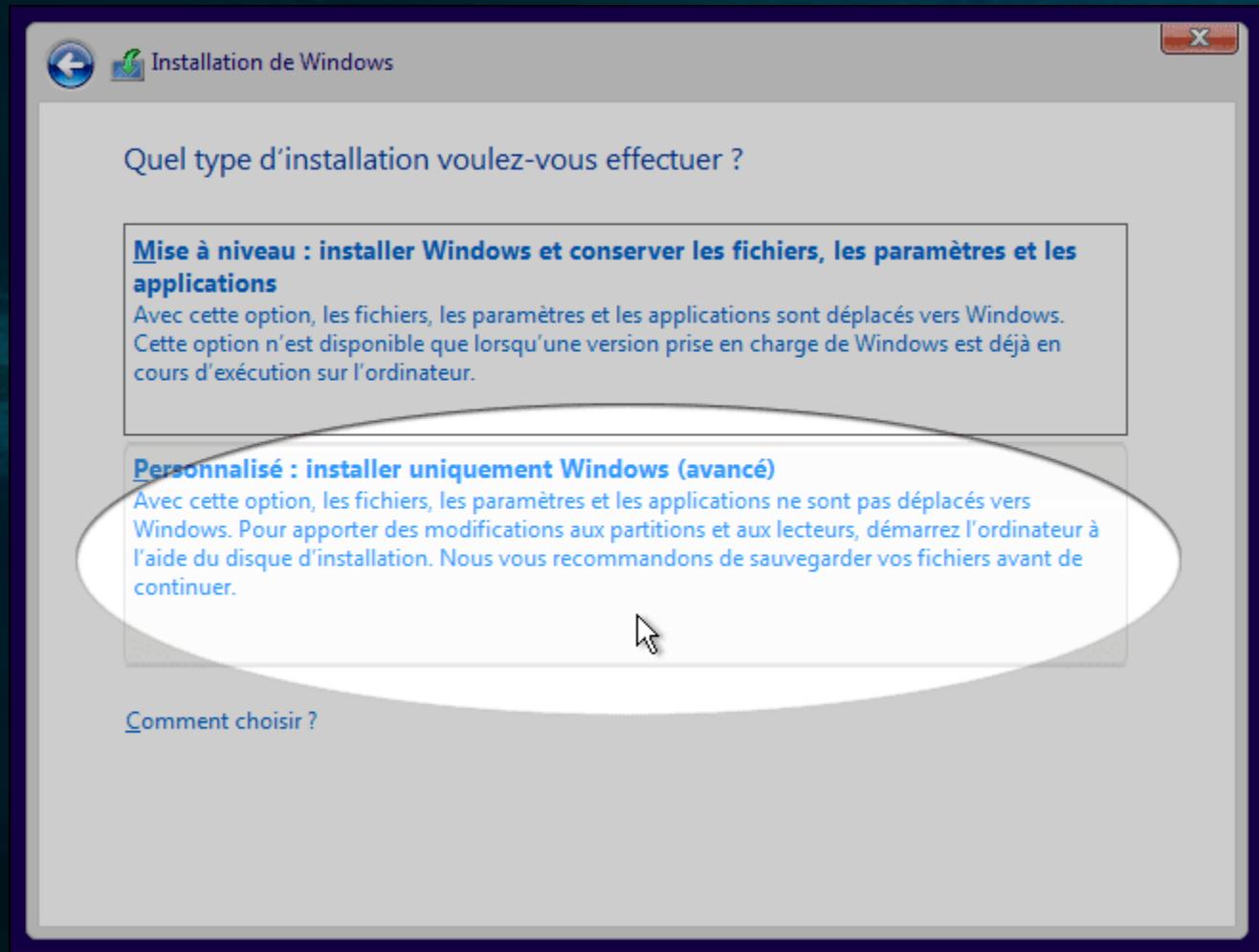
Le démarrage multiple, ou Multi-Boot, permet aux utilisateurs de sélectionner lors du démarrage le système d'exploitation de leur choix.



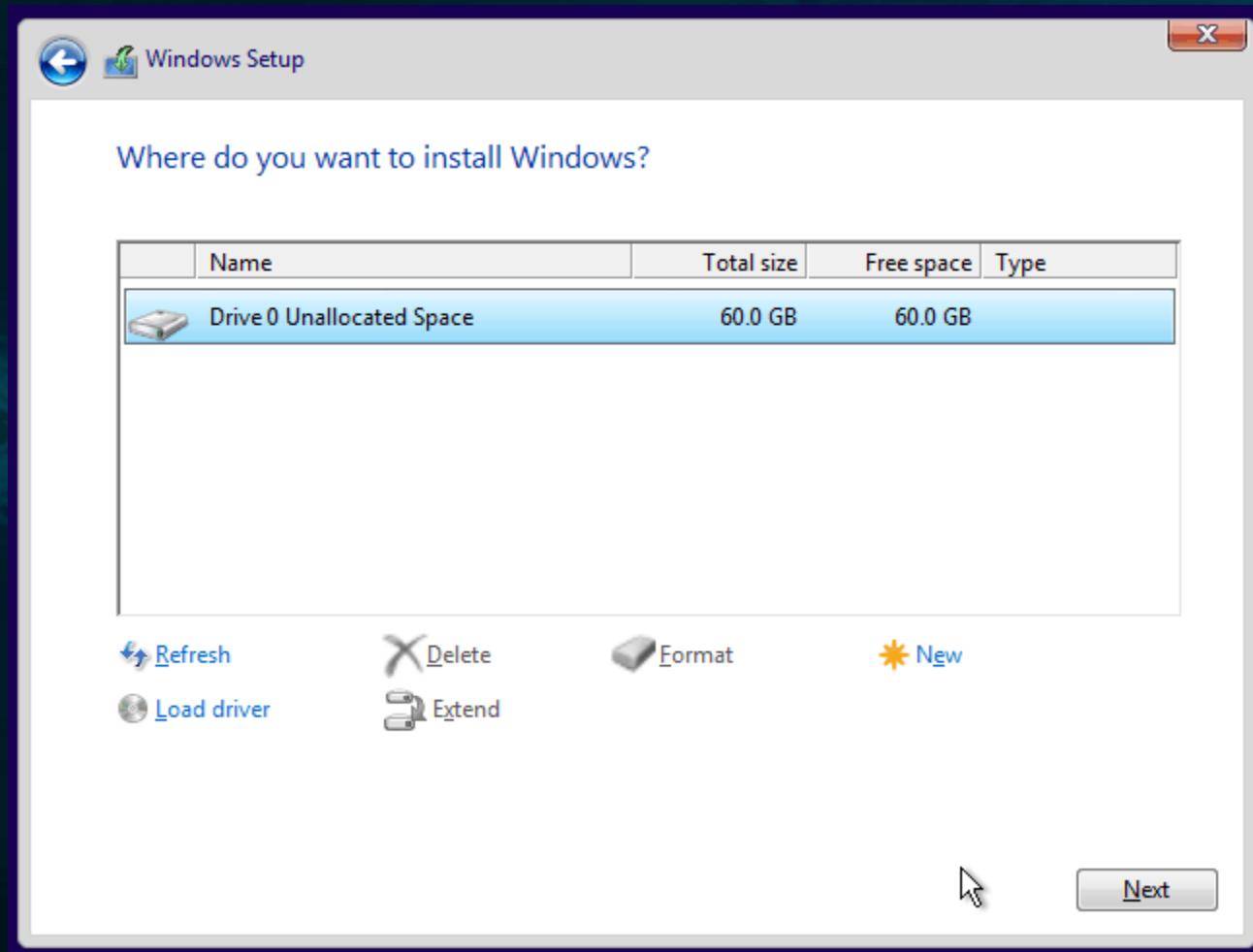
Installation

- Crée une clé USB bootable (utilitaire Windows,Rufus..)
- Vérifier l'ordre du boot dans le bios de la CM
- Booter sur l'ISO puis suivre l'assistant.

Partitionement



Partitionement



Installation

- Pas de demande de clé ??? :
- Clé OEM inclue dans la carte mère (Original Equipment Manufacturer)
- Plus d'étiquette sur le poste.

Principales

Le menu démarrer



L'assistante Cortana



Les bureaux virtuels



Le navigateur Microsoft
Edge

Centre de notifications



Gestion des outils tactiles

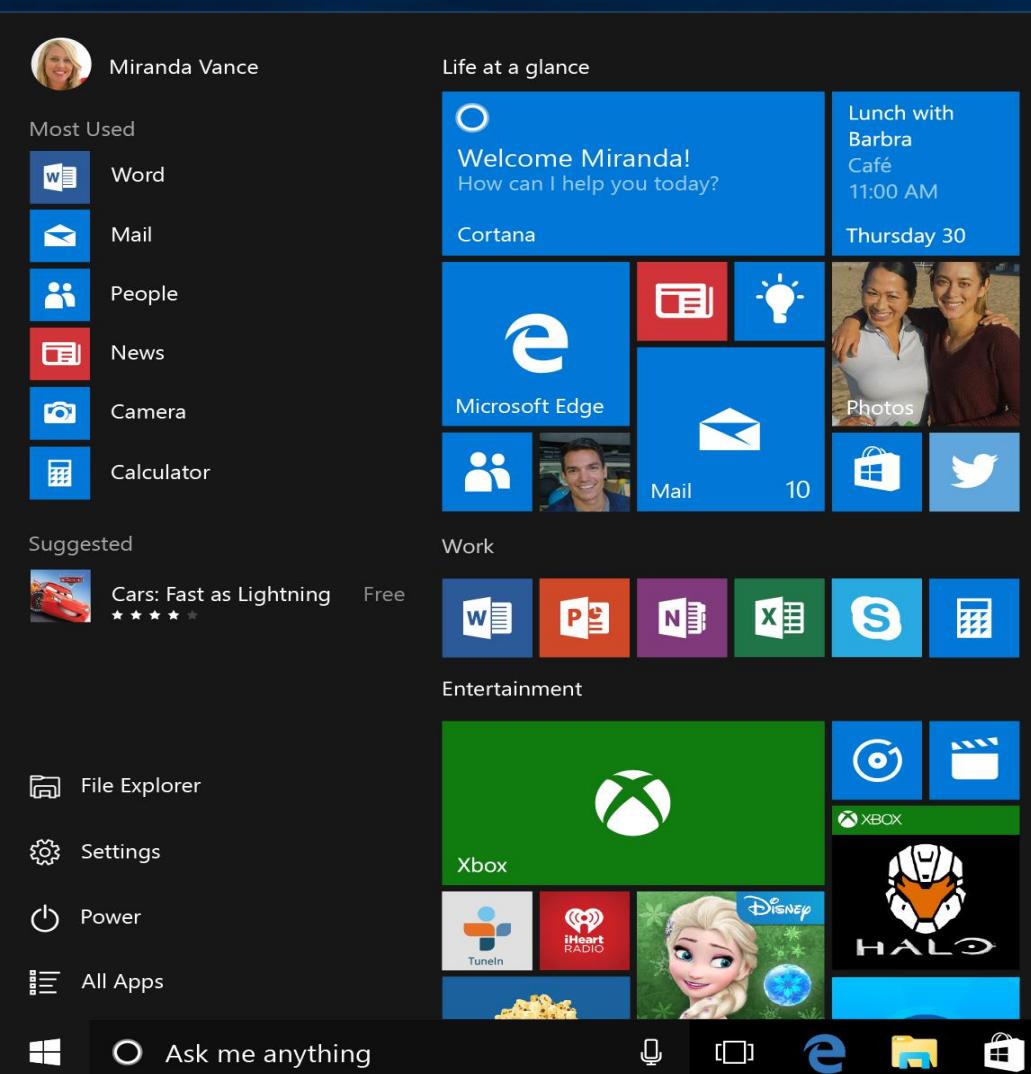


Amélioration Win Defender



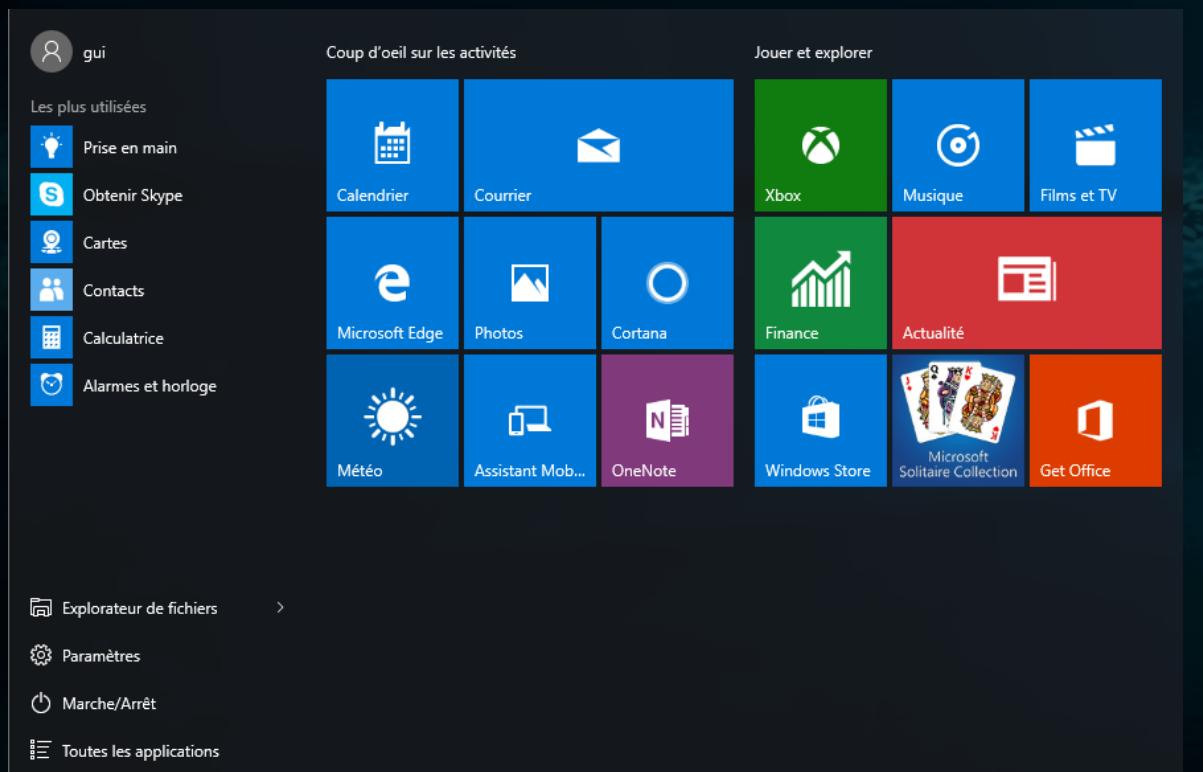
Edge

Windows 10 Interface

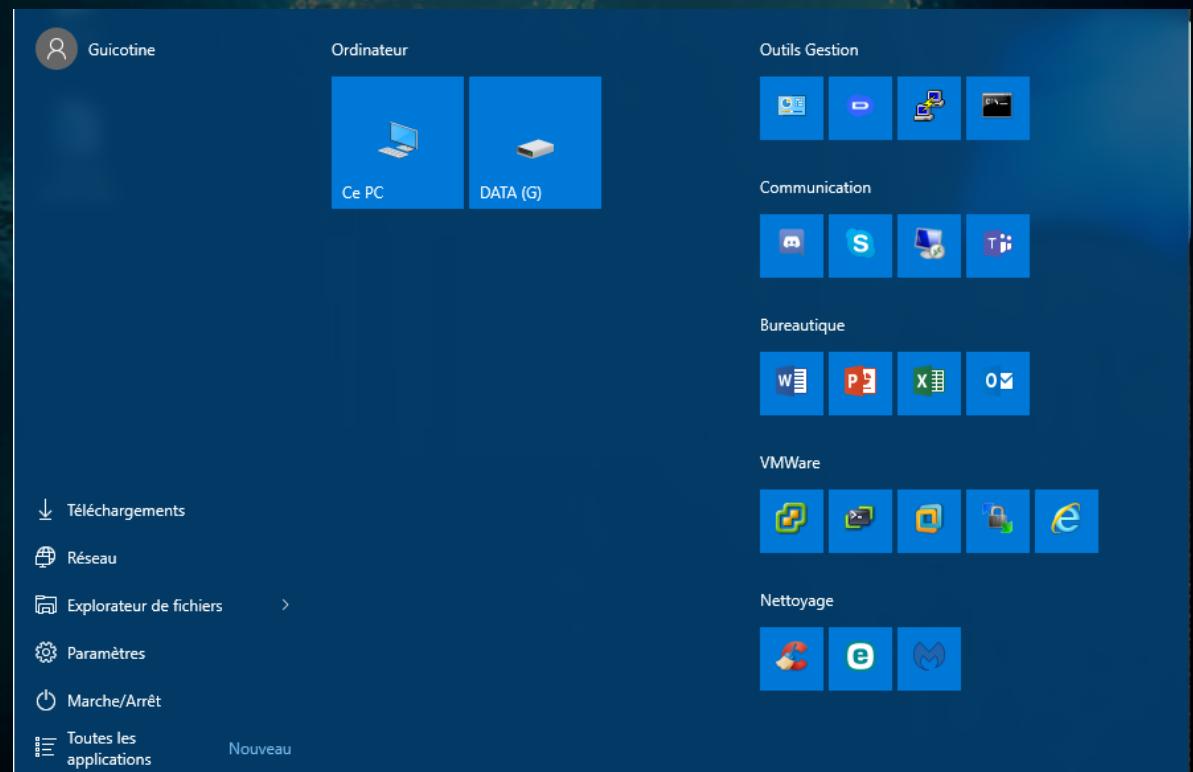


Les vignettes

Menu démarrer natif



Menu démarrer personnalisé



Les vignettes

The image shows the Windows Start menu interface. At the top left is a three-line menu icon. Below it are two sections: "Coup d'oeil sur les activités" (Overview of activities) and "Jouer et explorer" (Play and explore). The "Coup d'oeil sur les activités" section contains tiles for Calendrier, Courrier, Microsoft Edge, Photos, Cortana, Météo, Assistant Mobile, and OneNote. The "Jouer et explorer" section contains tiles for Xbox, Musique, Films et TV, Finance, Actualité, Windows Store, Microsoft Solitaire Collection, and Get Office. The bottom of the screen features the taskbar with icons for File Explorer, Edge, File Explorer, and Task View, along with a search bar and system status icons.

Coup d'oeil sur les activités

Jouer et explorer

Calendrier

Courrier

Microsoft Edge

Photos

Cortana

Météo

Assistant Mobile

OneNote

Xbox

Musique

Films et TV

Finance

Actualité

Windows Store

Microsoft Solitaire Collection

Get Office

Rechercher sur le web et dans Windows

File Explorer

Edge

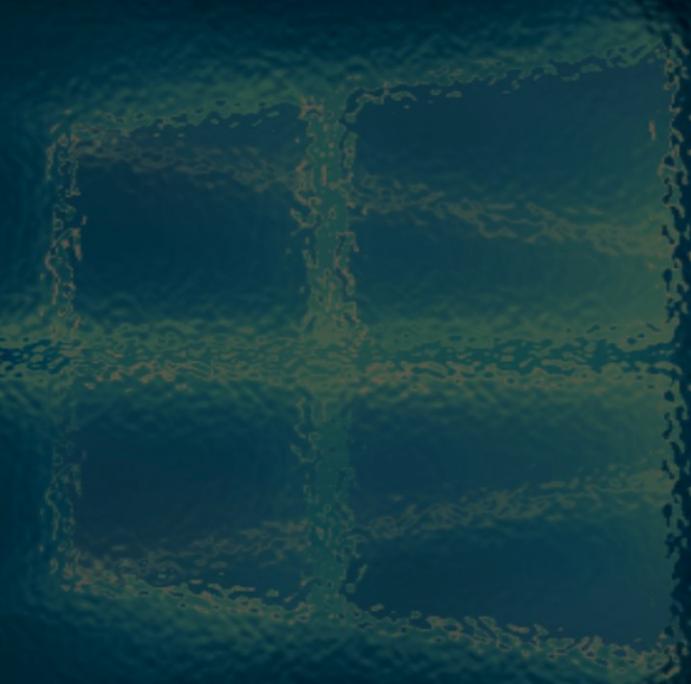
File Explorer

Task View

Les vignettes

La personnalisation :

- Taille du menu démarrer
- Passer du mode standard à plein écran
- Personnalisation des couleurs
- Ajout/Suppression de répertoires systèmes
- Ajout/Suppression d'éléments parmi les tuiles
- Modification/Activation/Suppression de tuiles



Outils

Panneau de configuration

Système et sécurité
Consulter l'état de votre ordinateur
Enregistrer des copies de sauvegarde de vos fichiers à l'aide de l'Historique des fichiers
Sauvegarder et restaurer (Windows 7)
Rechercher et résoudre des problèmes

Réseau et Internet
Se connecter à Internet
Afficher l'état et la gestion du réseau
Choisir les options de groupe résidentiel et de partage

Matériel et audio
Afficher les périphériques et imprimantes
Ajouter un périphérique
Ajuster les paramètres de mobilité communément utilisés

Programmes
Désinstaller un programme

Comptes d'utilisateurs
Modifier le type de compte

Apparence et personnalisation
Modifier le thème
Modifier la résolution de l'écran

Horloge, langue et région
Ajouter une langue
Modifier les méthodes d'entrée
Modifier les formats de date, d'heure ou de nombre

Options d'ergonomie
Laisser Windows suggérer les paramètres
Optimiser l'affichage

Paramètres

Système
Affichage, notifications, applications, alimentation

Périphériques
Bluetooth, imprimantes, souris

Réseau et Internet
Wi-Fi, mode Avion, VPN

Personnalisation
Arrière-plan, écran de verrouillage, couleurs

Comptes
Votre compte, synchroniser les paramètres, travail,

Heure et langue
Voix, région, date

Options d'ergonomie
Narrateur, loupe, contraste élevé

Confidentialité
Emplacement, caméra

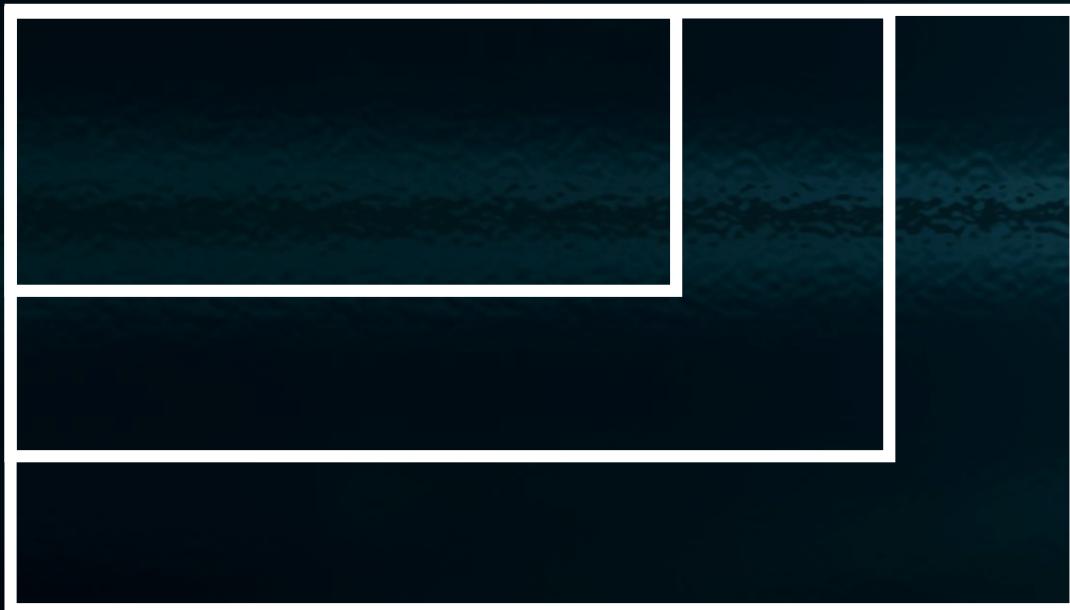
Mise à jour et sécurité
Windows Update, récupération, sauvegarde

Menu démarrer & Barre de tâches



Affichage

Résolution d'écran



Police d'affichage

Texte à 100%

Texte à 125%

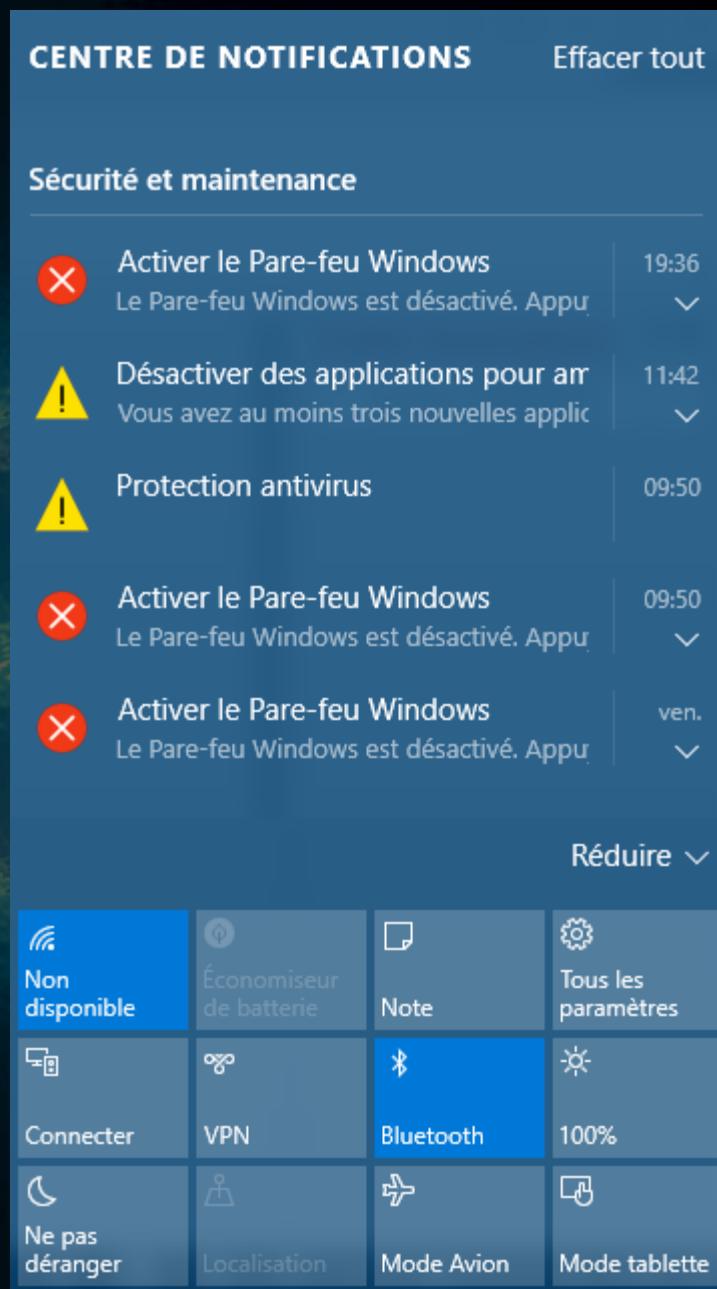
Texte à 150%

Texte à 175%

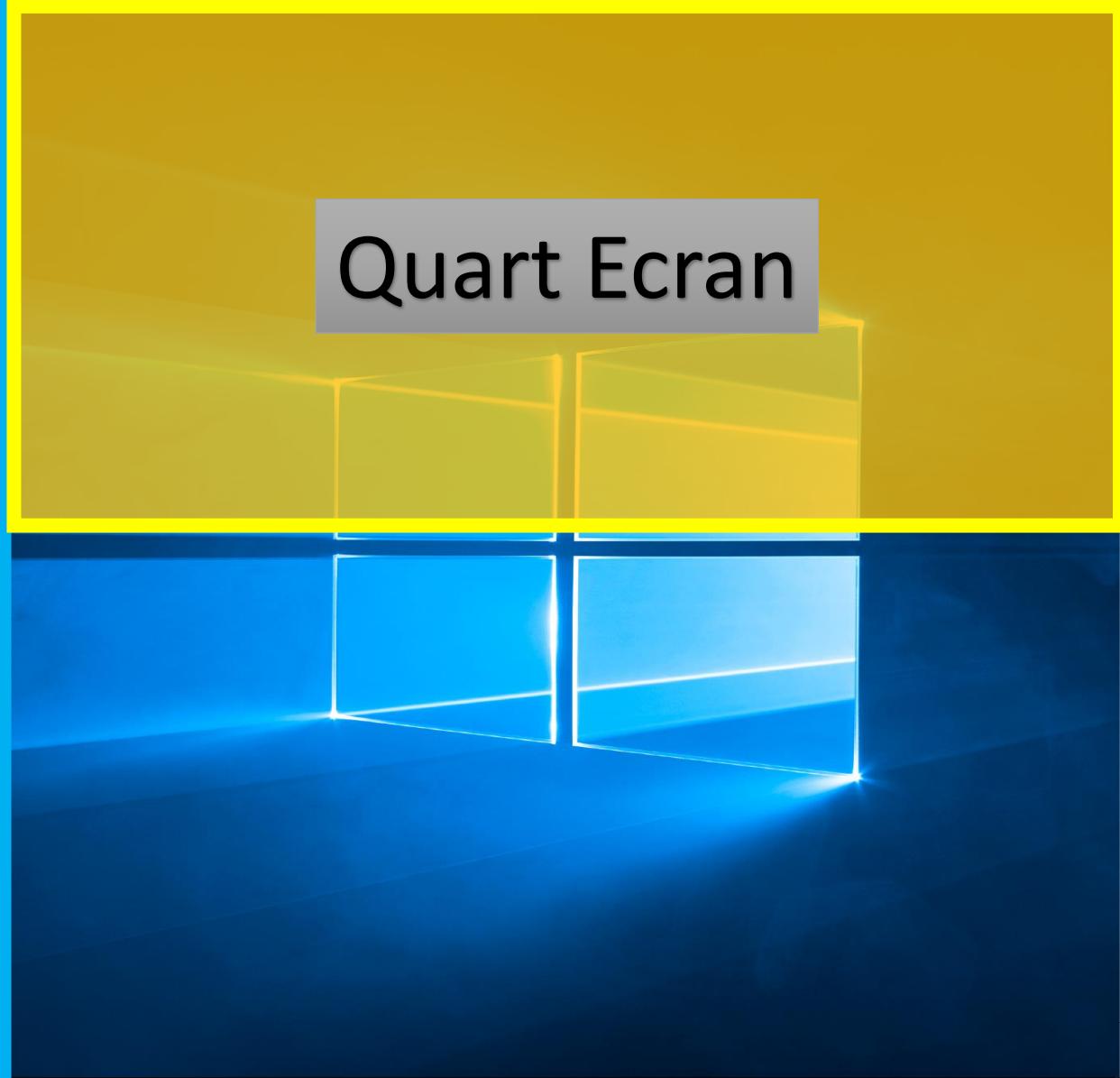
Notifications et Options

Notifications

Modes



Le positionnement (SnapAssist)

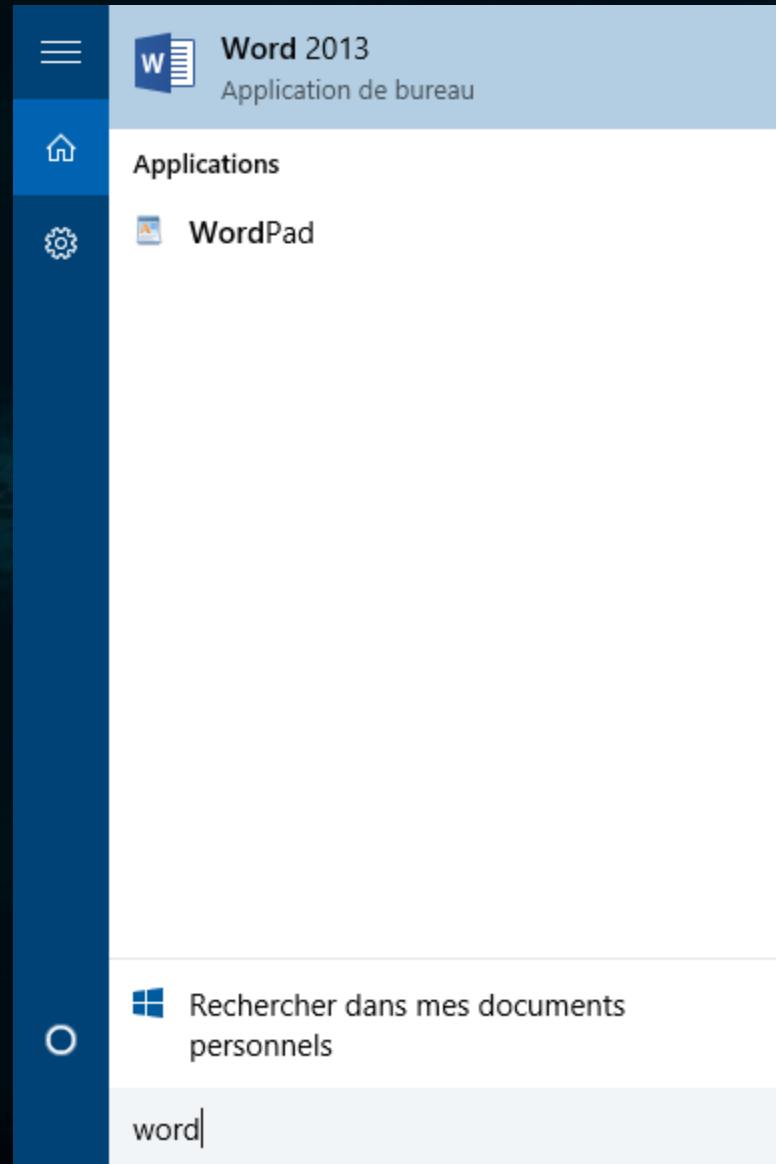


Recherche (Fichiers)

The screenshot shows a Windows File Explorer window with the title bar "Outils de recherche * .mp3 - Résultats de la recherche dans DATA (G:)" and the tab "Recherche" selected. The left sidebar shows standard folder icons like AppData, Bureau, Contacts, etc., and the "DATA (G:)" drive is highlighted. The main pane displays a list of mp3 files found in the DATA (G:) drive, each with its name, genre (mostly "Other"), duration, and size. A status bar at the bottom indicates "724 élément(s)".

Nom du fichier	Genre	Longueur	Taille
affirmative.mp3	Other	00:00:01	4,43 Ko
begin.mp3	Other	00:00:02	9,31 Ko
complete.mp3	Other	00:00:01	5,28 Ko
diagnostic.mp3	Other	00:00:03	13,7 Ko
processing.mp3	Other	00:00:01	6,15 Ko
transfer.mp3	Other	00:00:03	11,9 Ko
verified.mp3	Other	00:00:02	8,93 Ko
warning.mp3	Other	00:00:02	10,1 Ko
inputok.mp3	Other	00:00:00	2,78 Ko
inputfailed.mp3	Other	00:00:00	2,78 Ko
incominatransmission.mp3	Other	00:00:02	

Recherche (applications)

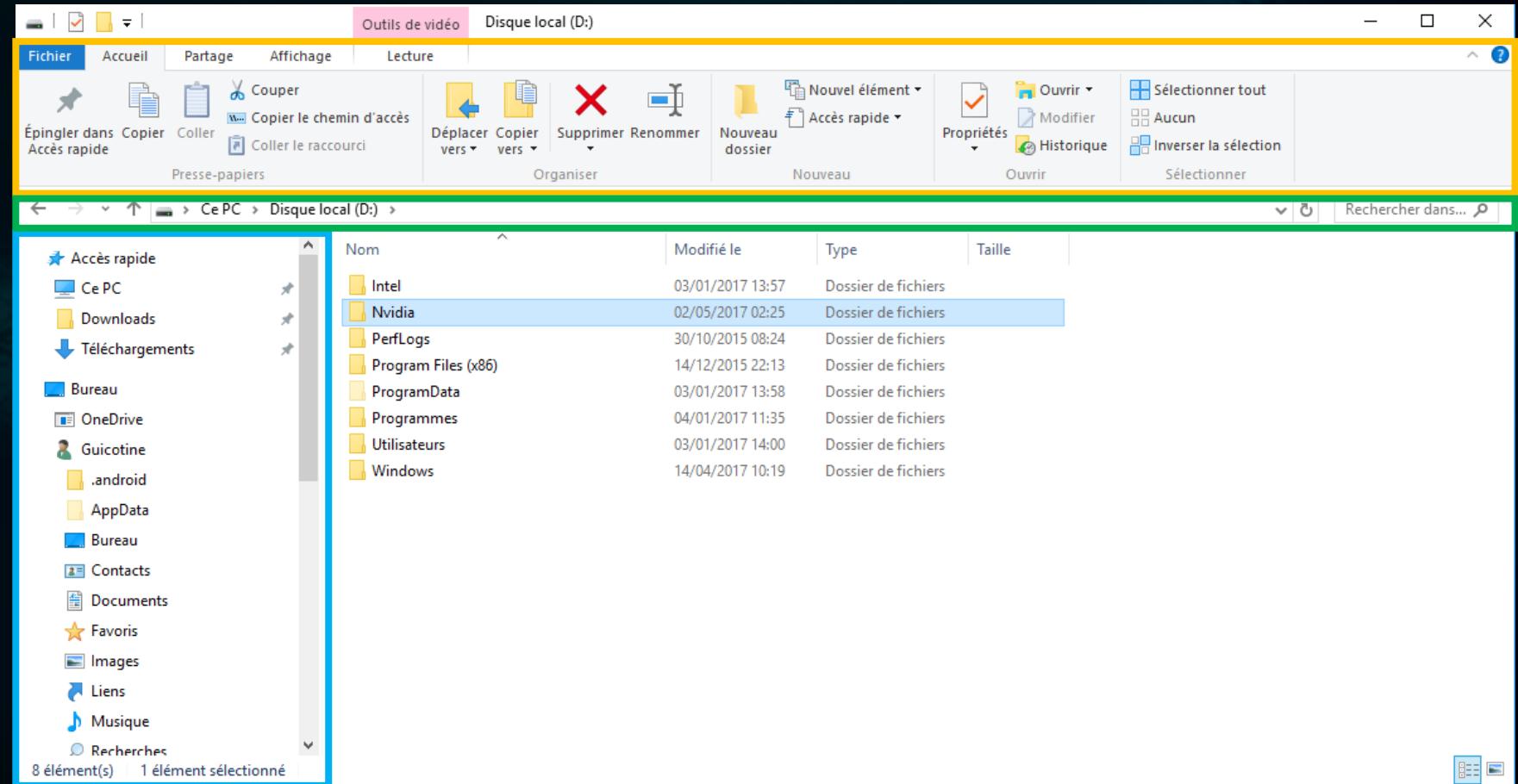


Explorateur Windows

Barre d'outils

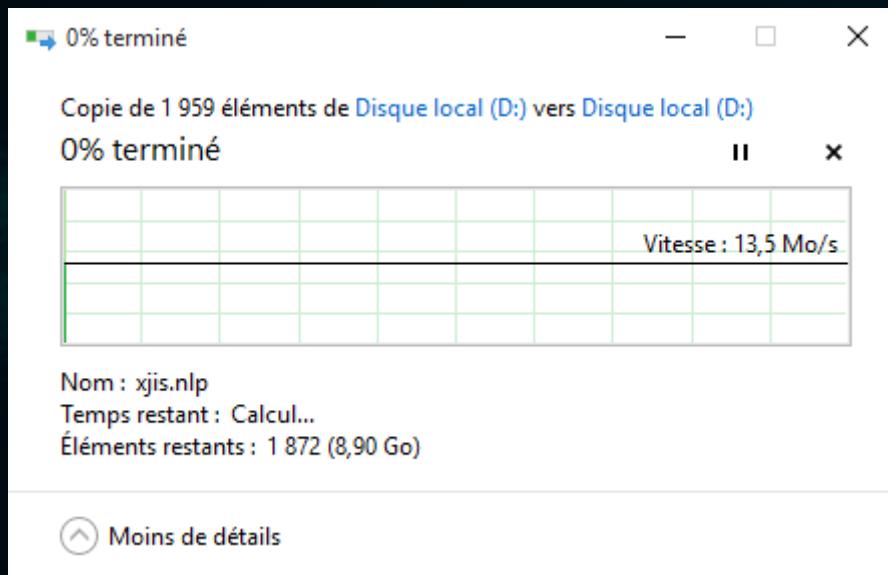
Barre de lien

Accès rapide &
Navigation

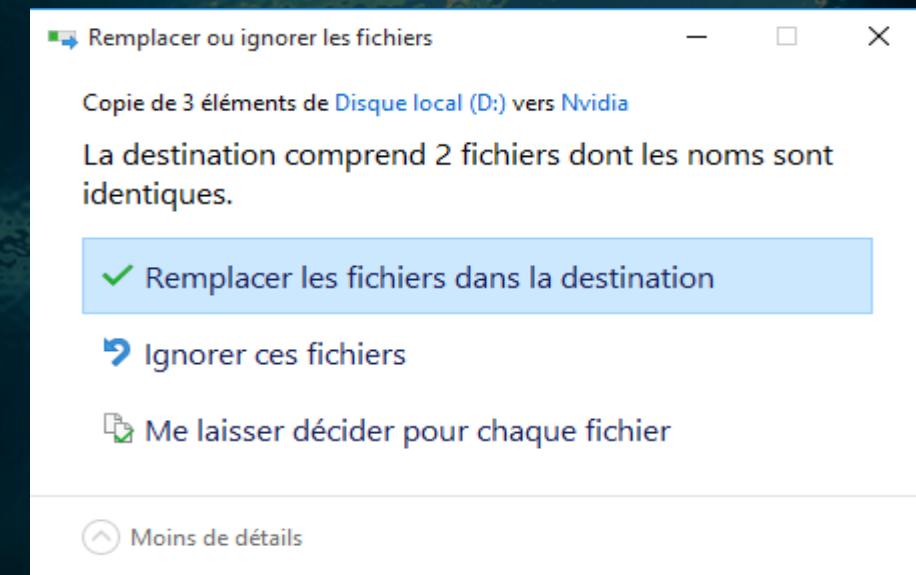


Déplacement et copie

Calcul et transfert

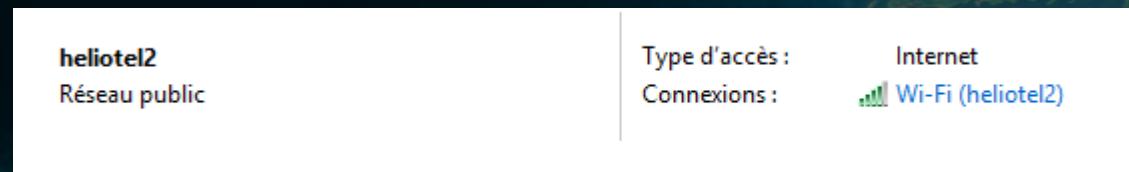


Conflit de fichiers

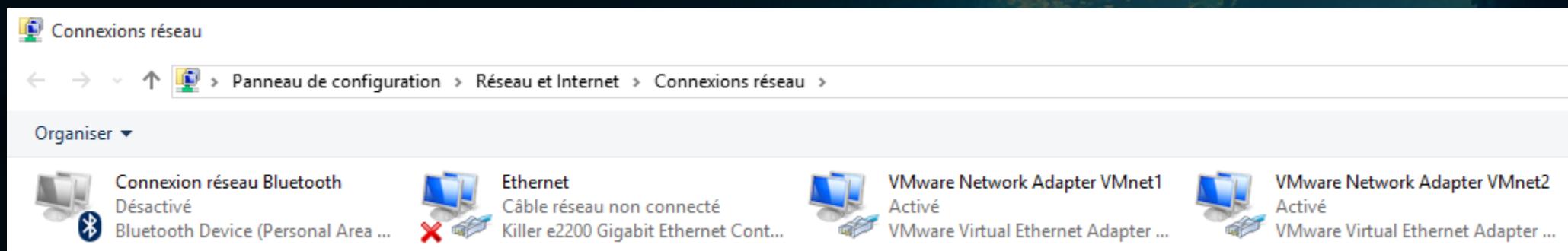


Centre de réseau et partage

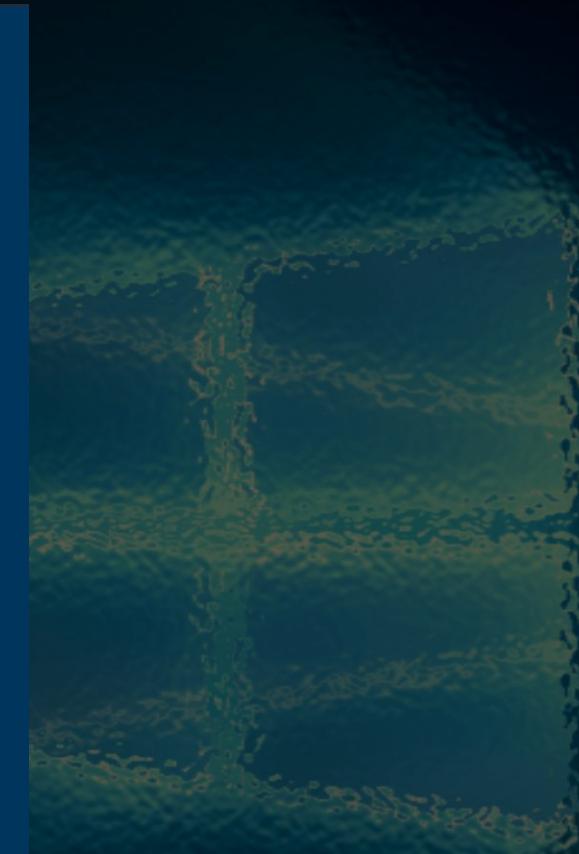
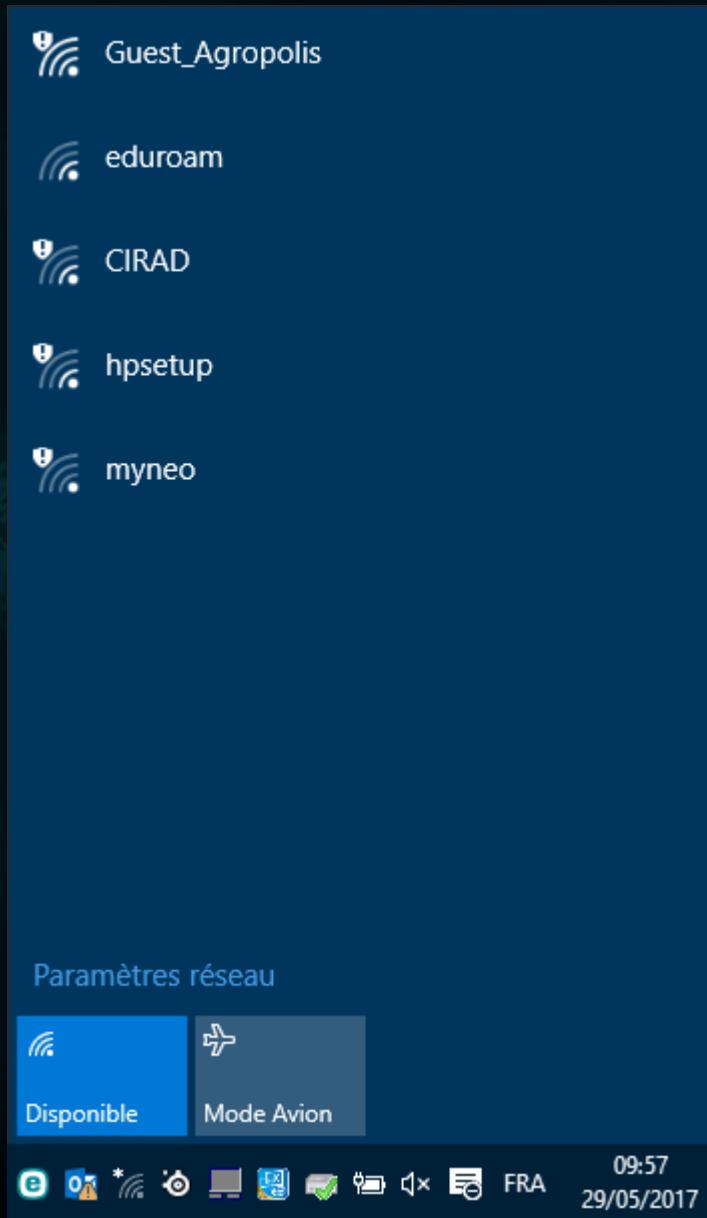
Connexions actives



Affichage des différentes cartes réseaux



Centre de réseau et partage



Bureaux virtuels



Isoler des applications

Pratique pour l'organisation

Présent nativement sur Windows 10

Bureaux virtuels

Créer un bureau virtuel : **WIN+CTRL+D**

Naviguer à travers les bureaux : **WIN+CTRL+FLECHES**

Vue synthétique : **WIN+TAB**

Les raccourcis utiles 1

Description	Raccourci
Ouvrir menu démarrer	Windows
Chercher une application	Windows + <Saisi de la recherche>
Verrouiller la session	Windows + L
Informations système	Windows + Pause
Déplacer la fenêtre vers l'extrême Gauche	Windows + <←>
Déplacer la fenêtre vers l'extrême Droite	Windows + <→>
Mettre une fenêtre en plein écran	Windows + <↑>
Réduire la fenêtre	Windows + <↓>

Les raccourcis utiles 2

Description	Raccourci
Passer à l'onglet suivant	CTRL + TAB
Passer à l'onglet précédent	CTRL + SHIFT + TAB
Fermer l'onglet courant	CTRL + F4
Passer à la fenêtre suivante	ALT + TAB
Passer à la fenêtre précédente	ALT + SHIFT + TAB
Afficher le Bureau	Windows + D
Afficher les tâches	Windows + TAB
Exécuter	Windows + R
Explorateur Windows	Windows + E

Sessions

Compte local :

- On ouvre sa session avec le nom d'utilisateur qu'on aura choisi (comme avant)
- On n'est pas obligé d'avoir un mot de passe
- Il faudra se connecter au coup par coup avec un compte Microsoft pour accéder aux applications Microsoft : Courrier, Calendrier, Contacts et à Windows Store

Sessions

Compte Microsoft

- On ouvre sa session avec l'adresse mail et le mot de passe de son compte Microsoft.
- On est automatiquement identifié lorsqu'on utilise Windows Store ou toute autre application Microsoft : Skype, Jeux / Xbox, Courrier, Calendrier, Contacts
- On est automatiquement connecté à OneDrive
- Le compte Microsoft est plus simple pour les utilisateurs débutants.

Reflexes

Désactiver les options trop bavardes et curieuses

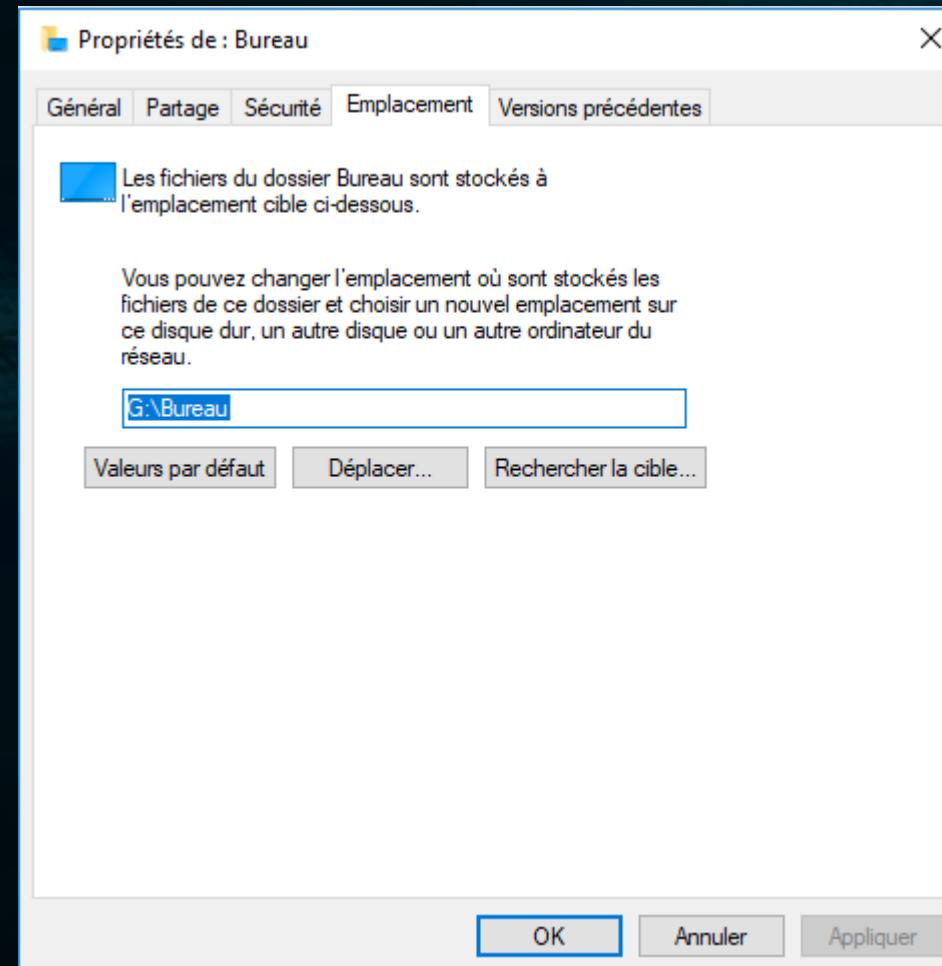
The screenshot shows the Windows Settings application window. The left sidebar has a tree view with 'Paramètres' at the top, followed by 'Accueil', a search bar, 'Confidentialité', 'Autorisations de Windows', and several sections under 'Général': 'Général', 'Voix, entrée manuscrite et frappe', 'Diagnostics et commentaires', 'Historique des activités', 'Autorisations pour les applications', and 'Emplacement'. The 'Général' section is currently selected. The main content area is titled 'Général' and 'Modifier les options de confidentialité'. It contains four settings, each with a toggle switch labeled 'Désactivé' (Disabled):

- Laisser les applications utiliser l'identifiant de publicité pour permettre l'affichage de publicités plus pertinentes en fonction de votre utilisation des applications (la désactivation de cette option réinitialise votre identifiant)
- Permettre aux sites Web d'accéder à ma liste de langues pour fournir du contenu local
- Autoriser Windows à suivre les lancements d'applications pour améliorer le menu Démarrer et les résultats de recherche
- Me montrer des contenus suggérés dans l'application Paramètres

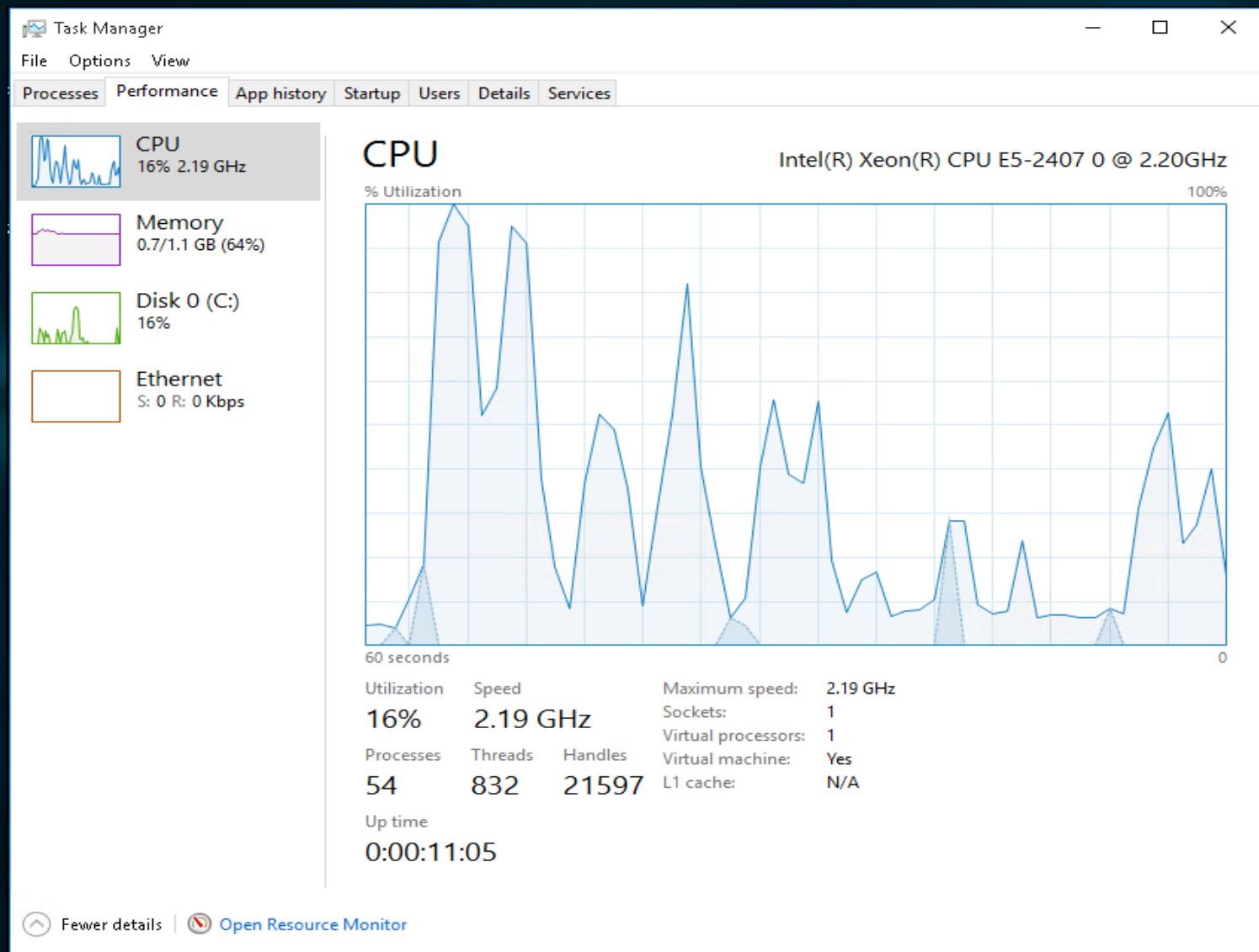
At the bottom of the main content area, there is a footer bar with the text 'Prenez connaissance de vos options de confidentialité'.

Reflexes

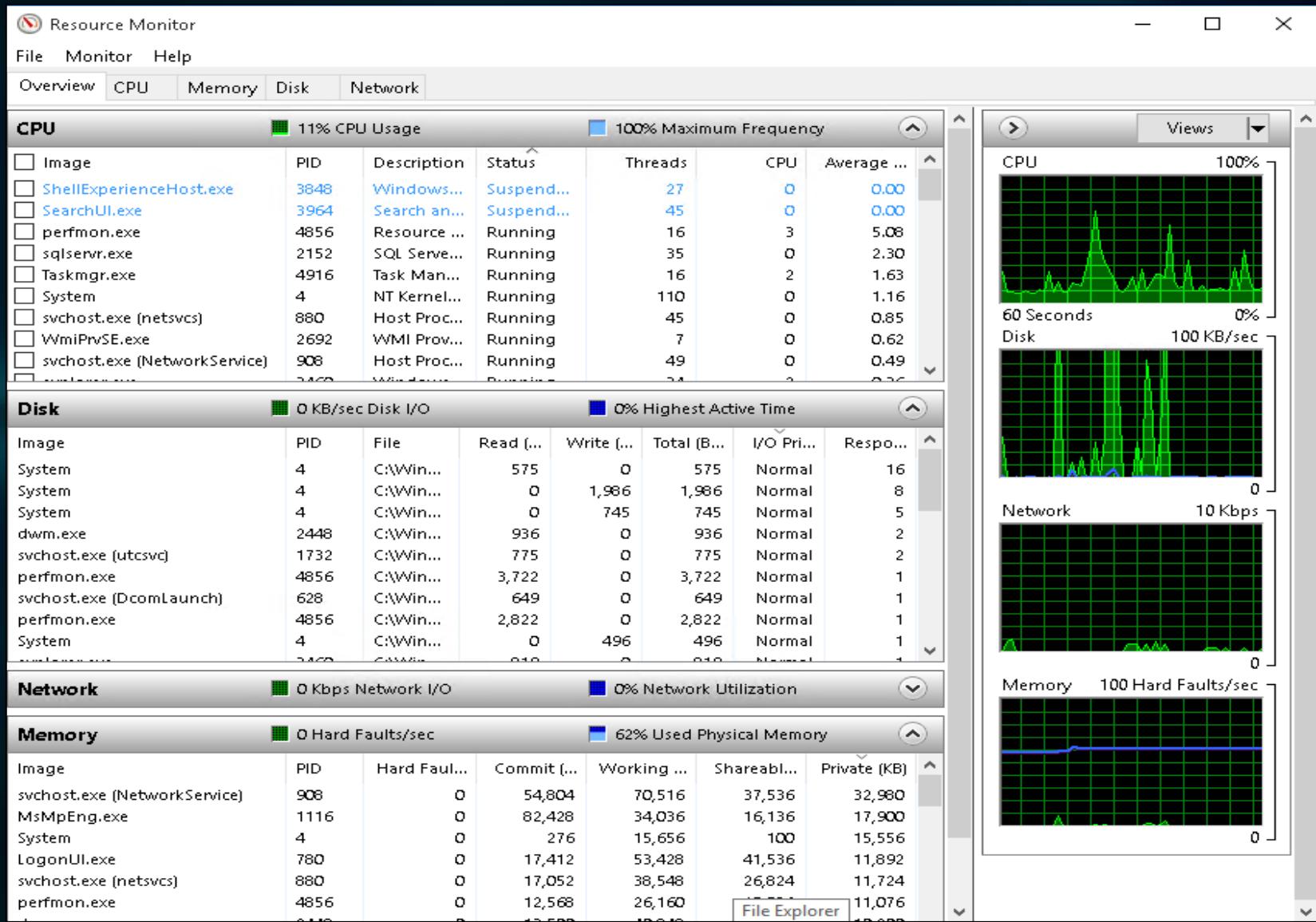
Changer les cibles des répertoires utilisateurs si partition 'DATA'



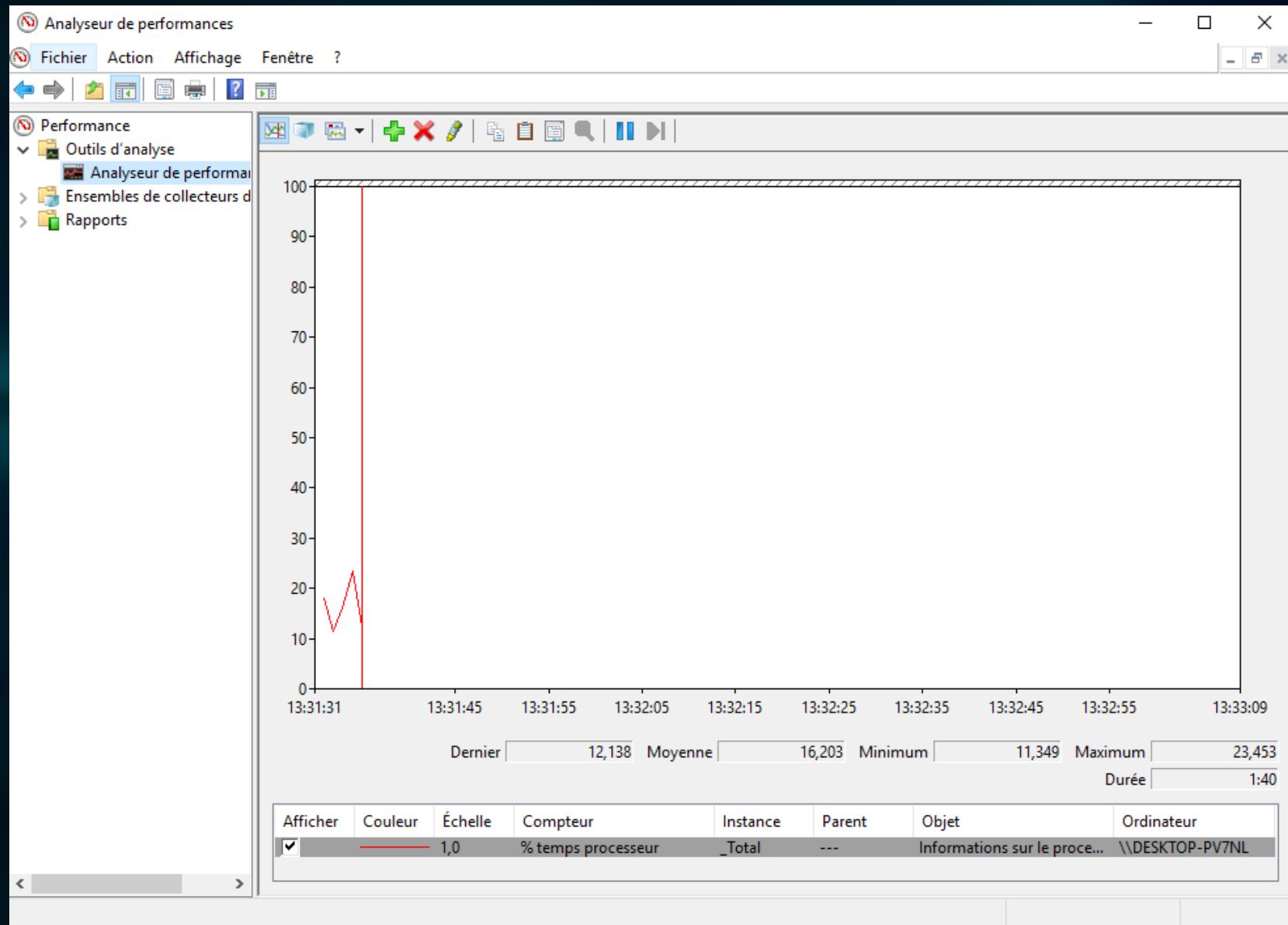
Mesure des performances



Moniteur de ressources



Mesure des performances



Moniteur de ressources

- 1 Repérer le processus qui consomme le plus en terme d'I/O disque
- 2 Repérer ce qui consomme le plus en terme de RAM
- 3 Repérer ce qui consomme le moins en terme de réseau
- 4 Réduire la taille des graphiques sur la droite
- 5 Quelle est l'utilisation actuelle du processeur ?

Observateur d'événements

Fichier Action Affichage ?



Observateur d'événements (Local)

Affichages personnalisés

Journaux Windows

Application

Sécurité

Installation

Système

Événements transférés

Journaux des applications et services

Abonnements

Présentation et synthèse

Dernière actualisation : 08/10/2018 14:33:47

Vue d'ensemble



Pour afficher les événements qui se sont produits sur votre ordinateur, choisissez la source, le journal ou le noeud d'affichage personnalisé approprié dans l'arborescence de la console. La vue personnalisée Événements d'administration contient tous les événements d'administration, quelle que soit la source. Une vue de synthèse de tous les journaux est affichée ci-dessous.

Résumé des événements d'administration

Type d'événement	ID de l'événement	Source	Journal	Cette dernière heure	24 heures	7 jours
[-] Critique	-	-	-	0	0	1
[-] Erreur	-	-	-	3	11	76
[-] Avertissement	-	-	-	1	2	13
[-] Information	-	-	-	24	229	1 835
[-] Succès de l'authentification	-	-	-	43	169	1 557

Actions

Observateur d'événements (Local)

Ouvrir le journal enregistré...

Créer une vue personnalisée...

Importer une vue personnalisée...

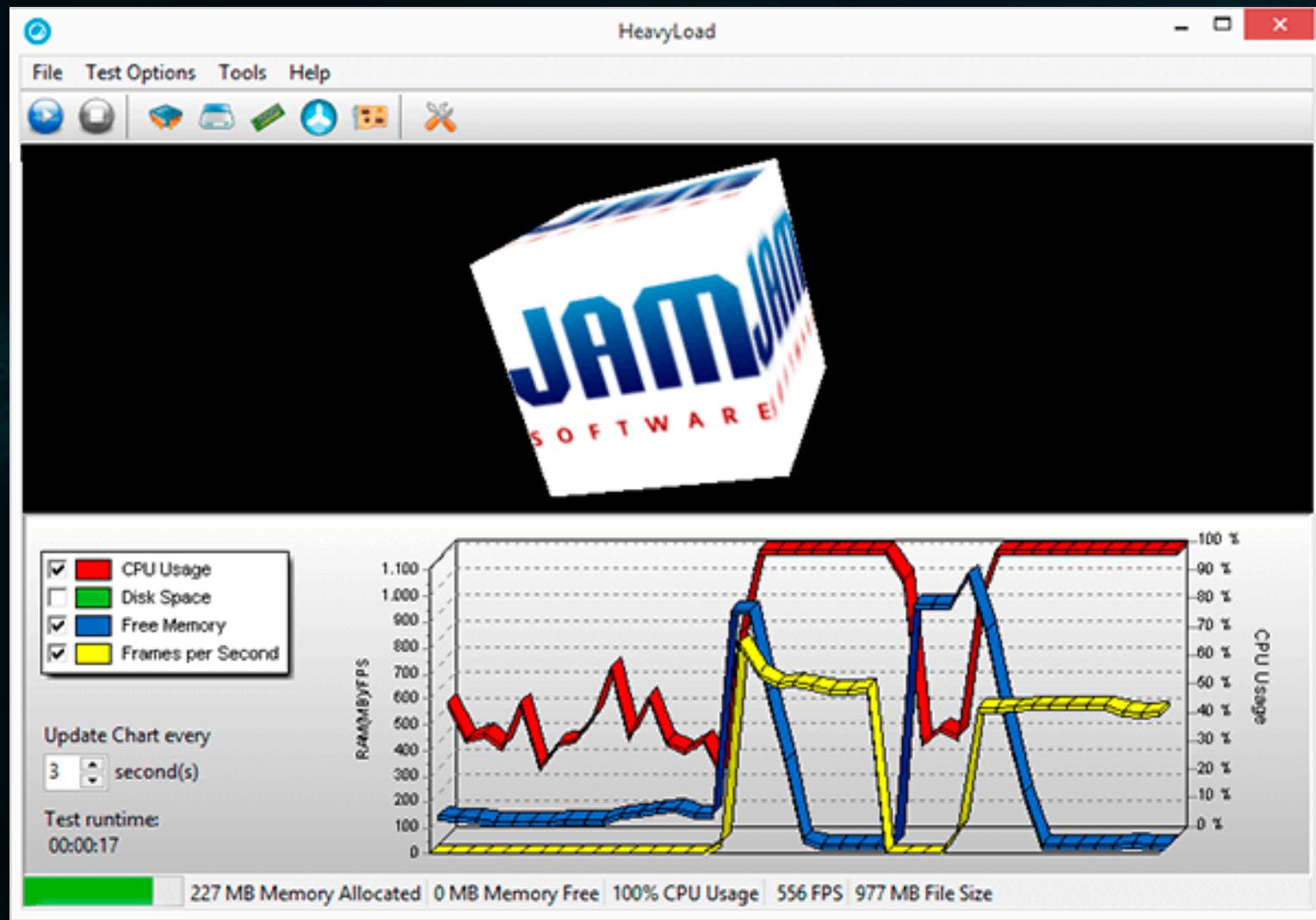
Se connecter à un autre ordinateur...

Affichage

Actualiser

Aide

Test de fiabilité et de performance

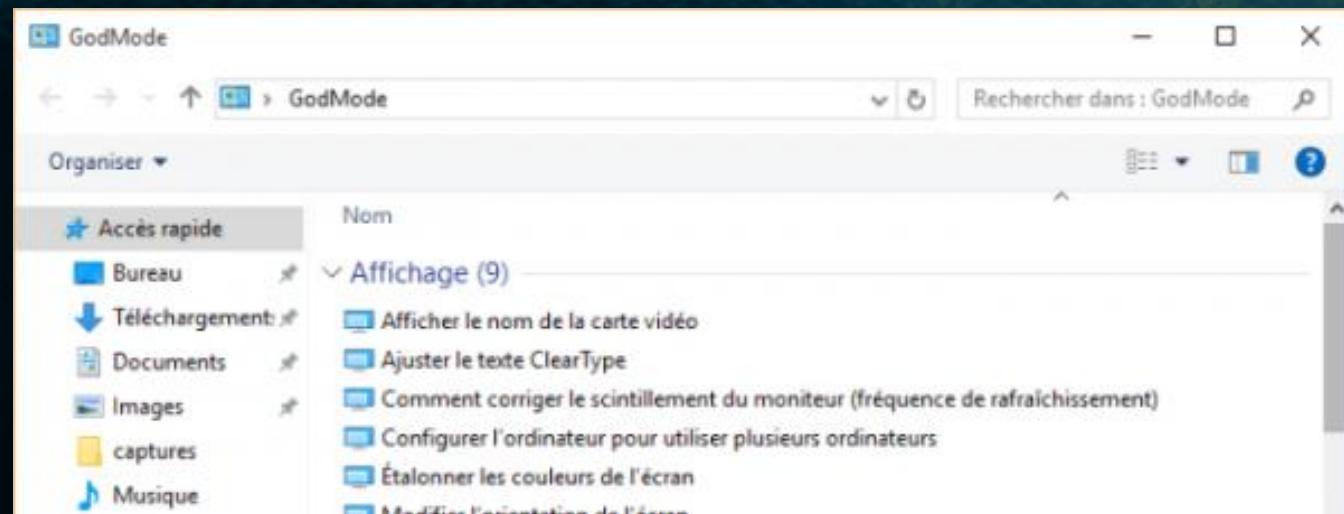


God Mode

Menu caché qui permet de disposer de tous les paramètres de configuration de l'OS dans un unique dossier.

Création :

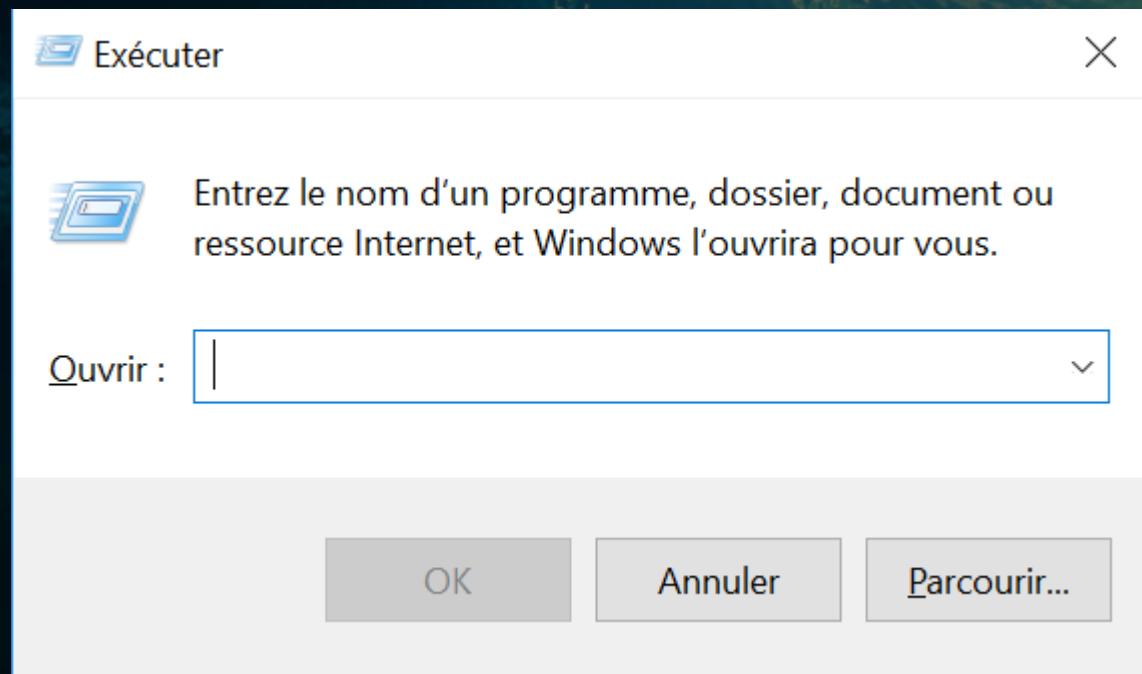
- Créer un nouveau dossier
- Lui donner comme nom : GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}



Executer

Console permettant d'exécuter plusieurs applicatifs.

Raccourci : WIN + R



Fichier

azman.msc

certmgr.msc

comexp.msc

compmgmt.msc

devmgmt.msc

diskmgmt.msc

eventvwr.msc

fsmgmt.msc

gpedit.msc

Composant

Gestionnaire d'autorisations

Gestion des Certificats

Services des composants

Gestion de l'ordinateur

Gestionnaire de périphériques

Gestion des disques

Observateur d'événements

Dossiers partagés

Editeur de stratégie de groupe locale
(uniquement dans les éditions Professionnelle
et Entreprise)

lusrmgr.msc	Gestion des Utilisateurs et groupes locaux (uniquement dans les éditions Professionnelle et Entreprise)
napclcfg.msc	Configuration du client NAP
perfmon.msc	Moniteur de fiabilité et de performances
printmanagement.msc	Gestion de l'impression
rsop.msc	Jeu de stratégie résultant (uniquement dans les éditions Professionnelle et Entreprise)
secpol.msc	Stratégie de sécurité locale (uniquement dans les éditions Professionnelle et Entreprise)
services.msc	Services
taskschd.msc	Planificateur de tâches
tpm.msc	Gestion de module de plateforme sécurisée sur l'ordinateur local
wf.msc	Pare-feu Windows avec fonctions avancées de sécurité
wmimgmt.msc	Racine de la console/Contrôle WMI

Console MMC

Microsoft Management Console.

Permet de réunir plusieurs composants enfichables sur une seule interface.

Facilite l'administration.

Console MMC

 Exécuter

X



Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.

Ouvrir :

mmc.exe

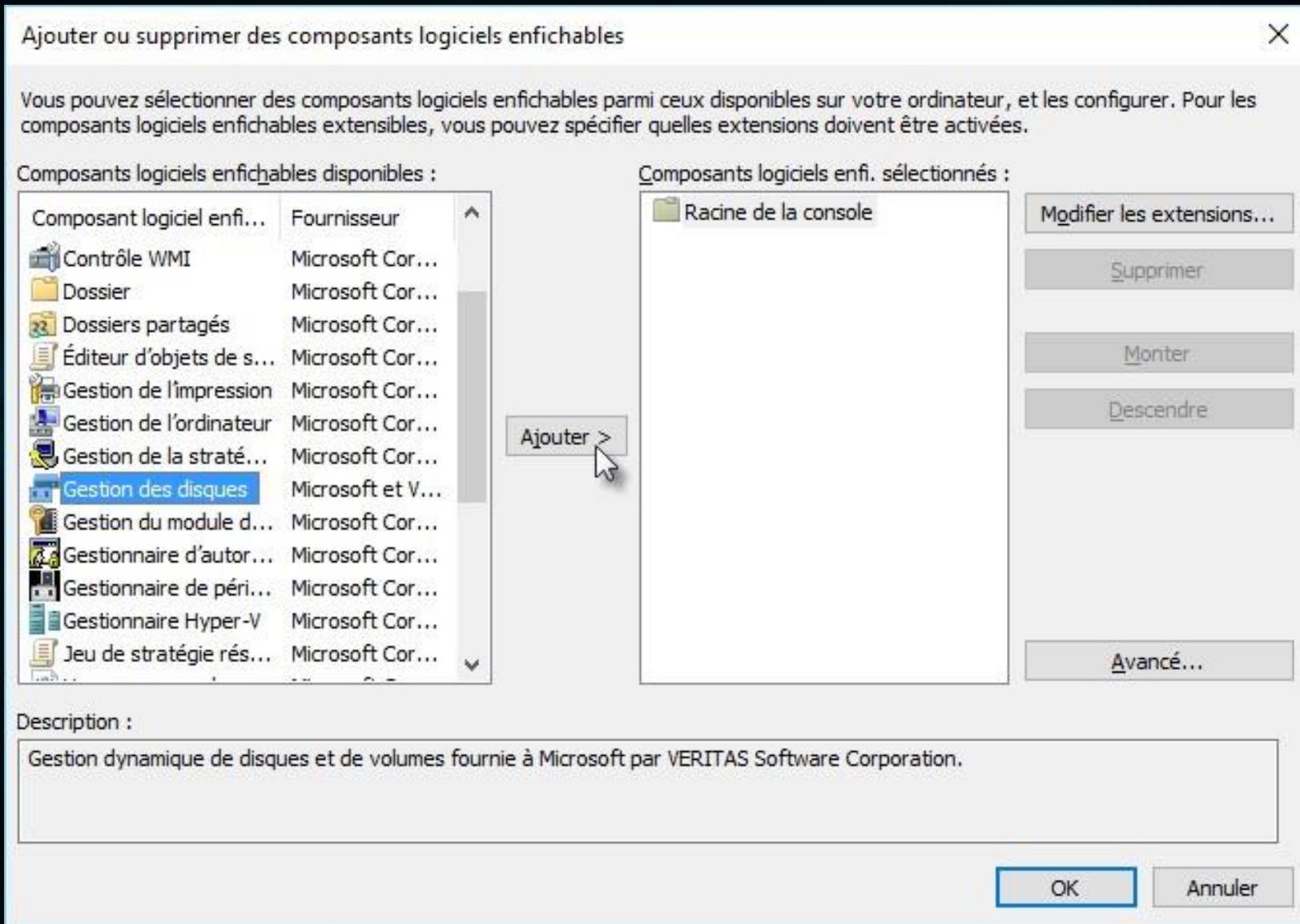


OK

Annuler

Parcourir...

Console MMC



Planificateur de tâches

Permet de programmer le lancement de tâches récurrentes.

Peut exécuter des scripts.

Planificateur de tâches

Planificateur de tâches

Fichier Action Affichage ?

Actions

- Bibliothèque du Planificateur de t...
- Créer une tâche de base...
- Créer une tâche...
- Importer une tâche...
- Afficher toutes les tâches acti
- Activer l'historique de toutes ...
- Nouveau dossier...
- Affichage
- Actualiser
- Aide

Élément sélectionné

- Exécuter
- Fin
- Désactiver
- Exporter...
- Propriétés
- Supprimer

Planificateur de tâches (Local)

Bibliothèque du Planificateur de tâches

Nom	Statut	Déclencheurs
ASUS Battery...	En cours	À l'ouverture de session d'un uti
ASUS Splend...	En cours	À l'ouverture de session d'un uti
ATK Package ...	Prêt	Filtre d'événement personnalisé
ATK Package ...	Prêt	
CCleaner Up...	Prêt	Plusieurs déclencheurs sont défi
CCleanerSkip	Prêt	

Général Déclencheurs Actions Conditions Paramètres

Nom : CCleanerSkipUAC

Emplacement : \

Auteur : Piriform Ltd

Description :

Options de sécurité

Utiliser le compte d'utilisateur suivant pour exécuter cette tâche

Planificateur de tâches

Fonction	Rajout	Résultat
Arrêter	-s -f	shutdown.exe -s -f
Redémarrer	-r -f	shutdown.exe -r -f
Fermer la session	-l -f	shutdown.exe -l -f
Mettre en veille	-h -f	shutdown.exe -h -f

Console MMC

Créer une nouvelle MMC qui contiendra

- La gestion des certificats
- La gestion des disques
- Les services.
- L'enregistrer.

Les outils d'administration du système

- **1 Des actions de maintenance d'un poste Windows 8.1 sont-elles nécessaires ?**
- **2 À quoi sert le planificateur de tâches ?**
- **3 À quoi sert la défragmentation du disque ?**
- **4 À quoi sert l'analyseur de performances ?**
- **5 Qu'apporte le moniteur de ressources par rapport au gestionnaire de tâches ?**
- **6 D'où proviennent les composants logiciels enfichables qu'il est possible d'utiliser lors de la création de consoles personnalisées ?**
- **7 Quel est l'intérêt de sauvegarder une console personnalisée ?**
- **8 Les MMC permettent-elles de gérer des machines à distance ?**

Gestion réseau

Actuellement, IPv4 est la version du protocole IP la plus dominante sur Internet. Standardisée en 1981, cette version forme la base du réseau Internet et s'appuie sur un modèle d'adressage en 32 bits des machines hôtes.

Chaque interface réseau se voit attribuer une voire plusieurs existent au total 2^{32} soit 4 294 967 296 adresses IP disponibles, certaines ne sont finalement pas utilisables ou bien réservées à des usages précis.

Gestion réseau

Adresse publiques :

Doivent-être uniques au monde, fournies par le FAI (après ICANN, RIPE...)

Adresses privées :

Adresse locale de la machine derrière un routeur

Gestion réseau

3 Classes en fonction de la taille du réseau

A: grand : 10.0.0.0 → 10.255.255.255 / 8

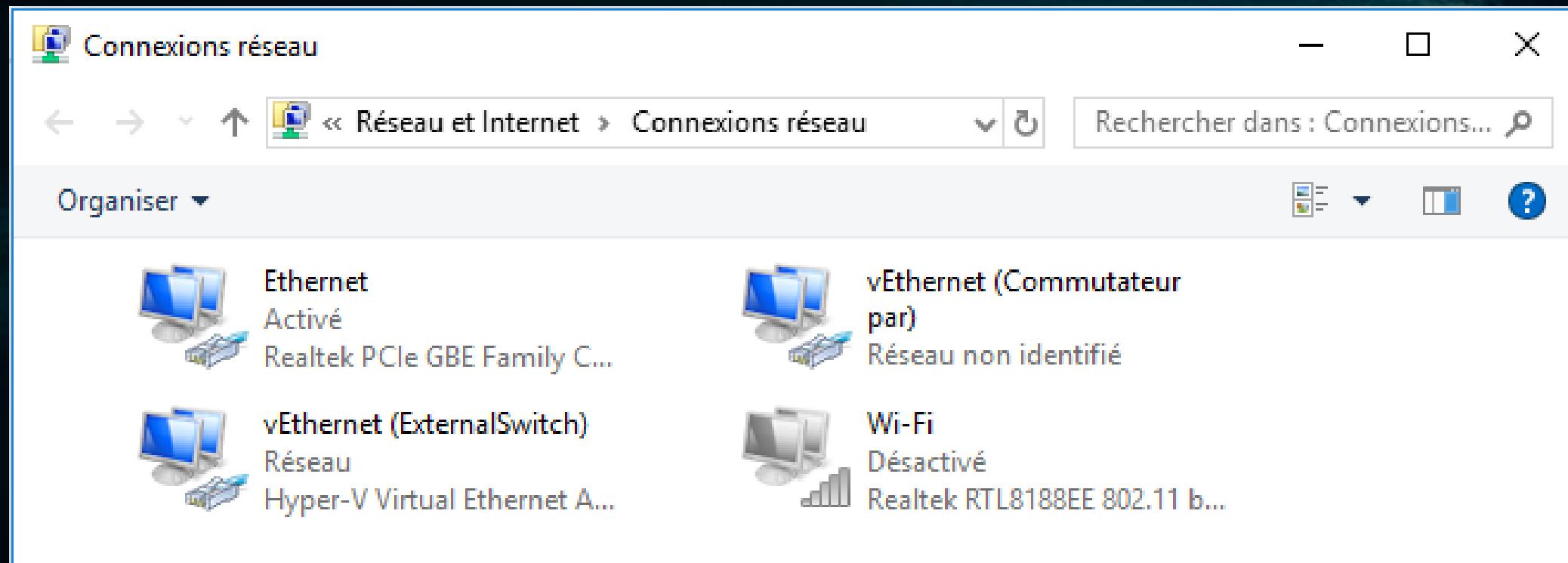
B: moyen : 172.16.0.0 → 172.31.255.255 / 16

C: petit : 192.168.0.0 → 192.168.255.255 / 24

Boucle: 127.0.0.1 (se cible soi même = 127.1)

APIPA: 169.X.X.X conflit d'IP et adresse automatique

Gestion réseau



Gestion réseau

Propriétés de vEthernet (Commutateur par)

Gestion de réseau Partage

Connexion en utilisant :

Hyper-V Virtual Ethernet Adapter

Configurer...

Cette connexion utilise les éléments suivants :

- Client pour les réseaux Microsoft
- Partage de fichiers et imprimantes Réseaux Microsoft
- Planificateur de paquets QoS
- Protocole Internet version 4 (TCP/IPv4)
- Protocole de multiplexage de carte réseau Microsoft
- Pilote de protocole LLDP Microsoft
- Protocole Internet version 6 (TCP/IPv6)

Installer... Désinstaller Propriétés

Description

Protocole TCP/IP (Transmission Control Protocol/Internet Protocol). Protocole de réseau étendu par défaut permettant la communication entre différents réseaux interconnectés.

OK Annuler

Propriétés de : Protocole Internet version 4 (TCP/IPv4)

Général Configuration alternative

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP :

Masque de sous-réseau :

Passerelle par défaut :

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré :

Serveur DNS auxiliaire :

Valider les paramètres en quittant

Avancé... OK Annuler

Gestion réseau

3 Classes en fonction de la taille du réseau

- Mettre le switch virtuel Hyper-V en mode Interne
- Fixer l'IP **10.0.45.32**
- Masque : **255.255.255.0**

DNS : **8.8.8.8 – 8.8.4.4**

Pas de passerelle

Bitlocker

BitLocker est un système de sécurité intégré à Windows et qui permet de chiffrer les données stockées sur votre ordinateur, ce qui permet d'assurer la confidentialité de vos données personnelles en cas de vol.

BitLocker est en lien direct avec votre ordinateur puisqu'il fonctionne grâce à une puce TPM (Trusted Platform Module). Intégré directement à la carte mère, il est utilisé pour le stockage d'information très sensible notamment les clés de chiffrement.

Bitlocker

AES 128 bits (possibilité de passer à du 256 bits via GPO)

BitLocker est en lien direct avec votre ordinateur puisqu'il fonctionne grâce à une puce TPM (Trusted Platform Module). Intégré directement à la carte mère, il est utilisé pour le stockage d'information très sensible notamment les clés de chiffrement.

Clé peut être stockée dans un annuaire Active Directory

Bitlocker

The screenshot shows the Windows Group Policy Management Editor interface. On the left, the navigation pane displays the following structure:

- Configuration ordinateur
- Stratégies
 - Paramètres du logiciel
 - Paramètres Windows
 - Modèles d'administration : définitions
 - Composants Windows
 - Ajouter des fonctionnalités à Windows
 - Analyse de fiabilité Windows
 - Assistance en ligne
 - Biométrie
 - Calendrier Windows
 - Carte à puce
 - Centre de mobilité Windows
 - Centre de sécurité
 - Chiffrement de lecteur BitLocker
 - Lecteurs de données amovibles
 - Lecteurs de données fixes
 - Lecteurs du système d'exploitation
 - Compatibilité des applications
 - Compatibilité des périphériques
 - Contrôle parental
 - Déploiement de package Applications
 - Dossiers de travail

Exiger une authentification supplémentaire au démarrage

Modifier [le paramètre de stratégie](#)

Configuration requise :
Au minimum Windows Server 2008 R2 ou Windows 7

Description :
Ce paramètre de stratégie vous permet de configurer si BitLocker exige une authentification supplémentaire à chaque démarrage de l'ordinateur et si vous utilisez BitLocker avec ou sans module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker.

Remarque : une seule des options d'authentification supplémentaire peut être exigée au démarrage, sans générer d'erreur de stratégie.

Si vous voulez utiliser BitLocker

Paramètre

- | Paramètre | Etat |
|--|------------------------|
| <input type="checkbox"/> Autoriser le déverrouillage réseau au démarrage | Non configuré |
| <input type="checkbox"/> Autoriser le démarrage sécurisé pour la validation de l'intégrité | Non configuré |
| <input checked="" type="checkbox"/> Exiger une authentification supplémentaire au démarrage | Non configuré |
| <input type="checkbox"/> Exiger une authentification supplémentaire au démarrage (Windows Server 2008 et Windows Vista) | Filtre activé |
| <input type="checkbox"/> Ne pas autoriser les utilisateurs standard à modifier le code confidentiel ou le mot de passe | Options des filtres... |
| <input type="checkbox"/> Activer l'utilisation de l'authentification BitLocker exigeant une saisie au clavier préalable au démarrage | Réappliquer le filtre |
| <input type="checkbox"/> Autoriser les codes confidentiels améliorés au démarrage | Toutes les tâches |
| <input type="checkbox"/> Configurer la longueur minimale du code confidentiel de démarrage | Aide |
| <input type="checkbox"/> Configurer l'utilisation du chiffrement au niveau matériel pour les lecteurs du système d'exploitation | Non configuré |
| <input type="checkbox"/> Appliquer le type de chiffrement de lecteur aux lecteurs du système d'application | Non configuré |
| <input type="checkbox"/> Configurer l'utilisation des mots de passe pour les lecteurs du système d'exploitation | Non configuré |
| <input type="checkbox"/> Sélectionner la méthode de récupération des lecteurs du système d'exploitation protégés par BitLocker | Non configuré |
| <input type="checkbox"/> Configurer le profil de validation de plateforme du module de plateforme sécurisée pour les configurations de démarrage | Non configuré |
| <input type="checkbox"/> Configurer le profil de validation de plateforme du module de plateforme sécurisée (Windows Vista) | Non configuré |
| <input type="checkbox"/> Configurer le profil de validation de plateforme du module de plateforme sécurisée pour les configurations de démarrage | Non configuré |
| <input type="checkbox"/> Réinitialiser les données de validation de plateforme après une récupération BitLocker | Non configuré |
| <input type="checkbox"/> Utiliser un profil amélioré de validation des données de configuration de démarrage | Non configuré |

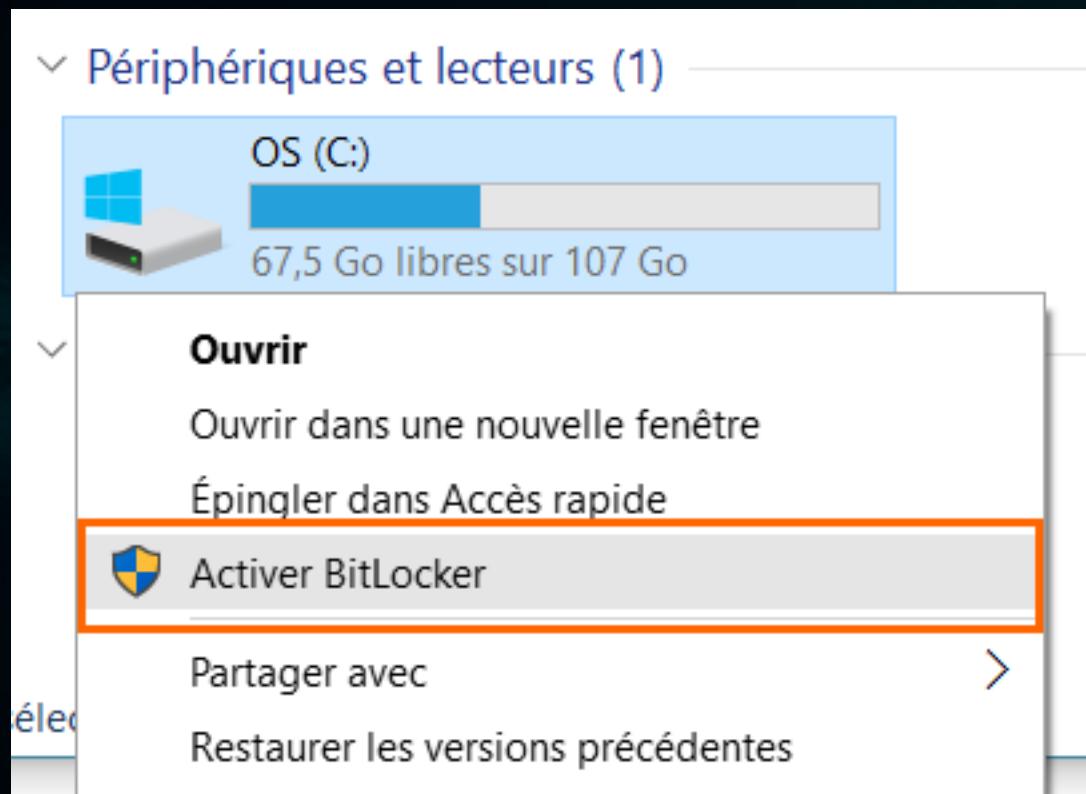
Etat

Non configuré
Non configuré
Non configuré

- Modifier
- Filtre activé
- Options des filtres...
- Réappliquer le filtre
- Toutes les tâches
- Aide

III

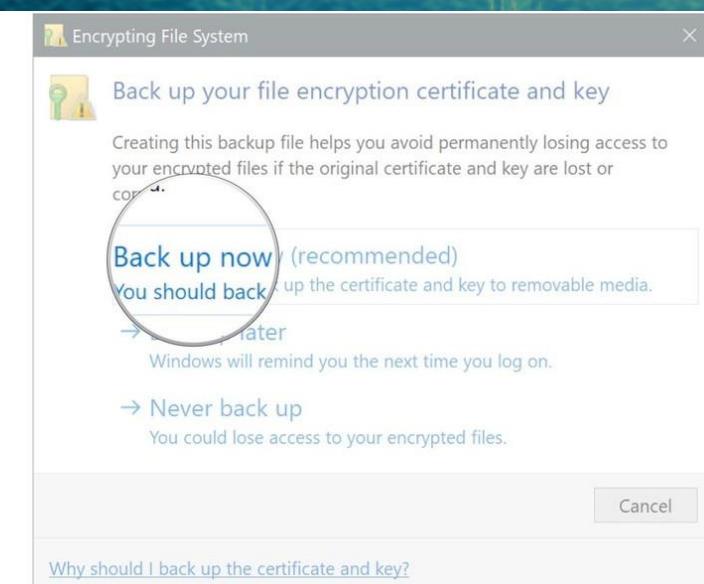
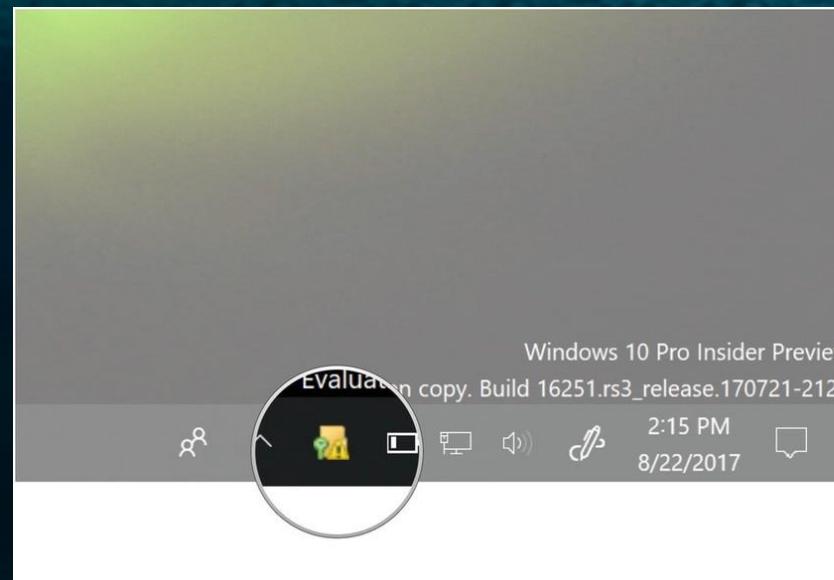
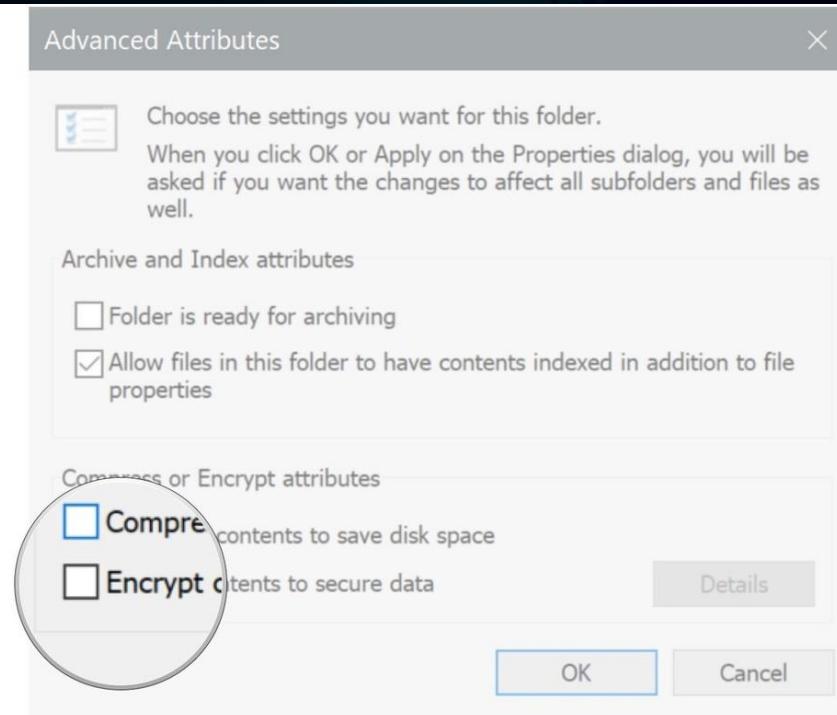
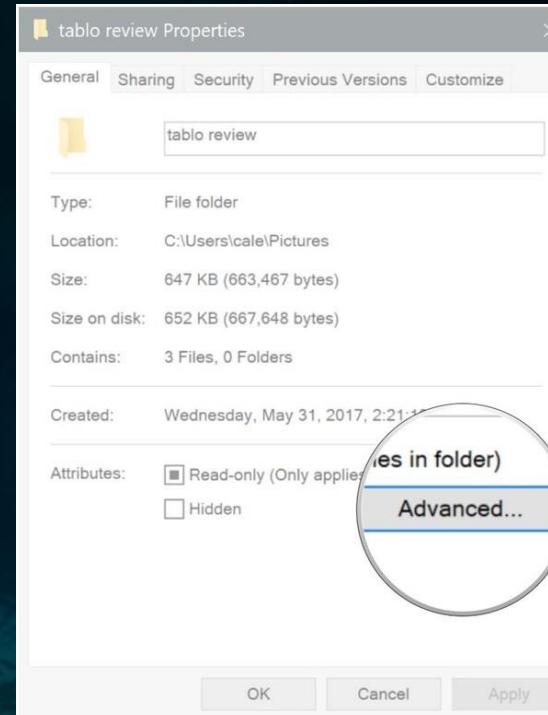
Bitlocker



EFS (Encrypting File System)

Il ne chiffre que des dossiers ou fichiers précis, un par un, sans chiffrer de lecteur, qui seront accessibles uniquement par un utilisateur à partir de son compte utilisateur. Si plusieurs utilisateurs utilisent le même ordinateur, chacun chiffrera ses propres fichiers et les autres n'en auront pas l'accès.

Clé stockée dans le profil de celui-ci sous Documents and Settings, username, Application Data, Microsoft, Crypto, RSA.
Clé peut être stockée dans un annuaire Active Directory





Windows Defender

L'Antivirus Windows Defender est préinstallé et prêt être utilisée à tout moment



Windows Defender – Efficace ?

Windows Defender se hisse parmi les meilleurs antivirus du marché

Auteur : Jérôme Gianoli | Dans sécurité-informatique | 30/03/2018 | 0 commentaires

Au fil du temps Microsoft a apporté des tas d'amélioration à son antivirus maison, Windows Defender. Les derniers tests montrent que tous ces efforts sont payants. La solution native de Windows 10 ou Microsoft Security Essentials pour Windows 7 sont désormais des antivirus redoutables en protection.

<https://www.generation-nt.com/av-test-windows-defender-antivirus-securite-actualite-1956487.html>

Windows Defender devient un produit d'excellence

Le mercredi 15 Août 2018 à 17:10 par Jérôme G. | 25 commentaire(s)



Windows Defender ne semble plus être à la traîne en matière de protection sur Windows 10. Un Top Produit d'après les derniers résultats de AV-Test.

<https://www.ginjfo.com/actualites/securite-informatique/windows-defender-se-hisse-parmi-les-meilleurs-antivirus-du-marche-20180330>



BUSINESS WINDOWS CLIENT

The Best Virus Protection for Windows 10



AV-TEST
The Independent IT-Security Institute
Magdeburg, Germany

Manufacturer	Product	AV-TEST-Certificate	Protection (max. 6 pts.)	Performance (max. 6 pts.)	Usability (max. 6 pts.)	Overall Points Total (max. 18 pts.)
Avast	Antivirus Business		6.0	5.5	5.5	17.0
Bitdefender	Endpoint Security		6.0	6.0	5.5	17.5
Bitdefender	Endpoint Security Elite		6.0	5.5	4.5	16.0
Ensilo	Ensilo		6.0	5.0	5.5	16.5
F-Secure	PSB Computer Protection		6.0	5.5	3.0	14.5
G Data	Antivirus Business		5.5	5.0	5.0	15.5
Kaspersky Lab	Endpoint Security		6.0	6.0	6.0	18.0
Kaspersky Lab	Small Office Security		6.0	6.0	6.0	18.0
McAfee	Endpoint Security		6.0	5.0	6.0	17.0
Microsoft	Windows Defender Antivirus		6.0	5.5	5.5	17.0
Palo Alto Networks	Traps		4.5	5.0	5.0	14.5
Seqrte	Endpoint Security		5.5	6.0	5.0	16.5
Sophos	Endpoint Security and Control		5.5	5.0	6.0	16.5
Symantec	Endpoint Protection		6.0	5.5	6.0	17.5
Symantec	Endpoint Protection Cloud		6.0	6.0	6.0	18.0
Trend Micro	Office Scan		6.0	6.0	6.0	18.0

[Accueil](#)[Protection contre les virus et menaces](#)[Protection du compte](#)[Pare-feu et protection du réseau](#)[Contrôle des applications et du navigateur](#)[Sécurité des appareils](#)[Performances et intégrité de l'appareil](#)[Options de contrôle parental](#)[Paramètres](#)

La sécurité en un clin d'œil

Affichez l'état de sécurité et d'intégrité de votre appareil, et prenez les mesures nécessaires.



Protection contre les virus et menaces
Aucune action requise.



Protection du compte
Connectez-vous à Microsoft pour bénéficier d'une sécurité renforcée.



Pare-feu et protection du réseau
Aucune action requise.



Contrôle des applications et du navigateur
Aucune action requise.



Sécurité des appareils
Aucune action requise.



Performances et intégrité de l'appareil
Le rapport d'intégrité indique des recommandations pour votre appareil.



Options de contrôle parental
Gérez la façon dont votre famille utilise ses appareils.

Afficher le rapport d'intégrité

Par-feu Windows

Applicatif physique ou logique définissant
quels sont les types de communications
autorisés sur un réseau ou des
périphériques.



Il surveille et contrôle les applications et les
flux de données (paquets).

Toujours utiliser les fonctionnalités avancées !

Par-feu Windows

Pare-feu Windows Defender avec fonctions avancées de sécurité

Fichier Action Affichage ?

Back Forward Refresh Help

Pare-feu Windows Defender avec fonctions avancées de sécurité

Règles de trafic entrant
Règles de trafic sortant
Règles de sécurité de connexion
Analyse
Pare-feu
Règles de sécurité de connexion
Associations de sécurité

Pare-feu

Nom	Profil	Action	Remplacer	Direction
✓ Avast Emergency Update	Public	Autoriser	Non	Entrant
✓ Avast Emergency Update	Public	Autoriser	Non	Entrant
✓ Brawlhalla	Tout	Autoriser	Non	Entrant
✓ Brawlhalla	Tout	Autoriser	Non	Entrant
✓ Canal arrière d'infrastructure d'affichage ...	Tout	Autoriser	Non	Entrant
✓ Clients de gestion Microsoft Hyper-V - W...	Tout	Autoriser	Non	Entrant
✓ Clients de gestion Microsoft Hyper-V - W...	Tout	Autoriser	Non	Entrant
✓ Clients de gestion Microsoft Hyper-V - W...	Tout	Autoriser	Non	Entrant
✓ Courier et calendrier	Tout	Autoriser	Non	Entrant
✓ DNS Server Forward Rule - TCP - 28b0ca2...	Tout	Autoriser	Non	Entrant
✓ DNS Server Forward Rule - UDP - 28b0ca...	Tout	Autoriser	Non	Entrant
✓ Gestion réseau de base - Destination inac...	Tout	Autoriser	Non	Entrant
✓ Gestion réseau de base - Destination inac...	Tout	Autoriser	Non	Entrant
✓ Gestion réseau de base - Internet Group ...	Tout	Autoriser	Non	Entrant
✓ Gestion réseau de base - IPv6 (Trafic entr...	Tout	Autoriser	Non	Entrant
✓ Gestion réseau de base - problème de pa...	Tout	Autoriser	Non	Entrant
✓ Gestion réseau de base - temps dépassé (...)	Tout	Autoriser	Non	Entrant
✓ Hyper-V - WMI (Async entrant)	Tout	Autoriser	Non	Entrant
✓ Hyper-V - WMI (DCOM entrant)	Tout	Autoriser	Non	Entrant
✓ Hyper-V - WMI (TCP entrant)	Tout	Autoriser	Non	Entrant
✓ Hyper-V (MIG-TCP entrant)	Tout	Autoriser	Non	Entrant
✓ Hyper-V (REMOTE_DESKTOP_TCP_IN)	Tout	Autoriser	Non	Entrant

Actions

- Pare-feu
 - Affichage
 - Actualiser
 - Exporter la liste...
- Aide

Par-feu Windows

Bloquer le port 45948

Bloquer le ping.

Bloquer le port 5265 : mettre seulement sur l'IP 192,168,1,232

Autoriser le port 34-35 seulement sur les IP 192.168.1.1-143

Bloquer intégralement le trafic depuis l'IP 88.120.39.24

Quelles sont les règles permettant de bloquer le partage de fichier SMB ?

GPO –Group Policy Objects

Les stratégies de groupe (ou GP pour group Policy) sont des fonctions de gestion centralisée

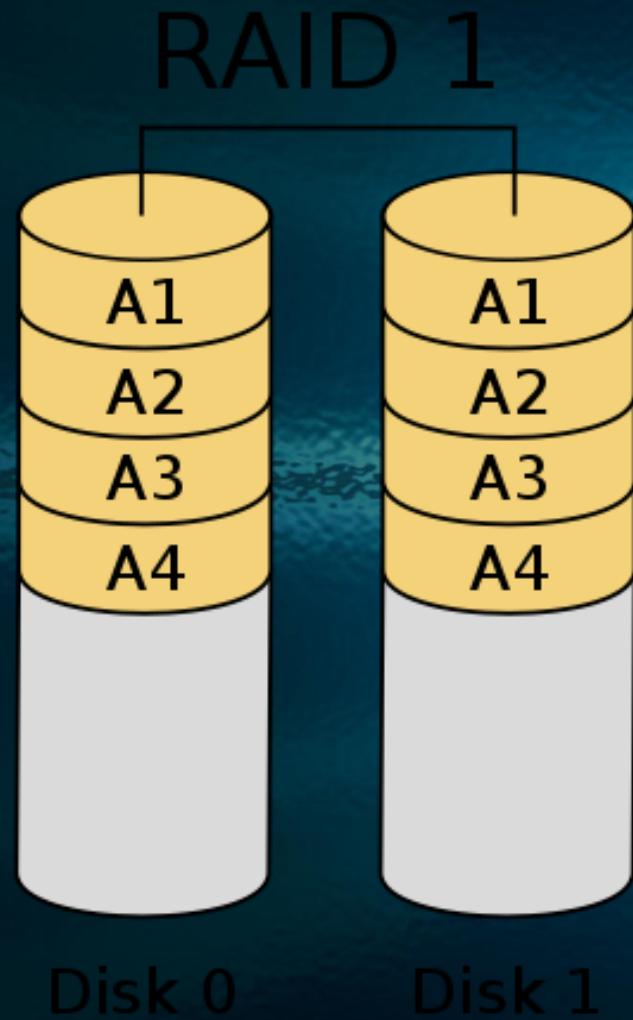
MMC Gestion de stratégie de groupe

Divisé en plusieurs catégories

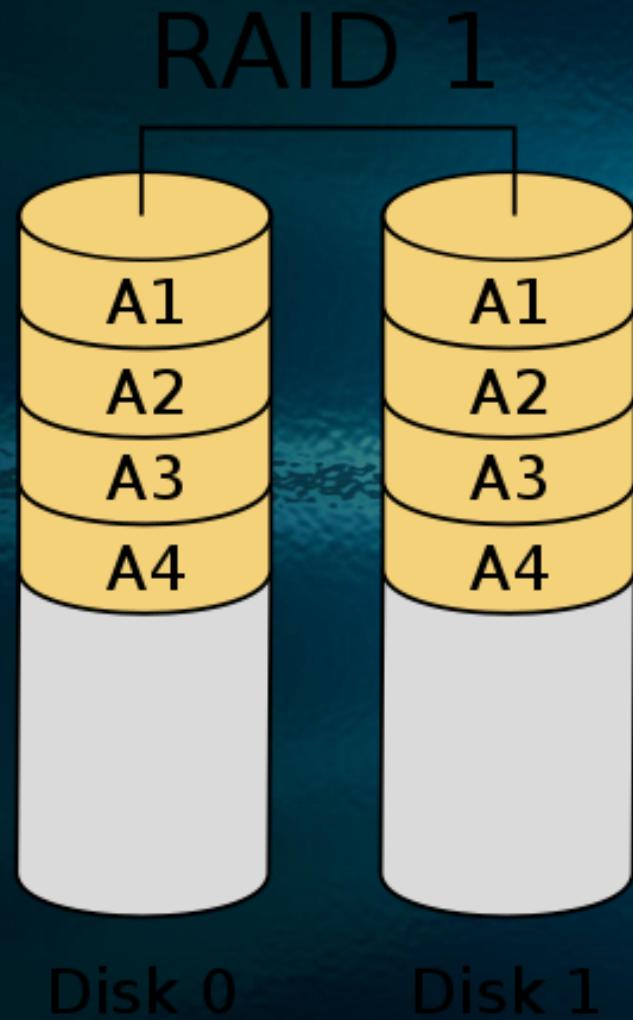
GPO –Group Policy Objects

- Interdire l'accès au panneau de configuration
- Empêcher la suppression de l'historique de nav sur IE
- Empêcher l'accès au Gestionnaire de tâches

Disques miroir



Disques miroir



Stockage Local

Un format de table de partition (ou style de partition) : méthode qu'utilise pour organiser des partitions ou des volumes sur un disque.

Stockage Local

MBR

Le format de table de partition MBR constitue le schéma de partition classique depuis les années 80

Une partition MBR prend en charge un maximum de quatre partitions principales par disque.

Sa taille maximale est de 2 téraoctets (To) ($2,19 \times 10^{12}$ octets). Si capacité est supérieure à 2 To à l'aide du MBR, les disques ne stockent des volumes qu'à hauteur de 2 To. (Convertir GPT)

Stockage Local

MBR

Le format de table de partition MBR constitue le schéma de partition classique depuis les années 80

Une partition MBR prend en charge un maximum de quatre partitions principales par disque.

Sa taille maximale est de 2 téraoctets (To) ($2,19 \times 10^{12}$ octets).

Si capacité est supérieure à 2 To à l'aide du MBR, les disques ne stockent des volumes qu'à hauteur de 2 To. (Convertir GPT)

Stockage Local

GPT

Le format GPT a été utilisé pour la première fois avec Windows Server 2003 et l'édition 64 bits de Windows XP pour dépasser les limites du MBR

Il prend en charge un maximum de 128 partitions par disque.

La taille d'une partition peut aller jusqu'à 18 exaoctets.

Un disque dur peut atteindre 8 zettaoctets (Zo),

Stockage Local

MBR

- Format de table de partition standard depuis le début des années 1980.
- Prend en charge un maximum de quatre partitions primaires par disque.
- Peut partitionner un disque jusqu'à 2 To

GPT

- Successeur du format de table de partition MBR
 - Prend en charge un maximum de 128 partitions par disque
 - Peut partitionner un disque jusqu'à 18 exaoctets
- ✓ **Utilisez MBR pour les disques plus petits que 2 To.**
- ✓ **Utilisez GPT pour les disques de plus de 2 To.**

Disques

DISQUE DE BASE

Un disque de base est initialisé pour du stockage simple et contient des partitions, telles que des partitions principales et des partitions étendue.

Par défaut lors de l'initialisation.

Disques

DISQUE DYNAMIQUE

Disque initialisé pour un stockage dynamique, et qui contient des volumes dynamiques.

Les disques dynamiques sont utilisés pour la configuration de stockage à tolérance de panne.

Volume et non partition.

Disques

Aucun avantage à passer de disque de base à dynamique. A convertir en cas de besoin.

Disque de base > Disque dynamique : Aucune perte de données.

Disque dynamique > Disque de base : Perte de données;

Systèmes de fichier

FAT :

FAT initiale ne pouvait accéder qu'aux partitions inférieures à 2 gigaoctets (Go).

Pour permettre l'utilisation de disques plus grands, Microsoft a développé le système FAT32, qui prend en charge des partitions supérieures à 2 To.

FAT ne fournit aucune sécurité pour les fichiers de la partition : INTERDIT SUR WS !

Systèmes de fichier

NTFS

NTFS représente le système de fichiers classique .

NTFS est nécessaire pour :

Active Directory Domain Services (AD DS),
le Système de fichiers DFS (Distributed File System)
Le service de réplication de fichiers

Systèmes de fichier

ReFS

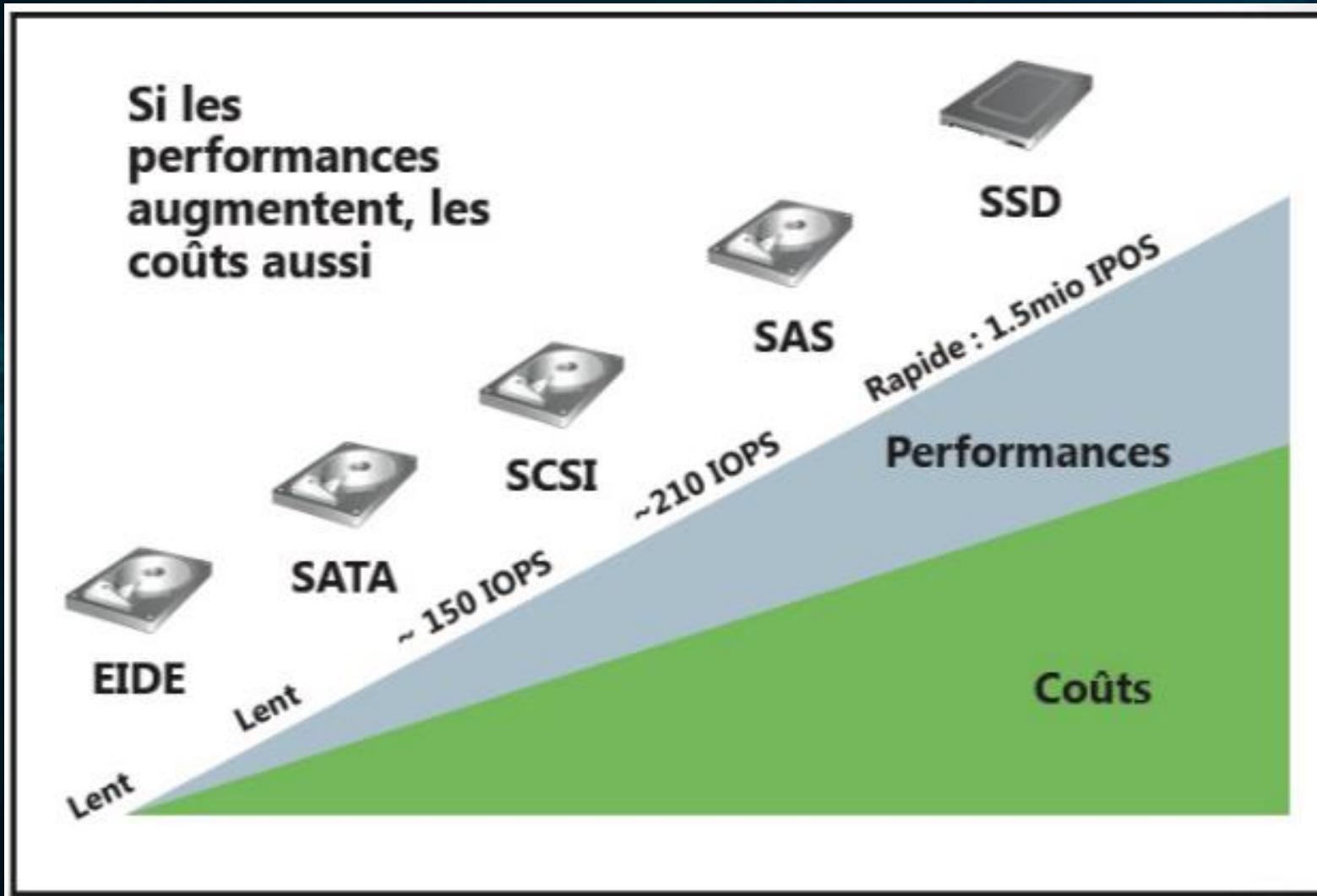
ReFS offre une plus grande résilience, ce qui signifie une vérification de données, une correction d'erreur et une extensibilité meilleures.

Excellent pour des très grands volumes.

A utiliser pour :

- Charges de travail de Microsoft Hyper-V. ReFS affiche des avantages en termes de performance lors de l'utilisation conjointe de fichiers .vhd et .vhdx.
- Espaces de stockage direct. Sous Windows Server 2016, les nœuds d'un cluster peuvent partager un stockage attaché direct.

Systèmes de fichier

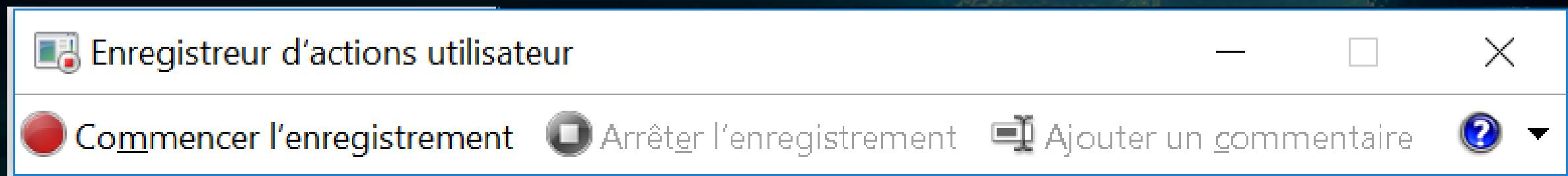


RAID 1

- Sur Hyper-V : Monter un RAID 1 logiciel sur la VM
- Tester le basculement

Enregistrer les étapes pour reproduire un problème

Génère un fichier reproduisant toutes les actions utilisateur.



Centre de sécurité

Sécurité et maintenance

← → ▾ ▾ Panneau de configuration > Système et sécurité > Sécurité et maintenance ▾ 🔍 Rechercher 🔎 ?

Page d'accueil du panneau de configuration

Modifier les paramètres du centre Sécurité et maintenance

Modifier les paramètres du contrôle de compte d'utilisateur

Afficher les messages archivés

Examiner les messages récents et résoudre les problèmes

Aucun problème n'a été détecté par le centre Sécurité et maintenance.

Sécurité

Maintenance

Si vous ne voyez pas votre problème dans la liste, essayez l'une des rubriques suivantes :

 Récupération

Actualisez votre PC sans affecter vos fichiers, ou réinitialisez-le et recommencez depuis le début.

Moniteur de fiabilité

Moniteur de fiabilité

« Système et sécurité > Sécurité et maintenance > Moniteur de fiabilité

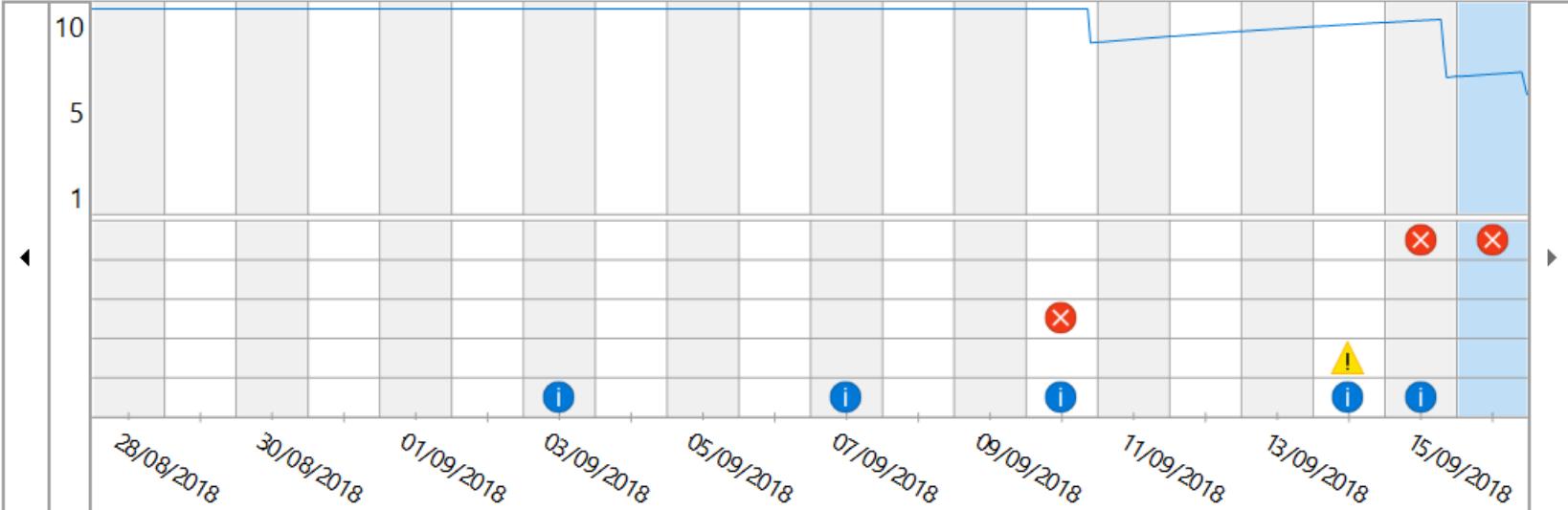
Rechercher

Examiner l'historique de fiabilité et des problèmes de votre ordinateur

L'indice de stabilité indique la stabilité globale de votre système sur une échelle de 1 à 10. En sélectionnant une période spécifique, vous pouvez examiner les problèmes particuliers d'ordre matériel ou logiciel qui affectent votre système.

Afficher par : [Jours](#) | [Semaines](#)

Dernière mise à jour : 16/09/2018 11:00



Échecs des applications
Échecs Windows
Échecs divers
Avertissements
Informations

Détails de fiabilité pour : 16/09/2018

Source	Résumé	Date	Action
Événements critiques			
	Search and Cortan... A cessé de fonctionner ... 16/09/2018 1...	16/09/2018 1...	Afficher l...

Historique de fichiers

Historique des fichiers

Page d'accueil du panneau de configuration

Restaurer des fichiers personnels

Sélectionner un lecteur

Exclure des dossiers

Paramètres avancés

Panneau de configuration > Système et sécurité > Historique des fichiers

Rechercher

?

Conservez un historique de vos fichiers.

L'historique des fichiers enregistre des copies de vos fichiers ; vous pouvez ainsi les récupérer s'ils sont perdus ou endommagés.

i Impossible de trouver un disque exploitable. Il est recommandé d'utiliser un lecteur externe pour l'historique des fichiers. Connectez un lecteur et actualisez cette page ou bien utilisez un emplacement réseau.

[Sélectionner un emplacement réseau](#)

L'historique des fichiers est désactivé.

Copier les fichiers à partir de : Bibliothèques, Bureau, Contacts et Favoris

Copier les fichiers vers : *Aucun lecteur utilisable n'a été trouvé.*

Activer

Robocopy

Robocopy possède de nombreuses fonctionnalités qui sont très appréciées car elle sont supérieures aux commandes internes COPY ou XCOPY de Windows

En particulier :

- **Une tolérance aux coupures réseau et une reprise une fois la connexion rétablie**
- **La conservation des attributs et des informations d'appartenances des fichiers ou (créateur, propriétaire, ACL NTFS, informations d'audit)**
- **Tri par extensions...**

Robocopy – Exercice

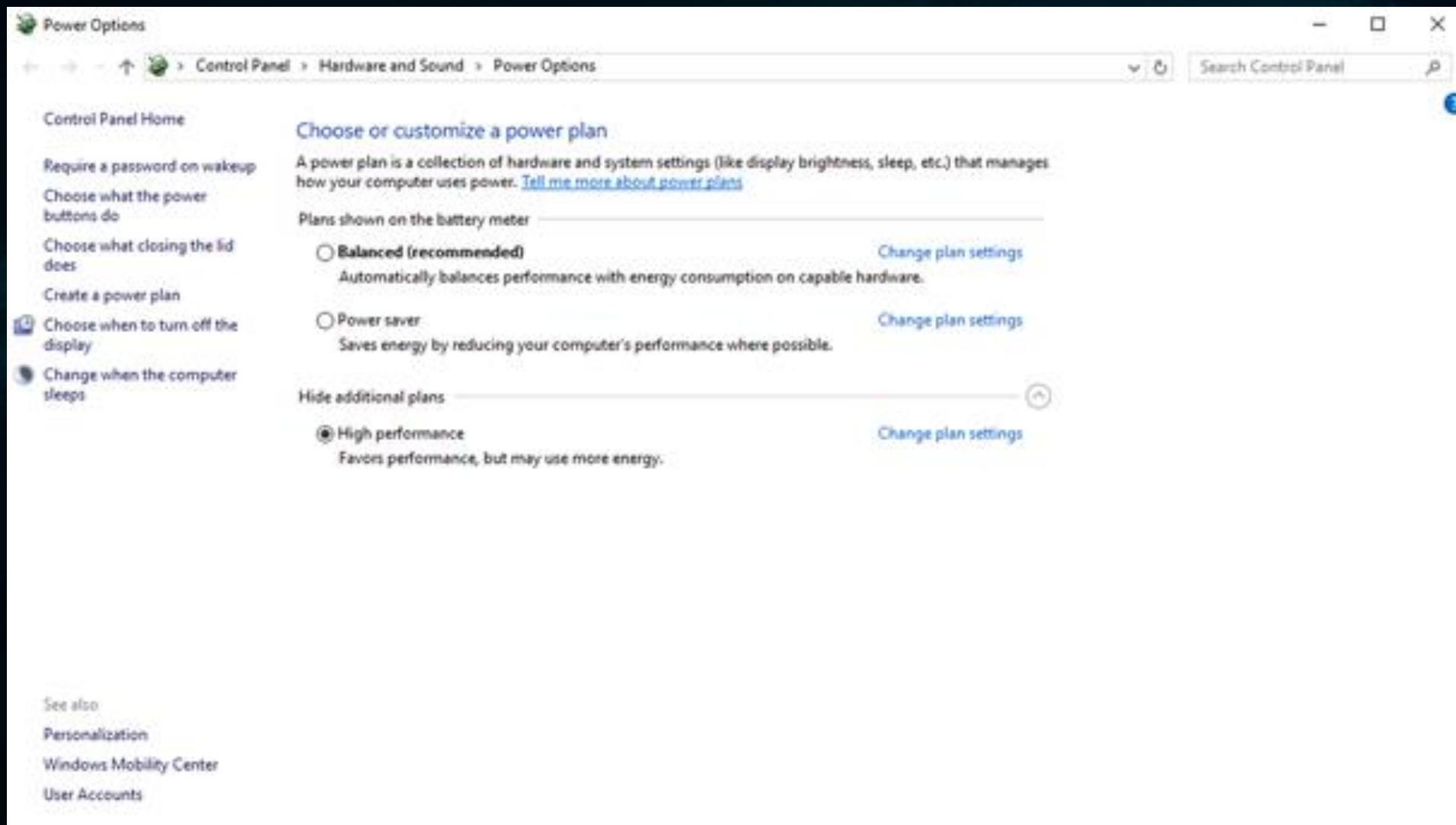
Télécharger un gros dossier avec plusieurs fichiers à l'intérieur (ex : repository Github)

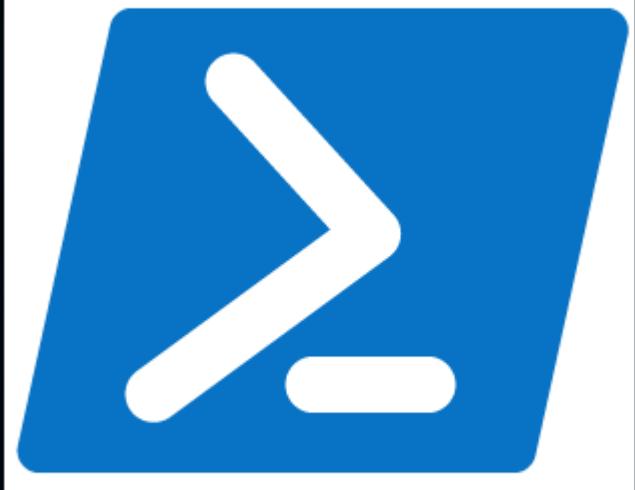
Créer un script Robocopy qui copiera ce dossier vers un autre endroit avec ces contraintes

- Le nombre d'essai si la copie initiale échoue : 2 essais
- Le délais d'attente entre 2 essais : 3 secondes
- Copier les sous dossiers même ceux vides
- Exclure les extensions « .sys »
- Utiliser l'argument « DATSOU ». A quoi sert-il ?

Astuces

Améliorer les performances





Powershell : PackageManagement

Nouveau module sous Powershell 5.0

Gestionnaire de paquets (se rapproche de Linux !)

Automatise l'installation de logiciels.

```
PS C:\Users\Taieb> Get-Command -Module PackageManagement
```

CommandType	Name	Version	Source
Cmdlet	Find-Package	1.0.0.1	PackageManagement
Cmdlet	Find-PackageProvider	1.0.0.1	PackageManagement
Cmdlet	Get-Package	1.0.0.1	PackageManagement
Cmdlet	Get-PackageProvider	1.0.0.1	PackageManagement
Cmdlet	Get-PackageSource	1.0.0.1	PackageManagement
Cmdlet	Import-PackageProvider	1.0.0.1	PackageManagement
Cmdlet	Install-Package	1.0.0.1	PackageManagement
Cmdlet	Install-PackageProvider	1.0.0.1	PackageManagement
Cmdlet	Register-PackageSource	1.0.0.1	PackageManagement
Cmdlet	Save-Package	1.0.0.1	PackageManagement
Cmdlet	Set-PackageSource	1.0.0.1	PackageManagement
Cmdlet	Uninstall-Package	1.0.0.1	PackageManagement
Cmdlet	Unregister-PackageSource	1.0.0.1	PackageManagement

- **Find-Package** : Rechercher un paquet au sein des sources de paquets disponibles
- **Get-Package** : Retourne la liste des tous les paquets installés
- **Get-PackageProvider** : Retourne la liste des fournisseurs de paquets (dépôts) utilisés sur la machine
- **Get-PackageSource** : Retourne la liste des sources disponibles pour récupérer les paquets
- **Install-Package** : Installer un paquet (logiciel) sur la machine
- **Register-PackageSource** : Ajouter une source dans un provider
- **Save-Package** : Sauvegarder un paquet en local sans l'installer
- **Set-PackageSource** : Définir un provider comme source pour les paquets
- **Uninstall-Package** : Désinstaller un paquet (logiciel)
- **Unregister-PackageSource** : Retirer l'utilisation un provider des sources pour les paquets

Gestionnaire de paquet

Installation du package :

```
Set-ExecutionPolicy Bypass -Scope Process -Force; iwr https://chocolatey.org/install.ps1 -UseBasicParsing | iex
```

choco search [keyword]

choco upgrade [packagename]

choco upgrade chocolatey

choco list –local-only

choco uninstall

1 – Installer Chocolatey

2 – Installer Ccleaner

3 – Réaliser un script qui va installer en même temps Chrome, Firefox et 7Zip sans demande de confirmation

Autre gestion package :

<https://ninite.com/>

Méthodologie

« Diviser pour mieux régner »

Chaque problème doit être décliné en des sous catégories

- **Hardware**
- **Software**
- **Utilisateur**

Et des sous catégories à cela

- **Hardware**
 - **Compatibilité**
 - **Usure**
 - **Branché**

Troubleshooting

Règle n°1 : On passera plus de temps à comprendre la question plutôt que la résoudre

Exemple de Ticket (Source Mairie, conseil général, ...) :

- Rien marche, Merci de venir dépanner.
- Le truc fait que la croix plante !
- La machine démarre plus
- Mon porte gobelet ne s'ouvre plus !!

Méthodologie

Règle n°2 : Le problème est généralement entre la chaise et le clavier

- Pourquoi quand je clique sur « mettre à jour et redémarrer », ça m'a tout coupé.
- J'avais tous mes fichiers importants dans la corbeille mais la je ne retrouve rien.
- J'ai débranché les câbles, ça gênait quand j'essayai d'étirer mes jambes

Méthodologie

Règle n°3 : Une résolution de problème entraînera souvent les foudres de l'utilisateur

- Ah mais du coup je dois retourner travailler ?
- Ouais bin, ça marchait mieux avant que vous passiez.
- Depuis Windows 10, je retrouve rien, je peux repasser à l'ancien ?

Méthodologie

Règle n°4 : Un dépannage en direct est toujours plus efficace qu'au téléphone

- Les utilisateurs penseront toujours que le problème sera résolu plus efficacement ou plus rapidement si vous « venez voir ce qui va pas sur mon écran depuis mon bureau », même si c'est juste un problème de résolution d'écran

Méthodologie

Règle principale : Organisation

Bips de l'ordinateur au démarrage



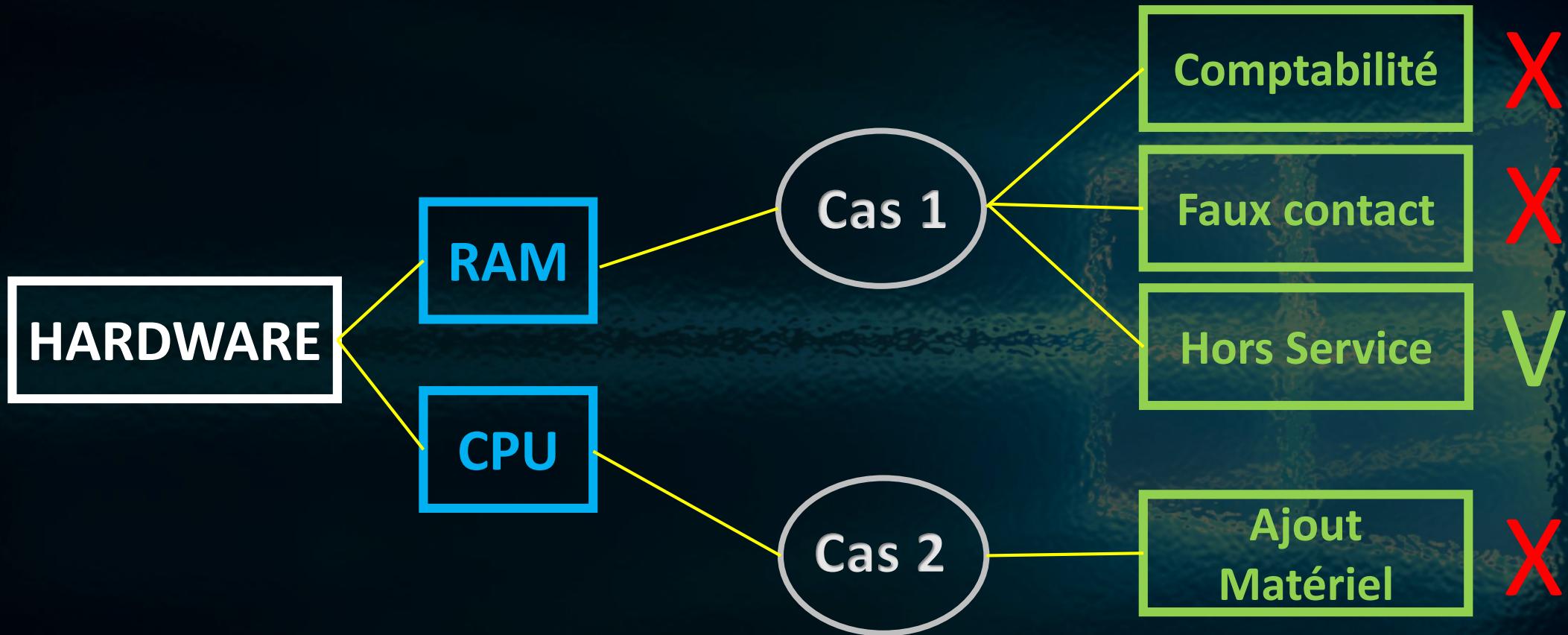
Série de bips séparés



Cas 1 : Barrettes branchées

Cas 2 : Barrettes débranchées

Méthodologie



Dépannage

Assemblage de l'ordinateur :

Bruit de frottement

Câble qui touche un ventilateur

Attention au détrompeur

Si ça force, ce n'est pas bon



Interpréter les codes POST (Bips)

1 Bip : aucune anomalie

1 Bip suivi de 2 Bips longs : Vérifier le branchement de la carte graphique

Une série de bips espacés : Vérifier les barettes de RAM

Une série de bips qui ressemblent à une alarme de pompier : Vérifier le processeur

Une série de bips très rapprochés : Vérifier qu'une touche du clavier ne soit pas bloquée

Un bip en continu : Vérifier l'alimentation

Dépannage

Problème matériel :

Retirer les composants pour trouver la faille

Ordre logique :

- 1- Périphériques externes (USB et parallèle)
- 2- Clavier et souris
- 3- Lecteurs de carte
- 4- Cartes internes (PCI, AGP)
- 5- Barrettes mémoire
- 6- Lecteurs de disques
- 7- Ventilateur de processeur
- 8- Processeur

Carte mère si écran noir, sans bip



wikiHow

Dépannage

Quelques cas usuels

Ecran noir au démarrage

- Câble alimentation écran
- Câble VGA – HDMI – DVI
- Alimentation tour

L'ordinateur se coupe juste après le démarrage

- Processeur ou carte mère

L'ordinateur fait du bruit

- Ventilateur

L'ordinateur ralentit au bout de quelques heures

- Surchauffe du processeur

Problème d'heure et date

message d'erreur : « CMOS Battery state low/has failed »



Dépannage

« Veryfing dmi pool data »

- BIOS ou carte mère

L'ordinateur s'éteint pendant l'utilisation

- Alimentation ou surchauffe

L'ordinateur se fige en cours d'utilisation

- Carte mère ou Barrette de RAM

L'ordinateur se fige de manière aléatoire

- Disque dur

L'ordinateur se fige à un moment déterminé

- Surchauffe du processeur

Problème d'affichage sur l'écran

- Carte vidéo



Outils AdwCleaner

Gratuit
Très léger
Pas d'installation

Supprime les éléments suivants :

- Adwares
- PUP/LPI
- Toolbars
- hijackers



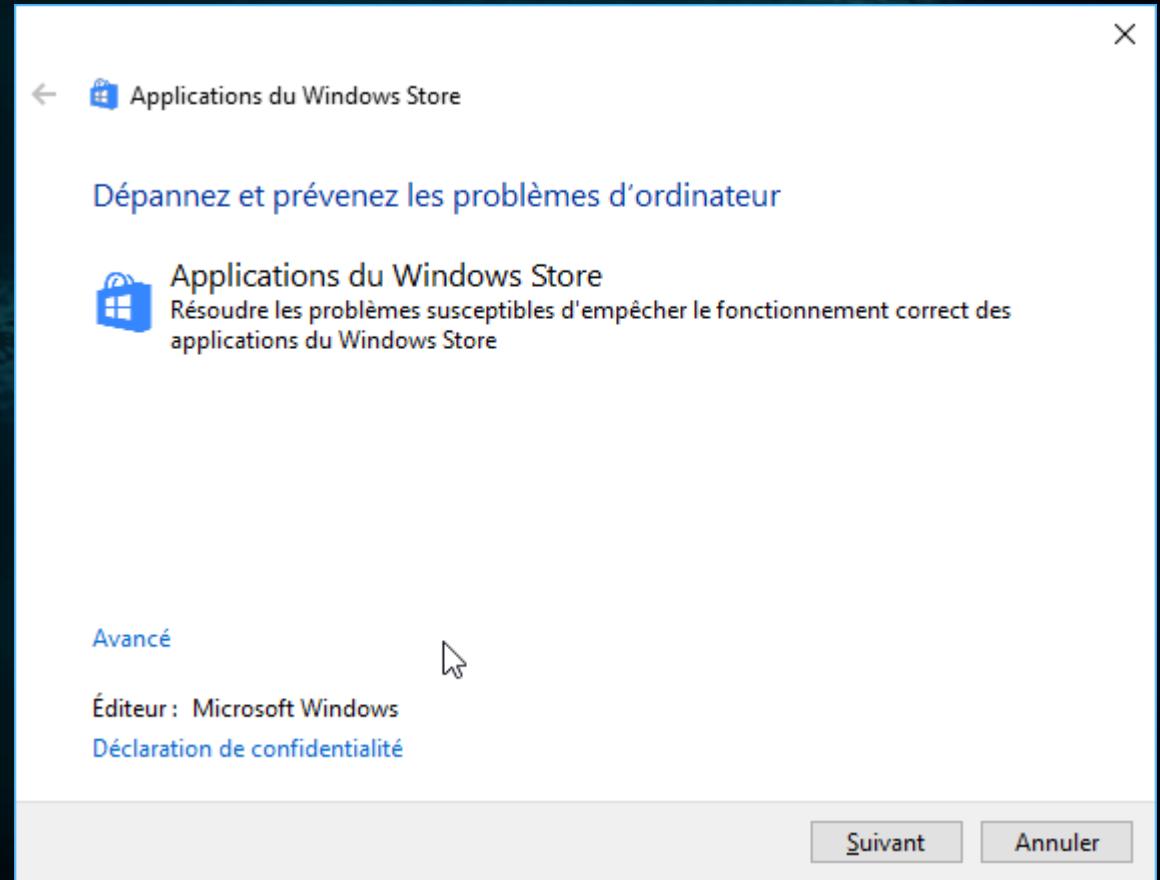
Outils

appsdiagnostic10.diagcab

Lié au Windows Store de Windows 10

Permet de fixer des problèmes liés au différentes manipulations du Store

- Téléchargement
- Installation
- Suppression



Outils BlueScreenView

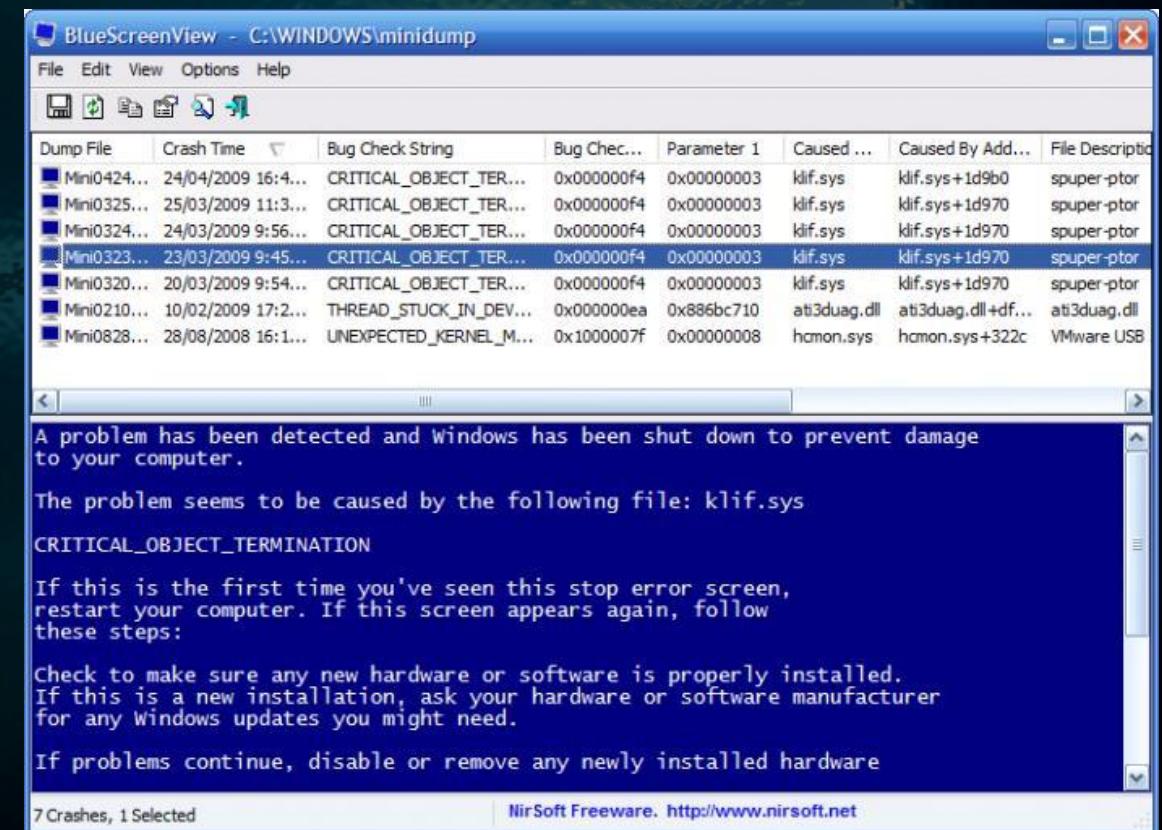
Gratuit

Sans installation

Permet de visualiser les MiniDump créés lorsque Windows s'arrête sur un Blue Screen

Permet d'afficher :

- Date
- Heure
- Bug Check Code
- Cause potentielle de la panne



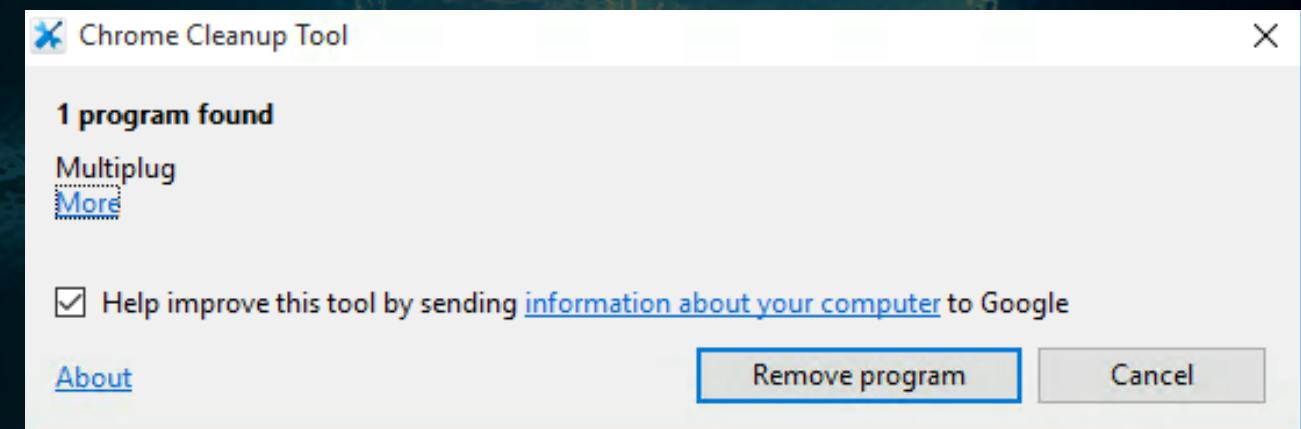
Outils CCT

Utilitaire de nettoyage pour Google Chrome

Plus proche de la réinitialisation que de la résolution

Supprime les indésirables :

- Toolbars
- page de démarrage
- annonces



Outils

Complete Internet Repair

Reset les informations de la carte réseau

Vide le cache DNS

Reset la plupart des options Internet

Plus utiliser dans le cas d'une réinitialisation
de tout ce qui concerne le réseau



Outils Dual Boot Repair

Réparation du gestionnaire de boot

Gestion du multi boot

Nécessite un OS fonctionnel déjà présent



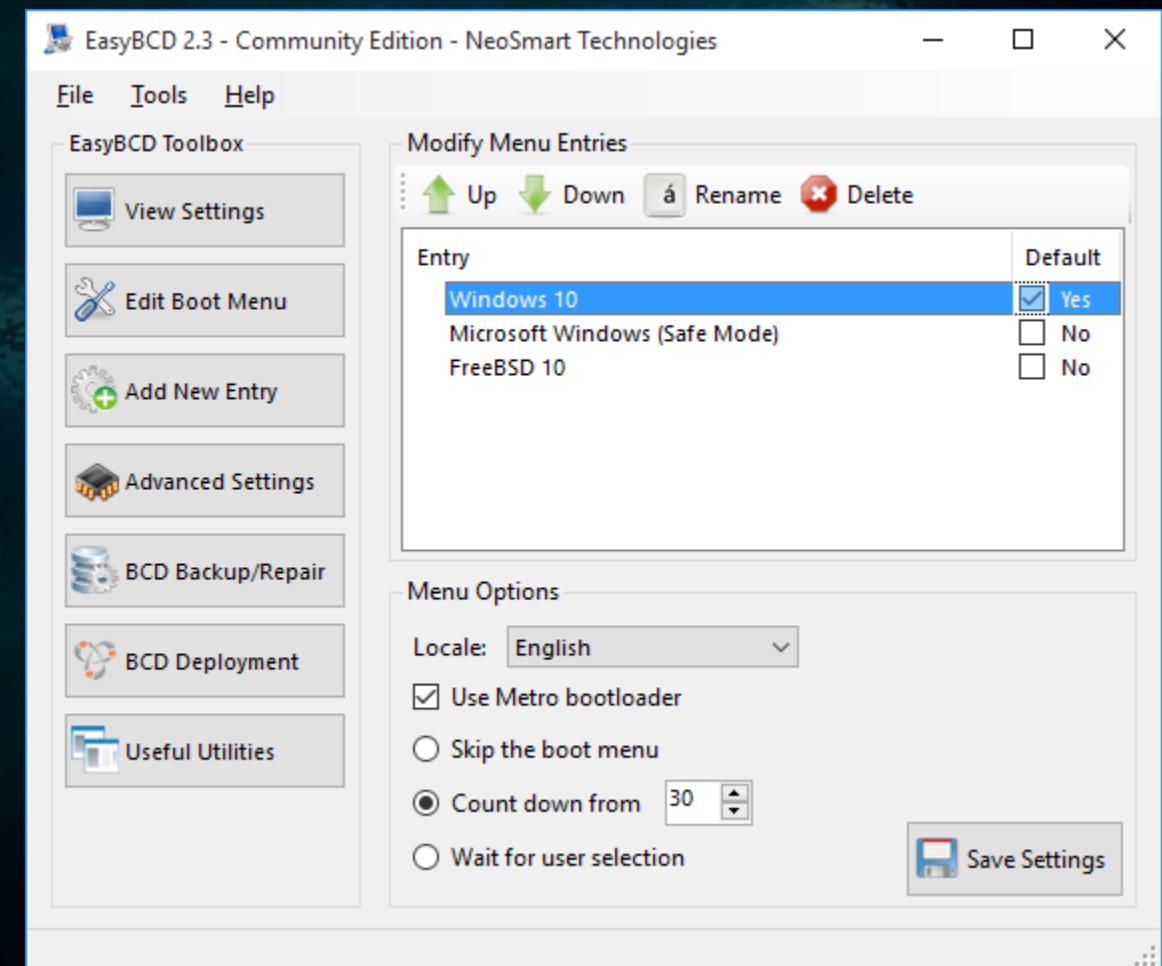
Outils

EasyBCD

Réparation du gestionnaire de boot

Gestion du multi boot

Nécessite un OS fonctionnel déjà présent



Outils

Hiren's boot

Hiren's BootCD se présente sous la forme d'une image disque à graver sur un CD

Les différentes catégories :

Antivirus

Sauvegarde

BIOS

Gestionnaire de fichiers

Nettoyeur

Disque dur

MBR

Optimisation

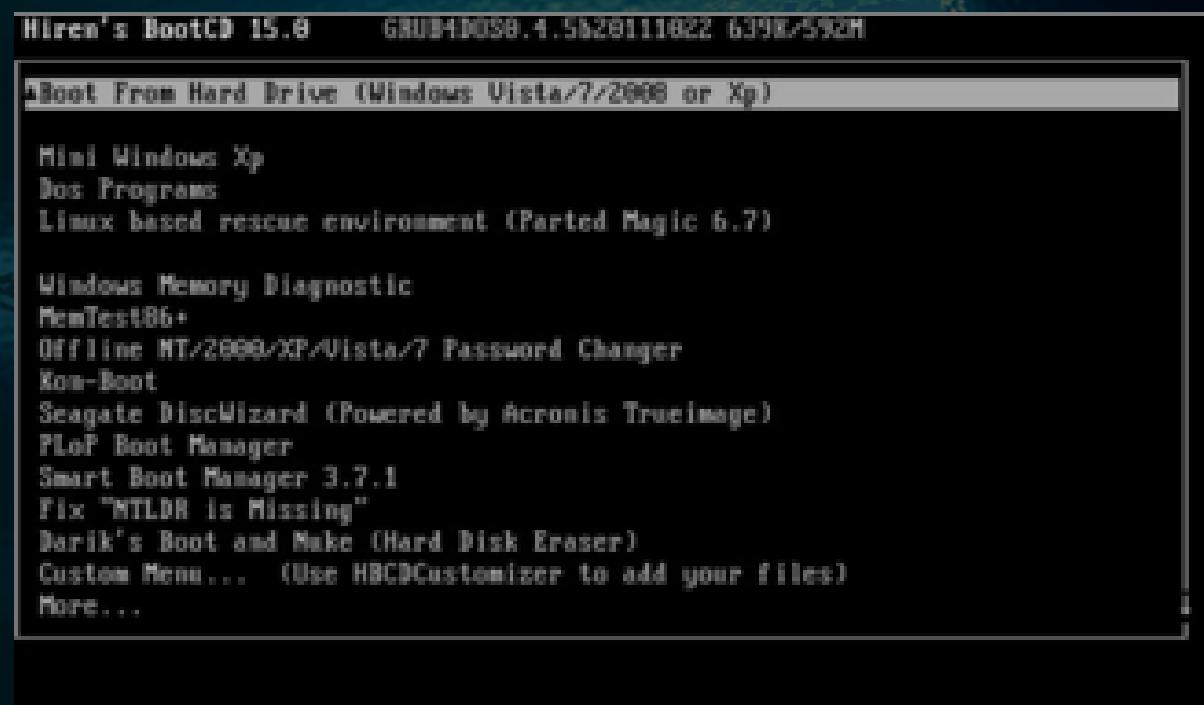
Test

Registre

Récupération

Mot de passe

Partition



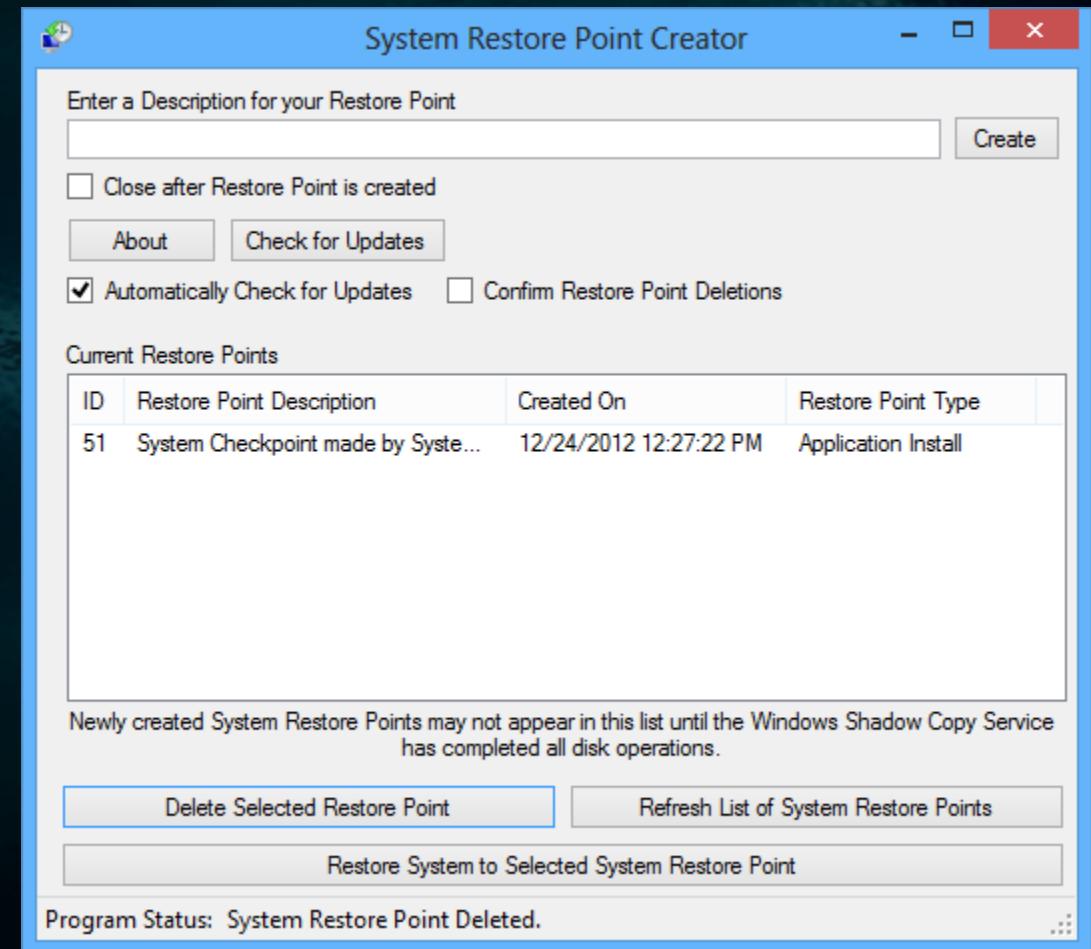
Outils

Restore Point Creator

Gratuit

Permet de créer facilement des points de restauration

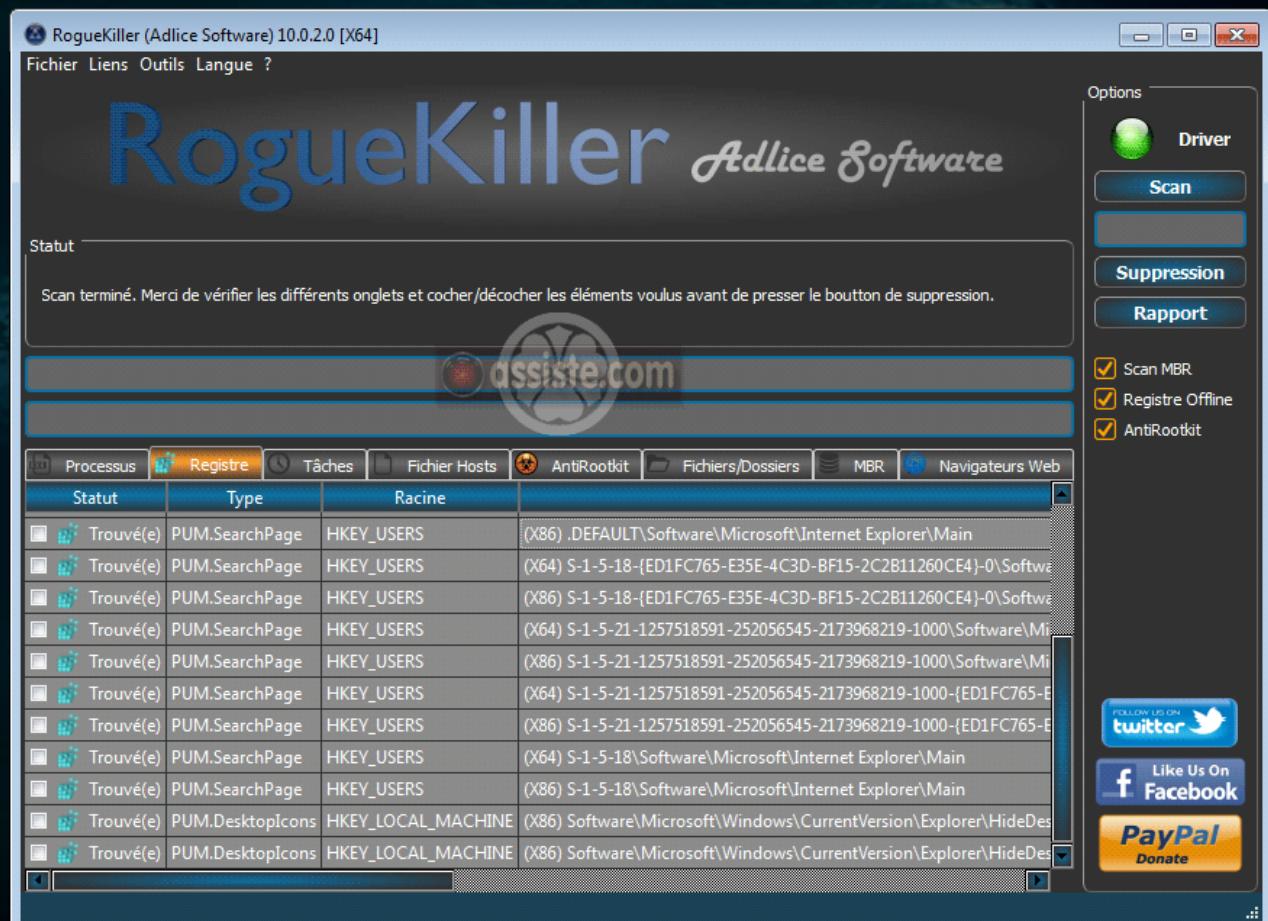
Permet de gérer une automisation de la création des points de restauration



Outils rogue Killer

Permet de terminer et supprimer des processus et programmes malveillants

Notamment utilisé pour les ransomwares



Outils

ZHPDiag

diagnostic rapide et complet du système d'exploitation

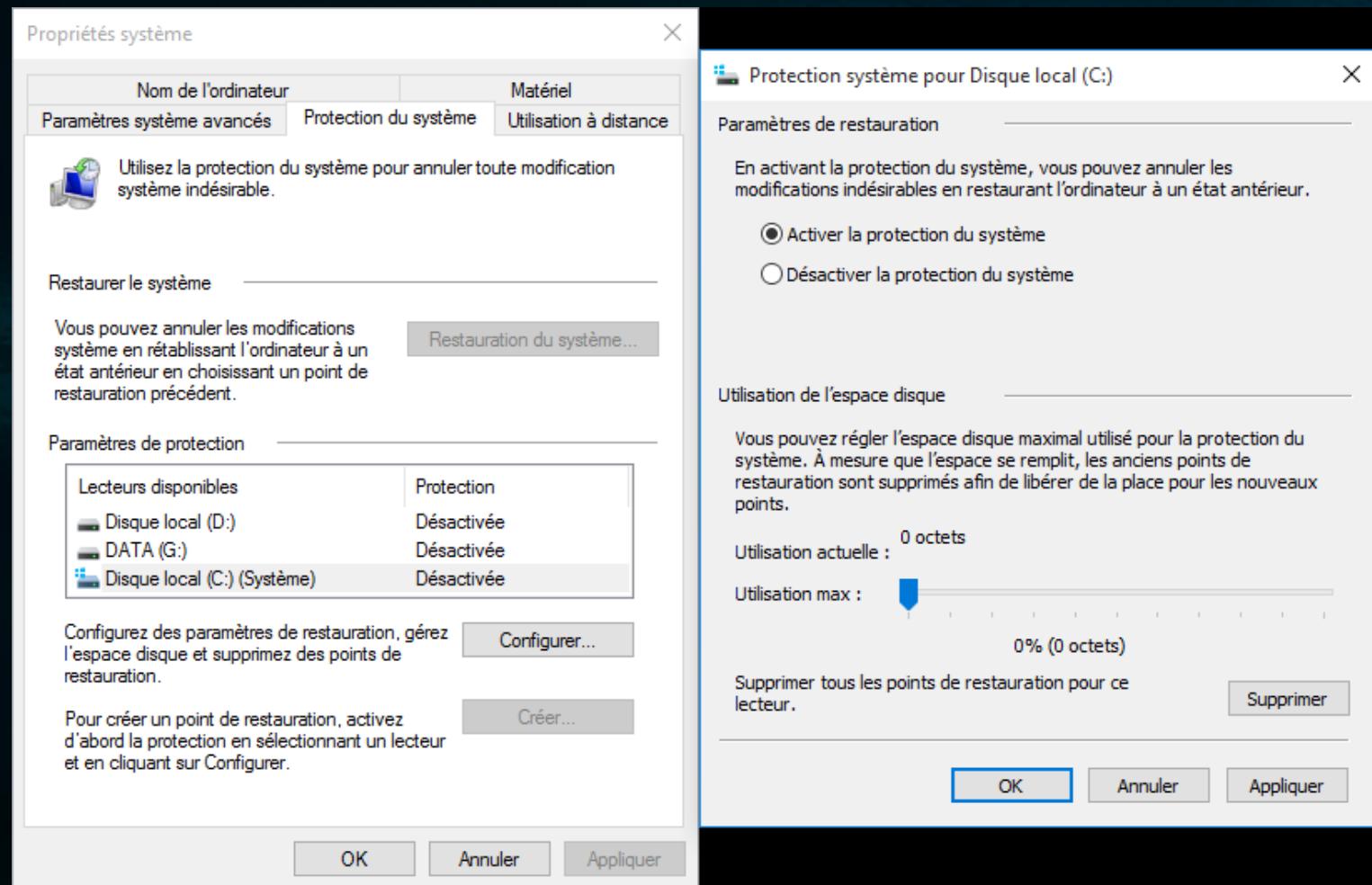
Gère Base de Registres et énumère les zones sensibles qui sont susceptibles d'être piratées

La liste de détection renvoie vers des fiches descriptives du malware.

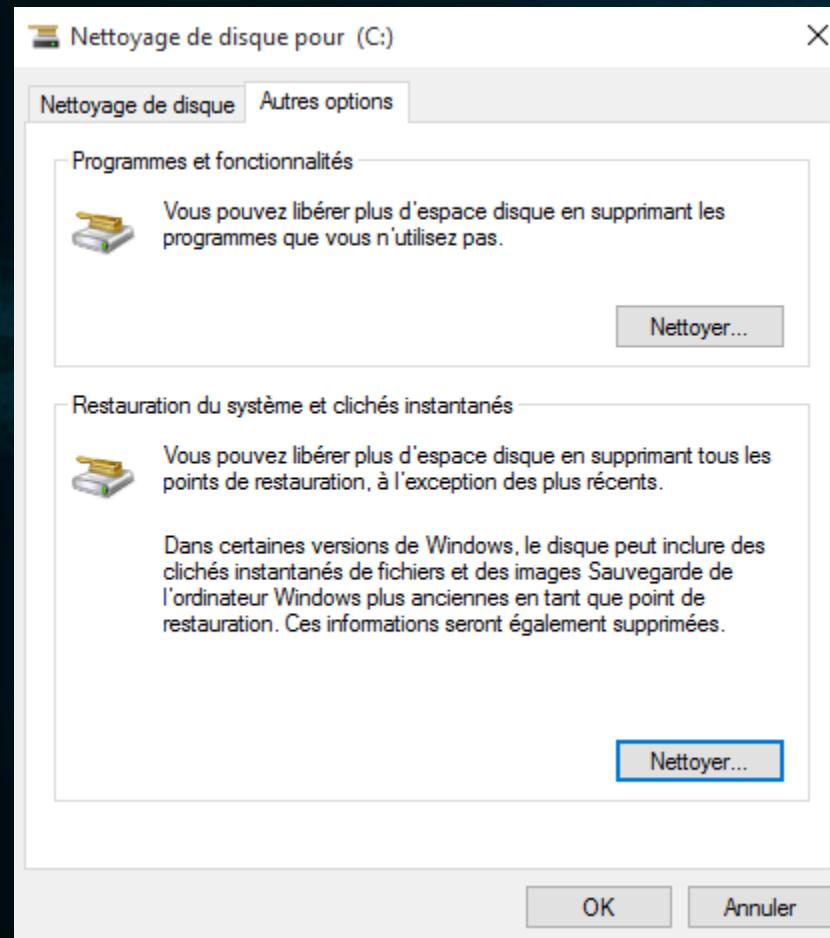


Récupération du système

Création d'un point de restauration

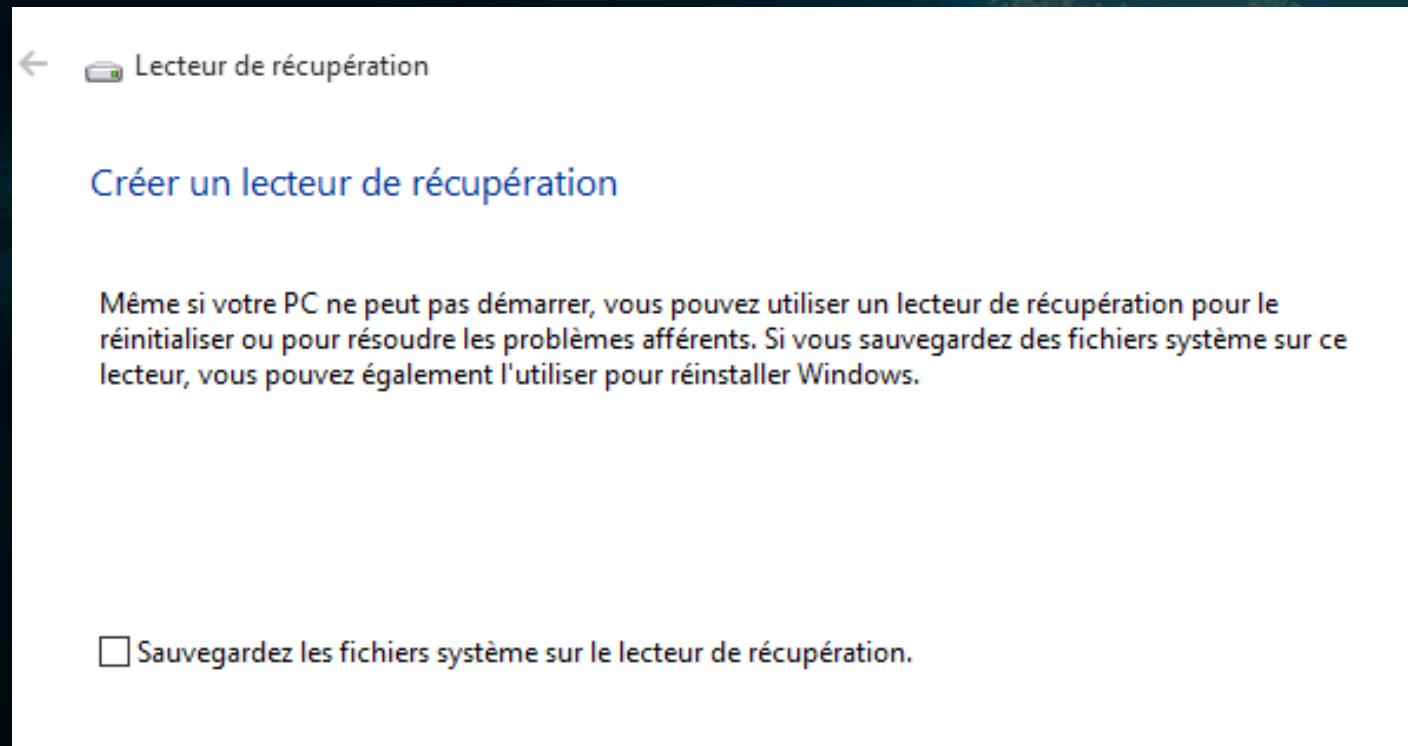


Récupération du système suppression des points obsolètes



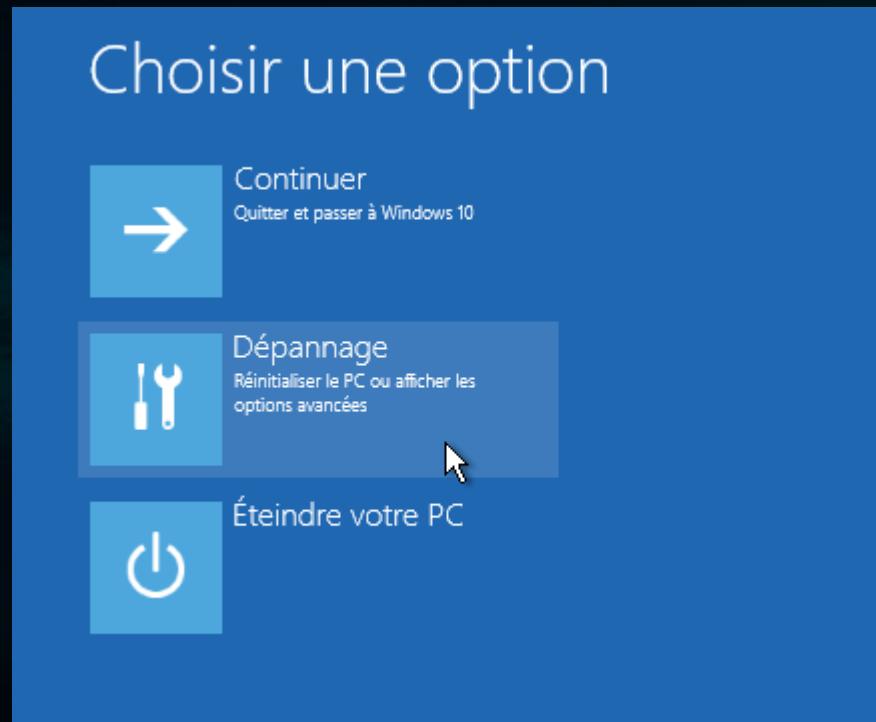
Récupération du système

Créer un lecteur de récupération



Récupération du système

Options de démarrage



Récupération du système

Options avancées

← Options avancées



Restauration du système

Utiliser un point de restauration sur votre PC pour restaurer Windows



Invite de commandes

Utiliser l'invite de commandes pour un dépannage avancé



Récupération de l'image système

Récupérer Windows à l'aide d'un fichier image système spécifique



Paramètres

Changer le comportement de Windows au démarrage



Outil de redémarrage système

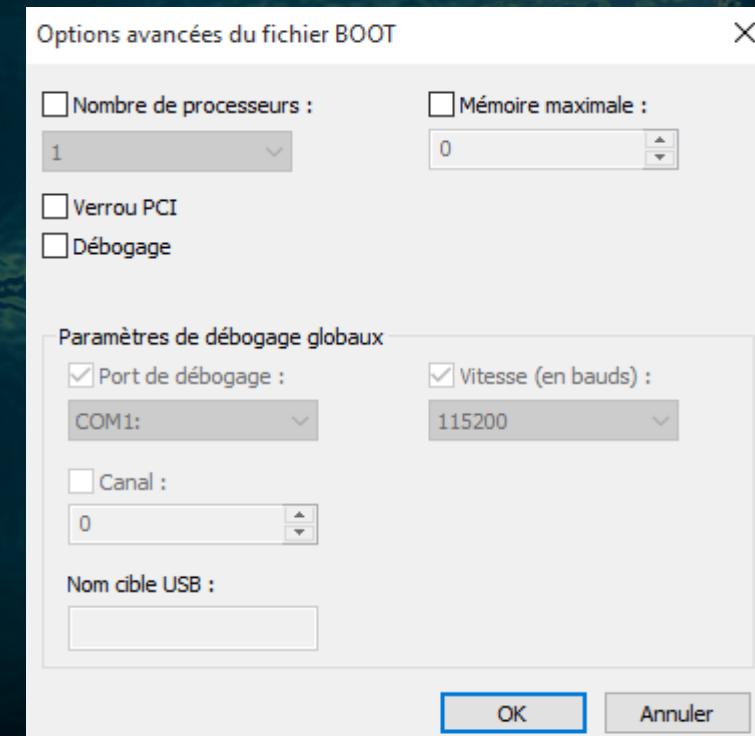
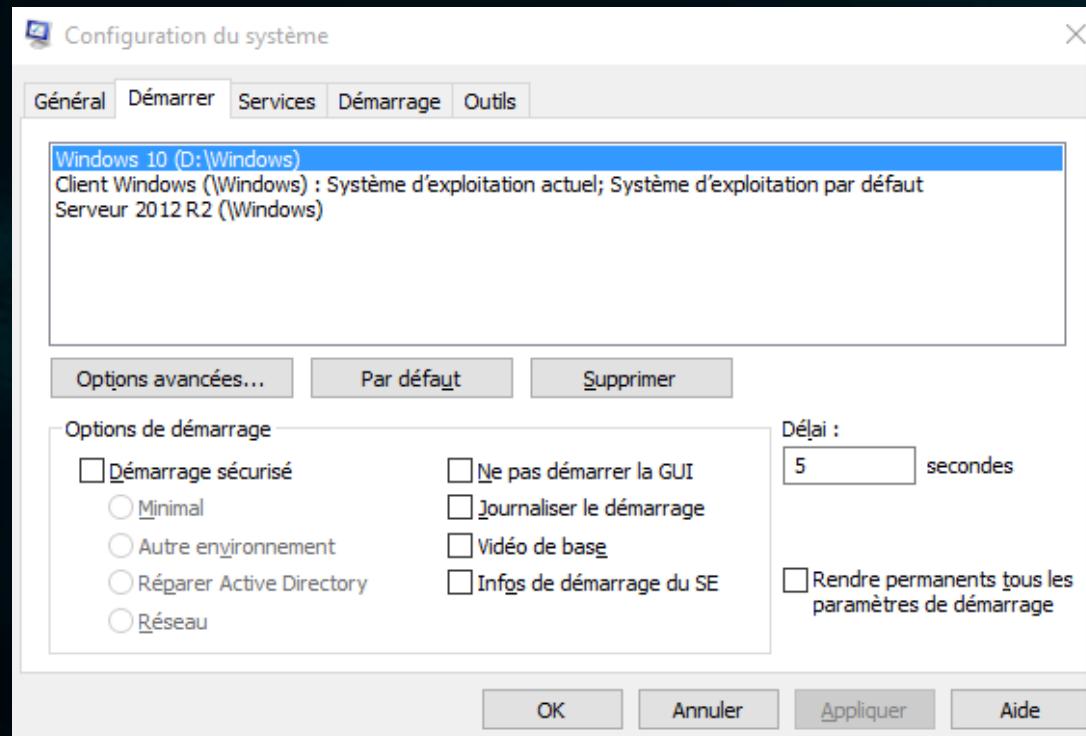
Corriger les problèmes qui empêchent le chargement de Windows



Rétrograder vers la version précédente

Récupération du système

msconfig



Récupération du système

Windows Boot Manager

Windows failed to start. A recent hardware or software change might be the cause. To fix the problem:

1. Insert your Windows installation disc and restart your computer.
2. Choose your language settings, and then click "Next."
3. Click "Repair your computer."

If you do not have this disc, contact your system administrator or computer manufacturer for assistance.

File: \Windows\system32\winload.exe

Status: 0xc0000225

Info: The selected entry could not be loaded because the application is missing or corrupt.

Registre (BDR)

Base de données fonctionnelles de la machine

Les informations du registre sont stockées à l'intérieur de dossiers appelés « clés »

On appelle valeur les différentes données contenues dans ces clés comme les licences, chemin, ...

Accessible via l'exécutable « regedit » présent dans C:\Windows

Registre (BDR)

HKEY_CLASSES_ROOT

Sert à la gestion des types de fichiers, gestion de l'OS

On parle aussi de raccourci vers une sous clef de HKEY_LOCAL_MACHINE

HKEY_CURRENT_USER

Contient les données du profil de l'utilisateur courant.

On parle aussi de raccourci vers une sous clef de HKEY_USERS

HKEY_LOCAL_MACHINE

Contient les informations de l'ordinateur lui-même, matériels, config réseau, sécurité

HKEY_USERS

Recense tous les profils utilisateurs, apparence, personnalisation

HKEY_CURRENT_CONFIG

Contient des préférences d'utilisation du matériel, pilotes, mode de gestion

On parle aussi de raccourci vers une sous clef de HKEY_LOCAL_MACHINE

Registre (BDR)

Les valeurs sont composées de 3 éléments : Nom, Type, Données

Types :

REG_SZ

Valeur textuelle standard

REG_DWORD

Valeur numérique (nombre entier hexadécimale ou binaire)

REG_MULTI_SZ

Valeurs textuelles multiples (séparées par un caractère particulier)

REG_EXPAND_SZ

Valeurs textuelles extensibles (Texte générique qui s'adapte à la configuration)

Exemple : %systemroot% → C:\Windows

→ D:\Windows

→ C:\Winnt

Registre (BDR)

Les clefs et valeurs utiles

- **Changer son numéro de série**

Clef : HKEY_LOCAL_MACHINE \ Software \ Microsoft \ Windows \ CurrentVersion

Valeur : ProductKey

- **Supprimer les DLL inutiles de la mémoire**

Clef : HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer

Valeur : Créez une valeur DWORD. Nommez-la "AlwaysUnloadDll" et donnez lui la valeur « 1 »

- **Activer le pavé numérique**

Clef : HKEY_USERS \ .Default \ Control Panel \ Keyboard

Valeur : Attribuez la valeur 2 à InitialKeyboardIndicators

- **Activer le chiffrement EFS dans le menu contextuel**

Clef : HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Explorer \ Advanced

Valeur : Créez une valeur DWORD. Nommez-la « EncryptionContextMenu" et donnez lui la valeur « 1 »

Registre (BDR)

Les clefs et valeurs utiles

- Supprimer le redémarrage forcé de Microsoft (reporté dans 10 min/ 1h/ 4h)

Clef : HKEY_LOCAL_MACHINE \ SOFTWARE \ Policies \ Microsoft \ Windows \ WindowsUpdate \ AU

Valeur : Créez une valeur DWORD « NoAutoRebootWithLoggedOnUsers » et donnez lui la valeur « 1 »

- Faire planter Windows avec 3 touches

Si clavier USB

Clef : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kbdhid\Parameters

Valeur : Créez une valeur DWORD. Nommez-la "CrashOnCtrlScroll" et donnez lui la valeur « 1 »

Si clavier en PS2

Clef : HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\i8042prt\Parameters

Valeur : Créez une valeur DWORD. Nommez-la "CrashOnCtrlScroll" et donnez lui la valeur « 1 »

Applications Natives

Get-AppxPackage -AllUsers

Get-AppxPackage -AllUsers | Remove-AppxPackage

3D printing

*Get-AppxPackage *3d* | Remove-AppxPackage*

Xbox app

*Get-AppxPackage *xbox* | Remove-AppxPackage*

Money/Sports/News/Weather

*Get-AppxPackage *bing* | Remove-AppxPackage*

Music and TV/Videos

*Get-AppxPackage *zune* | Remove-AppxPackage*

Eviter la propagation des packages sur un nouveau profile

Get-AppXProvisionedPackage -online | Remove-AppXProvisionedPackage –online