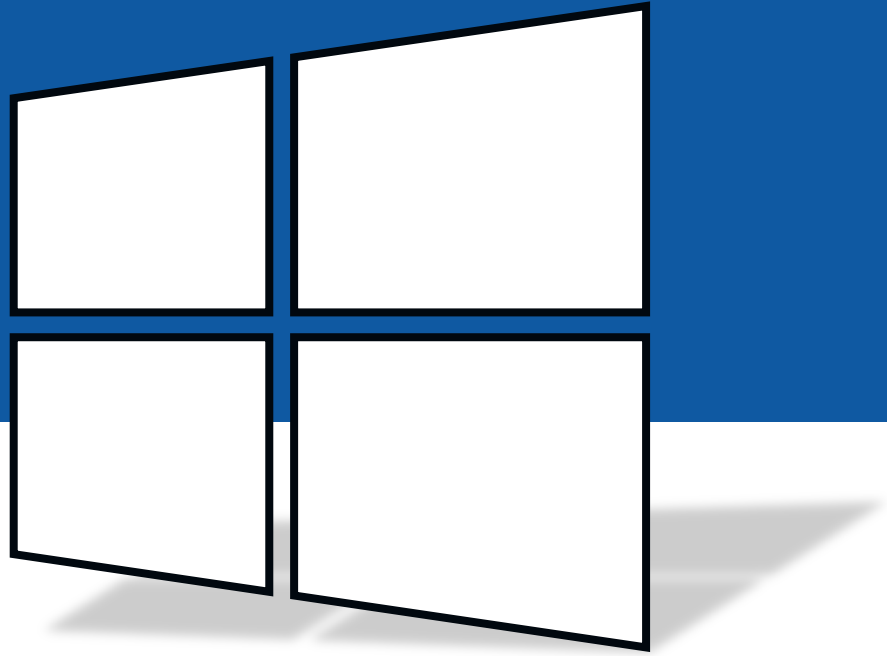




Démarrage

420-1S6 Systèmes d'exploitation



Windows

Séquence d'amorçage



Le démarrage de Windows est subdivisé en plusieurs phases :

- ❖ **Pré-amorçage**, avant que Windows démarre (la phase BIOS)
- ❖ **Amorçage** (boot loader)
- ❖ **Chargement du noyau** (kernel)
- ❖ **Ouverture de session**

Pré-amorçage



Lorsqu'un ordinateur démarre, le premier programme exécuté est contenu sur une puce mémoire soudée sur la carte mère. Ce programme s'appelle le ***firmware***.

Il existe deux types de firmware qui équipent les ordinateurs conventionnels:

- > **BIOS** (Basic Input/Output System)
- > **UEFI** (Unified Extensible Firmware Interface)

Les ordinateurs récents utilisent UEFI par défaut, mais on peut les configurer en mode BIOS (legacy)

Pré-amorçage



La première étape du pré-amorçage est le **POST** (Power On Self Test). Elle sert à tester le matériel et la mémoire, et identifier d'éventuels problèmes.

```
Award Modular BIOS v6.00PG, An Energy Star Ally
Copyright (C) 1984-2007, Award Software, Inc.

Intel X38 BIOS for X38-DQ6 F6b

Main Processor : Intel(R) Core(TM)2 Extreme CPU X9770 @ 3.20GHz (400x8)
<CPUID:0676 Patch ID:0606>
Memory Testing : 2096064K OK

Memory Runs at Dual Channel Interleaved
IDE Channel 1 Master : WDC WD3200AAJS-00RYA0 12.01B01

Detecting IDE drives ...

<DEL>:BIOS Setup <F9>:XpressRecovery2 <F12>:Boot Menu <End>:Qflash
10/30/2007-X38-ICH9-6A790G0QC-00
```

Phoenix Technologies, LTD System Configurations									
CPU Type	:	AMD Athlon(tm) XP	Base Memory	:	640K				
CPU ID	:	0681	Extended Memory	:	1047552K				
CPU Clock	:	2000MHz	L1 Cache Size	:	128K				
			L2 Cache Size	:	256K				
Diskette Drive A	:	1.44M, 3.5 in.	Display Type	:	EGA/UGA				
Pri. Master Disk	:	LBA,ATA 100,40822MB	Serial Port(s)	:	3F8 2F8				
Pri. Slave Disk	:	LBA,ATA 100,40062MB	Parallel Port(s)	:	378				
Pri. Master Disk	:	DVD,ATA 33	DDR DIMM at Rows	:	2 3 4 5				
Sec. Slave Disk	:	CHS,PIO 4, 512MB							
PCI device listing ...									
Bus No.	Device No.	Func No.	Vendor/Device	Class	Device Class	IRQ			
0	2	0	10DE 0067	0C03	USB 1.0/1.1 OHCI Controller	10			
0	2	1	10DE 0067	0C03	USB 1.0/1.1 OHCI Controller	11			
0	2	2	10DE 0068	0C03	USB 2.0 EHCI Controller	5			
0	9	0	10DE 0065	0101	IDE Controller	14			
0	13	0	10DE 006E	0C00	Serial Bus Controller	10			
1	8	0	1106 3043	0200	Network Controller	11			
1	9	0	1102 0002	0401	Multimedia Device	11			



Ensuite, le *firmware* identifie l'information d'amorçage:

BIOS: Lit le MBR (Master Boot Record) du disque dur et transfère le contrôle vers la partition active

UEFI: Lit l'information contenue dans la puce mémoire (NVRAM ou CMOS) qui la dirige vers la partition active du disque GPT



La partition qui contient le système d'exploitation a été trouvée, et le contrôle est passé à Windows Boot Manager

Le Boot Manager lit les informations de démarrage de la partition active se trouvant dans la BCD (Boot Configuration Database)

Si plusieurs systèmes d'exploitation sont installés sur la même machine, on peut donner un choix. On appelle ça le « dual-boot », ou « multi-boot ».

Amorçage



La configuration du Boot Manager de Windows peut être obtenue grâce à l'utilitaire BCDEDIT.

Cet utilitaire peut aussi être utilisé pour modifier les options.

```
Administrateur : Windows PowerShell
PS C:\Windows\system32> .\bcdedit.exe

Gestionnaire de démarrage Windows
-----
identificateur      {bootmgr}
device              partition=\Device\HarddiskVolume2
path                \EFI\Microsoft\Boot\bootmgfw.efi
description          Windows Boot Manager
locale              fr-FR
inherit              {globalsettings}
default              {current}
resumeobject         {03a4f851-c923-11e9-85bc-abf45dcd6302}
displayorder         {current}
toolsdisplayorder    {memdiag}
timeout              30

Chargeur de démarrage Windows
-----
identificateur      {current}
device              partition=C:
path                \Windows\system32\winload.efi
description          Windows 10
locale              fr-FR
inherit              {bootloadersettings}
recoverysequence     {03a4f853-c923-11e9-85bc-abf45dcd6302}
displaymessageoverride Recovery
recoveryenabled       Yes
isolatedcontext       Yes
allowedinmemorysettings 0x15000075
osdevice             partition=C:
systemroot           \Windows
resumeobject         {03a4f851-c923-11e9-85bc-abf45dcd6302}
nx                   OptIn
bootmenupolicy        Standard
PS C:\Windows\system32>
```




Chargement du noyau

Le Boot Manager exécute ensuite le **Boot Loader**

- > **BIOS**: C:\Windows\system32\winload.exe
- > **UEFI**: C:\Windows\system32\winload.efi

Le Boot Loader démarre le **noyau** (kernel), puis:

- > Les **périphériques** sont énumérés, les **pilotes** sont chargés
- > Le gestionnaire de session **SMSS** est créé
- > Les **sous-systèmes** sont exécutés (CSRSS, LSASS, etc.)
- > Les **services** sont lancés
- > **WinLogon** affiche l'écran de bienvenue (logon)



Ouverture de session

Lorsqu'un utilisateur démarre une session, WinLogon:

Procède à son **authentification** (via LSASS)

Lance **UserInit.exe**

- > **Crée le profil** utilisateur s'il n'existe pas (à partir de C:\Users\Default)
- > Charge le **profil de l'utilisateur** (C:\Users\%USERNAME%\)
- > Charge la **ruche de registre de l'utilisateur** (HKCU ← NTUSER.DAT)
- > Lance l'interface graphique : C:\Windows\system32\explorer.exe

Explorer.exe initialise le bureau, le menu Démarrer, la barre de tâches et les tâches de démarrage (Run, RunOnce, Startup...)



Dépannage Windows





Lorsque l'ordinateur ne démarre pas, on peut avoir une idée à quelle étape du démarrage l'erreur se produit.

Pré-amorçage:

- > Écran noir qui parle de périphériques (*boot device*)

Amorçage:

- > Écran d'erreur qui réfère à Windows ou au Boot Manager.
- > On vous propose des options de récupération

Noyau:

- > Écran bleu (BSOD) avec une baboune :(et un code QR



Lorsque le système est incapable de démarrer après la phase d'amorçage, on peut tenter de lancer le mode sans échec.

À l'échec de trois tentatives de démarrage successives, Windows charge l'environnement de récupération: WinRE.

WinRE offre diverses options de réparation de Windows

Entrer dans WinRE



Automatique après trois échecs

À partir des paramètres de Windows:

- > Mise à jour et sécurité,
- > Récupération,
- > Démarrage avancé,
- > Redémarrer maintenant.

À partir de l'écran de bienvenue:

- > Shift + Redémarrer

Démarrage avancé

Démarrez à partir d'un périphérique ou d'un disque (par exemple, un lecteur USB ou un DVD), changez les paramètres de microprogramme de votre PC, changez les paramètres de démarrage de Windows ou restaurez Windows à partir d'une image système. Votre PC va être redémarré.

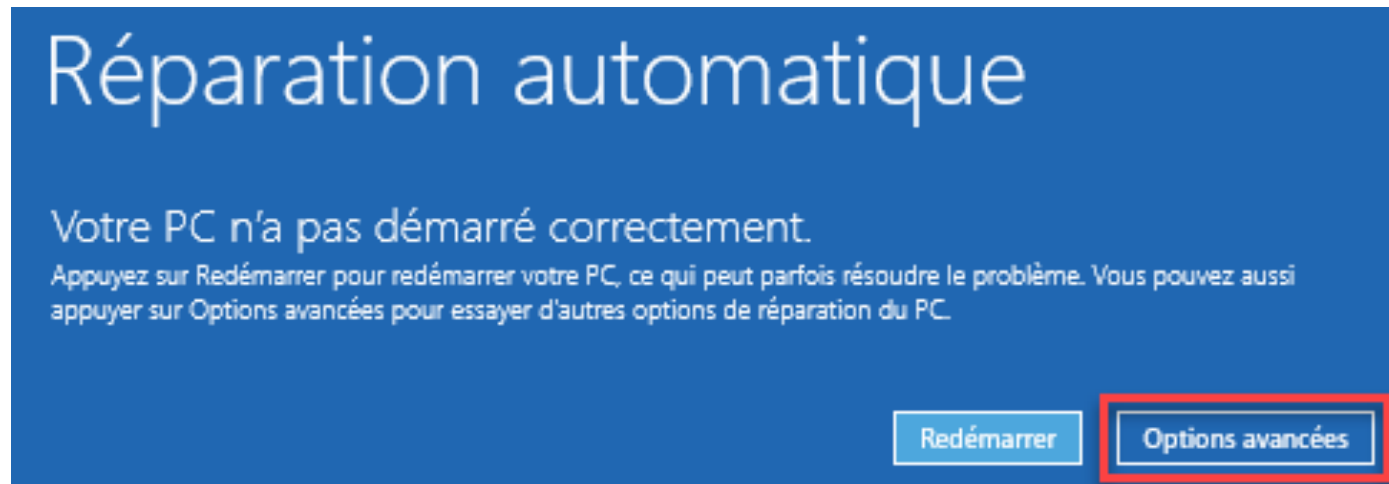
Redémarrer maintenant



Démarrage de WinRE en cas d'échec



Lorsque WinRE démarre automatiquement, ce message est affiché. Vous pouvez accéder aux outils de récupération en choisissant les options avancées.

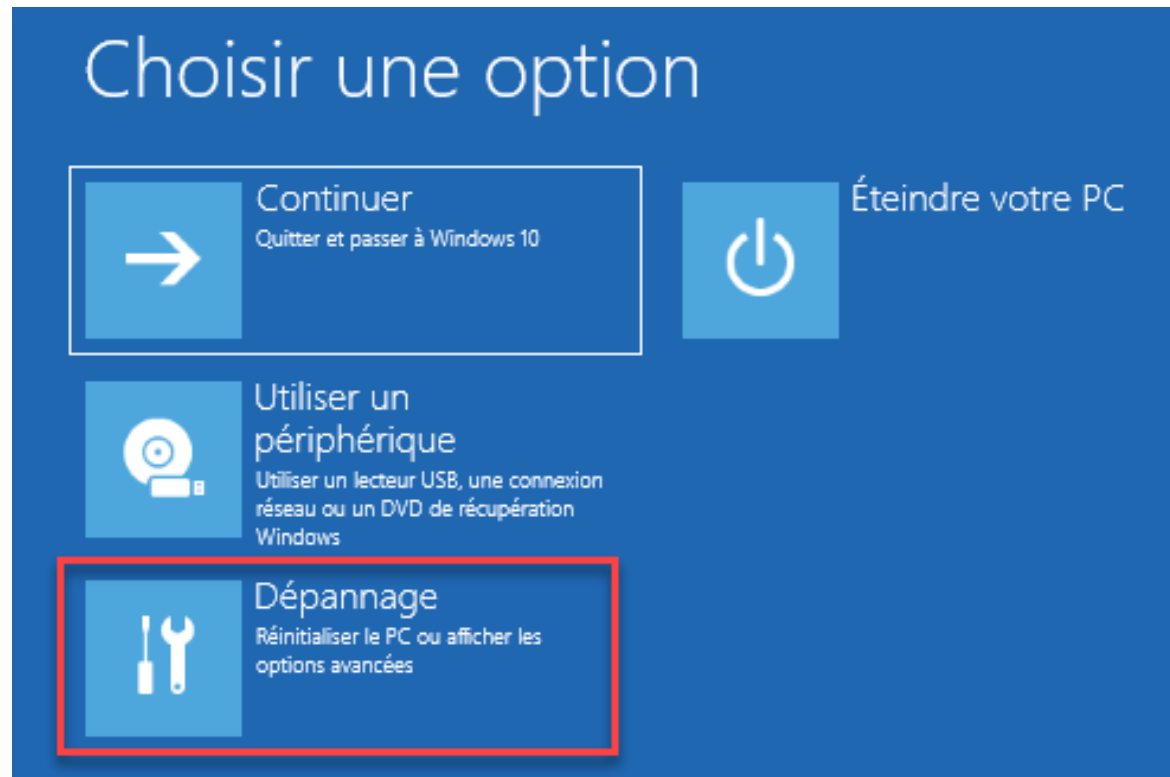


Accès aux outils de dépannage



L'option Dépannage vous offre des outils

Vous pouvez aussi charger médium de récupération... si on a pensé à en créer un !

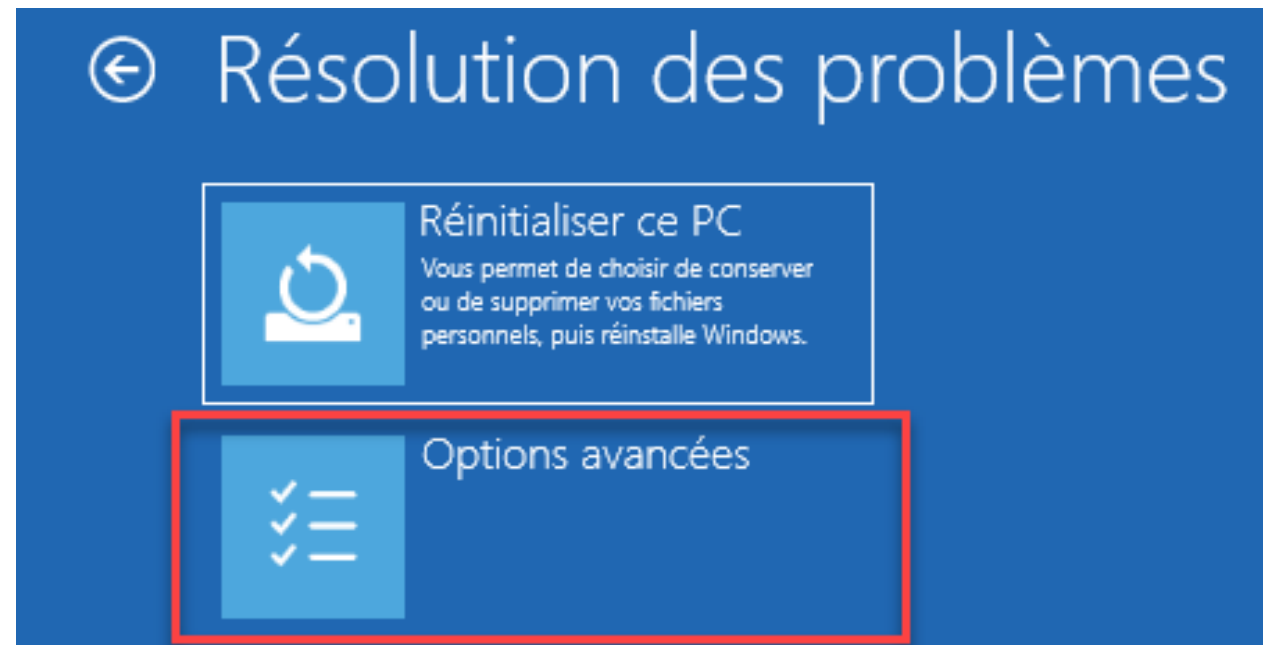


Accès aux outils de dépannage



Vous pouvez alors réinitialiser le PC (essentiellement, une réinstallation de Windows)

Ou encore accéder aux options avancées...



Accès aux outils de dépannage



Plusieurs options s'offrent à vous...



Mode sans échec



Le mode sans échec peut être utilisé lorsque Windows n'arrive pas à démarrer.

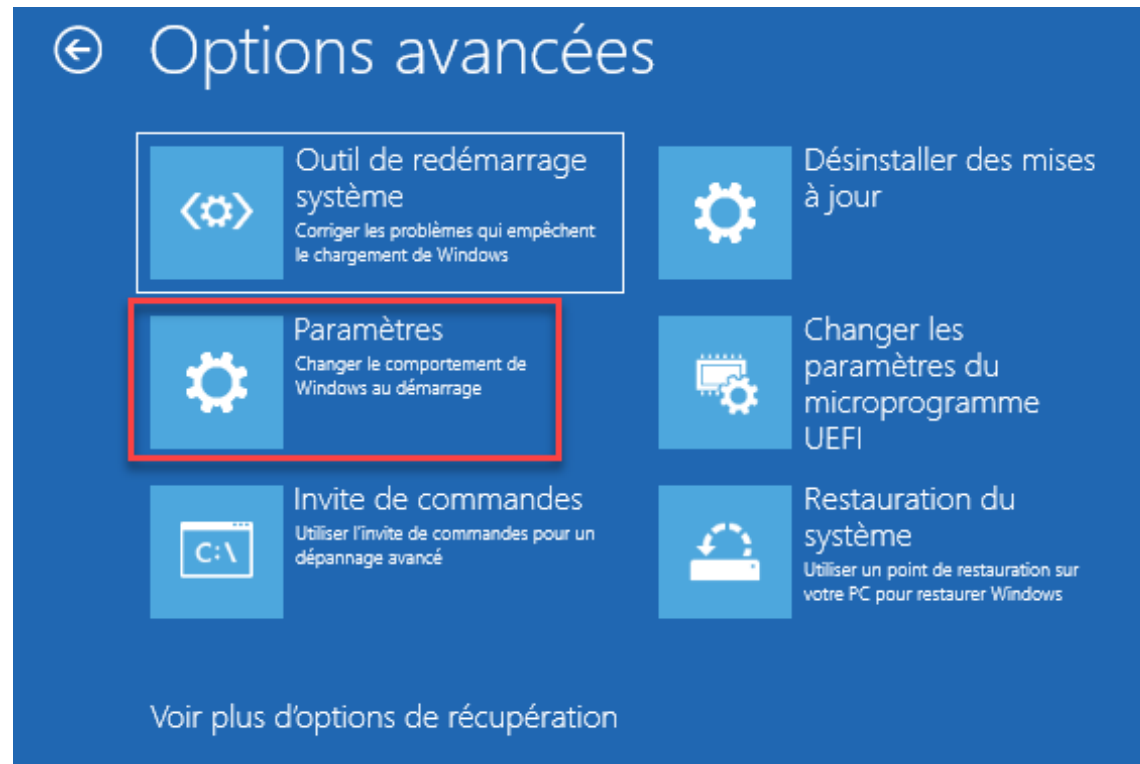
Il charge Windows avec un minimum de dépendance afin d'augmenter les chances d'avoir accès au système d'exploitation.

On peut alors tenter de trouver la source du problème dans les journaux et procéder à sa résolution.

Mode sans échec



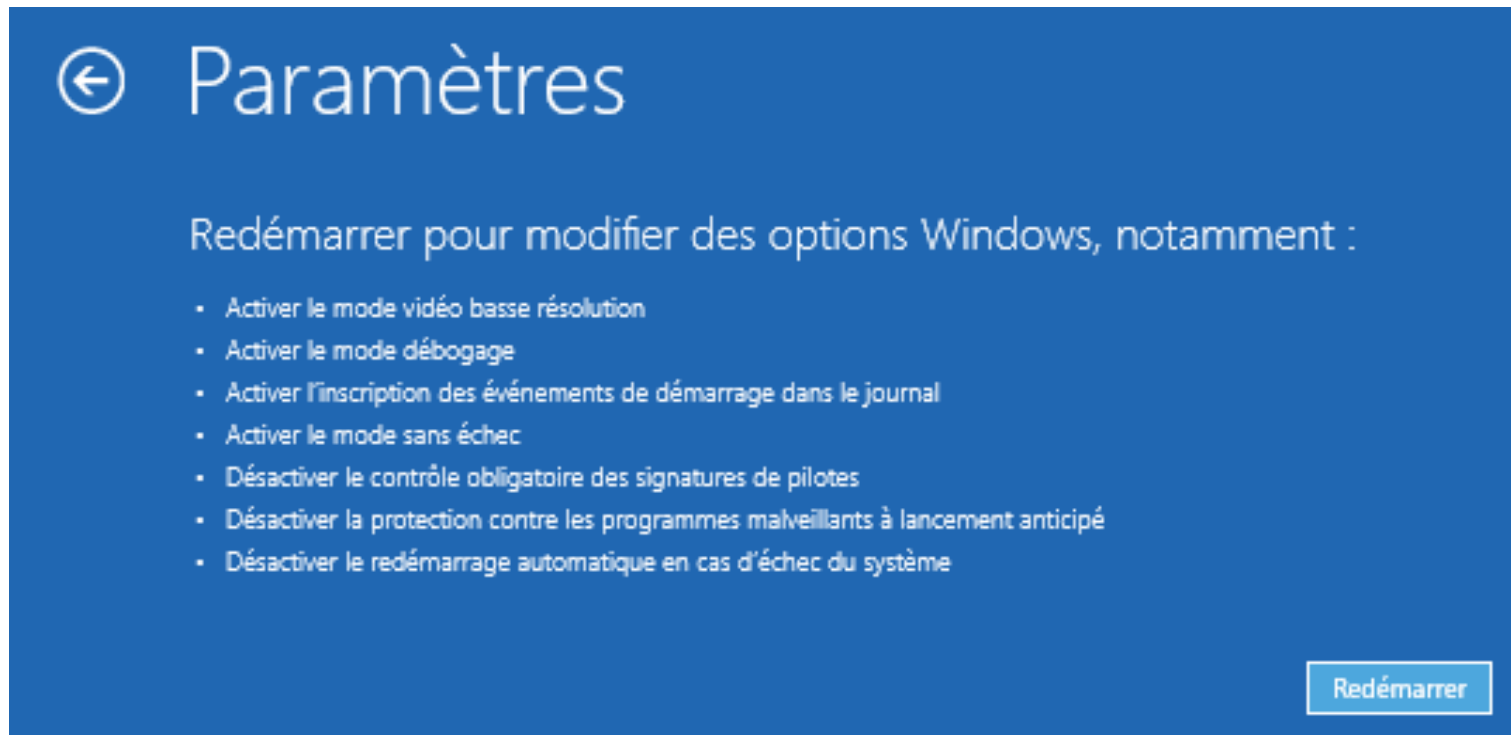
Pour activer le mode sans échec, cliquez sur Paramètres dans les options avancées de WinRE.



Mode sans échec



Puis cliquez sur Redémarrer pour accéder à un menu qui offre plusieurs modes alternatifs de démarrage...



Mode sans échec



Appuyez sur la touche correspondante au mode voulu.

- Sans réseau
- Avec réseau
- Avec invite de commande seulement (pas de GUI)
- Autres options...

Paramètres de démarrage

Appuyez sur un chiffre pour sélectionner l'une des options ci-dessous :

Utilisez les touches numériques ou les touches de fonction F1 à F9.

- 1) Activer le débogage
- 2) Activer la journalisation du démarrage
- 3) Activer la vidéo basse résolution
- 4) Activer le mode sans échec
- 5) Activer le mode sans échec avec prise en charge réseau
- 6) Activer le mode sans échec avec invite de commandes
- 7) Désactiver le contrôle obligatoire des signatures de pilotes
- 8) Désactiver la protection du logiciel anti-programme malveillant à lancement anticipé
- 9) Désactiver le redémarrage automatique en cas d'échec

Appuyez sur F10 pour obtenir d'autres options

Appuyez sur Entrée pour revenir au système d'exploitation



Applications au démarrage



Programmes au démarrage

Les services à démarrage automatique sont lancés automatiquement au démarrage du système (avant qu'un utilisateur démarre une session)

On peut aussi lancer une application au démarrage d'une session utilisateur.

- > Par le menu Démarrer
- > Par les valeurs Run et RunOnce de la base de registre
- > Par les tâches planifiées

Menu Démarrer



Le contenu du menu Démarrer (la liste à gauche, pas les tuiles) est la superposition de deux structures de répertoires:

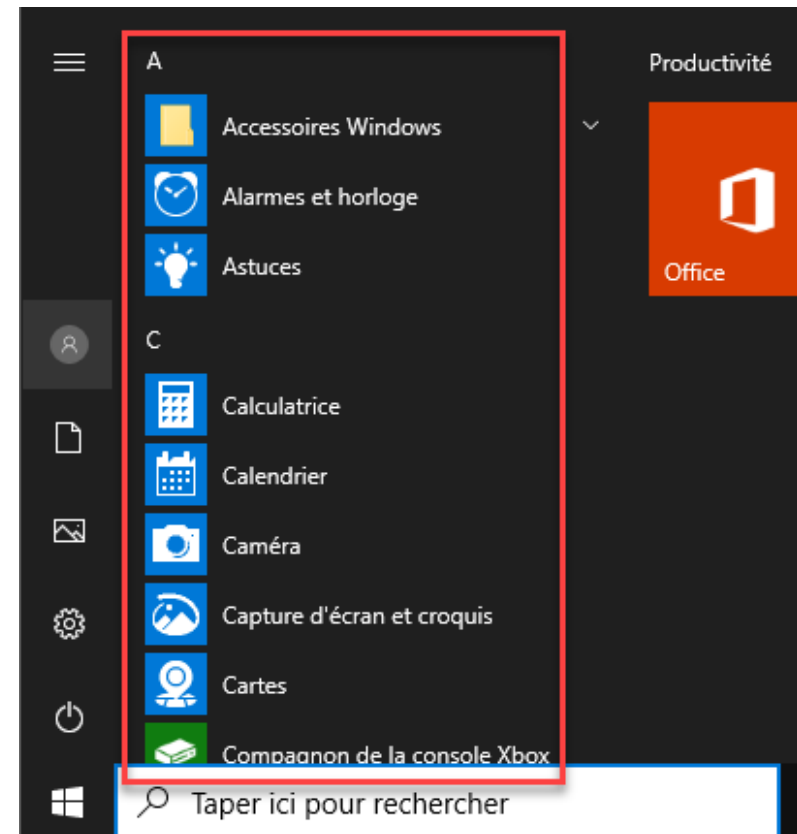
Pour chaque utilisateur:

```
C:\Users\%USERNAME%\
AppData\Roaming\Microsoft\
Windows\Start Menu\Programs
```

Pour tous les utilisateurs:

```
C:\ProgramData\Microsoft\
Windows\Start Menu\Programs
```

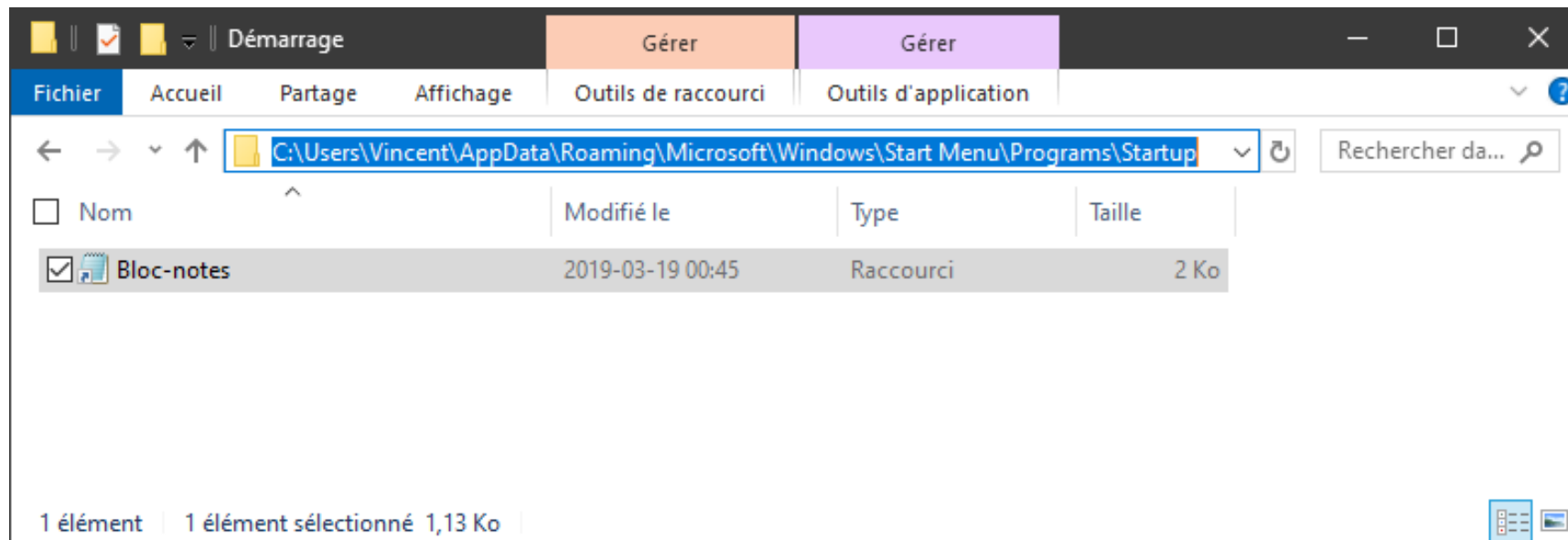
Il contient des raccourcis qui encapsulent une ligne de commande.



Menu Démarrer



Dans ces deux structures, tous les raccourcis qui se trouvent dans le répertoire Programs\Startup\ seront lancés automatiquement au démarrage de la session.





On ouvre la base de registre avec l'outil Regedit.exe

Dans la base de registre, on voit une arborescence avec plusieurs « dossiers » racine:

- > **HKEY_LOCAL_MACHINE**, ou **HKLM**, spécifiques au système. Modifier son contenu exige des droits d'administration.
- > **HKEY_CURRENT_USER**, ou **HKCU**, propres à l'utilisateur courant. L'utilisateur a le droit de modifier son contenu sans droit d'administration.
- > **HKEY_USERS**, ou **HKU**, rassemble les HKCU de chaque utilisateur présentement loggé sur le système.



Les clés qui contiennent les commandes à lancer au démarrage de session sont :

Pour tous les utilisateurs :

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Pour un utilisateur en particulier :

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

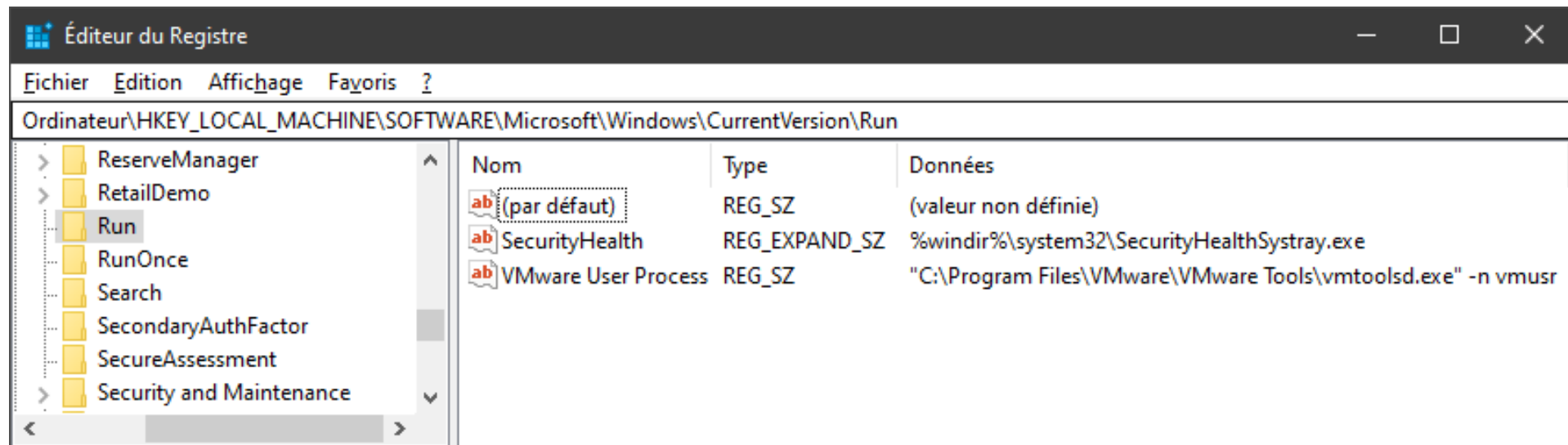
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Base de registre



Toutes les valeurs de la clé Run contiennent une ligne de commande qui sera lancée chaque fois que la session démarre (HKLM : tous les utilisateurs).

Les valeurs de la clé RunOnce ne sont lancées qu'une seule fois.

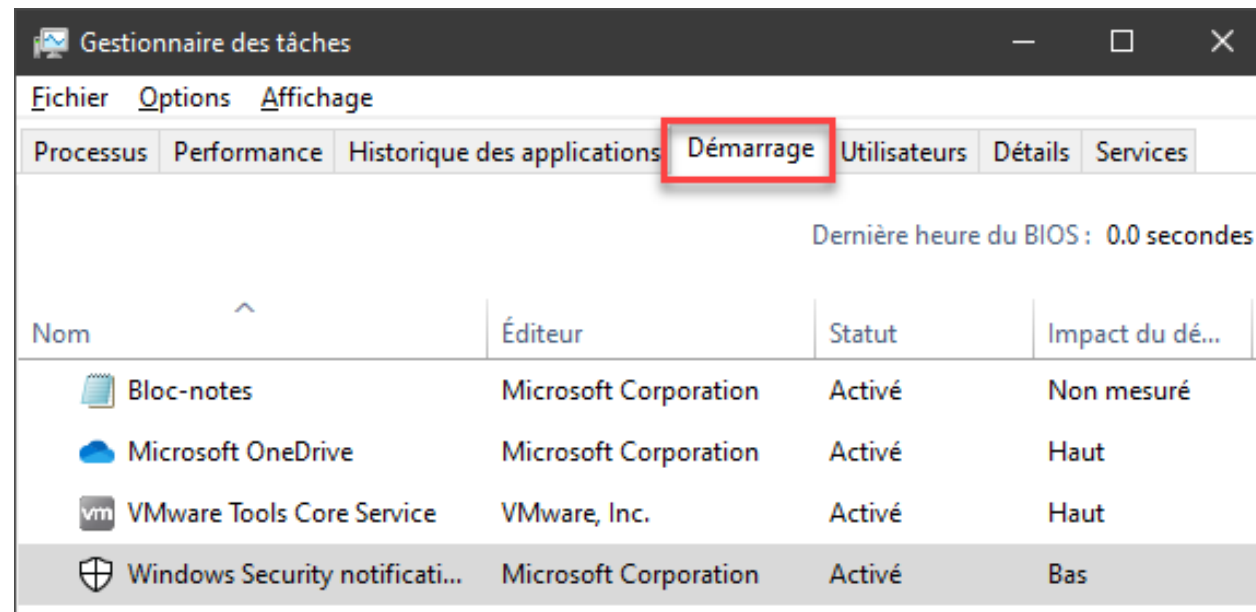


Programmes au démarrage



Sous Windows 10, les tâches au démarrage sont affichées dans le gestionnaire de tâches.

Dans les versions plus anciennes, on peut les voir en lançant l'outil msconfig.exe.

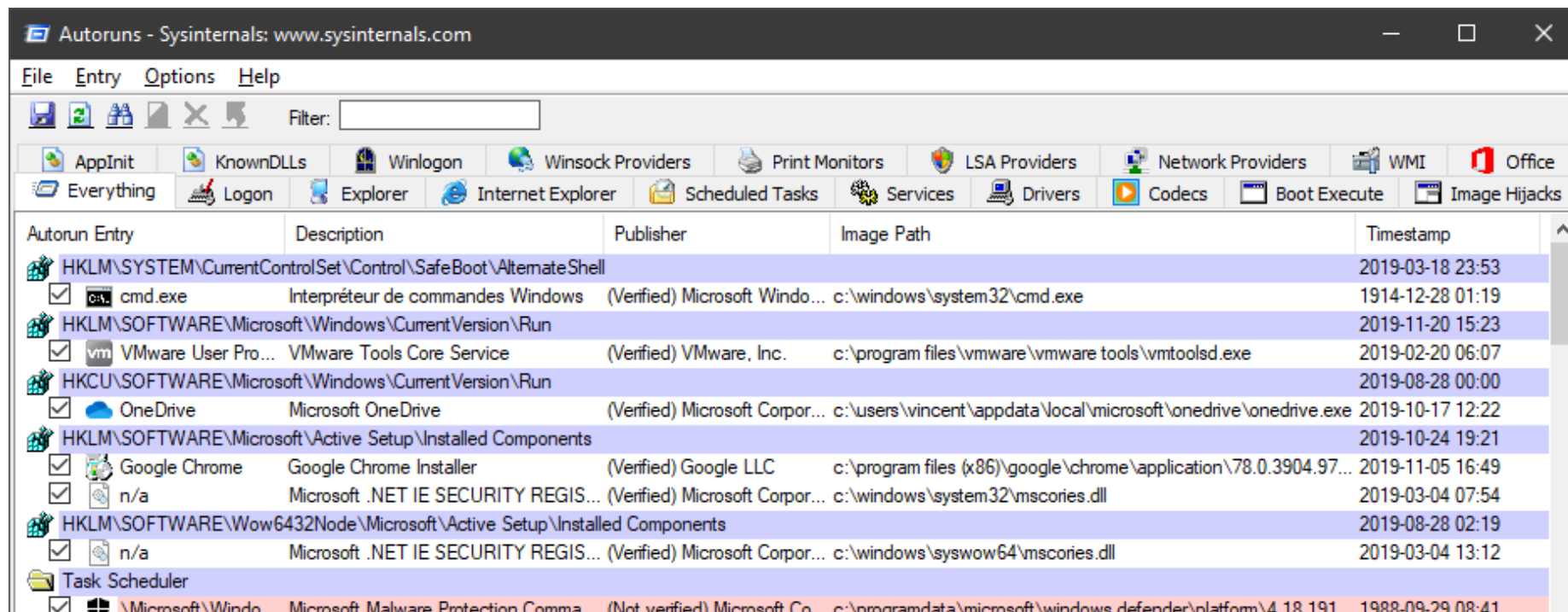


Programmes au démarrage



En vérité, il y a beaucoup plus que ça! Pour tout voir, vous pouvez télécharger l'outil AUTORUNS.

<https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>



The screenshot shows the Autoruns application window with the title bar 'Autoruns - Sysinternals: www.sysinternals.com'. The menu bar includes 'File', 'Entry', 'Options', and 'Help'. The toolbar contains icons for various system components. The main pane displays a list of startup programs with columns for 'Autorun Entry', 'Description', 'Publisher', 'Image Path', and 'Timestamp'. The list includes entries for 'cmd.exe', 'VMware User Pro...', 'OneDrive', 'Google Chrome', and 'Microsoft .NET IE SECURITY REGIS...'. The 'Task Scheduler' section is also visible at the bottom.

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2019-03-18 23:53
<input checked="" type="checkbox"/> cmd.exe	Interpréteur de commandes Windows	(Verified) Microsoft Windo...	c:\windows\system32\cmd.exe	1914-12-28 01:19
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2019-11-20 15:23
<input checked="" type="checkbox"/> VMware User Pro...	VMware Tools Core Service	(Verified) VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	2019-02-20 06:07
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2019-08-28 00:00
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	(Verified) Microsoft Corpor...	c:\users\vincent\appdata\local\microsoft\onedrive\onedrive.exe	2019-10-17 12:22
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2019-10-24 19:21
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	(Verified) Google LLC	c:\program files (x86)\google\chrome\application\78.0.3904.97...	2019-11-05 16:49
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corpor...	c:\windows\system32\mscories.dll	2019-03-04 07:54
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				2019-08-28 02:19
<input checked="" type="checkbox"/> n/a	Microsoft .NET IE SECURITY REGIS...	(Verified) Microsoft Corpor...	c:\windows\syswow64\mscories.dll	2019-03-04 13:12
Task Scheduler				
<input checked="" type="checkbox"/> \Microsoft\Windo	Microsoft Malware Protection Comma	(Not verified) Microsoft Co	c:\programdata\microsoft\windows defender\platform\4.18.191	1988-09-29 08:41