



Les processus Windows

Gestion des processus sous Windows

Automne 2022

Séance 10A



Contenu

- ✓ Différence entre un fichier exécutable et un processus (rappel)
- ✓ Qu'est-ce qu'un processus? (rappel)
- ✓ Les processus sous Windows
 - ✓ Le gestionnaire de tâches sous Windows
 - ✓ Visualiser l'utilisation des ressources
 - ✓ Détails / Démarrage des processus
 - ✓ Multiples instances d'un programme
 - ✓ Gestionnaire de tâches : privilèges élevés (UAC) et ligne de commandes
 - ✓ Créer un processus
 - ✓ Lorsqu'on ferme une session...
 - ✓ Ligne de commande
 - ✓ Processus spéciaux
 - ✓ Outil intéressant



Programmes exécutables (rappel)

Certains fichiers sont dits **exécutables**, car ils contiennent des **programmes**. Sous Windows, par exemple, ils ont souvent l'extension .exe et plus rarement .com lorsqu'ils sont disponibles à l'utilisateur.

Les fichiers exécutables contiennent des **instructions** pour le processeur, peu lisibles pour les humains.

The screenshot shows a Notepad window titled "EXE.exe - Notepad". The window displays the raw binary code of an executable file. The code includes various memory addresses, assembly-like instructions, and data segments. A prominent string of text is visible in the upper right area: "Í! , „LÍ!This program must be run u ^". The Notepad interface includes a menu bar with File, Edit, Format, View, and Help, and a status bar at the bottom showing "Ln 1, Col 1", "100%", "Windows (CRLF)", and "ANSI".



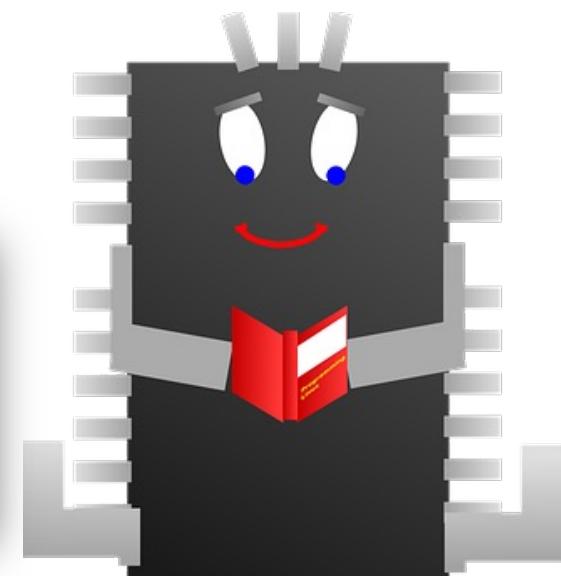
Programmes exécutables (rappel)

Lorsqu'un programme (par exemple, fait en C++) est compilé, il devient un ensemble de valeurs binaires parfaitement compréhensibles par la machine. On appelle cela le **langage machine** ou **programme exécutable** tout simplement.

Le langage machine est en fait un ensemble d'instructions que le processeur peut directement exécuter.

Certains éditeurs de fichiers peuvent améliorer la lisibilité du code binaire...

0093FFF0	7D 08 57 8B CE 0F B7 55 FE 8B C3 E8 E0 7C C3 FF	}.W<Î..-Up<Ãèà Ãý
00940000	80 BB 29 03 00 00 00 74 39 8B CF 8B D6 8B C3 E8	€»)....t9<Î<Ö<Ãè
00940010	90 02 00 00 8B F0 0F B6 83 28 03 00 00 84 C0 75<δ.¶f(....,Àu
00940020	0B 8B D6 8B C3 E8 6E 01 00 00 EB 0D 3C 01 75 09	. <x>Ö<Ãèn...ë.<.u.</x>
00940030	8B D6 8B C3 E8 D3 00 00 00 8B D6 8B C3 E8 22 02	<Ö<ÃèÓ...<Ö<Ãè".
00940040	00 00 5F 5E 5B 59 5D C2 04 00 8B C0 55 8B EC 51	..._^[Y]Â..<ÀU<iQ
00940050	3 56 D8 C 5 F B 45 08 F0	...T-W d F P<E.P



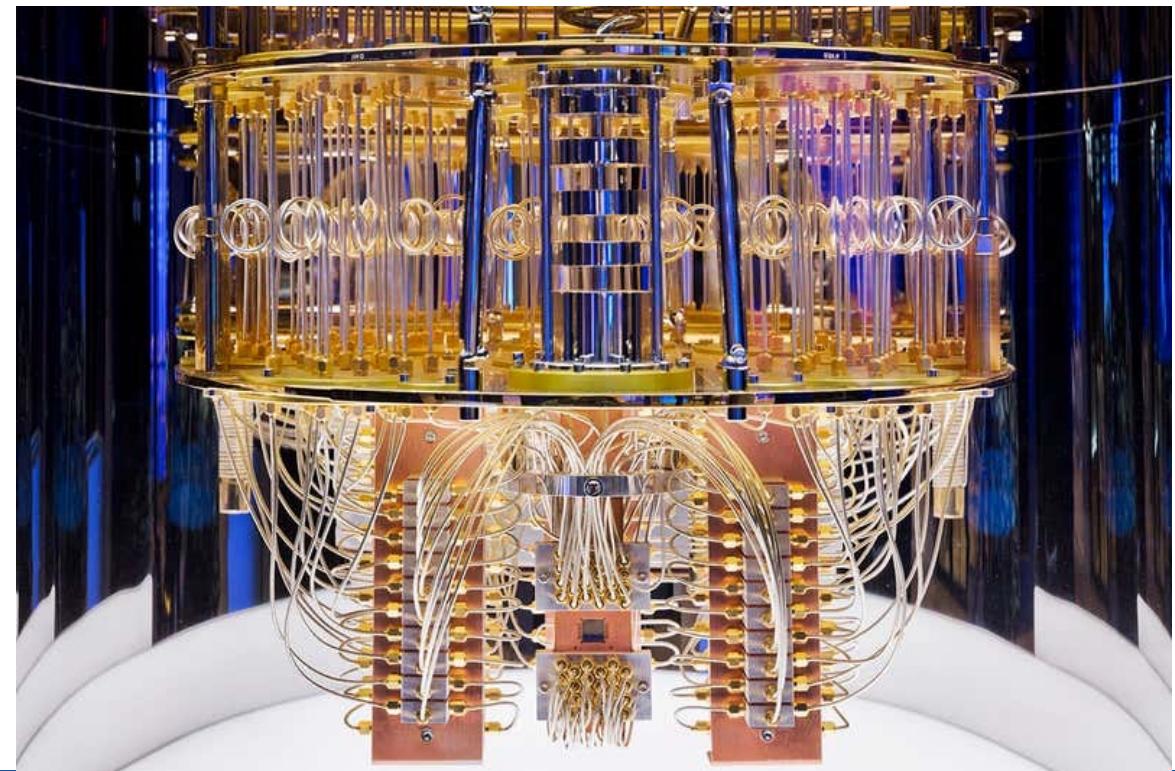
Systèmes numériques (rappel)

Le langage machine est en binaire car basé sur un signal électrique : le courant passe (1) ou ne passe pas (0). L'humain utilise le système décimal en base 10 (0-9), l'ordinateur utilise le binaire en base 2 (0-1) et l'hexadécimal en base 16 (0-9, A-F).

L'ordinateur quantique promet une infinité de valeurs car basé sur toutes les probabilités entre 0 et 1 !

C'est un domaine de recherche de pointe très actif actuellement car les possibilités d'un tel ordinateur sont prodigieuses...

...ce sujet dépasse cependant les objectifs de ce cours!





Programme exécutable vs. processus (rappel)

Le programme exécutable n'est qu'un ensemble d'instructions contenues dans un **fichier**. Les instructions qui s'y trouvent n'ont aucun effet; c'est un fichier comme un autre.

Pour que le processeur puisse exécuter ces instructions, le programme doit être chargé dans la **mémoire vive**.

Quand l'utilisateur exécute ce fichier, un **processus** est créé par le système d'exploitation (Windows/Linux/autre), et alloue une partie des ressources du système (mémoire, temps de processeur).

L'organisation des programmes en processus est pratique pour le SE car nos besoins modernes exigent l'usage (exécution) de plusieurs applications (programmes) à la fois.



Le processus (rappel)

Le processus est un conteneur qui a pour but de fournir un environnement d'exécution et des ressources système pour qu'un programme puisse être exécuté par le processeur.

Tous les programmes ont besoin d'un processus, même les composants internes du système d'exploitation.

Chaque programme est encapsulé dans son processus, ce qui permet de l'isoler des autres programmes en cours d'exécution. Le système d'exploitation gère l'accès aux ressources du système de sorte qu'un programme ne puisse pas nuire aux autres.

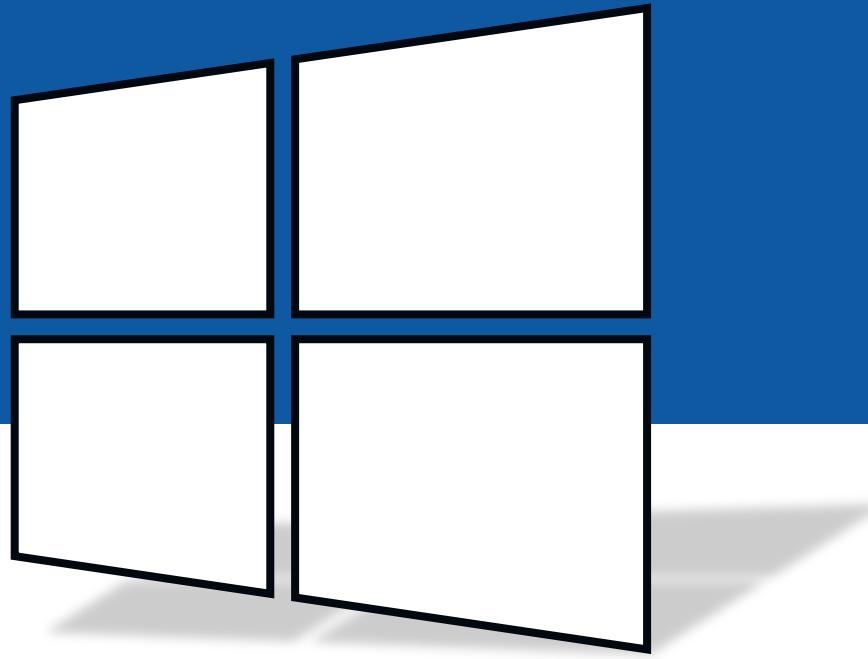


Processus et multitâche (rappel)

Les anciens ordinateurs ne pouvaient pas exécuter plusieurs programmes en même temps. Lorsqu'un programme était exécuté, il s'accaparait toutes les ressources du système. Lorsqu'il plantait, l'ordinateur au complet plantait.

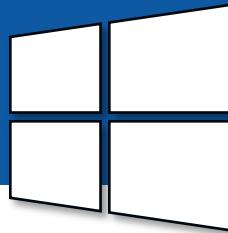
Ensuite, les systèmes d'exploitation ont introduit le multitâche coopératif. Les processus permettaient de partager des ressources entre les programmes, mais si un programme devenait hors de contrôle et consommait toutes les ressources, les autres programmes étaient inutilisables.

De nos jours, les systèmes d'exploitation offrent du multitâche préemptif. Le noyau du système est donc un chef d'orchestre qui attribue les ressources aux processus en les régulant pour les empêcher d'interférer sur les autres programmes, ce qui améliore grandement leur stabilité.



Windows

Le gestionnaire de tâches sous Windows



```
C:\Windows\system32\cmd.exe
C:\Users\Etudiant>taskmgr
```

ctrl

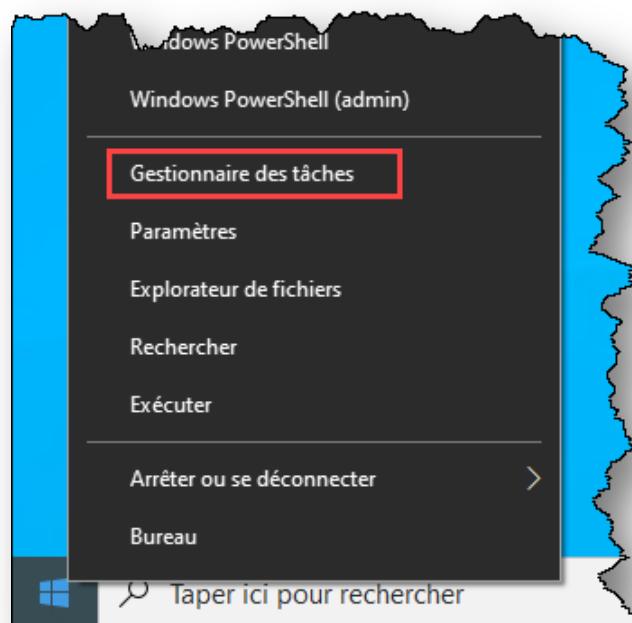
+

maj

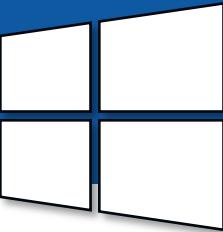
+

esc

C:\Windows\System32\taskmgr.exe



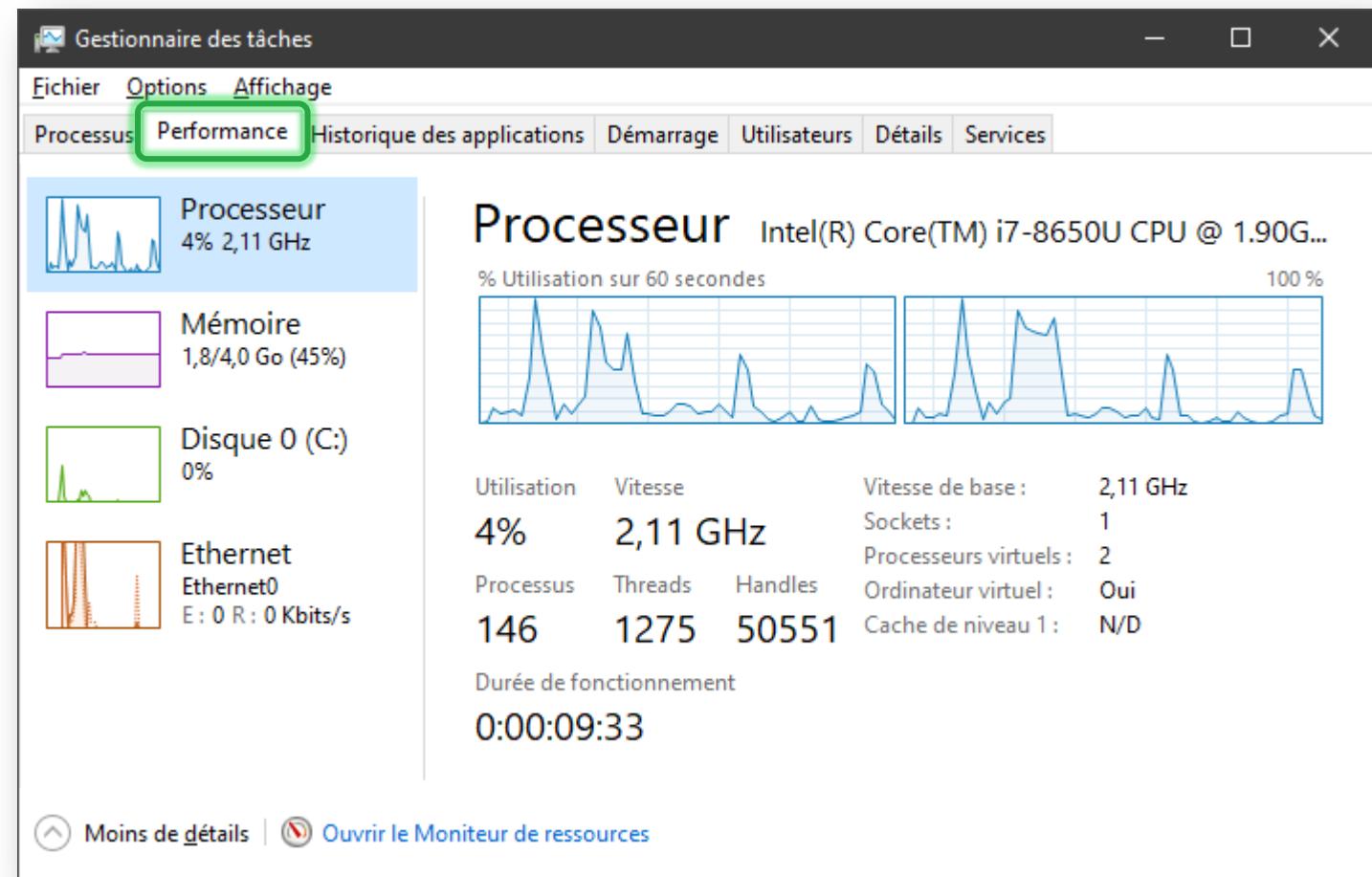
Nom	Statut	Processeur	Mémoire	Disque	Réseau	Consommati...	Tendance de c...
Applications (1)							
> Gestionnaire des tâches	1,2%	20,5 Mo	0 Mo/s	0 Mbits/s	Très faible		
Processus en arrière-plan (40)							
> Adaptateur inverse de perfor...	0%	0,9 Mo	0 Mo/s	0 Mbits/s	Très faible		
> Antimalware Service Executa...	0,5%	79,8 Mo	0 Mo/s	0 Mbits/s	Très faible		
> Application Frame Host	0%	2,7 Mo	0 Mo/s	0 Mbits/s	Très faible		
> Application sous-système sp...	0%	3,3 Mo	0 Mo/s	0 Mbits/s	Très faible		
> Chargeur CTF	0%	2,5 Mo	0 Mo/s	0 Mbits/s	Très faible		



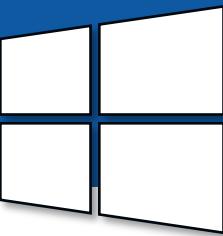
Visualiser l'utilisation des ressources

Les ressources du système sont partagées entre les différents programmes en cours d'exécution.

L'onglet performance du gestionnaire de tâches permet de visualiser l'état de leur utilisation.



Détails des processus



Nom	PID	Statut	Nom d'utilisateur	Processeur	Mémoire (pla...)	Virtual...
Processus inactif du système	0	En cours d'exécution	Système	98	8 Ko	
System	4	En cours d'exécution	Système	02	20 Ko	
Taskmgr.exe	7496	En cours d'exécution	Vincent	01	17 660 Ko	Non a...
MicrosoftEdgeCP.exe	2948	En cours d'exécution	Vincent	00	41 560 Ko	Désac...
MsMpEng.exe	3008	En cours d'exécution	Système	00	111 980 Ko	Non a...
Interruptions système	-	En cours d'exécution	Système	00	0 Ko	
lsass.exe	672	En cours d'exécution	Système	00	4 448 Ko	Non a...
explorer.exe	5848	En cours d'exécution	Vincent	00	16 044 Ko	Désac...

Nom du fichier exécutable contenant le programme (image)

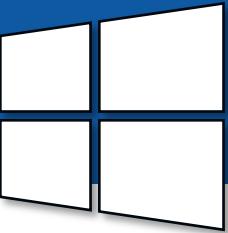
Numéro d'identification du processus (PID)

Utilisateur qui exécute le programme

Temps de CPU utilisé (en %)

Quantité de mémoire vive utilisée

Démarrage d'un processus

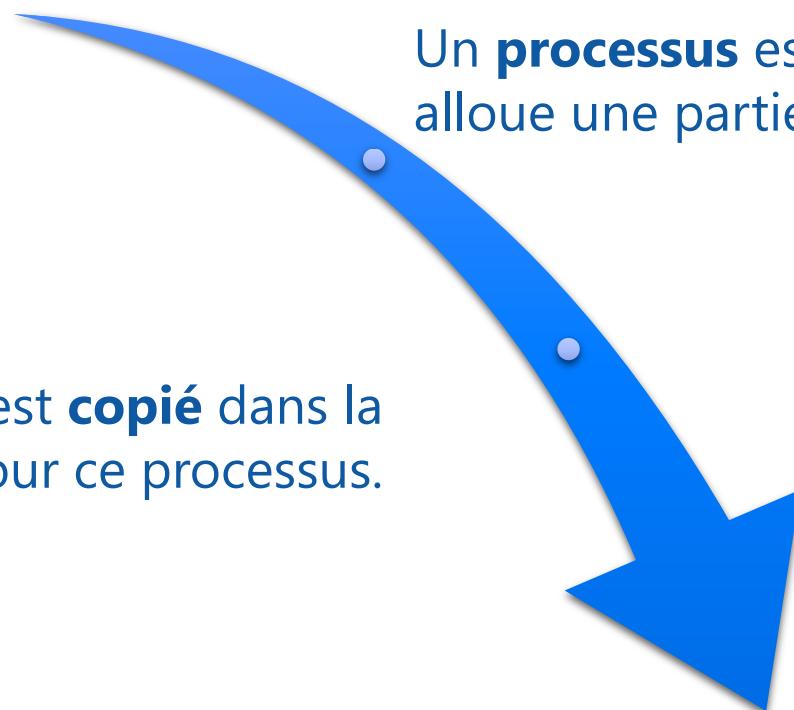


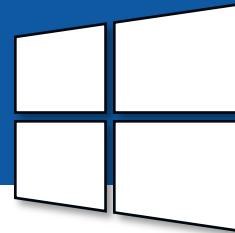
Un **fichier exécutable** est exécuté

Un **processus** est créé pour ce programme et alloue une partie de la mémoire vive

Le contenu du fichier est **copié** dans la mémoire réservée pour ce processus.

La **première instruction** du programme s'exécute.





Multiples instances d'un programme

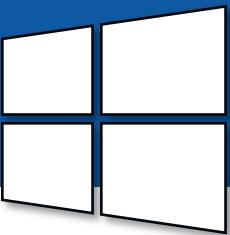
Le même fichier de programme peut être exécuté à plusieurs exemplaires. Chaque instance d'un programme se trouve alors dans un processus séparé et indépendant.

Certaines applications utilisent même plusieurs processus distincts tel Chrome pour chaque onglet, son gestionnaire de mot de passe, les modules d'extension, etc.

The screenshot illustrates the concept of multiple program instances. At the top, a web browser window is open with five tabs: Google, Facebook, Instagram, Amazon, and Omnivox. Below the browser, the Windows Task Manager is displayed, specifically the 'Gestionnaire des tâches' (Task Manager) window. The 'Processus' (Processes) tab is selected, showing a list of six entries, all of which are instances of the 'chrome.exe' process. Each entry includes details such as PID, Status, User, Processor usage, and Memory/Virtual memory usage. This visual evidence demonstrates that even though there is one browser application, it runs as multiple separate processes, each managing its own tabs and resources.

Nom	PID	Statut	Nom d'utilisateur	Processeur	Mémoire (pla...)	Virtuel...
chrome.exe	4756	En cours d'exécution	Vincent	00	6 268 Ko	Désac...
chrome.exe	7892	En cours d'exécution	Vincent	00	8 444 Ko	Désac...
chrome.exe	9400	En cours d'exécution	Vincent	00	10 912 Ko	Désac...
chrome.exe	1780	En cours d'exécution	Vincent	01	49 640 Ko	Désac...
chrome.exe	3656	En cours d'exécution	Vincent	03	31 732 Ko	Désac...
chrome.exe	10012	En cours d'exécution	Vincent	00	21 568 Ko	Désac...

Gestionnaire de tâches : privilèges élevés (UAC)



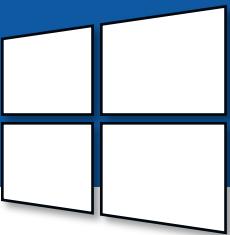
Certains processus bénéficient de privilèges élevés car ils sont exécutés en tant qu'administrateur. On peut voir quels processus possèdent ces droits supplémentaires.

The diagram illustrates the process of identifying processes with elevated privileges:

- Task Manager Initial View:** Shows the Task Manager window with the "Utilisateurs" tab selected. A red circle highlights the "Sélectionner des colonnes" button in the toolbar, and a red box highlights the "Sélectionner des colonnes" option in the context menu of the header row.
- Select Columns Dialog:** A blue arrow points from the initial Task Manager to this dialog. It lists columns that can be added to the table, with "Élevé" checked and highlighted by a yellow background.
- Final Task Manager View:** A blue arrow points from the "Select Columns" dialog to this final Task Manager window. The "Détails" tab is selected. The "Élevé" column is now visible, with the first two rows (powershell.exe processes) showing "Oui" and the third row (Procédurage actif du système) showing "Non". A red box highlights the "Élevé" column header.

Nom	PID	Statut	Nom d'utilisateur	Processeur	Élevé	Virtualisation du ...
powershell.exe	10560	En cours d'exécution	Vincent	00	Oui	Non autorisé
powershell.exe	2220	En cours d'exécution	Vincent	00	Non	Désactivé
Procédurage actif du système	0	En cours d'exécution		99		

Gestionnaire de tâches: ligne de commande

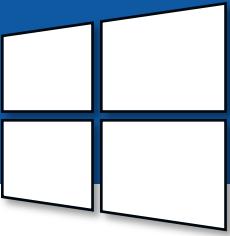


On peut voir la ligne de commande complète qui a mené à l'exécution du programme.

The diagram illustrates the process of viewing command line arguments in the Windows Task Manager:

- Initial View:** The first screenshot shows the Task Manager window with the "Processus" tab selected. A red circle highlights the "Nom" column header. A right-click context menu is open over the "MusNotifyIcon.exe" row, with the "Sélectionner des colonnes" option highlighted by a red box.
- Column Selection:** The second screenshot shows the "Sélectionner des colonnes" dialog box. It contains a list of columns with checkboxes. The "Ligne de commande" checkbox is checked and highlighted with a yellow background, indicating it has been selected.
- Final View:** The third screenshot shows the Task Manager window again, but now with the "Détails" tab selected. The "Ligne de commande" column is visible, displaying the full command line for each process. For example, the "notepad.exe" process has the command line "C:\Windows\system32\NOTEPAD.EXE" and the "OneDrive.exe" process has the command line "C:\Users\Vincent\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background.

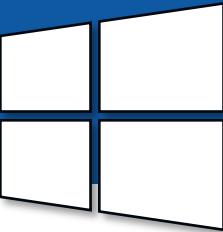
Créer un processus



Pour créer un processus, il suffit d'exécuter un fichier exécutable.

Un nouveau processus est automatiquement créé pour ce programme. Windows lui attribue alors un nouvel identifiant (PID).

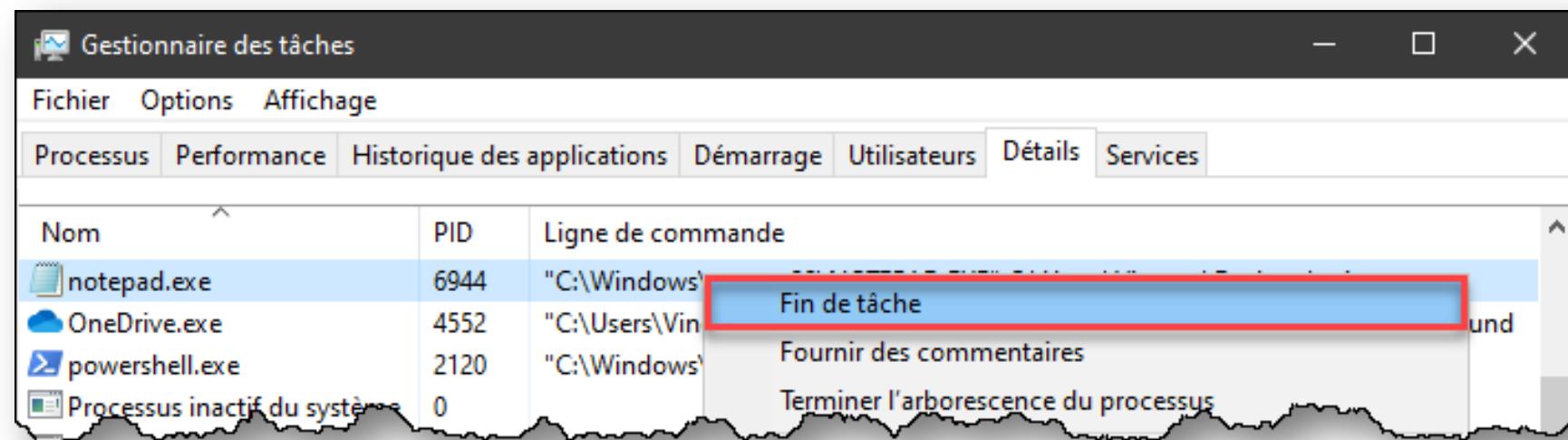
Le nouveau processus hérite du contexte de sécurité du parent. Par exemple, si on lance un fichier exécutable à partir d'une invite de commande élevée (en tant qu'admin), ce programme sera élevé lui aussi.



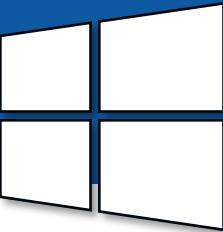
Terminer de force un processus

Il arrive qu'une application gèle et ne réponde plus aux commandes de l'utilisateur.

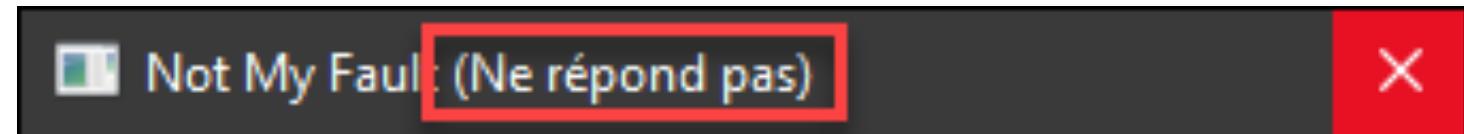
On peut alors forcer la fermeture du processus (en anglais, on dit « kill process »). C'est violent! C'est l'équivalent d'interrompre l'ordinateur par son commutateur ou en le débranchant...



Quand doit-on terminer de force un processus?



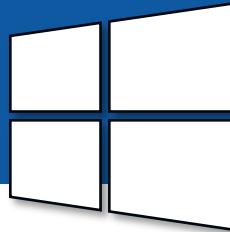
Lorsque le **programme gèle** pendant trop longtemps et cesse de répondre



Lorsque le **système devient instable**, que l'ordinateur commence à chauffer et que le ventilateur fait du bruit, et qu'un processus dans le gestionnaire des tâches prend un grand pourcentage du processeur pendant un bon moment

Lorsque vous êtes **incapable de quitter** une application (en raison d'un bug ou d'un plantage)

Terminer un processus : mise en garde



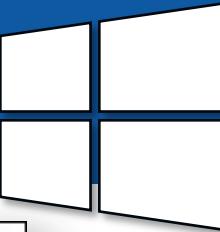
Souvent, à la fermeture d'une application, celle-ci doit exécuter des tâches afin de fermer proprement

- > Sauvegarde des configurations dans le registre
- > Fermeture des connexions établies
- > etc.

Lorsqu'on termine un processus de force, le programme n'a pas la chance de poser ces actions.

Il y a donc un risque d'affecter d'autres programmes, de causer de la corruption, etc.

N'utilisez cette technique qu'en dernier recours!



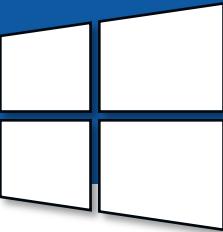
Lorsqu'on ferme une session...

Tous les processus d'un utilisateur sont automatiquement terminés lorsque celui-ci ferme sa session.

Nom	PID	Statut	Nom d'utilisateur	Pro...	Mémoire (...)	Virtua...
dllhost.exe	5700	En cours d'exécution	Etudiant	00	668 Ko	Désac...
StartMenuExperienceH...	5992	En cours d'exécution	Etudiant	00	13 584 Ko	Désac...
msdtc.exe	5316	En cours d'exécution	SERVICE RÉSEAU	00	628 Ko	Non i...
RuntimeBroker.exe	3284	En cours d'exécution	Etudiant	00	2 124 Ko	Désac...
SearchUI.exe	6232	Interrompu	Etudiant	00	0 Ko	Désac...
RuntimeBroker.exe	6384	En cours d'exécution	Etudiant	00	2 488 Ko	Désac...
ApplicationFrameHost....	6484	En cours d'exécution	Etudiant	00	4 588 Ko	Désac...
sychart.exe	7068	En cours d'exécution	Etudiant	00	1 064 Ko	Non i...

Les processus qui appartiennent à l'utilisateur SYSTÈME (ou d'autres comptes spéciaux comme « SERVICE LOCAL », « SERVICE RÉSEAU ») persistent après la fin de la session puisqu'ils appartiennent au système.

En même temps, ces processus assurent l'ouverture de session lorsque demandée par un utilisateur.



Ligne de commande (cmd)

Obtenir la liste des processus:

tasklist

```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.18362.418]
(c) 2019 Microsoft Corporation. Tous droits réservés.

C:\Users\Vincent>tasklist

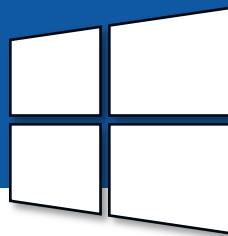
Nom de l'image          PID Nom de la session Numéro de s Utilisation
=====
System Idle Process      0 Services                  0      8 Ko
System                   4 Services                  0     144 Ko
Registry                 88 Services                0    73 544 Ko
smss.exe                 336 Services                0    1 196 Ko
csrss.exe                 420 Services                0    5 092 Ko
wininit.exe                496 Services                0    6 844 Ko
csrss.exe                 1 n/a                      0      0 Ko
```

Terminer un processus:

taskkill /im *nomduprocessus.exe*

```
C:\Windows\system32\cmd.exe
C:\Users\Vincent>taskkill /im notepad.exe
Opération réussie : un signal de fin a été envoyé au processus "notepad.exe" de PID 4344.
```

Processus spéciaux : Processus inactif du système



Ce n'est pas vraiment un processus. Il désigne les ressources inutilisées par les processus, en attente.

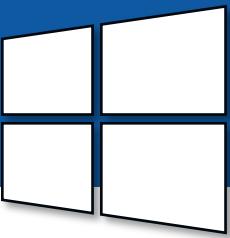
Cela facilite l'interrogation du système en ligne de commande ou en script.

Contrairement aux autres processus, un haut pourcentage de processeur est sain. Cela signifie que le système est sous-utilisé.

A screenshot of the Windows Task Manager window titled "Gestionnaire des tâches". The window has a menu bar with "Fichier", "Options", and "Affichage". Below the menu is a tab bar with "Processus", "Performance", "Historique des applications", "Démarrage", "Utilisateurs", "Détails", and "Services". The "Détails" tab is selected. A table displays process information with columns: Nom, PID, Processeur, Nom d'utilisateur, Statut, Mémoire (pla..., and Virtual... . The table shows four entries: "Processus inactif du système" (PID 0), "procexp64.exe" (PID 3776), "MsMpEng.exe" (PID 1020), and "lwp.exe" (PID 284). The "Processus inactif du système" row is highlighted in blue. The status bar at the bottom shows system performance metrics: CPU usage (0%), RAM usage (41-212 Ko), and disk usage (N/A).

Nom	PID	Processeur	Nom d'utilisateur	Statut	Mémoire (pla...	Virtual...
Processus inactif du système	0	92	Système	En cours d'exécution	8 Ko	
procexp64.exe	3776	05	Vincent	En cours d'exécution	27 808 Ko	Non a...
MsMpEng.exe	1020	02	Système	En cours d'exécution	72 832 Ko	Non a...
lwp.exe	284	01	WM-1	En cours d'exécution	41-212 Ko	N/A

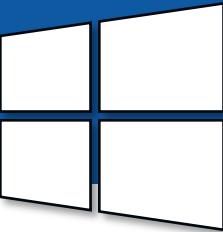
Processus spéciaux : System



Le processus System englobe les programmes de base de Windows, le cœur du système.

Ce n'est pas un vrai processus, donc impossible d'y mettre fin.

A screenshot of the Windows Task Manager window. The title bar says "Gestionnaire des tâches". The menu bar has "Fichier", "Options", and "Affichage". The tabs at the top are "Processus", "Performance", "Historique des applications", "Démarrage", "Utilisateurs", "Détails" (which is selected), and "Services". The main table has columns: Nom, PID, Processeur, Nom d'utilisateur, Statut, Mémoire (pla..., and Virtual...). There are five rows: 1. svchost.exe, PID 6280, Processeur 00, Nom d'utilisateur Vincent, Statut En cours d'exécution, Mémoire 580 Ko, Virtual... Désac... 2. svchost.exe, PID 1716, Processeur 00, Nom d'utilisateur Système, Statut En cours d'exécution, Mémoire 680 Ko, Virtual... Non a... 3. System, PID 4, Processeur 00, Nom d'utilisateur Système, Statut En cours d'exécution, Mémoire 20 Ko, Virtual... 4. SystemSettings.exe, PID 3928, Processeur 00, Nom d'utilisateur Vincent, Statut Interrompu, Mémoire 0 Ko, Virtual... Désac... 5. TabTip.exe, PID 6716, Processeur 00, Nom d'utilisateur Vincent, Statut En cours d'exécution, Mémoire 1 280 Ko, Virtual... Désac... The "System" row is highlighted with a blue selection bar.



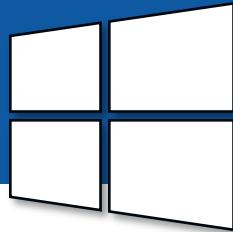
Processus spéciaux: SVCHOST

Il y a un grand nombre de processus SVCHOST.EXE

Ces processus soutiennent les services, des programmes qui roulent en arrière-plan.

Nom	PID	Processeur	Nom d'utilisateur	Statut	Mémoire (pla...)	Virtual...
svchost.exe	724	00	Système	En cours d'exécution	264 Ko	Non a...
svchost.exe	804	00	Système	En cours d'exécution	8 336 Ko	Non a...
svchost.exe	924	00	SERVICE RÉSEAU	En cours d'exécution	5 812 Ko	Non a...
svchost.exe	972	00	Système	En cours d'exécution	836 Ko	Non a...
svchost.exe	648	00	SERVICE LOCAL	En cours d'exécution	792 Ko	Non a...
svchost.exe	1028	00	SERVICE LOCAL	En cours d'exécution	376 Ko	Non a...
svchost.exe	1056	00	Système	En cours d'exécution	852 Ko	Non a...

Processus spéciaux: CSRSS, SMSS, LSASS



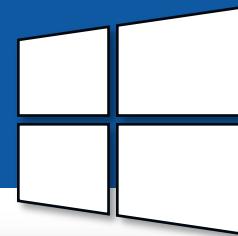
SMSS.EXE, CSRSS.EXE et LSASS.EXE sont des processus extrêmement importants pour Windows, sans lesquels rien ne pourrait fonctionner.

Ces programmes gèrent les fonctionnalités clés de Windows, telles que les environnements d'exécution, la mémoire et la sécurité.

Il ne faut jamais y mettre fin.

- > C'est dangereux...
- > Ça vous tente d'essayer? ☺

Outil intéressant : Process Explorer



Si vous voulez explorer les processus plus en détails, essayez cet outil:

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

Process	CPU	Private Bytes	Working Set	PID
explorer.exe	0.32	47 260 K	124 912 K	4960
SecurityHealthSystray.exe		1 728 K	8 296 K	7996
vmtoolsd.exe	0.11	16 148 K	25 864 K	8100
OneDrive.exe		26 744 K	56 372 K	4552
powershell.exe	0.02	62 764 K	50 588 K	2120
conhost.exe	< 0.01	4 160 K	15 364 K	2452
Taskmgr.exe	0.69	24 448 K	40 892 K	260
chrome.exe	0.01	43 988 K	78 948 K	5156
chrome.exe		1 612 K	6 048 K	5176
chrome.exe		1 924 K	8 208 K	6084
chrome.exe		35 124 K	37 300 K	7532
chrome.exe		12 636 K	22 952 K	818
chrome.exe		38 164 K	47 740 K	5688
chrome.exe		17 652 K	24 340 K	424
chrome.exe		12 420 K	16 000 K	2124
notmyfault64.exe		2 092 K	12 168 K	5088
proexp.exe		3 072 K	10 984 K	8068
proexp64.exe	4.29	32 544 K	59 372 K	3776
notepad.exe	< 0.01	3 252 K	17 192 K	2396
GoogleCrashHandler.exe		1 712 K	296 K	7644
GoogleCrashHandler64.exe		1 720 K	464 K	7652