CAMPUS DE LONGUEUIL
CÉGEP ÉDOUARD MONTPETIT

Les processus Windows

Gestion des processus sous Windows

Automne 2022

Séance 10A

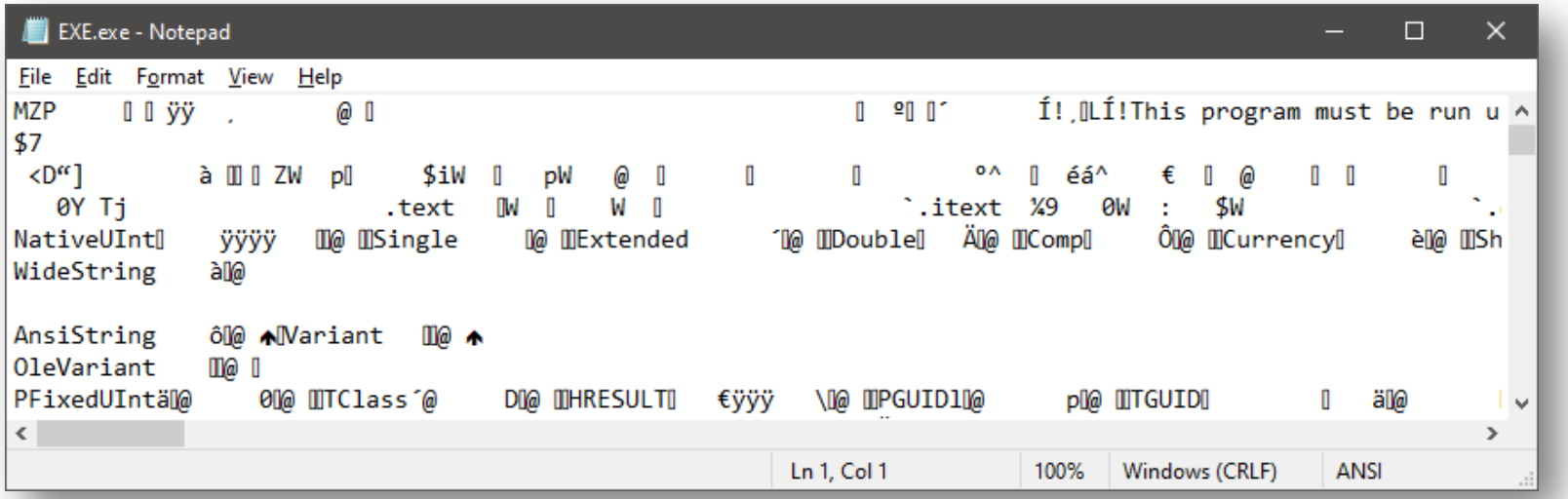
Contenu

- ✓ 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.



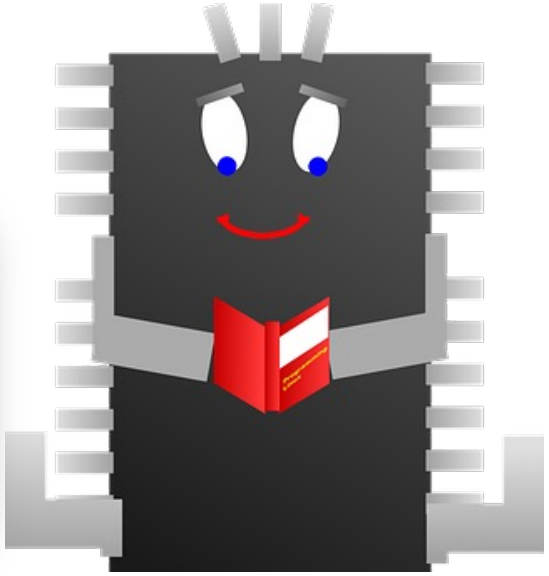
Programmes exécutables (rappel)

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.·Uþ‹Ãèà|Ãÿ
00940000   80 BB 29 03 00 00 00 74   39 8B CF 8B D6 8B C3 E8   €»)....t9‹Ï‹Ö‹Ãè
00940010   90 02 00 00 8B F0 0F B6   83 28 03 00 00 84 C0 75   ....‹ð.¶ƒ(...„Àu
00940020   0B 8B D6 8B C3 E8 6E 01   00 00 EB 0D 3C 01 75 09   .‹Ö‹Ãèn...ë.<.u.
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‹ìQ
```



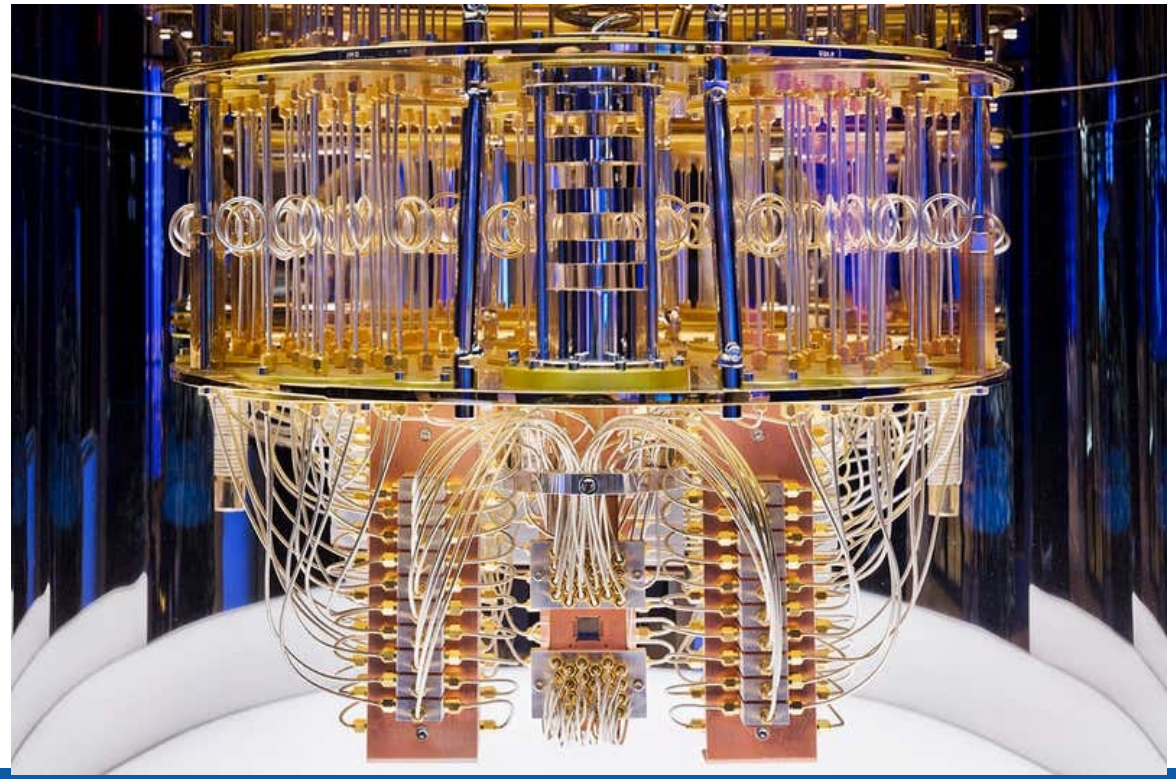
Systèmes numériques (rappel)

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.

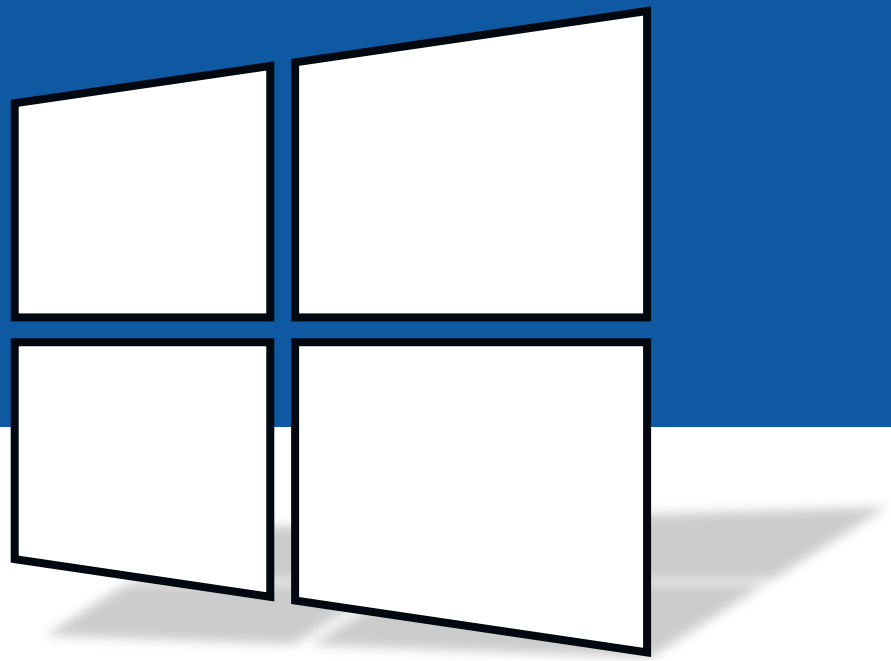
Chaque programme est encapsulé dans son processus, ce qui permet de l'isoler des autres programmes en cours d'exécution. Le système d'exploitation gère l'accès aux ressources du système de sorte qu'un programme ne puisse pas nuire aux autres.

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.

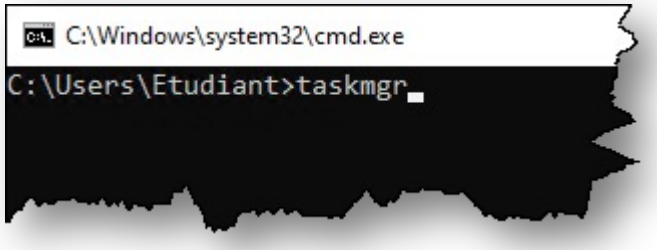
Ensuite, les systèmes d'exploitation ont introduit le multitâche coopératif. Les processus permettaient de partager des ressources entre les programmes, mais si un programme devenait hors de contrôle et consommait toutes les ressources, les autres programmes étaient inutilisables.

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.

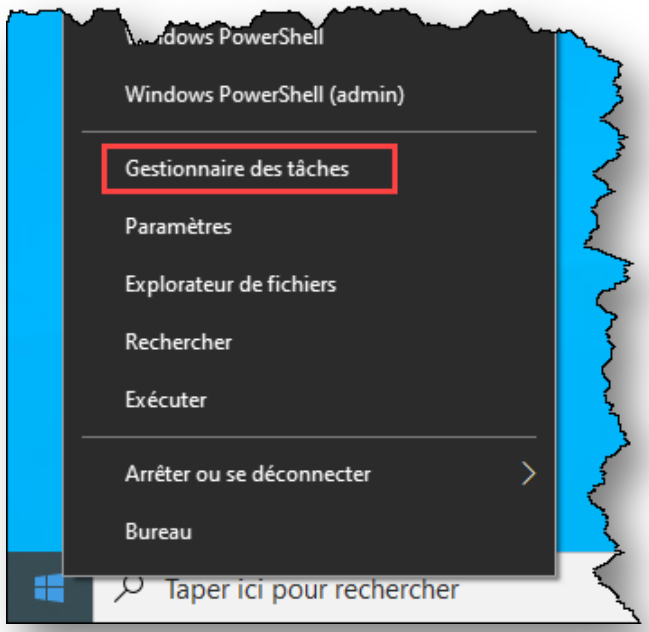


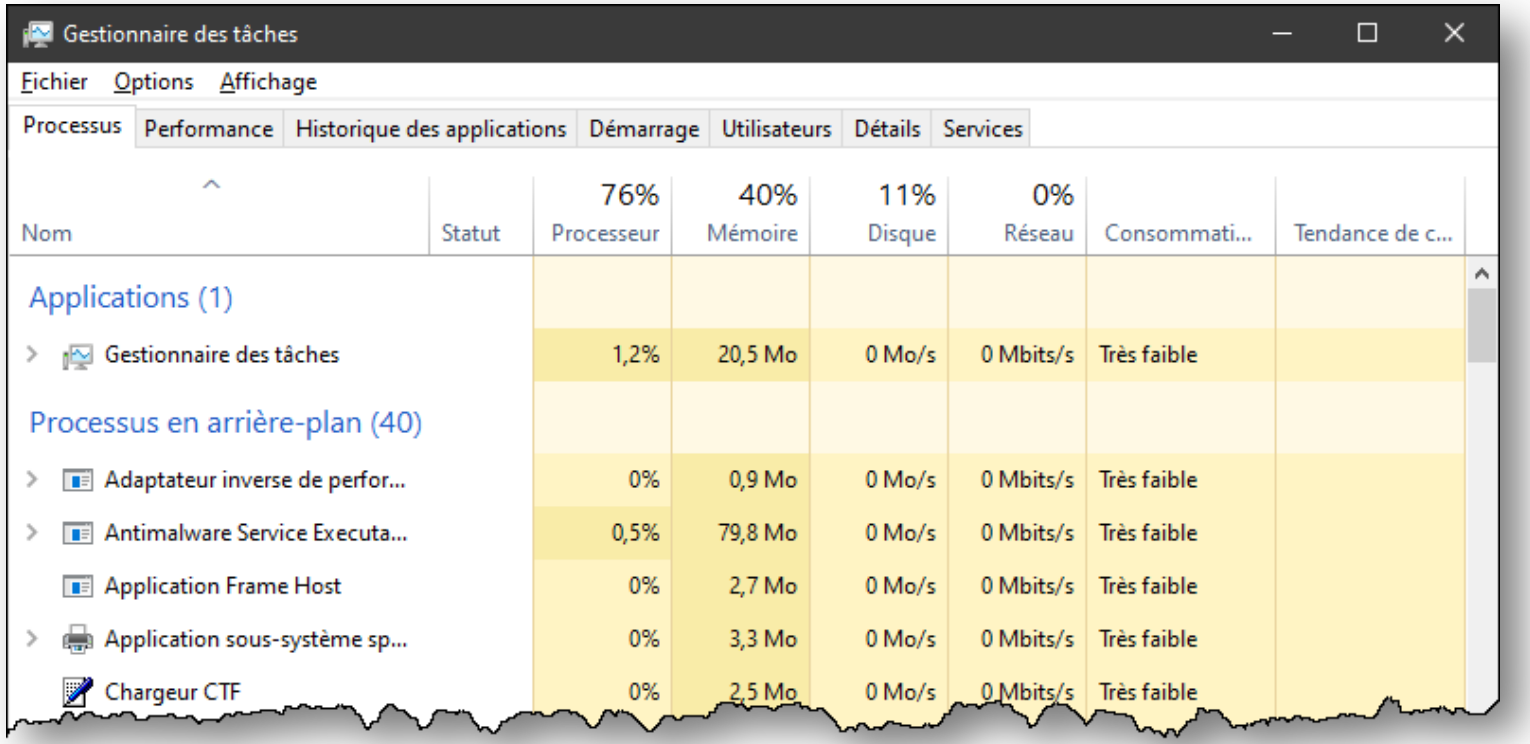
Windows

Le gestionnaire de tâches sous Windows



C:\Windows\System32**taskmgr.exe**

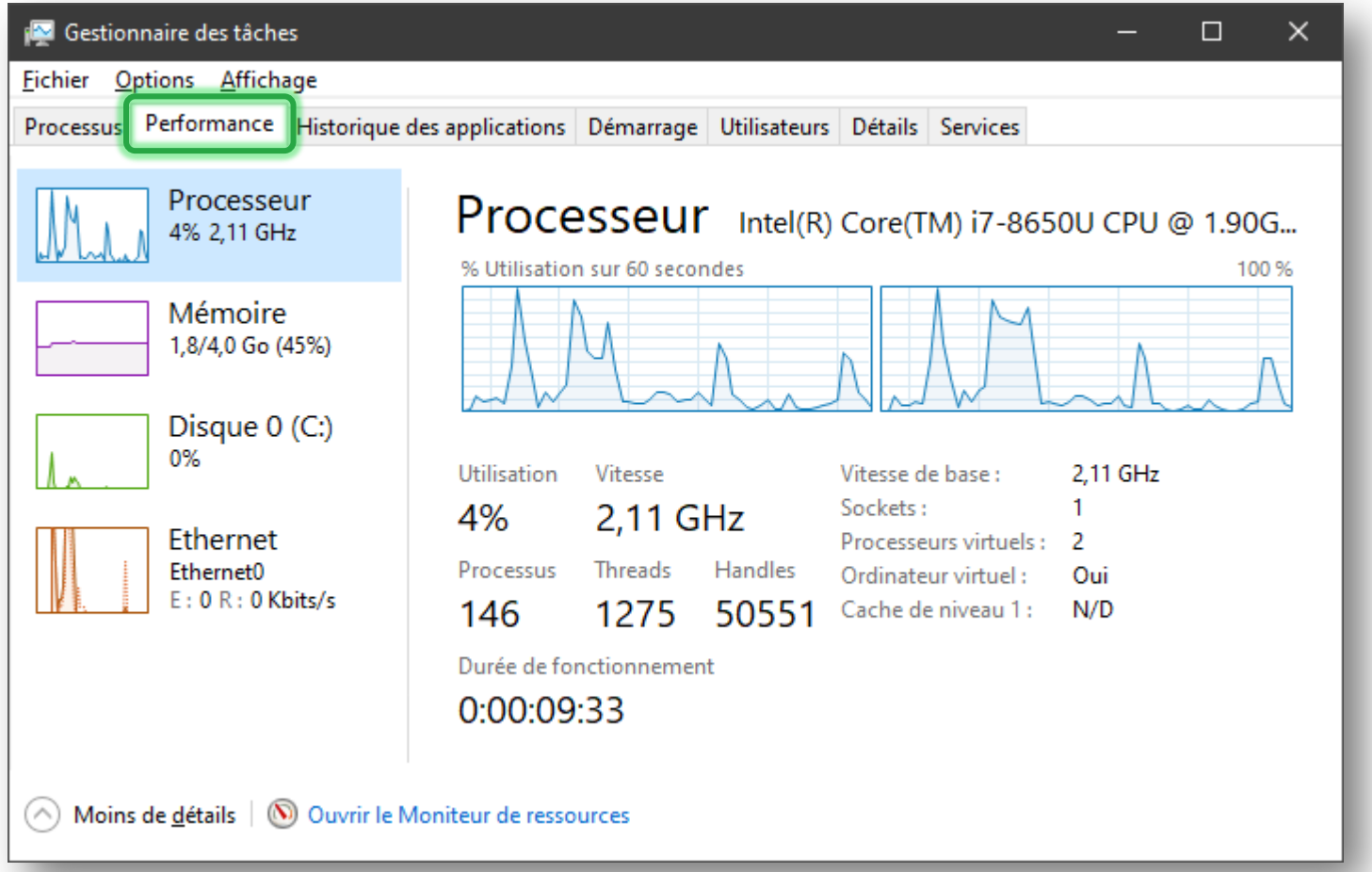




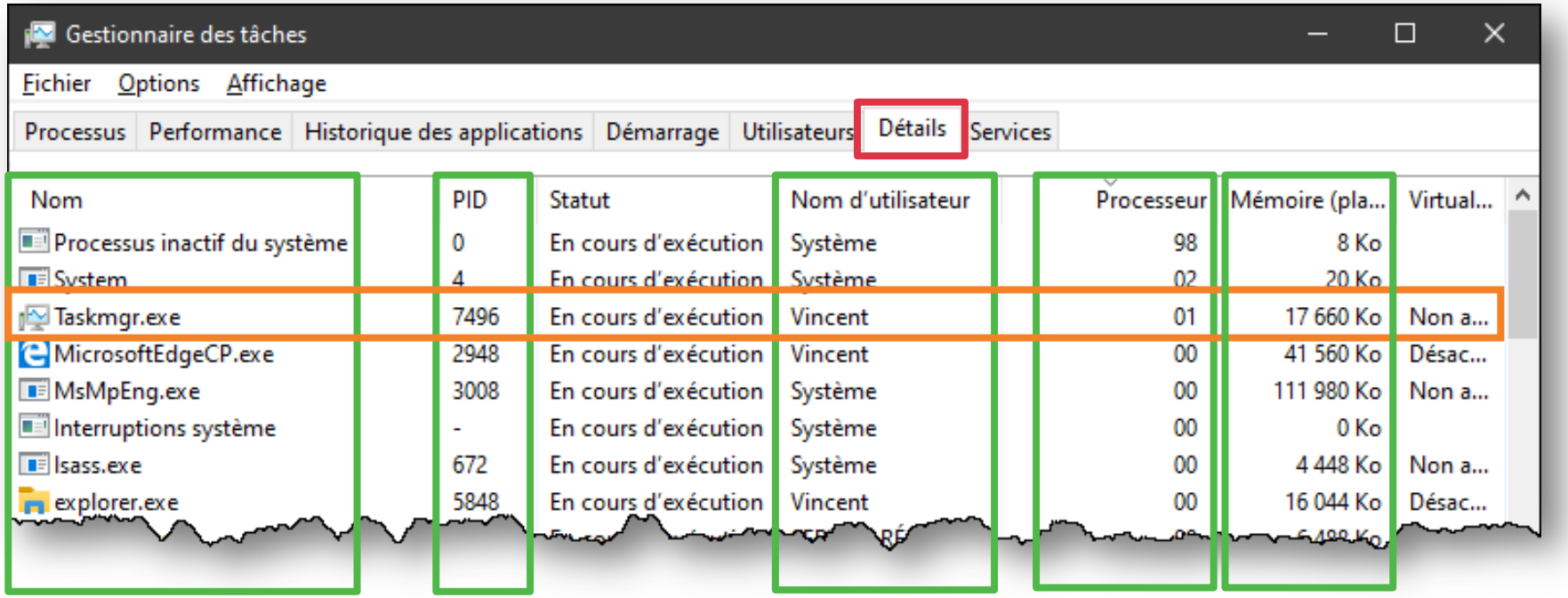
Visualiser l'utilisation des ressources

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 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

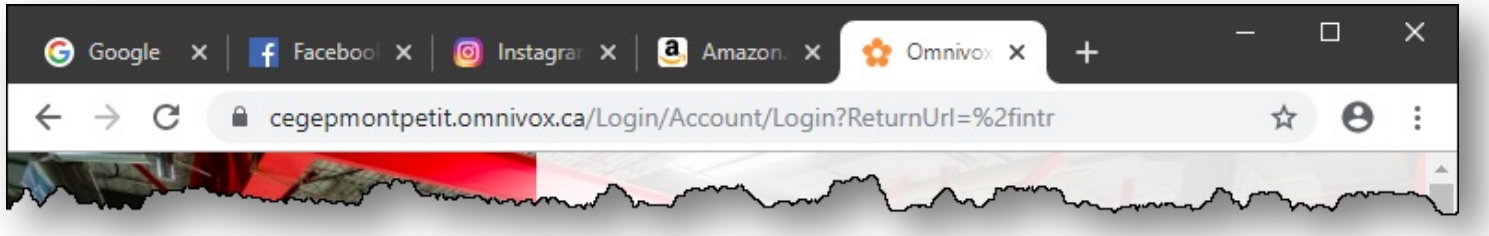
Le contenu du fichier est **copié** dans la mémoire réservée pour ce processus.

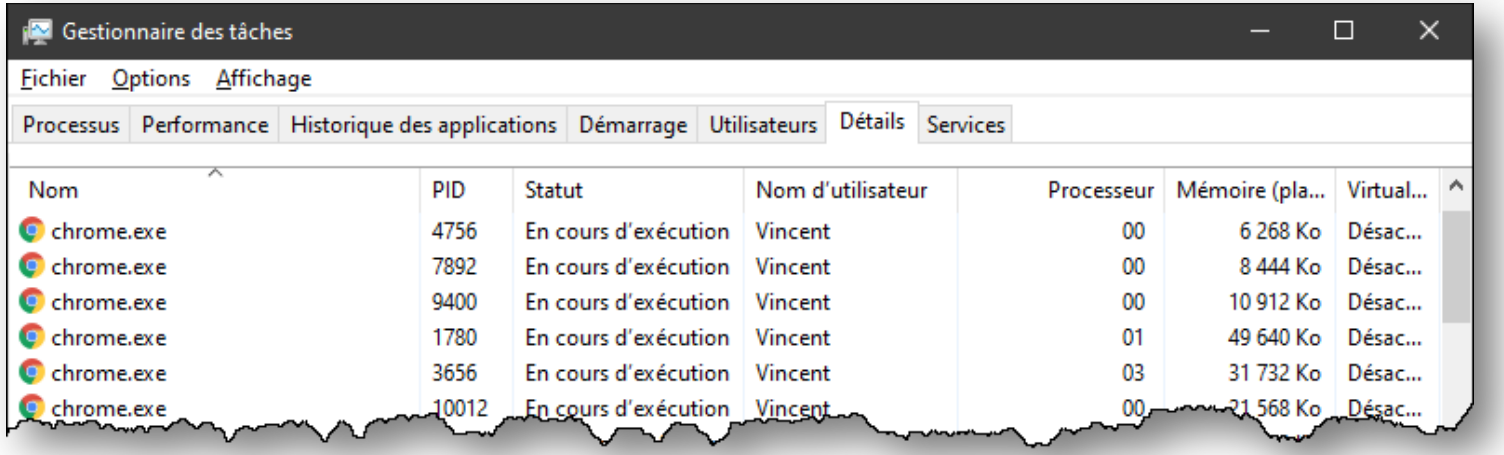
La **première instruction** du programme s'exécute.

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.

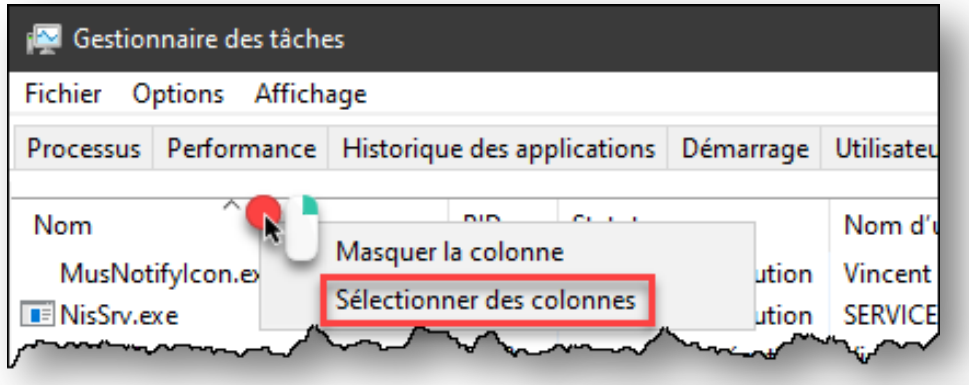
Certaines applications utilisent même plusieurs processus distincts tel Chrome pour chaque onglet, son gestionnaire de mot de passe, les modules d'extension, etc.

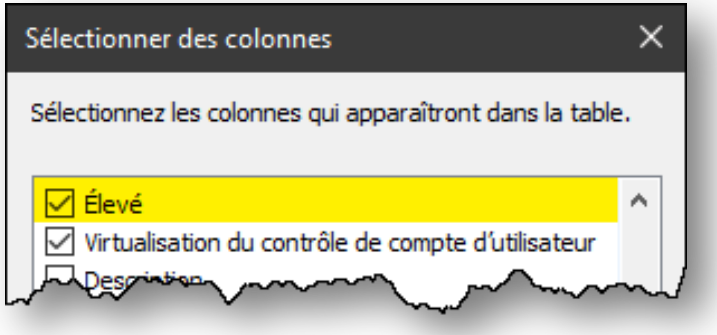


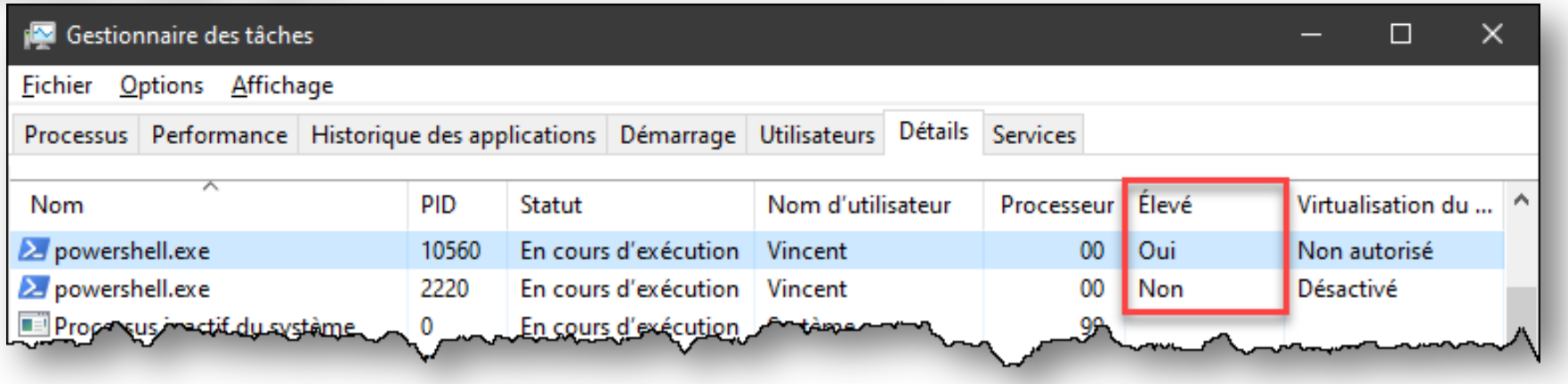


Gestionnaire de tâches : privilèges élevés (UAC)

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

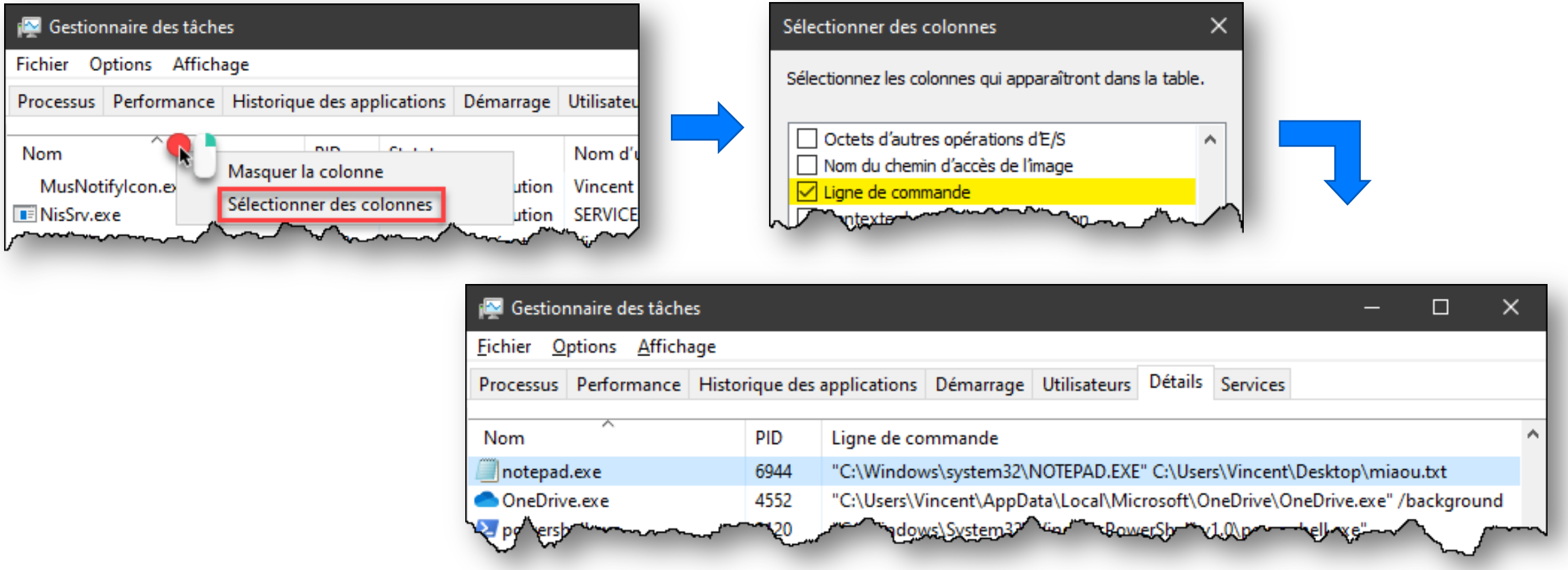




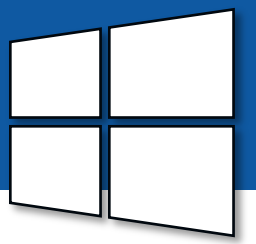


Gestionnaire de tâches: ligne de commande

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



Créer un processus



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

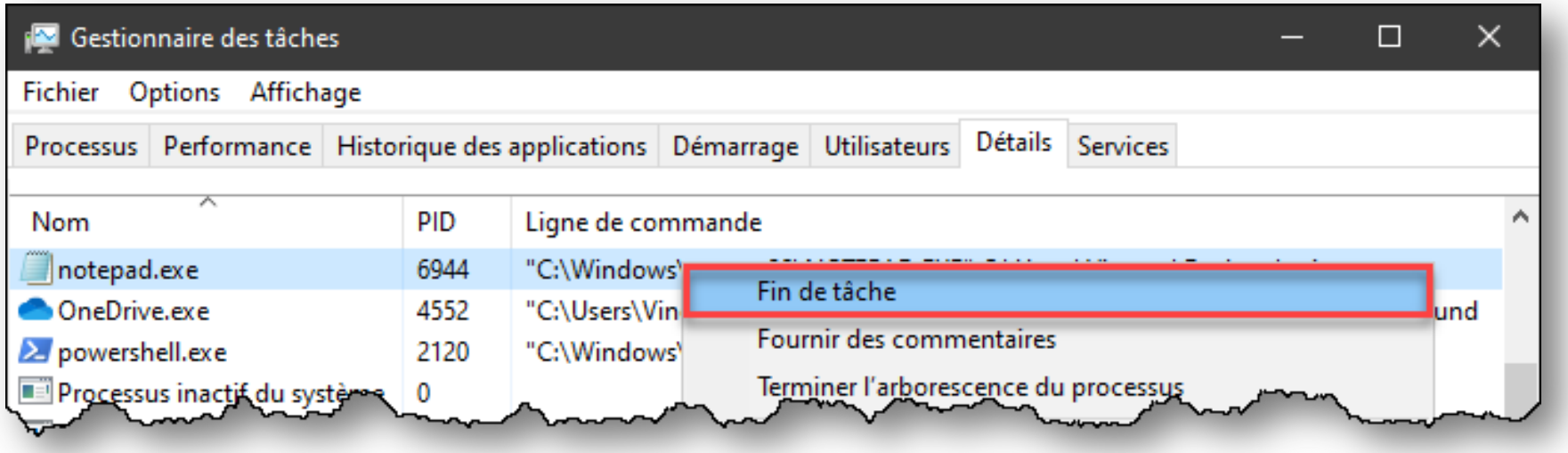
Un nouveau processus est automatiquement créé pour ce programme. Windows lui attribue alors un nouvel identifiant (PID).

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

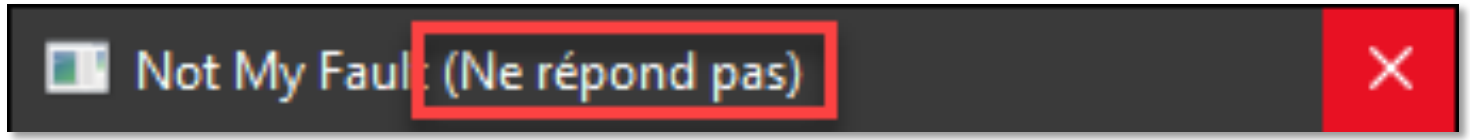
Il arrive qu'une application gèle et ne réponde plus aux commandes de l'utilisateur.

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.

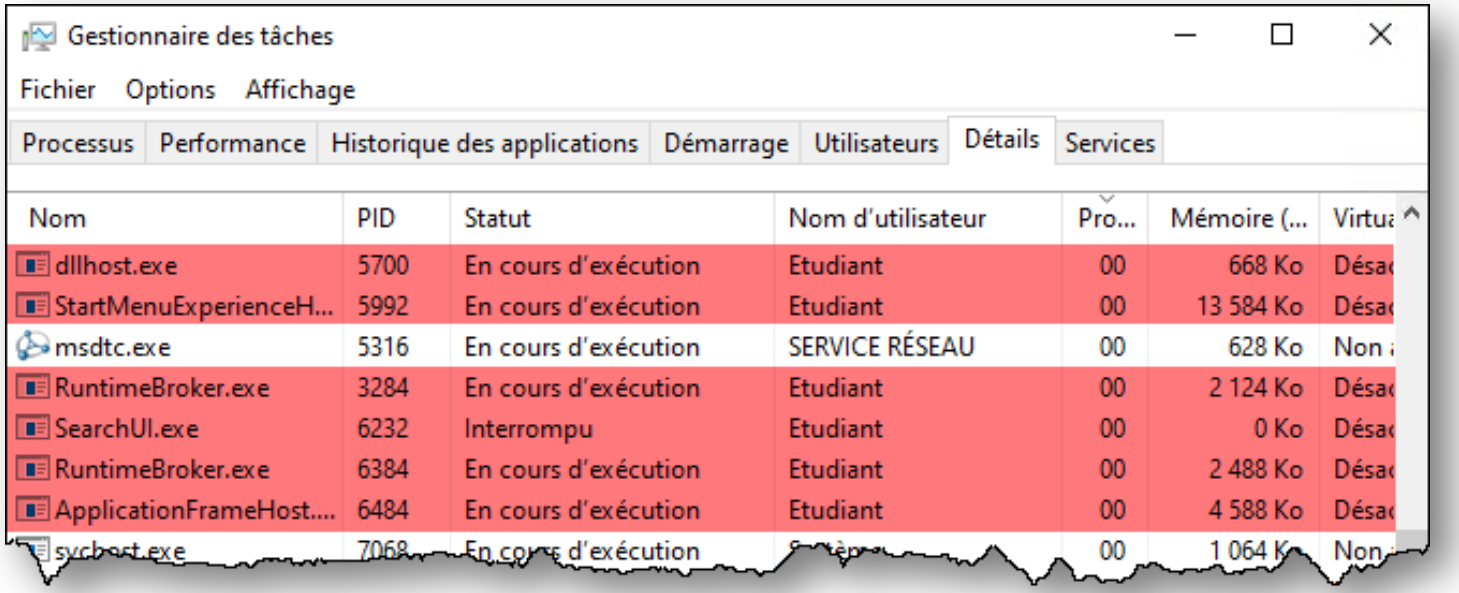
Lorsqu'on termine un processus de force, le programme n'a pas la chance de poser ces actions.

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.



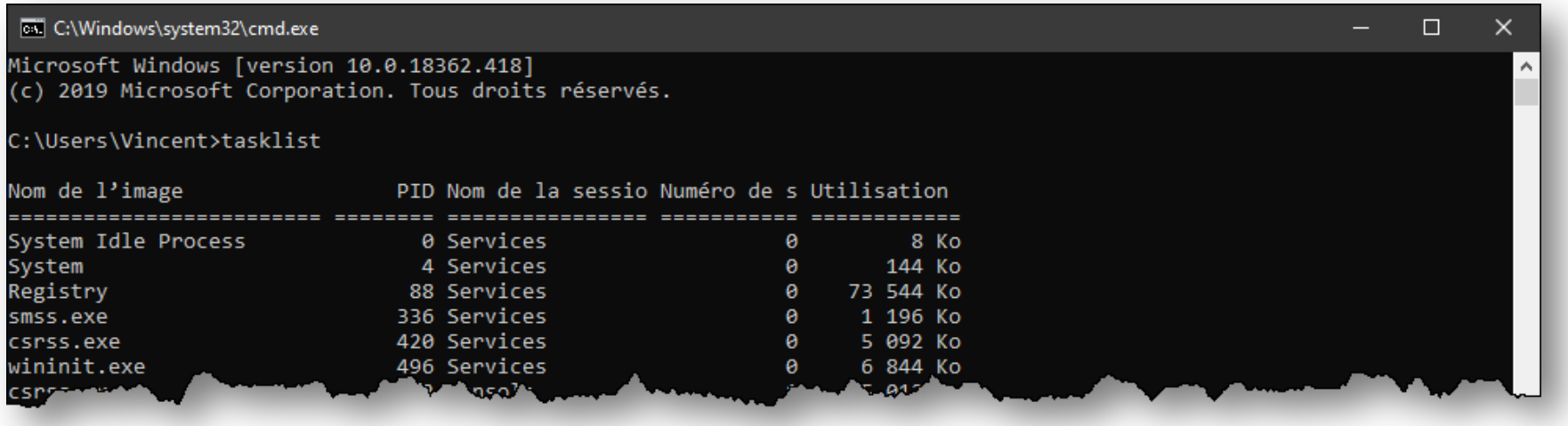
Les processus qui appartiennent à l'utilisateur SYSTÈME (ou d'autres comptes spéciaux comme « SERVICE LOCAL », « SERVICE RÉSEAU ») persistent après la fin de la session puisqu'ils appartiennent au système.

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

Ligne de commande (cmd)

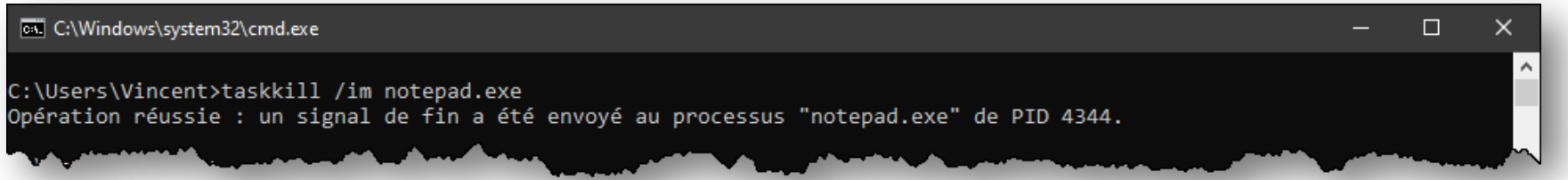
Obtenir la liste des processus:

`tasklist`



Terminer un processus:

`taskkill /im *nomduprocessus*.exe`

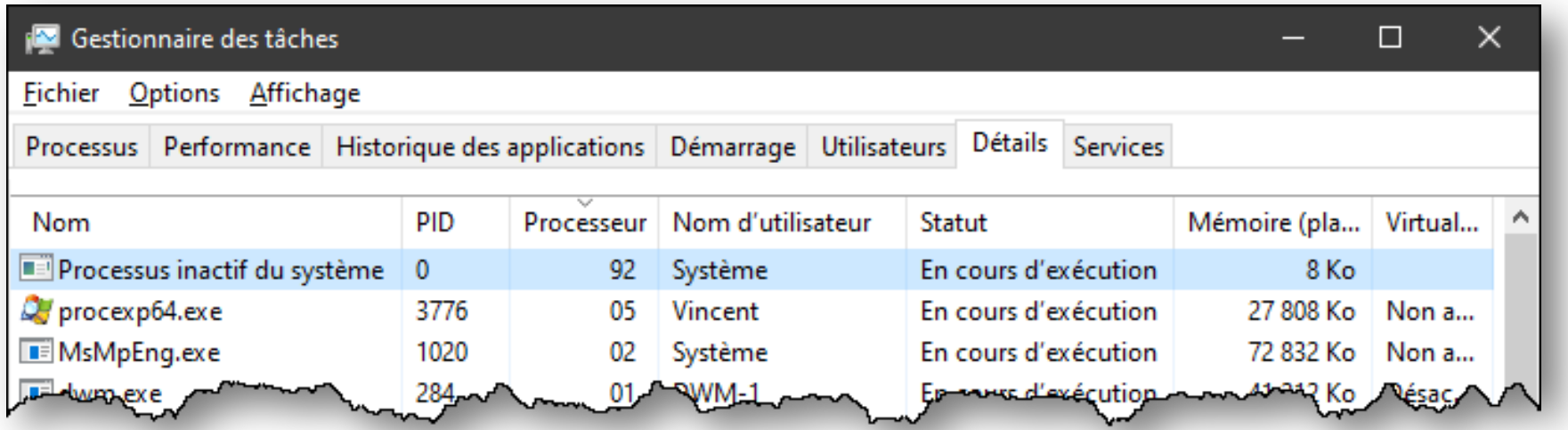


Processus spéciaux : Processus inactif du système

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.

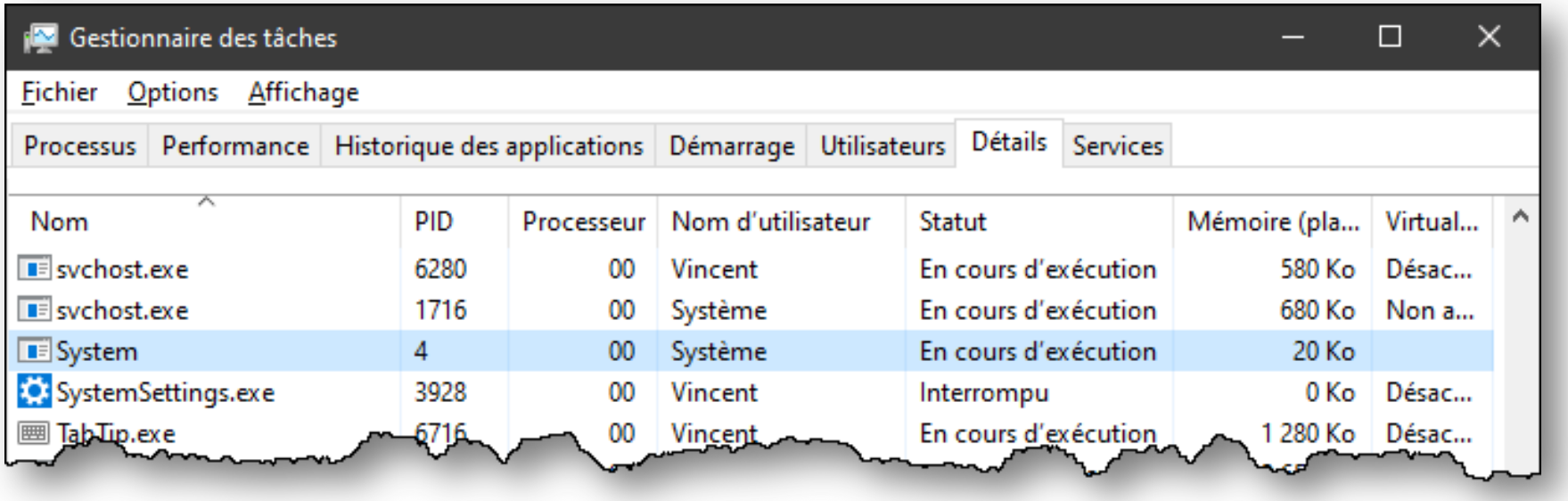
Contrairement aux autres processus, un haut pourcentage de processeur est sain. Cela signifie que le système est sous-utilisé.



Processus spéciaux : System

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

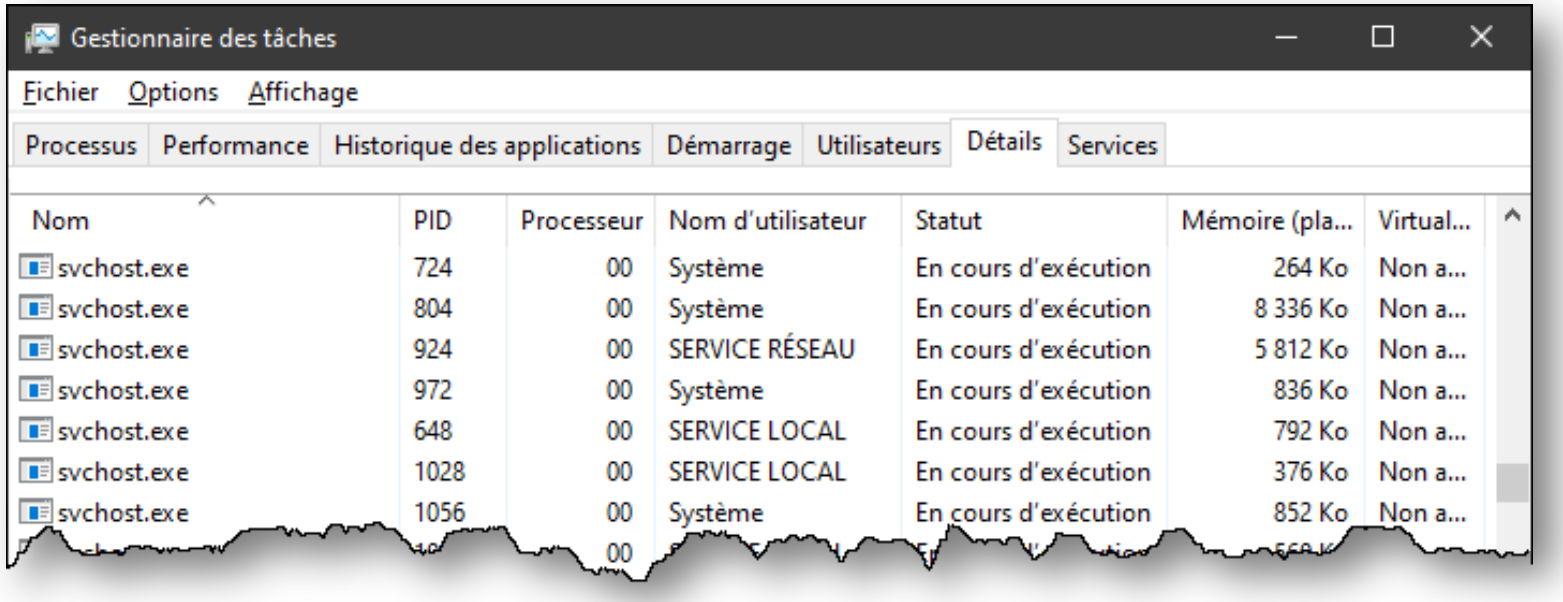
Ce n'est pas un vrai processus, donc impossible d'y mettre fin.



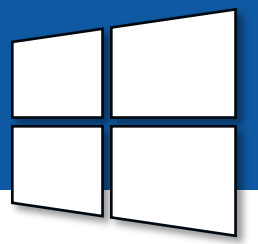
Processus spéciaux: SVCHOST

Il y a un grand nombre de processus SVCHOST.EXE

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



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