Process Explorer

C’est quoi ?

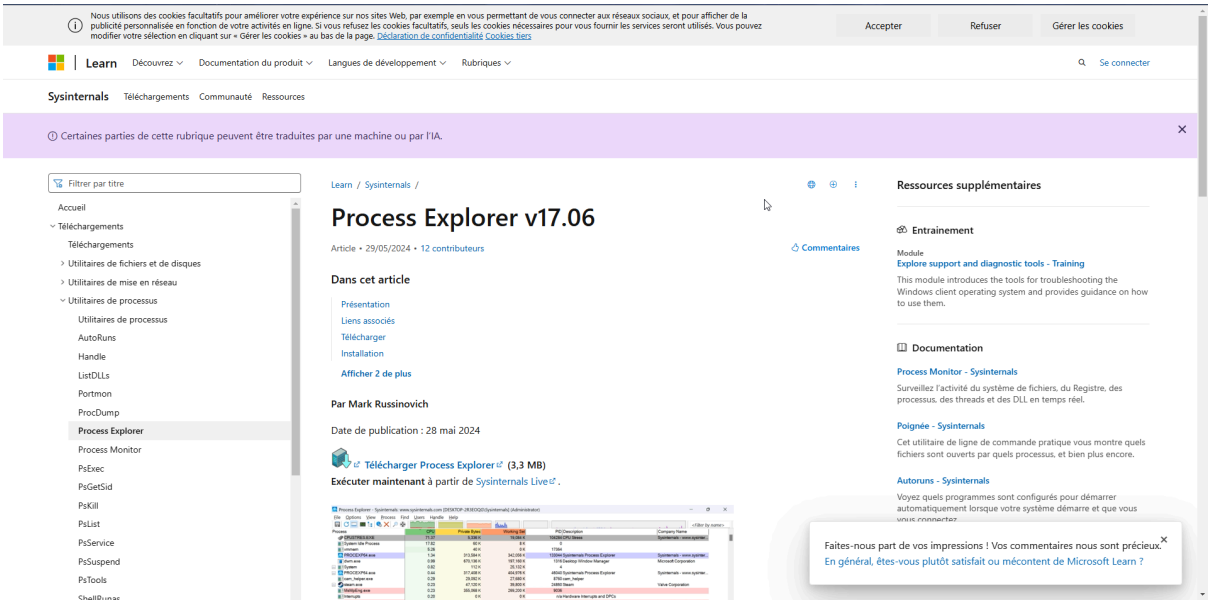
c’est un outil avancé pour surveiller et gérer les processus qui s'exécutent sur un ordinateur windows.Cette outil a été développé par Microsoft, il permet de voir en détail :

- Les programmes en cours d'exécution
- Les ressource qu’ils utilisent (mémoire, cpu)
- Les relations entre les processus
- Les fichier et bibliothèque utilisé par chaque processus

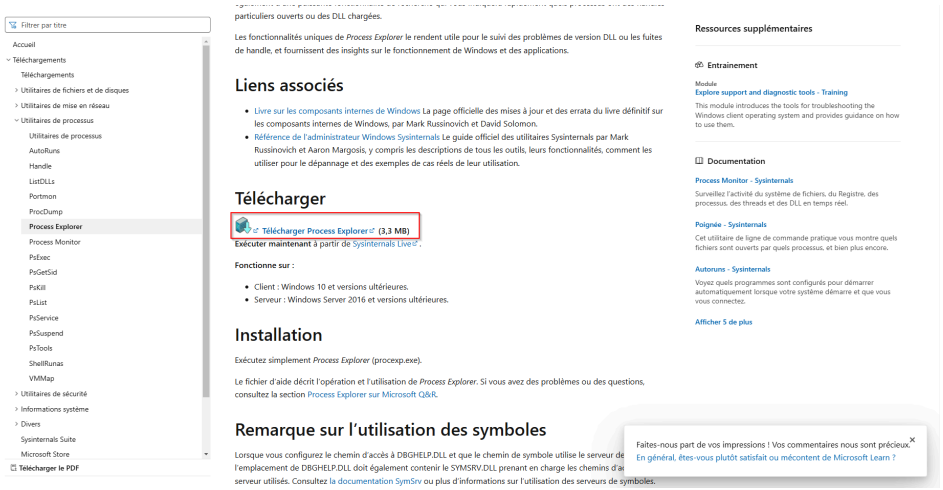
Sommaire

Installation

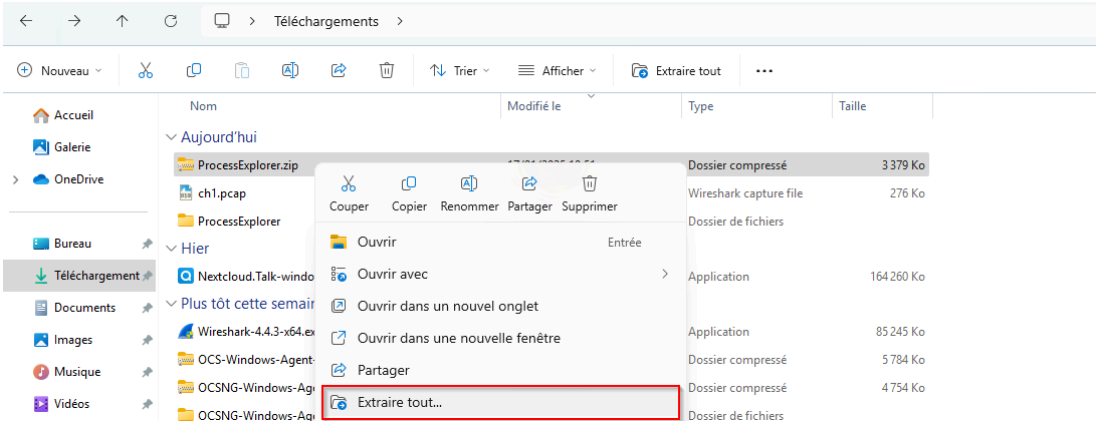
Pour pouvoir installer le logiciel Process explorer, il faut se rendre sur le site de Microsoft.



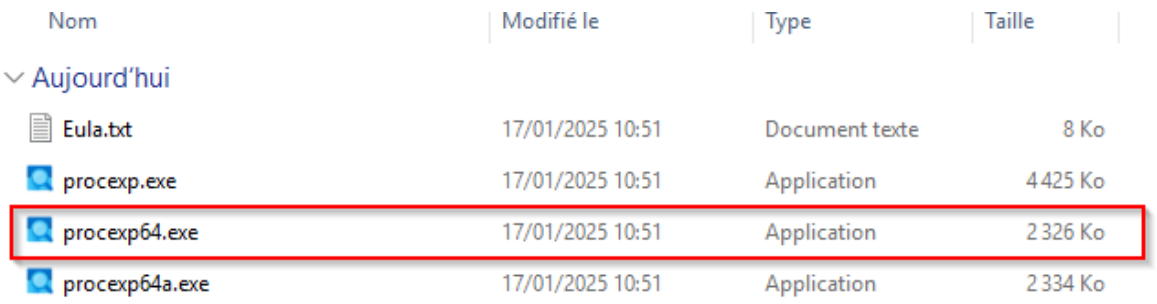
Ensuite, il faut cliquer sur “**Télécharger Process Explorer**” :



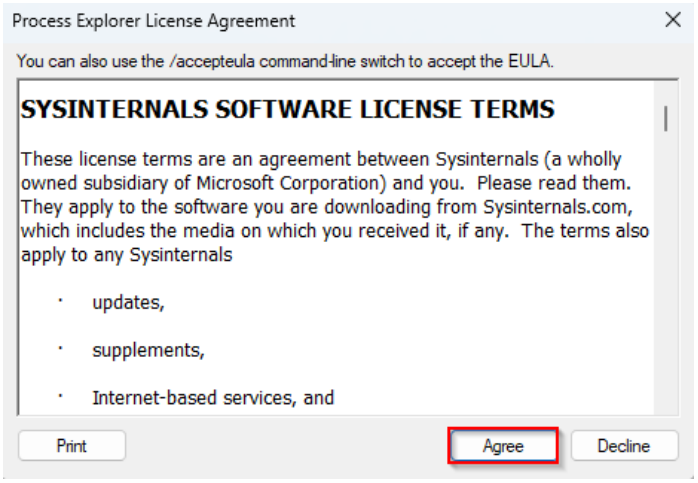
Une fois que c’est fait, il faut ouvrir un explorateur de fichier, aller dans “**téléchargement**” et extraire le dossier .



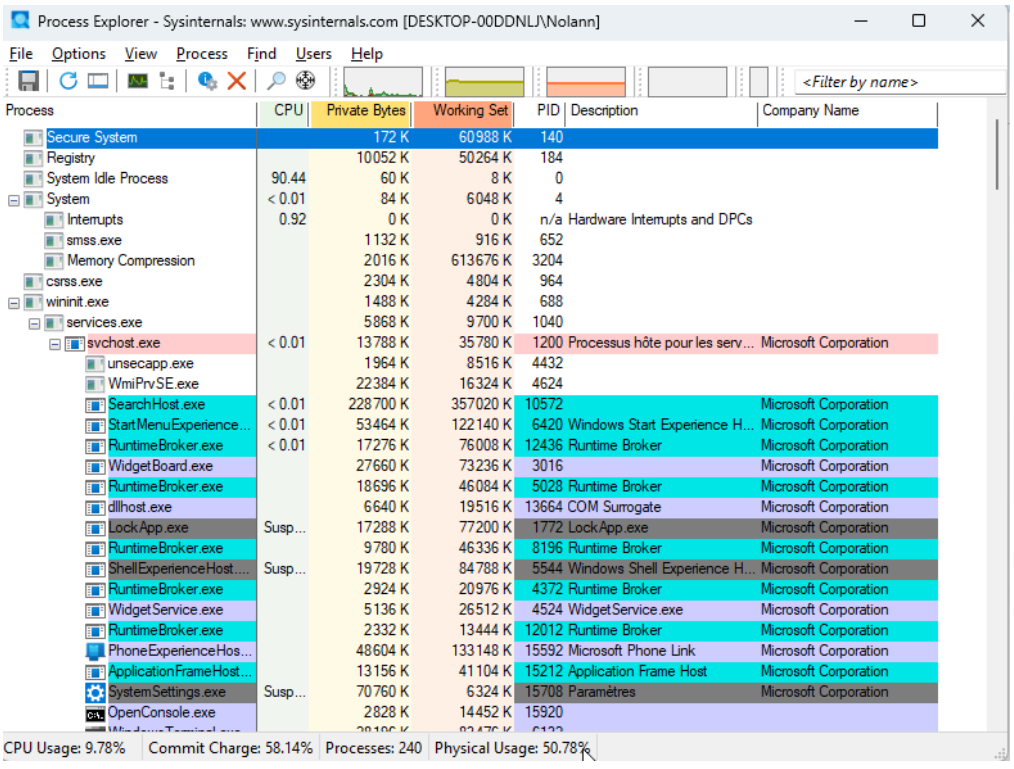
Une fois que le dossier est extrait, On l'ouvre et on lance "**procexp64.exe**".



Une fois que le .exe est lancée, une petite page va s'ouvrir, il faut évidemment "**accepter**".



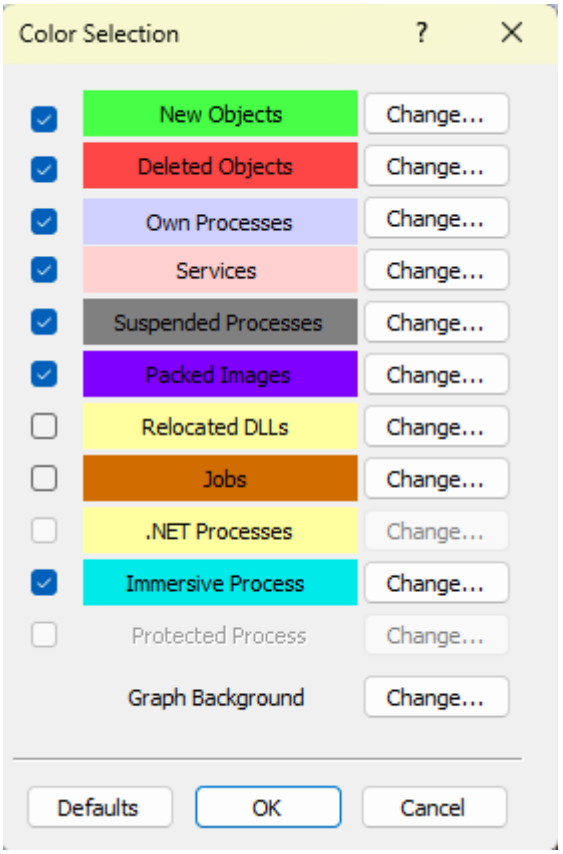
Quand vous aurez accepté, le logiciel va se lancer directement.



Utilisation

Code couleurs

- **New objets :** Nouveau processus lancé. Le processus qui vient d'être lancé sera en légende rouge pour passer dans une autre couleur selon le type d'élément.
- **Deleted Objets :** Processus en cours de terminaison
- **Own Processes :** Processus démarrés par l'utilisateur courant.
- **Services :** ce sont les services
- **Suspended Process :** processus suspendu ("en pause")
- **Packed Images :** Processus packé. Les packers sont des utilitaires qui permettent de compresser et/ou crypter des exécutables.
- **Relocated DLL :** La DLL n'est pas chargée dans un espace mémoire habituelle.
- **Jobs :** ce sont les tâches planifiées.
- **.NET Processes :** Programmes écrit en .NET
- **Immersive Process :** c'est tout ce qui va etre application UWP (Universal Windows Platform). Ce sont toutes les applications du "Store" et les applications intégrées nativement à Windows.



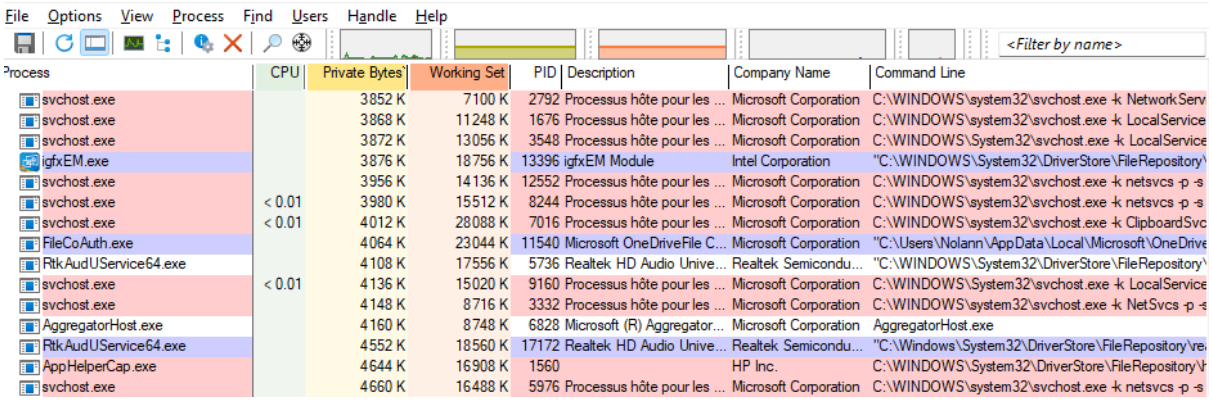
Affichage

Une fois que Process Explorer est démarré, vous verrez une liste de plusieurs processus en cours d'exécution. Par défaut, les colonnes qui s'affiche sont :

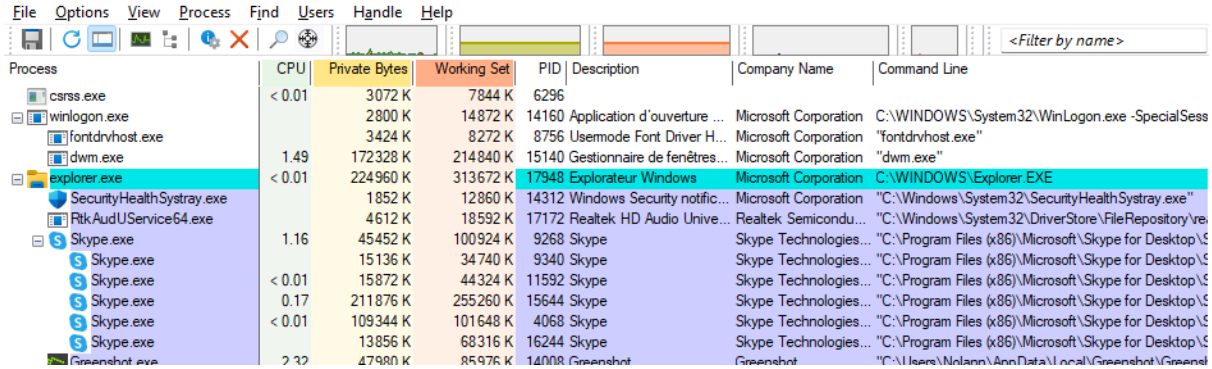
- **Process :** le nom du processus
- **PID :** le numéro du processus
- **CPU :** l'utilisation du processus
- **Description :** description du processus
- **Company Name :** Le nom de l'éditeur

L'affichage des processus peut se faire de manière linéaire ou en arborescence (**View/ Show Process Tree**)

Linéaire :



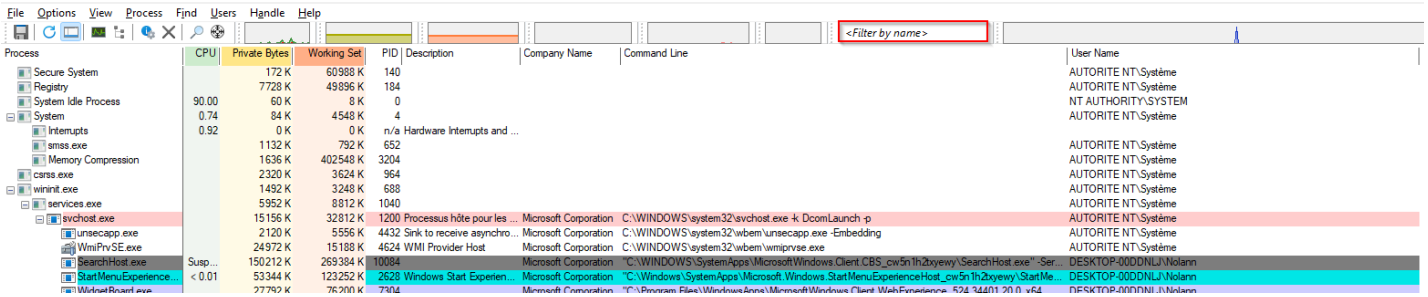
arborescence :



La visualisation en mode "arborescence", peut être plus appropriée pour identifier les processus parents et enfants.

Rechercher un processus

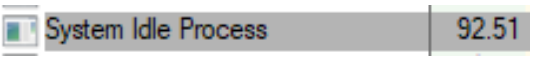
Pour rechercher un processus, en haut à droite, il y a un case avec marqué “filters by name”.



Il suffira de mettre le nom du processus recherché et il le trouvera .

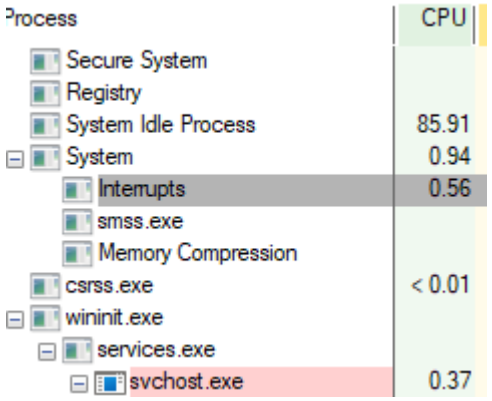
Identifier un problème

La question est : comment savoir qu'un processus prend trop de ressources ?
Dans un premier temps, on aura un processus d'indication, c'est-à-dire qu'il y a un processus qui calcule en pourcentage la quantité du Processeur (CPU) inutilisé.

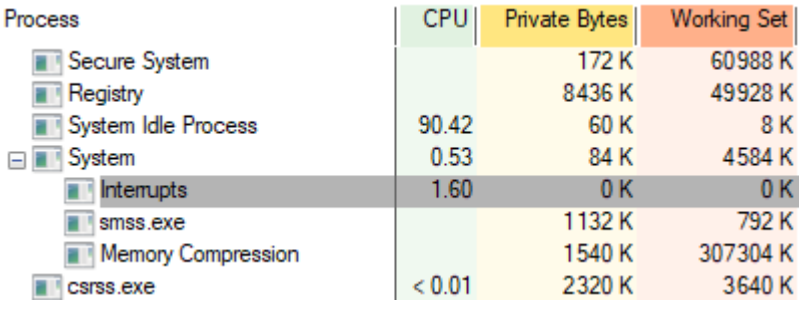


Donc la, on peut voir qu'il y a 92% de mon processeur qui n'est pas utilisé. Si cette donnée est basse, il faut commencer à regarder ce qui prend autant de ressources.

Dans un premier temps, on peut donc regarder la consommation CPU de chaque processus. Il faut observer la colonne "CPU", où les valeurs sont données en pourcentage.



Si la valeur CPU est élevée pour un ou plusieurs processus, cela indique un problème.
Ensuite, on peut aussi regarder la consommation de mémoire.
Il y a deux colonnes, la colonne Private Bytes (mémoire ram utilisée uniquement par ce processus) et la colonne Working Set (mémoire ram totale que le processus utilise : Private Bytes + mémoire partagée).



Si la valeur de la colonie Private Bytes est élevée, la valeur de "Working Set" le sera aussi, ce qui peut provoquer des ralentissements.

Si on veut avoir un global de toutes les informations, on peut aller dans le menu “**View**” et cliquer sur “**System Information**”

Ces graphiques montrent le pourcentage d’utilisation de plusieurs composants.

Interagir avec les processus

- **Kill Process :** tuer le processus en cours
- **Kill Process Tree :** tue le processus parent et enfants
- **Restart :** termine et relance le processus
- **Suspend :** Suspend l'exécution du processus, il est freeze
- **Properties :** permet d'ouvrir un fenêtre informative sur le processus.