## **Process Explorer**

## <u>C'est quoi ?</u>

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

Process Explorer	1
Installation	
Utilisation	5
Code couleurs	5
Affichage	6
Recherche	
Valeur de référence	7
Interagir avec les processus	9
5 .	

#### 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" :

177 Ph	particuliers ouverts ou des DLL chargées.	
S Fitter par otre	Les fonctionnalités uniques de Process Explorer le rendent utile pour le suivi des problèmes de version DLL ou les fuites	Ressources supplémentaires
Accueil	de handle, et fournissent des insights sur le fonctionnement de Windows et des applications.	
~ Téléchargements		6 Entrainement
Téléchargements		
> Utilitaires de fichiers et de disques	Liens associes	Module Explore support and diagnostic tools - Training
> Utilitaires de mise en réseau	Livra sur les composants internes de Winchwe La page officielle des mises à jour et des errate du livre définitif sur	This module introduces the tools for troubleshooting the
~ Utilitaires de processus	les composants internes de Windows, par Mark Russinovich et David Solomon.	Windows client operating system and provides guidance on how to use them.
Utilitaires de processus	Référence de l'administrateur Windows Sysinternals Le guide officiel des utilitaires Sysinternals par Mark	
AutoRuns	Russinovich et Aaron Margosis, y compris les descriptions de tous les outils, leurs fonctionnalités, comment les	
Handle	utiliser pour le dépannage et des exemples de cas réels de leur utilisation.	Documentation
ListDLLs		Process Monitor - Sysinternals
Portmon	Télécharger	Surveillez l'activité du système de fichiers, du Registre, des
ProcDump	Telecharger	processus, des threads et des DLL en temps réel.
Process Explorer	Tildebarner Drocers Emlerert (2.2 MD)	Poignée - Sysinternals
Process Monitor	Exécuter maintenant à partir de Svsinternais Live 2	Cet utilitaire de ligne de commande pratique vous montre quels
PsExec		fichiers sont ouverts par quels processus, et bien plus encore.
PsGetSid	Fonctionne sur :	Autoruns - Sysinternals
PaKill	<ul> <li>Client : Windows 10 et versions ultérieures.</li> </ul>	Voyez quels programmes sont configurés pour démarrer
Palist	<ul> <li>Serveur : Windows Server 2016 et versions ultérieures.</li> </ul>	automatiquement lorsque votre systeme demarre et que vous vous connectez.
PaService		
PsSuspend	Installation	Afficher 5 de plus
PsTopis	Installation	
ShellBunas	Exécutez simplement Process Explorer (procexp.exe).	
VMMan		
> Utilitaires de sécurité	Le tichier d'aide decrit l'operation et l'utilisation de Process Explorer. Si vous avez des problemes ou des questions, consulter la section Process Explorer sur Microsoft O&B	
> Informations système		
> Divers		
Susinternals Suite	Remarque sur l'utilisation des symboles	×
Mirroroft Store	Faites-nous	s part de vos impressions ! Vos commentaires nous sont précieux.
E Télécharger le PDF	l'emplacement de DBGHELP.DLL doit également contenir le SYMSRV.DLL prenant en charge les chemins d'au	etes-vous plutôt satisfait ou mecontent de Microsoft Learn ?
	serveur utilisés. Consultez la documentation SymSrv ou plus d'informations sur l'utilisation des serveurs de symboles.	

Nouveau 🕤 🔏	o 🗋 🍳	🖻 🖞 🛝 Trier 🗸 🗮 Afficher	Co Extra	aire tout •••	
Accueil	Nom	Modifié le		Туре	Taille
Calerie	✓ Aujourd'hui				
	🚞 ProcessExplorer.zip	17/01/2005 40 5		Dossier compressé	3 379 Ko
<ul> <li>OneDrive</li> </ul>	🔚 ch1.pcap	Courser Conjer Renommer Partager Supp	] imer	Wireshark capture file	276 Ko
	ProcessExplorer	couper copier renommer ranager supp	inter	Dossier de fichiers	
📕 Bureau 🛛 📌	∨ Hier	a Ouvrir	Entrée		
🞍 Téléchargement 🖈	Q Nextcloud.Talk-windo	😳 Ouvrir avec	>	Application	164 260 Ko
🛯 Documents 🛛 🖈	$\sim$ Plus tôt cette semair	Ouvrir dans un nouvel onglet			
🔀 İmages 🛛 🖈	属 Wireshark-4.4.3-x64.ex	Ouvrir dans une nouvelle fenêtre		Application	85 245 Ko
🕑 Musique 🔹 🖈	👼 OCS-Windows-Agent-	🖻 Partager		Dossier compressé	5 784 Ko
-	🚞 OCSNG-Windows-Agi	Extraina tout		Dossier compressé	4 754 Ko
videos 📌	CSNG-Windows-Aqu	Lo Extraire tout		Dossier de fichiers	

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

Nom	Modifié le	Туре	Taille
✓ Aujourd'hui			
Eula.txt	17/01/2025 10:51	Document texte	8 Ko
🔍 procexp.exe	17/01/2025 10:51	Application	4 425 Ko
🔍 procexp64.exe	17/01/2025 10:51	Application	2 326 Ko
👤 procexp64a.exe	17/01/2025 10:51	Application	2 334 Ko

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

Process Explorer License Agreement	×
You can also use the /accepteula command-line switch to accept the EULA.	
SYSINTERNALS SOFTWARE LICENSE TERMS	
These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Sysinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals	
· updates,	
· supplements,	
Internet-based services, and	
Print Agree Decline	,

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

👤 Process Explorer - Sysinternals: v	🔽 Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-00DDNLJ\Nolann] – 🗆 X								
<u>F</u> ile <u>O</u> ptions <u>V</u> iew <u>P</u> rocess F <u>i</u> nd <u>U</u> sers <u>H</u> elp									
🔚   C 🗆   🔤 🗄   🗞 🗙	, 👰					<filter by="" n<="" td=""><td>ame&gt;</td><td></td></filter>	ame>		
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name			
Secure System		172 K	60988 K	140		1			
Registry		10052 K	50264 K	184					
System Idle Process	90.44	60 K	8 K	0					
System	< 0.01	84 K	6048 K	4					
Interrupts	0.92	0 K	0 K	n/a	Hardware Interrupts and DPCs				
smss.exe		1132 K	916 K	652					
Memory Compression		2016 K	613676 K	3204					
csrss.exe		2304 K	4804 K	964					
🖃 🔳 wininit.exe		1488 K	4284 K	688					
services.exe		5868 K	9700 K	1040					
svchost.exe	< 0.01	13788 K	35780 K	1200	Processus hôte pour les serv	Microsoft Corporatio	'n		
unsecapp.exe	1	1964 K	8516 K	4432					
WmiPrvSE.exe		22384 K	16324 K	4624					
Search Host.exe	< 0.01	228700 K	357020 K	10572		Microsoft Corporatio	n		
Start Menu Experience	< 0.01	53464 K	122140 K	6420	Windows Start Experience H	Microsoft Corporatio	n		
RuntimeBroker.exe	< 0.01	17276 K	76008 K	12436	Runtime Broker	Microsoft Corporatio	n		
WidgetBoard.exe		27660 K	73236 K	3016		Microsoft Corporatio	'n		
RuntimeBroker.exe		18696 K	46084 K	5028	Runtime Broker	Microsoft Corporatio	'n		
dllhost.exe		6640 K	19516 K	13664	COM Surrogate	Microsoft Corporatio	'n		
Lock App.exe	Susp	17288 K	77200 K	1772	Lock App.exe	Microsoft Corporatio	in		
RuntimeBroker.exe		9780 K	46336 K	8196	Runtime Broker	Microsoft Corporatio	n		
ShellExperienceHost	Susp	19728 K	84788 K	5544	Windows Shell Experience H	. Microsoft Corporatio	n		
RuntimeBroker.exe		2924 K	20976 K	4372	Runtime Broker	Microsoft Corporatio	n		
WidgetService.exe		5136 K	26512 K	4524	WidgetService.exe	Microsoft Corporatio	'n		
RuntimeBroker.exe		2332 K	13444 K	12012	Runtime Broker	Microsoft Corporatio	n		
PhoneExperienceHos		48604 K	133148 K	15592	Microsoft Phone Link	Microsoft Corporatio	'n		
Application Frame Host		13156 K	41104 K	15212	Application Frame Host	Microsoft Corporatio	n		
System Settings.exe	Susp	70760 K	6324 K	15708	Paramètres	Microsoft Corporatio	n		
OpenConsole.exe		2828 K	14452 K	15920					
M/:- J T I		20100 1/	00.470 1/	C100					
CPU Usage: 9.78% Commit Charge	: 58.14%	Processes: 240	Physical Usa	ge: 50.7	78%				

## 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 :

File Options View Process Fi	nd <u>U</u> s	ers H <u>a</u> ndle	<u>H</u> elp			
🔚   C 🔲 🔤 🚼   🎨 🗙	, 👰					<filter by="" name=""></filter>
Process	CPU	Private Bytes`	Working Set	PID Description	Company Name	Command Line
svchost.exe		3852 K	7100 K	2792 Processus hôte pour les	Microsoft Corporation	C:\WINDOWS\system32\svchost.exe -k NetworkServ
svchost.exe		3868 K	11248 K	1676 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe +k LocalService
svchost.exe		3872 K	13056 K	3548 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\System32\svchost.exe +k LocalService
🛃 igfxEM.exe		3876 K	18756 K	13396 igfxEM Module	Intel Corporation	"C:\WINDOWS\System32\DriverStore\FileRepository\
svchost.exe		3956 K	14136 K	12552 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe +k netsvcs -p -s
svchost.exe	< 0.01	3980 K	15512 K	8244 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe +k netsvcs -p -s
svchost.exe	< 0.01	4012 K	28088 K	7016 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe +k ClipboardSvc
FileCoAuth.exe		4064 K	23044 K	11540 Microsoft OneDriveFile C.	. Microsoft Corporation	"C:\Users\Nolann\AppData\Local\Microsoft\OneDrive
Rtk Aud UService 64.exe		4108 K	17556 K	5736 Realtek HD Audio Unive.	Realtek Semicondu	"C:\WINDOWS\System32\DriverStore\FileRepository\
svchost.exe	< 0.01	4136 K	15020 K	9160 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\System32\svchost.exe +k LocalService
svchost.exe		4 148 K	8716 K	3332 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe +k NetSvcs -p -s
AggregatorHost.exe		4160 K	8748 K	6828 Microsoft (R) Aggregator	Microsoft Corporation	AggregatorHost.exe
Rtk Aud UService 64.exe		4552 K	18560 K	17172 Realtek HD Audio Unive.	Realtek Semicondu	"C:\Windows\System32\DriverStore\FileRepository\re-
AppHelperCap.exe		4644 K	16908 K	1560	HP Inc.	C:\WINDOWS\System32\DriverStore\FileRepository\r
svchost.exe		4660 K	16488 K	5976 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe -k netsvcs -p -s

#### arborescence :

<u>File Options View Process Fi</u>	nd <u>U</u> s	ers H <u>a</u> ndle	<u>H</u> elp			
🔚   C 🔲 🔤 🗄   🎨 🗙	, 👳					<filter by="" name=""></filter>
Process	CPU	Private Bytes	Working Set	PID Description	Company Name	Command Line
Csrss.exe	< 0.01	3072 K	7844 K	6296	1	1
🖃 🔚 winlogon.exe		2800 K	14872 K	14160 Application d'ouverture	Microsoft Corporation	C:\WINDOWS\System32\WinLogon.exe -SpecialSess
fontdrvhost.exe		3424 K	8272 K	8756 Usermode Font Driver H	Microsoft Corporation	"fontdrvhost.exe"
dwm.exe	1.49	172328 K	214840 K	15140 Gestionnaire de fenêtres	Microsoft Corporation	"dwm.exe"
🖃 🚘 explorer.exe	< 0.01	224960 K	313672 K	17948 Explorateur Windows	Microsoft Corporation	C:\WINDOWS\Explorer.EXE
SecurityHealthSystray.exe		1852 K	12860 K	14312 Windows Security notific	. Microsoft Corporation	"C:\Windows\System32\SecurityHealthSystray.exe"
Rtk Aud UService 64.exe		4612 K	18592 K	17172 Realtek HD Audio Unive	. Realtek Semicondu	"C:\Windows\System32\DriverStore\FileRepository\re
🖃 S Skype.exe	1.16	45452 K	100924 K	9268 Skype	Skype Technologies	. "C:\Program Files (x86)\Microsoft\Skype for Desktop\\$
S Skype.exe		15136 K	34740 K	9340 Skype	Skype Technologies	. "C:\Program Files (x86)\Microsoft\Skype for Desktop\\$
Skype.exe	< 0.01	15872 K	44324 K	11592 Skype	Skype Technologies	. "C:\Program Files (x86)\Microsoft\Skype for Desktop\5
S Skype.exe	0.17	211876 K	255260 K	15644 Skype	Skype Technologies	. "C:\Program Files (x86)\Microsoft\Skype for Desktop\5
S Skype.exe	< 0.01	109344 K	101648 K	4068 Skype	Skype Technologies	. "C:\Program Files (x86)\Microsoft\Skype for Desktop\\$
S Skype.exe		13856 K	68316 K	16244 Skype	Skype Technologies	. "C:\Program Files (x86)\Microsoft\Skype for Desktop\5
Sreenshot eve	2 3 2	47980 K	85976 K	14008 Greenshot	Greenshot	"C·\Lleere\Nolann\AnnData\Local\Greenehot\Greeneł

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".

<u>File Options View Process</u> F	ind <u>U</u> s	ers H <u>a</u> ndle	Help						
🔲 🖸 🛄 🔤 🗄 🔍 🗙	🔎 🚭						<filter by="" name=""></filter>		1
Process	CPU	Private Bytes	Working Set	PID Description	Company Name	Command Line		User Name	
Secure System	i i	172 K	60 988 K	140				AUTORITE NT\Système	
Registry		7728 K	49896 K	184				AUTORITE NT\Système	
System Idle Process	90.00	60 K	8 K	0				NT AUTHORITY\SYSTEM	
🖃 💽 System	0.74	84 K	4548 K	4				AUTORITE NT\Système	
Interrupts	0.92	0 K	0 K	n/a Hardware Interrupts and					
smss.exe		1132 K	792 K	652				AUTORITE NT\Système	
Memory Compression		1636 K	402548 K	3204				AUTORITE NT\Système	
Csrss.exe		2320 K	3624 K	964				AUTORITE NT\Système	
🖃 💽 wininit.exe		1492 K	3248 K	688				AUTORITE NT\Système	
services.exe		5952 K	8812 K	1040				AUTORITE NT\Système	
svchost.exe		15156 K	32812 K	1200 Processus hôte pour les	. Microsoft Corporation	C:\WINDOWS\system32\svchost.exe + DcomL	.aunch -p	AUTORITE NT\Système	
unsecapp.exe		2120 K	5556 K	4432 Sink to receive asynchro	. Microsoft Corporation	C:\WINDOWS\system32\wbem\unsecapp.exe	-Embedding	AUTORITE NT\Système	
WmiPrvSE.exe		24972 K	15188 K	4624 WMI Provider Host	Microsoft Corporation	C:\WINDOWS\system32\wbem\wmiprvse.exe		AUTORITE NT\Système	
SearchHost.exe	Susp	150212 K	269384 K	10084	Microsoft Corporation	"C:\WINDOWS\SystemApps\MicrosoftWindows	s.Client.CBS_cw5n1h2txyewy\SearchHost.exe" -Ser.	DESKTOP-00DDNLJ\Nolann	
StartMenuExperience	< 0.01	53344 K	123252 K	2628 Windows Start Experien	Microsoft Corporation	"C:\Windows\SystemApps\Microsoft.Windows.S	StartMenuExperienceHost_cw5n1h2txyewy\StartMe.	DESKTOP-00DDNLJ\Nolann	
WidgetBoard eve		27792 K	76 200 K	7304	Microsoft Comparation	"C:\Pmaram Filee\WindoweAnne\MicmeaftWind	owe Client WebEvnerience, 524 34401 20.0 x64	DESKTOP-00DDNL IVNolann	the second s

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).

Process	CPU	Private Bytes	Working Set
Secure System		172 K	60988 K
Registry		8436 K	49928 K
System Idle Process	90.42	60 K	8 K
🖃 🔳 System	0.53	84 K	4584 K
Interrupts	1.60	0 K	0 K
smss.exe		1132 K	792 K
Memory Compression		1540 K	307304 K
Csrss.exe	< 0.01	2320 K	3640 K

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.

	<u>W</u> indow	
	Set <u>A</u> ffinity	
	Set Priority	+
×	<u>K</u> ill Process	Del
	Kill Process <u>T</u> ree	Shift+Del
	<u>R</u> estart	
	S <u>u</u> spend	
	<u>C</u> reate Dump	•
	Check VirusTotal.	com
<b>Q</b> 2	<u>P</u> roperties	
	Search <u>O</u> nline	Ctrl+M