

Les outils Sysinternals

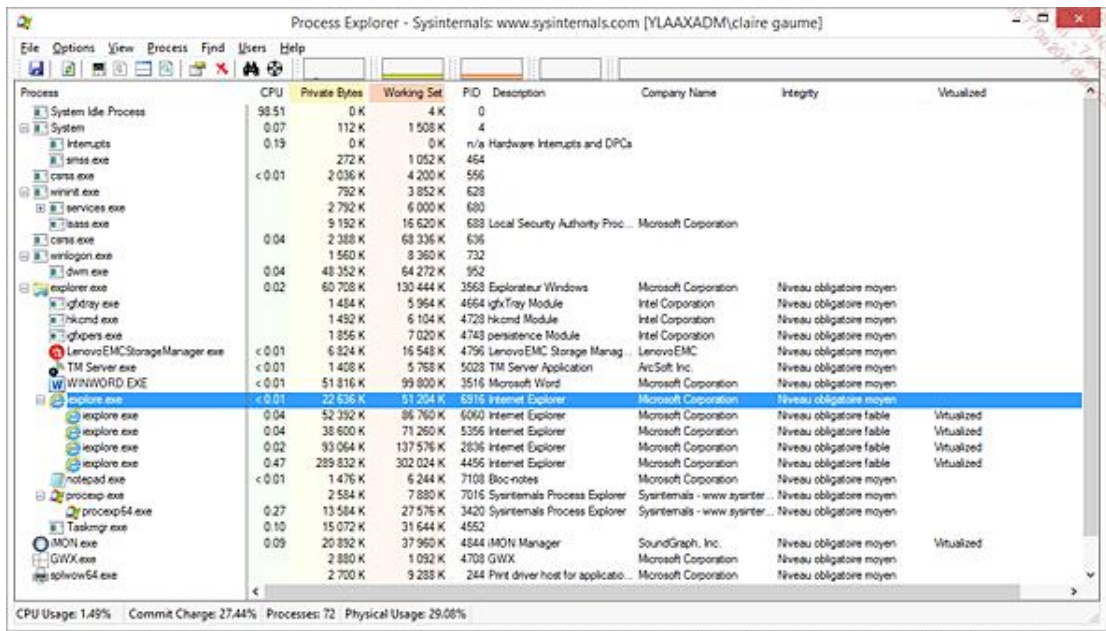
Cette suite d'outils, issue du rachat par Microsoft de Sysinternals en 2006, étend les capacités de diagnostic et dépannage des outils intégrés par défaut à Windows que nous avons vus précédemment.

Ces outils sont disponibles individuellement en téléchargement gratuit depuis le site de Microsoft. Vous pouvez également obtenir l'ensemble des outils en téléchargeant la suite Sysinternals depuis la page suivante : <https://docs.microsoft.com/fr-fr/sysinternals/downloads/sysinternals-suite>

La suite Sysinternals se compose de nombreux outils (plus de 70) pour la gestion de la sécurité, du réseau, du système de fichiers et des disques, mais aussi du système au sens large.

On trouve souvent ces outils dans les scripts d'exploitation personnalisés des postes de travail Windows.

Si on prend par exemple l'outil **Process Explorer**, bien qu'il soit proche en termes de fonctionnalités du Gestionnaire de tâches, de nombreux administrateurs l'utilisent toujours pour la surveillance en temps réel des performances des processus. Il permet, par exemple, sur une interface unique de visualiser l'arborescence et les niveaux d'intégrité des processus en cours d'exécution. Vous pouvez également visualiser, comme sur la copie d'écran suivante, si les processus utilisent le mode de compatibilité du contrôle de compte utilisateur, c'est-à-dire la notion de virtualisation du processus.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Integrity	Virtualized
System Idle Process	98.51	0 K	4 K	0				
System	0.07	112 K	1 508 K	4				
smss.exe	0.19	0 K	0 K	n/a	Hardware Interrupts and DPCs			
csrss.exe		272 K	1 052 K	464				
conhost.exe	< 0.01	2 036 K	4 200 K	556				
smss.exe		792 K	3 852 K	628				
services.exe		2 792 K	6 000 K	680				
lsass.exe		9 152 K	16 620 K	688	Local Security Authority Proc...	Microsoft Corporation		
csrss.exe	0.04	2 388 K	68 336 K	636				
winlogon.exe		1 560 K	8 360 K	732				
dwim.exe	0.04	48 352 K	64 272 K	952				
explorer.exe	0.02	60 708 K	130 444 K	3568	Explorateur Windows	Microsoft Corporation	Niveau obligatoire moyen	
ghltdrv.exe		1 484 K	5 964 K	4664	ghlTray Module	Intel Corporation	Niveau obligatoire moyen	
hikcmd.exe		1 452 K	6 104 K	4728	hikcmd Module	Intel Corporation	Niveau obligatoire moyen	
ghlspers.exe		1 856 K	7 020 K	4743	persistence Module	Intel Corporation	Niveau obligatoire moyen	
LenovoEMCStorageManager.exe	< 0.01	6 824 K	16 548 K	4756	LenovoEMC Storage Manag...	LenovoEMC	Niveau obligatoire moyen	
TM Server.exe	< 0.01	1 408 K	5 768 K	5023	TM Server Application	ArcSoft Inc.	Niveau obligatoire moyen	
WINWORD.EXE	< 0.01	51 816 K	99 800 K	3516	Microsoft Word	Microsoft Corporation	Niveau obligatoire moyen	
explore.exe	< 0.01	22 532 K	57 024 K	5315	Internet Explorer	Microsoft Corporation	Niveau obligatoire moyen	
explore.exe	0.04	52 332 K	86 760 K	6060	Internet Explorer	Microsoft Corporation	Niveau obligatoire faible	Virtualized
explore.exe	0.04	38 600 K	71 260 K	5356	Internet Explorer	Microsoft Corporation	Niveau obligatoire faible	Virtualized
explore.exe	0.02	93 064 K	137 576 K	2636	Internet Explorer	Microsoft Corporation	Niveau obligatoire faible	Virtualized
explore.exe	0.47	289 832 K	302 024 K	4456	Internet Explorer	Microsoft Corporation	Niveau obligatoire faible	Virtualized
notepad.exe	< 0.01	1 476 K	6 244 K	7108	Bloc-notes	Microsoft Corporation	Niveau obligatoire moyen	
processp.exe		2 584 K	7 880 K	7016	Sysinternals Process Explorer	Sysinternals - www.sysinter...	Niveau obligatoire moyen	
processp64.exe	0.27	13 584 K	27 576 K	3420	Sysinternals Process Explorer	Sysinternals - www.sysinter...	Niveau obligatoire moyen	
Taskmgr.exe	0.10	15 072 K	31 644 K	4852				
MON.exe	0.09	20 892 K	37 960 K	4844	MON Manager	SoundGraph, Inc.	Niveau obligatoire moyen	Virtualized
GWX.exe		2 880 K	1 092 K	4708	GWX	Microsoft Corporation	Niveau obligatoire moyen	
spivow64.exe		2 700 K	9 288 K	244	Print driver host for applicatio...	Microsoft Corporation	Niveau obligatoire moyen	

L'outil **Process Monitor**, qui est un autre exemple d'outil système, est plutôt utilisé pour tracer l'activité en temps réel d'un processus dans le Registre ou sur le système de fichiers, par exemple.

La multitude des outils proposés par la suite Sysinternals facilite souvent les opérations de maintenance et dépannage dans l'environnement Windows.

Pour terminer cette section, notez la présence d'autres outils d'administration, dans **Panneau de configuration - Système et sécurité - Outils d'administration**. Vous y retrouverez certains des outils décrits dans cette section et d'autres non abordés.