Les outils Sysinternals

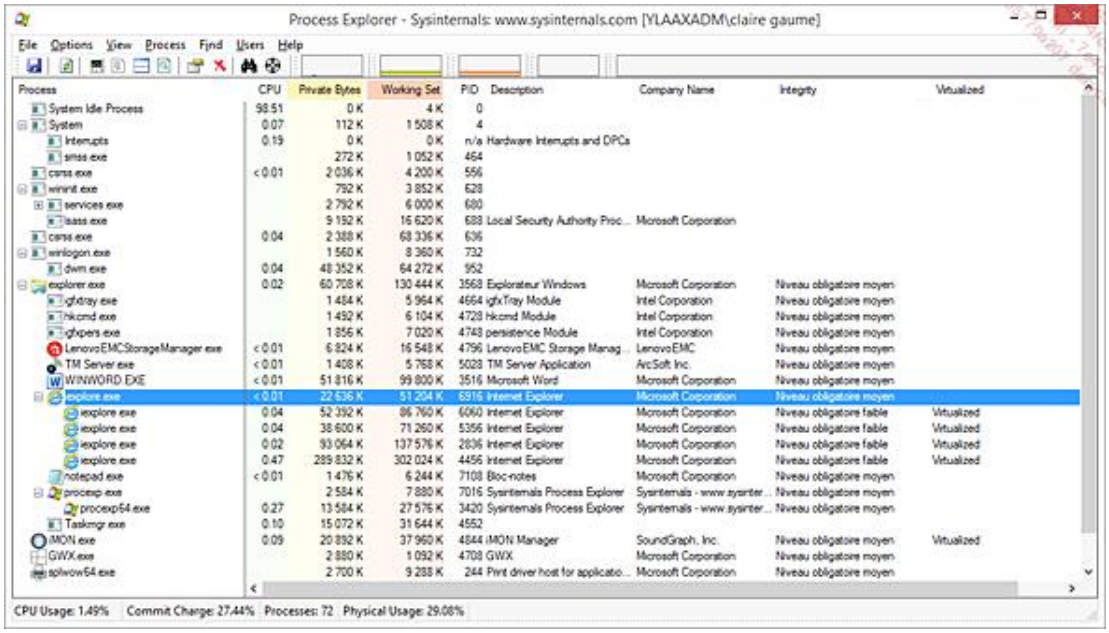
Cette suite d'outils, issue du rachat par Microsoft de Sysinternals en 2006, étend les capacités de diagnostic et dépannage des outils intégrés par défaut à Windows que nous avons vus précédemment.

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.



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.