Text

Description automatically generated with low confidence

Shape

Description automatically generated

|  |
| --- |
| Cheat sheet Win |

Sylvain Depasse

1-20-2023

**Table des matières   
  
Introduction  
  
Compte utilisateur  
  
Processus  
  
Prestations de service  
  
Planificateur de tâches  
  
Startup  
  
Entrées de registre  
  
Ports TCP et UDP actifs  
  
Partage de fichiers  
  
Des dossiers  
  
Paramètres du pare-feu  
  
Sessions  
  
Entrées des journaux**

**Introduction**Ce document est donc un ‘aide-mémoire’ ou cheat sheet visant à vous épauler lors de manipulation windows. Chaque étape est documentée et illustrée de façon à permettre une entière compréhension. Néanmoins, il est sujet à être modifié, à évoluer.

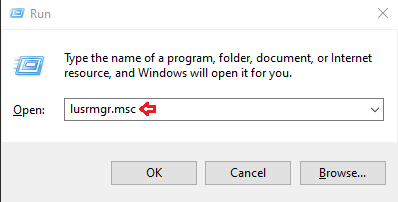
**Comptes utilisateur**

Dans la réponse aux incidents, il est nécessaire d'enquêter sur l'activité de l'utilisateur pour déterminer si un compte utilisateur suspect est présent ou si des autorisations ont été attribuées à un utilisateur. En vérifiant le compte d'utilisateur, on peut être en mesure d'obtenir des réponses aux questions telles que l'utilisateur actuellement connecté et le type de compte d'utilisateur dont on dispose.

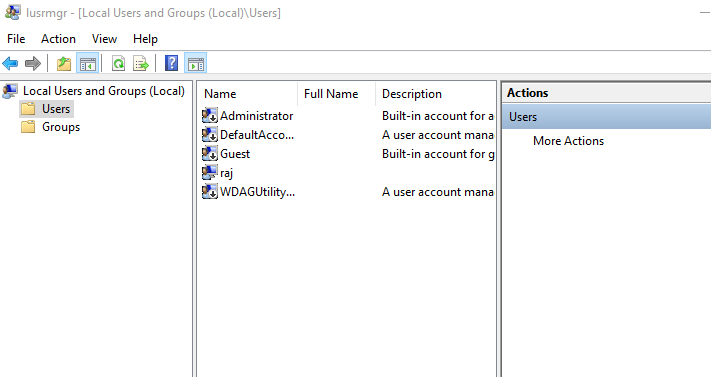
Les façons dont on peut afficher les comptes d'utilisateurs sont:

Pour afficher les comptes d'utilisateurs locaux dans l'interface graphique, appuyez sur ' **Windows + R** ', puis tapez

>lusrmgr.msc

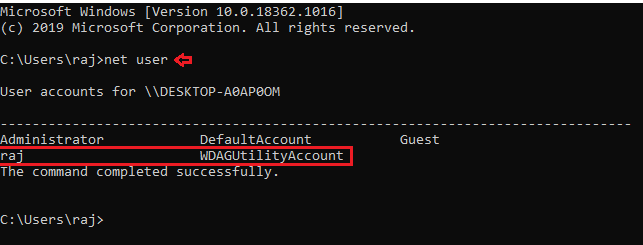


Cliquez maintenant sur ' **ok** ', et ici vous pourrez voir les comptes d'utilisateurs et leurs descriptions.



Pour voir maintenant les **comptes** d'utilisateurs du système et le type de compte en question, Exécutez l'invite de commande en tant qu'administrateur et tapez la commande

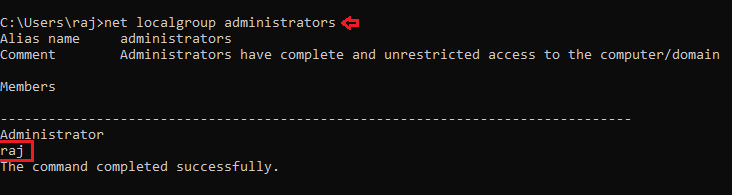
>net user



Net localgroup ‘**Le nom de groupe’** est utilisé pour gérer les groupes d'utilisateurs locaux sur un système. En utilisant cette commande, un administrateur peut ajouter des utilisateurs locaux ou de domaine à un groupe, supprimer des utilisateurs d'un groupe, créer de nouveaux groupes et supprimer des groupes existants.

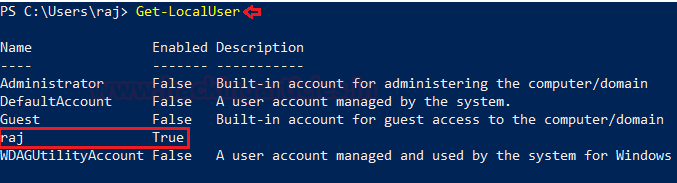
Ouvrez l'invite de commande et exécutez en tant qu'administrateur, puis tapez

>net localgroup administrators



Pour voir les comptes utilisateurs locaux, avec leurs noms, s'ils sont activés et leur description, Exécutez PowerShell en tant qu'administrateur, tapez

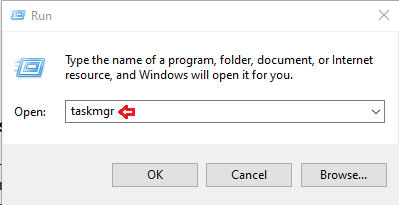
>Get-LocalUser



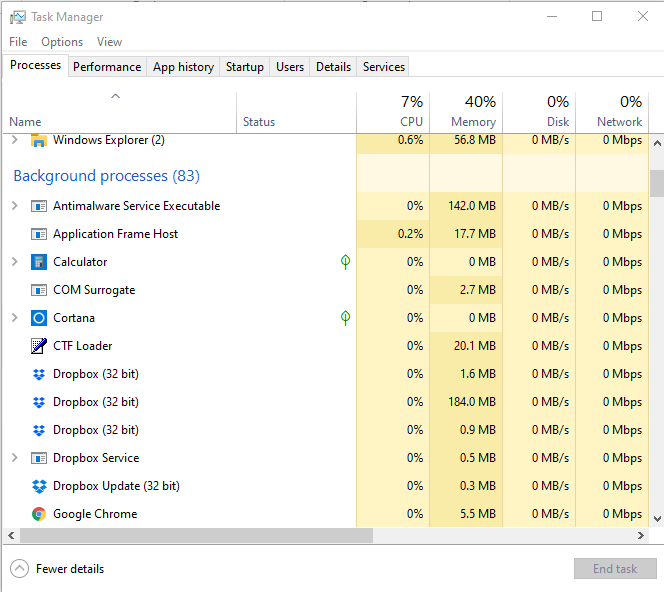
**Processus**

Pour afficher les processus, vous pouvez utiliser les méthodes suivantes; Pour afficher les processus en cours d'exécution dans une interface graphique, appuyez sur ' **Windows + R** ', puis tapez

>taskmgr.exe



Maintenant, cliquez sur ' **OK** ' et vous pourrez voir tous les processus en cours d'exécution dans votre système et pourrez vérifier s'il y a des processus inutiles en cours d'exécution.



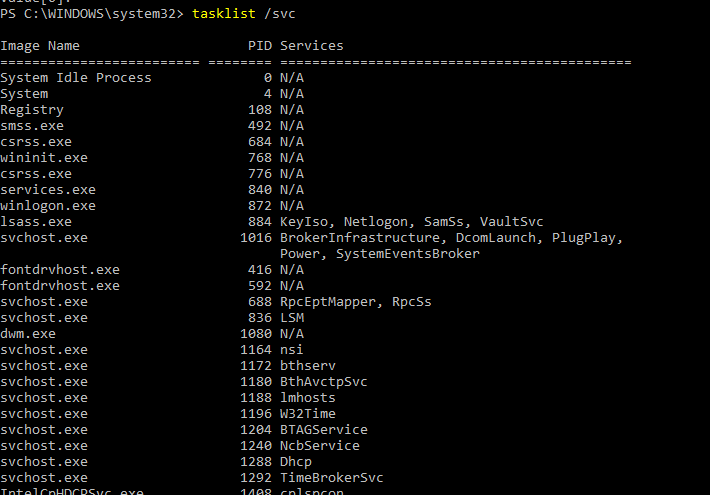
Pour voir tous les processus en cours d'exécution avec leur ID de processus (PID) et leur nom de session et la quantité de mémoire utilisée. Exécutez l'invite de commande en tant qu'administrateur et tapez

>tasklist



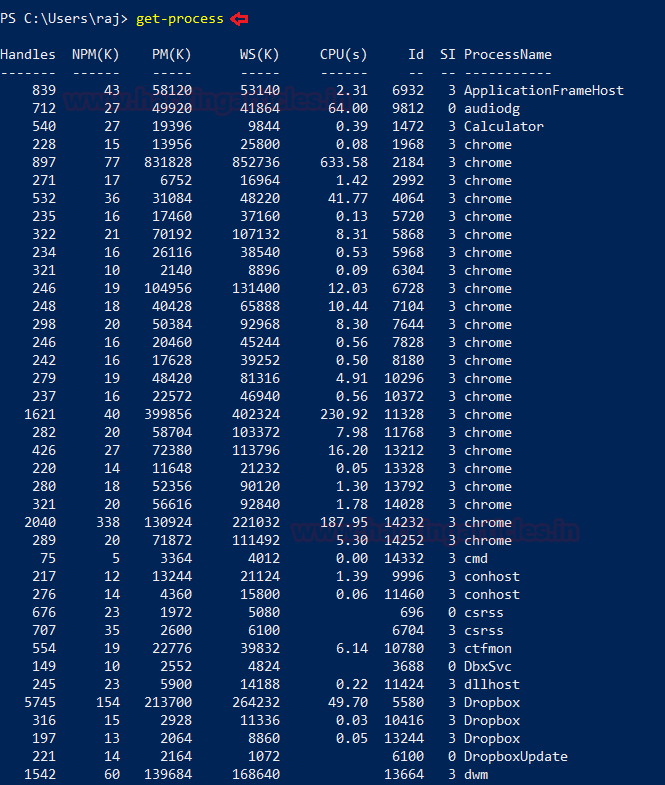
Si vous voulez une liste des processus en cours d'exécution avec leurs services associés dans l'invite de commande, exécutez l'invite de commande en tant qu'administrateur, puis tapez

>tasklist /svc



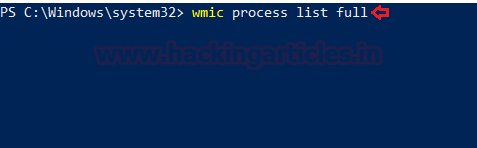
Pour obtenir une liste de tous les processus actifs en cours d'exécution sur la machine local, exécutez PowerShell en tant qu'administrateur et tapez

>get-process



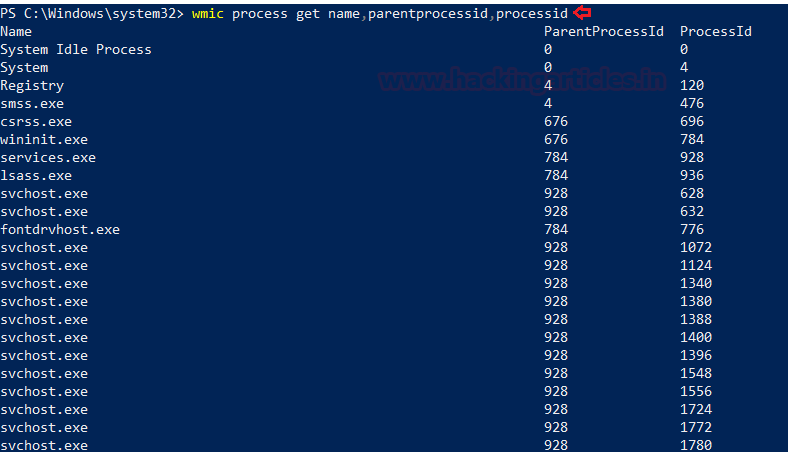
Le système Windows dispose d'un outil extrêmement puissant avec la commande Windows Management Instrumentation (WMIC). Wmic est très utile en matière de réponse aux incidents. Cet outil est suffisant pour remarquer certains signes anormaux dans le système. Cette commande peut être utilisée dans l'invite de commande ainsi que dans PowerShell lors de l'exécution en tant qu'administrateur.

>**wmic process list full**



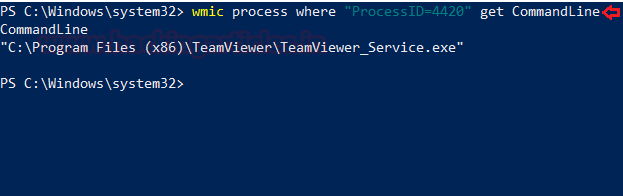
Pour obtenir plus de détails sur les **ID de processus parent, le nom du processus et l'ID de processus** , ouvrez PowerShell en tant qu'administrateur et tapez

>wmic process get name,parentprocessid,processid

****

Pour obtenir le chemin du processus avec Wmic, ouvrez PowerShell et tapez

>wmic process where 'ProcessID=PID’ get CommandLine



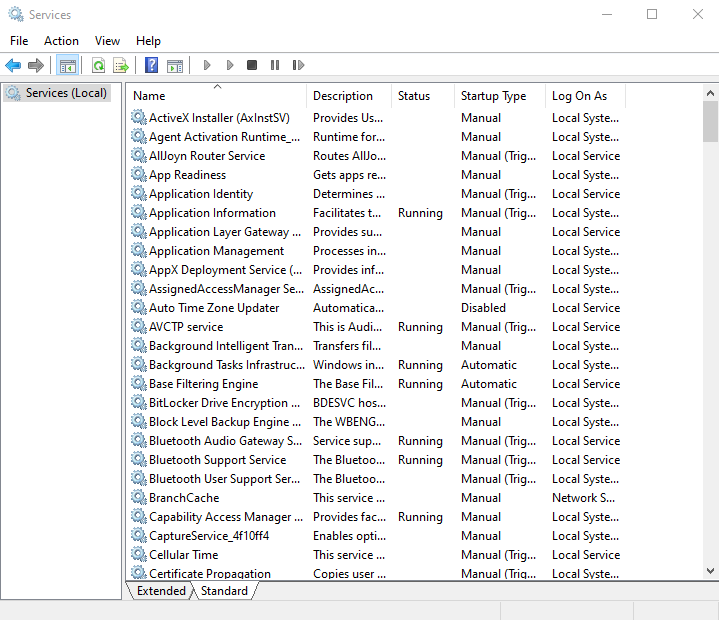
**ID service**

Pour identifier s'il y a un **service anormal en** cours d'exécution dans votre système ou si un service ne fonctionne pas correctement, vous pouvez afficher vos services.

Pour afficher tous les services dans l'interface graphique, appuyez sur ' **Windows + R** ' et tapez

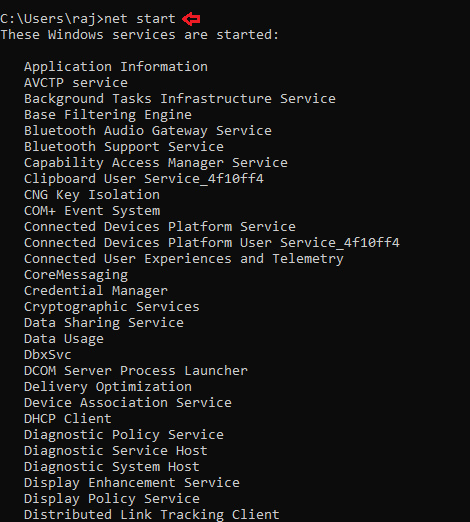
>services.msc

Cliquez maintenant sur ' **Ok** ' pour voir la liste des processus.



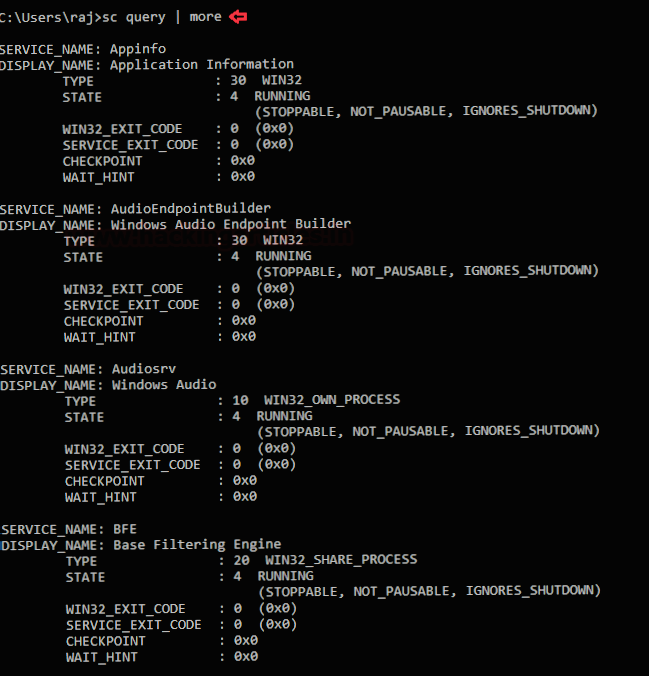
Pour démarrer et afficher la liste des services en cours d'exécution sur votre système, ouvrez l'invite de commande en tant qu'administrateur, tapez

>net start



Pour voir si un service est en cours d'exécution et pour obtenir plus de détails comme son nom de service, son nom d'affichage, etc.

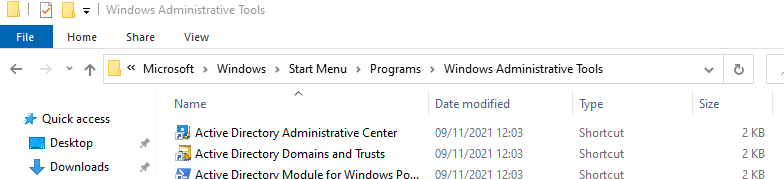
>sc query | more ***// need value??***



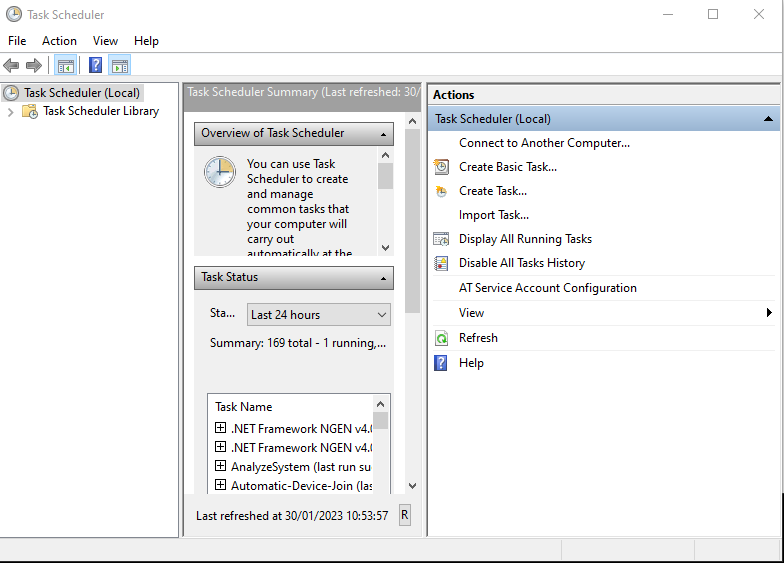
**Planificateur de tâches**

Le planificateur de tâches est un composant de Windows qui permet de programmer le lancement de programmes ou de tout script à une heure prédéfinie ou après des intervalles de temps spécifiés. Vous pouvez afficher ces tâches planifiées qui ont des privilèges élevés et semblent suspectes.

Pour afficher le planificateur de tâches dans l'interface graphique, accédez au chemin suviant  
  
**C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools**

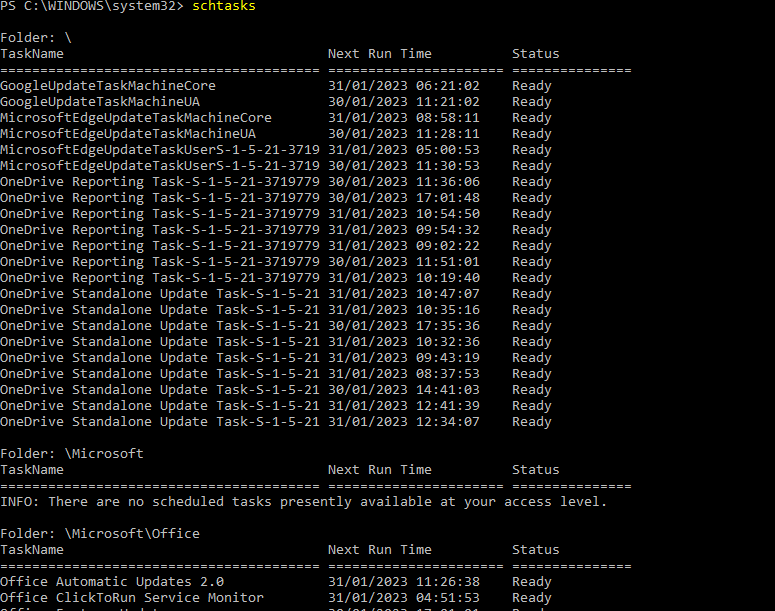
****

Vous pourrez voir en bas de page ‘Task Scheduler’.  
Ouvrez le.



Pour afficher les tâches planifiées dans l'invite de commande, exécutez l'invite de commande en tant qu'administrateur, tapez

>schtasks

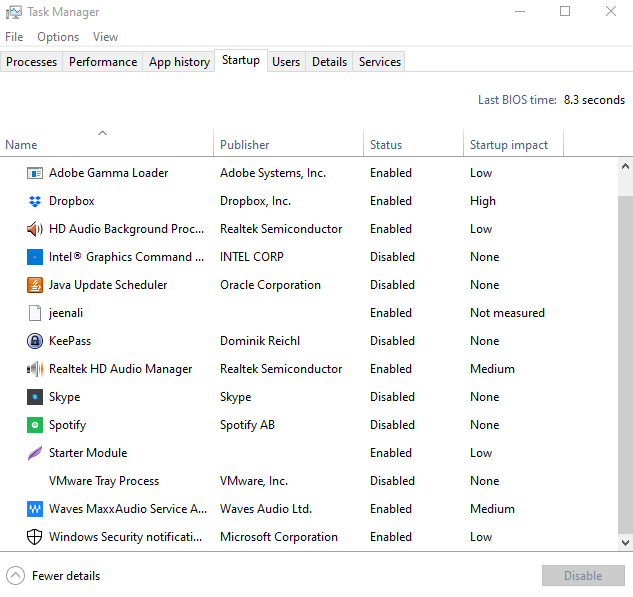


**Startup**

Le *Startup* dossier de *Windows* exécute automatiquement les applications lorsque vous vous connectez. Ainsi, en tant que gestionnaire d'incidents, vous devez observer les applications qui démarrent automatiquement.

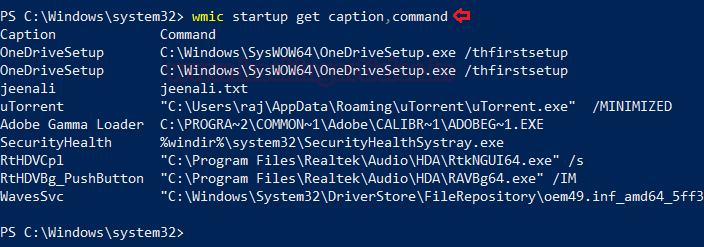
Pour afficher les applications dans le menu de démarrage de l'interface graphique, ouvrez le gestionnaire de tâches et cliquez sur le **' Startup**'. En faisant cela, vous pouvez voir quelles applications sont activées et désactivées au démarrage. En ouvrant le chemin suivant, il vous donnera la même option

>taskmgr



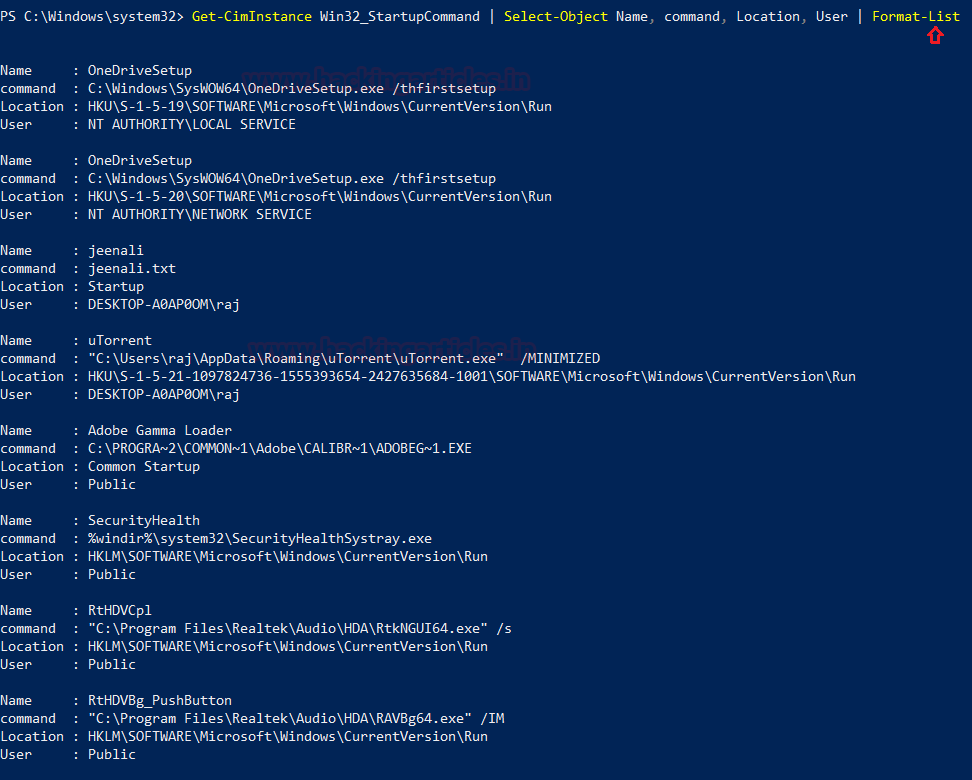
Pour afficher, les applications de démarrage dans le PowerShell exécutent le PowerShell en tant qu'administrateur, tapez

>wmic startup get caption,command



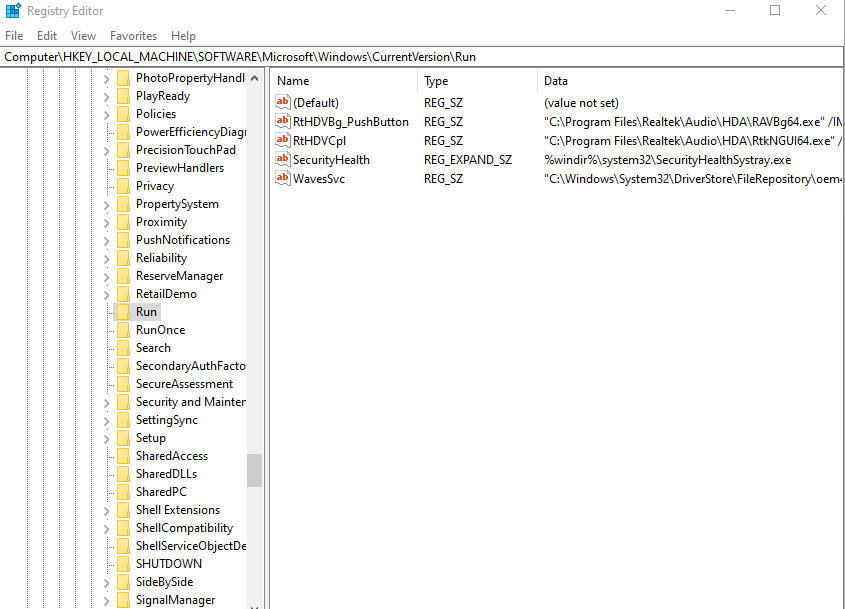
Pour obtenir une liste détaillée des applications AutoStart dans PowerShell, vous pouvez l'exécuter en tant qu'administrateur et saisir

> Get-CimInstance Win32\_StartupCommand | Select-Object Name, command, Location, User | Format-List



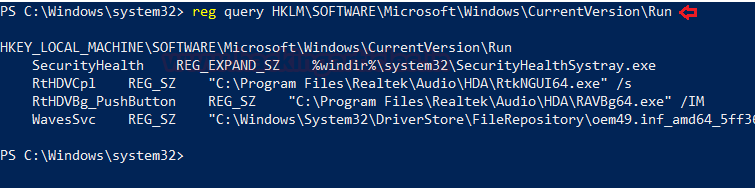
**Entrées de registre**

Parfois, s'il y a présence de logiciels malveillants non sophistiqués, vous pouvez les trouver en examinant la clé d'exécution du registre Windows. Pour afficher l'interface graphique de la clé de registre, vous pouvez ouvrir **REGEDIT et** accéder manuellement à la clé d'exécution.



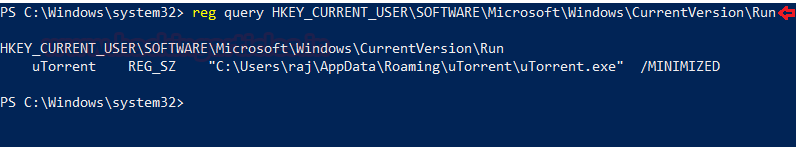
Vous pouvez également afficher le registre de la machine locale de la Run Key dans le PowerShell, en l'exécutant en tant qu'administrateur, puis en tapant

>reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

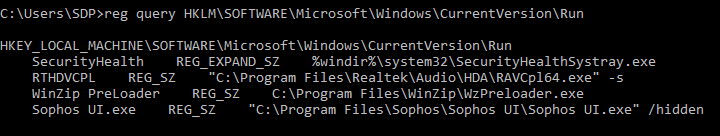


Vous pouvez également afficher le registre de l'utilisateur actuel de la Run Key dans le PowerShell, en l'exécutant en tant qu'administrateur, puis en tapant

>reg query HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



>reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

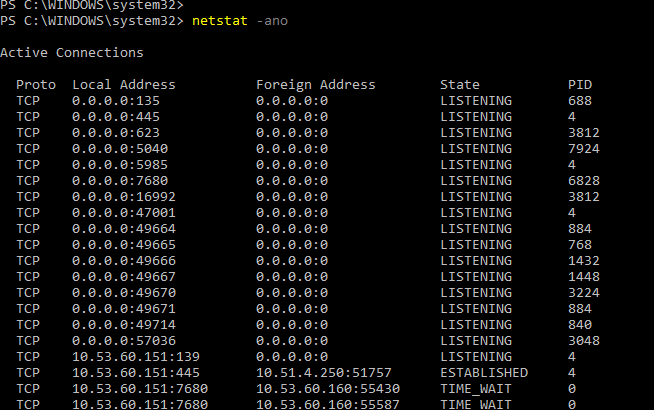


**Ports TCP et UDP actifs**

En tant que répondant aux incidents, vous devez prêter une attention particulière aux ports TCP et UDP actifs de votre système.

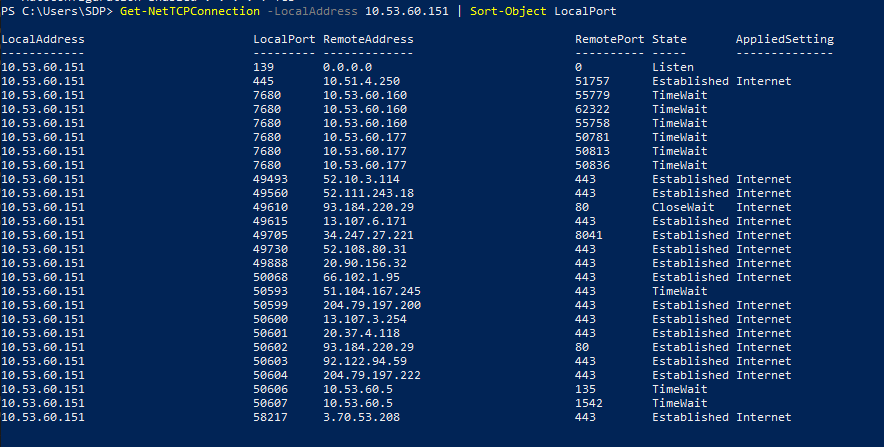
Les statistiques réseau d'un système peuvent être analysées à l'aide d'un outil. Les critères testés sont les connexions entrantes et sortantes, les tables de routage, l'écoute des ports et les statistiques d'utilisation. Ouvrez l'invite de commande, tapez

>netstat -ano



Eh bien, cela peut également être vérifié dans PowerShell avec une commande différente pour voir l'adresse IP et les ports locaux. Exécutez PowerShell et tapez

>Get-NetTCPConnection -LocalAddress “IP Local” | Sort-Object LocalPort

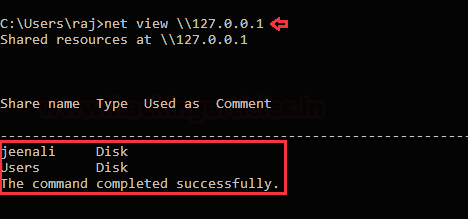


**Partage de fichiers**

En tant qu'intervenant en cas d'incident, vous devez vous assurer que chaque partage de fichiers est responsable et raisonnable et qu'il n'y a pas de partage de fichiers inutile.

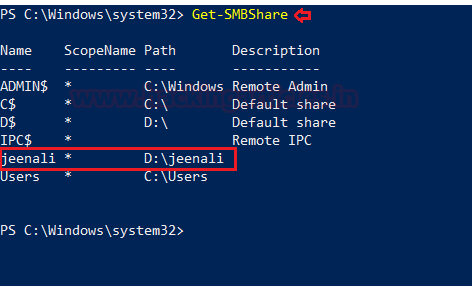
Pour vérifier les options de partage de fichiers dans l'invite de commande, tapez

>net view \\<localhost>’



Pour voir le partage de fichiers dans PowerShell, vous pouvez taper

>Get-SMBShare

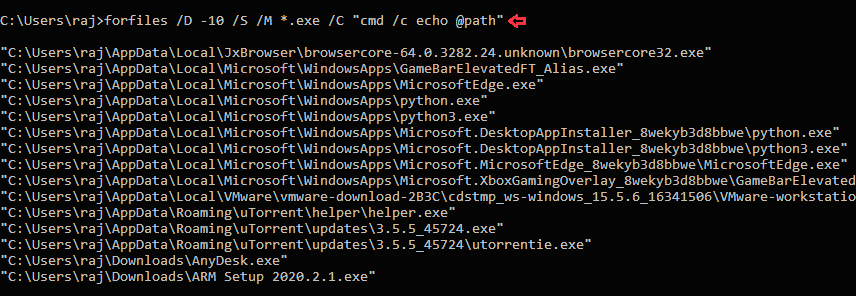


**Des dossiers**

Pour afficher les fichiers qui pourraient être malveillants ou se terminer par une extension particulière, vous pouvez utiliser la commande 'forfiles'. Forfiles est un logiciel utilitaire en ligne de commande. Il a été livré avec Microsoft Windows Vista. Pendant ce temps, la gestion de plusieurs fichiers via la ligne de commande était difficile car la plupart des commandes de l'époque étaient conçues pour fonctionner sur des fichiers uniques.

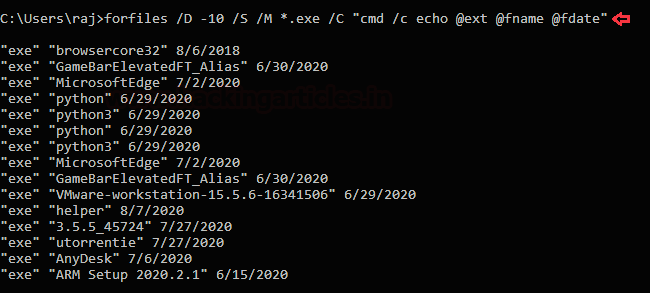
Pour afficher les fichiers .exe avec leur chemin pour les localiser dans l'invite de commande, tapez

>forfiles /D -10 /S /M \*.exe /C "cmd /c echo @path"



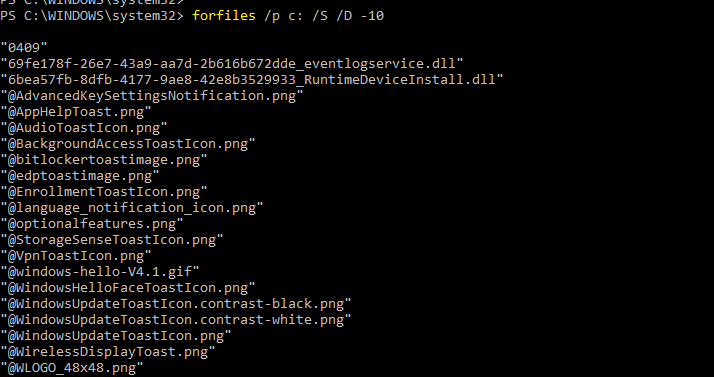
Pour afficher les fichiers sans son chemin et plus de détails sur l'extension de fichier particulière et sa date de modification, tapez

>forfiles /D -10 /S /M \*.exe /C "cmd /c echo @ext @fname @fdate"



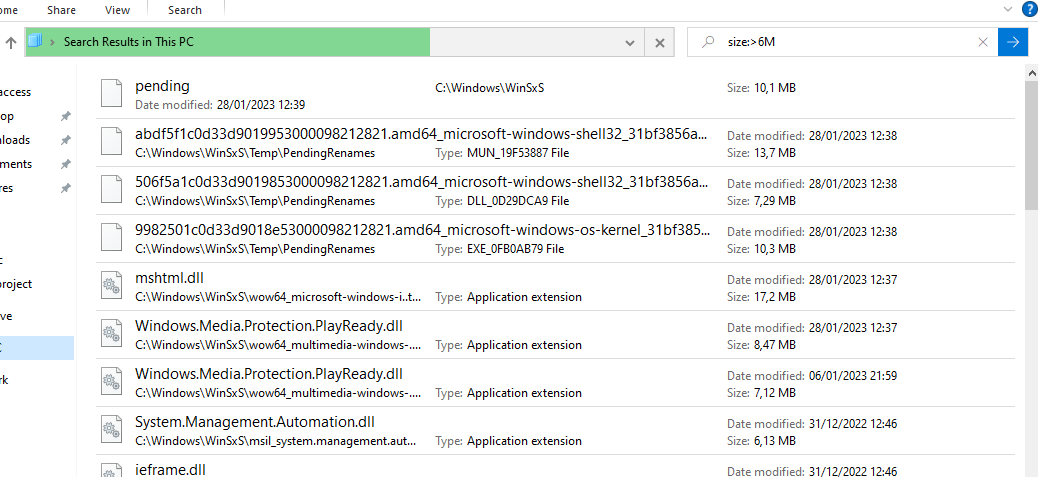
Pour vérifier les fichiers modifiés au cours des 10 derniers jours, tapez

>forfiles /p c: /S /D -10



Pour vérifier la taille du fichier en dessous de 6 Mo, vous pouvez utiliser la zone de recherche de l'explorateur de fichiers et entrer

size:>6M

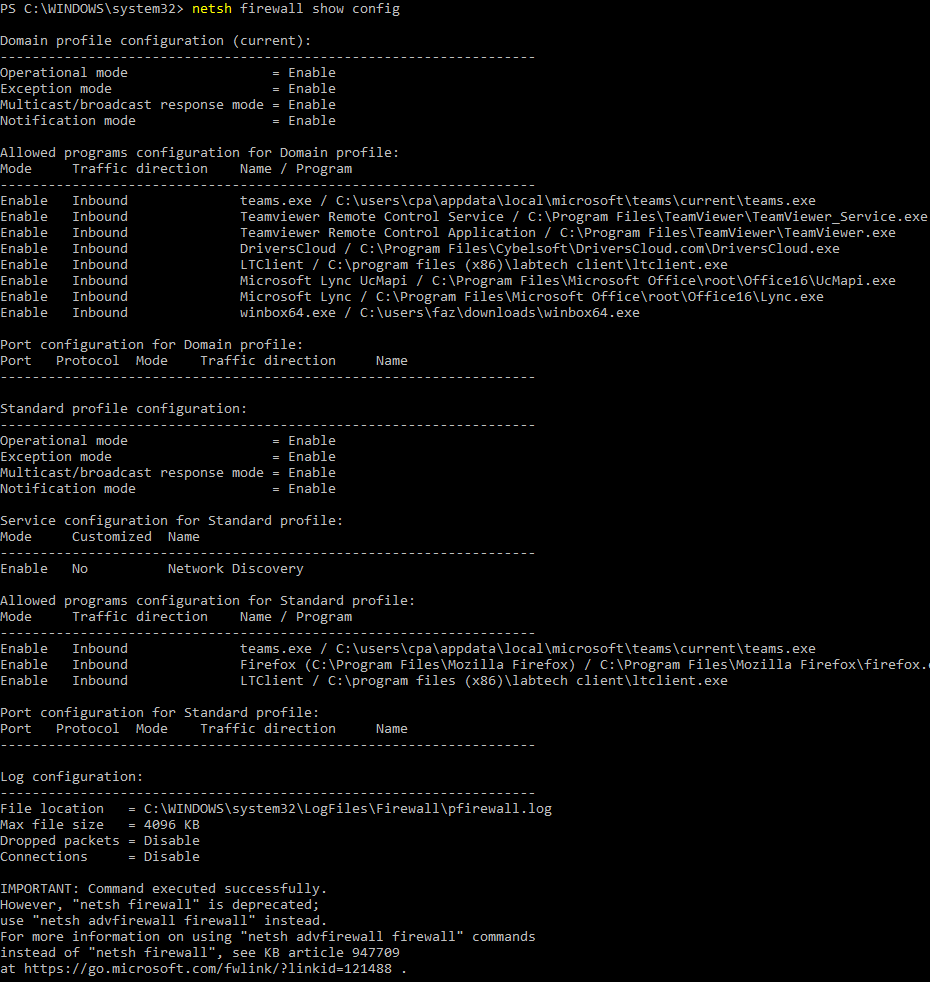


**Paramètres du pare-feu**

L'intervenant en cas d'incident doit prêter attention aux configurations et aux paramètres du pare-feu et doit le maintenir régulièrement.

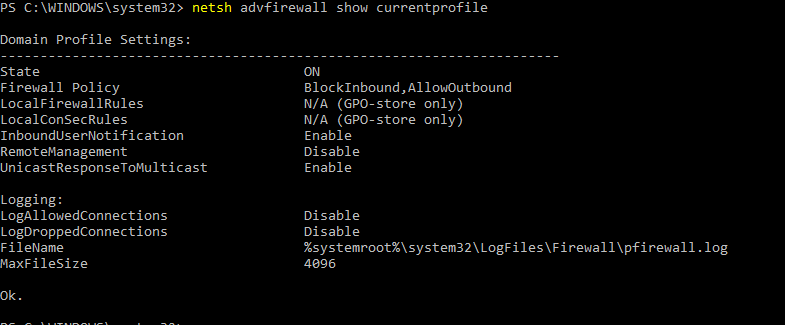
Pour afficher les configurations de pare-feu et le trafic entrant et sortant dans l'invite de commande, tapez

>netsh firewall show config



Pour afficher les paramètres de pare-feu du profil actuel dans l'invite de commande, tapez

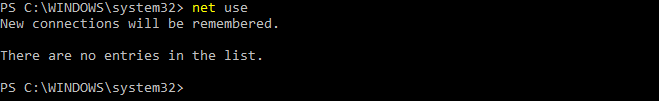
>netsh advfirewall show currentprofile



**Sessions**

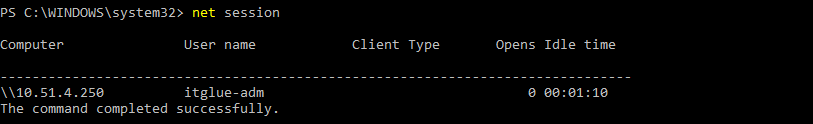
Pour vérifier les détails de la session créé avec d'autres systèmes, vous pouvez exécuter l'invite de commande et taper

>net use



Pour voir toutes les sessions ouvertes de votre système, vous pouvez obtenir des détails sur la durée de la session, exécutez l'invite de commande et tapez

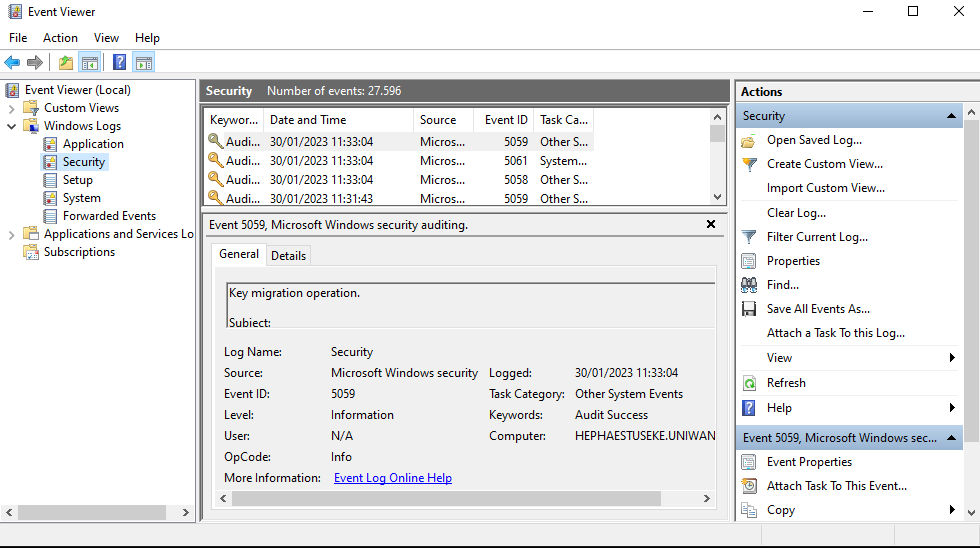
 >net session



**Entrées des journaux**

Pour afficher les entrées de journaux dans l'interface graphique, vous pouvez ouvrir l'observateur d'événements et consulter les journaux. Appuyez sur ' **Windows+ R'** et tapez

>eventvwr.msc

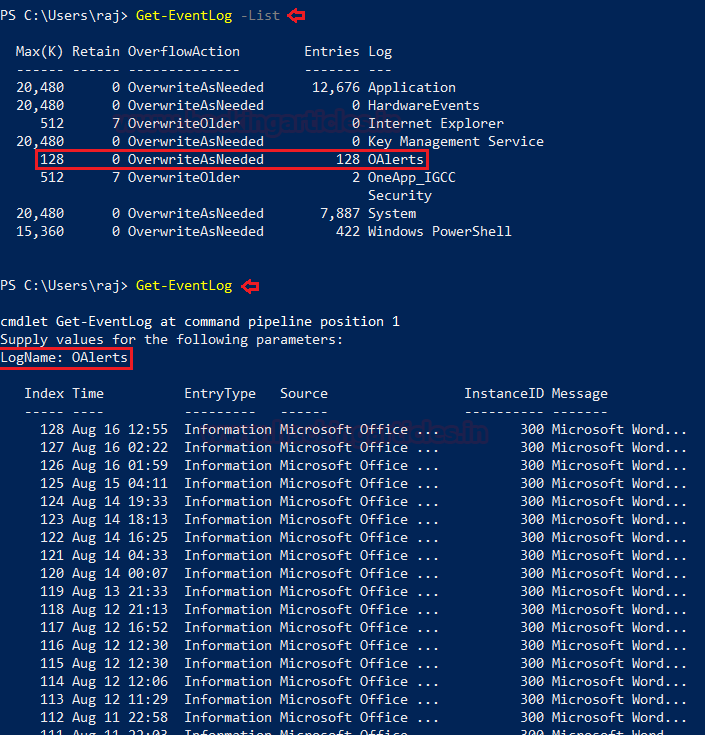


Pour exporter certains journaux d'un événement particulier dans le type d'invite de commande

>wevtutil qe security ***// Voir la réponse… ?***

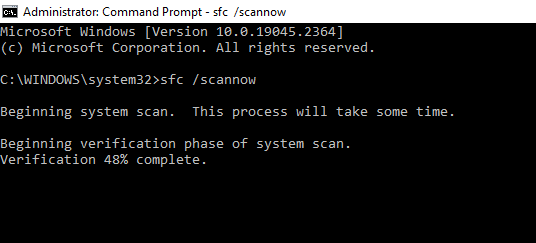
Pour obtenir la liste des journaux d'événements dans le PowerShell, tapez

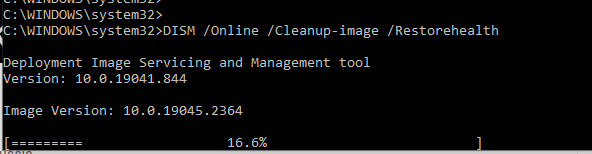
>Get-EventLog -List



Et tapez l'événement particulier dans la valeur de l'offre et vous obtiendrez les détails de l'événement de cet événement particulier.

Pour conrôler l’intégrité de vos fichiers système, vous pouvez utilisez cette commande

>sfc /scannow  
  


**DISM : réparer les fichiers systems  
  
>DISM /Online /Cleanup-image /Restorehealth  
  
**