Recuperación PowerShell→Jesús Padilla Crespo

1.hacer un script que pida un nombre de servicio(get-service nos permite mostrar todos).se debe comprobar que ese servicio existe y en caso contrario debe volver a pedirlo. Si el proceso está parado debe preguntar si se quiere iniciar y si está iniciado debe preguntar si se quiere parar.

```
do
{
    $nombre = Read-Host "Dime el nombre de un servicio"
    $compservicio = (Get-Service -name $nombre -ErrorAction
SilentlyContinue).count

    if ($compservicio -ne 0)
    {
        $compstatus = (Get-Service -Name $nombre).Status

        if ($compstatus -eq "Stopped")
        {
            $parado = Read-Host "Este proceso se encuentra parado. ¿Desea
iniciarlo? Pulsa Y para iniciarlo y N para no iniciarlo"
            switch ($parado)
            {
                "Y" { Write-Host "Iniciando programa..."
                    Start-Service -Name $nombre}
                "N"{Write-Host "No se han realizado modificaciones"}

            }
        }
        else
        {
          $iniciado = Read-Host "Este proceso se encuentra iniciado. ¿Desea
pararlo? Pulsa Y para pararlo y N para no pararlo"
          switch ($iniciado)
            {
                "Y" {Write-Host "Cerrando programa..."
                    Stop-Service -Name $nombre}
                "N"{Write-Host "No se han realizado modificaciones"}

            }
        }
    }
    else
    {
        Write-Host "No existe ningún proceso con este nombre. Vuelva a
intentarlo"
    }
} while ($compservicio -eq 0)
```

Haré la comprobación con “ALG”

```
PS C:\Windows\system32> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_10d5dc      Agent Activation Runtime_10d5dc
Stopped  AJRouter           Servicio de enrutador de AllJoyn
Stopped  ALG                Servicio de puerta de enlace de niv...
Stopped  AppIDSvc           Identidad de aplicación
Running  Appinfo            Información de la aplicación
```

```
PS C:\Windows\system32> C:\Users\asir27\Desktop\script1.ps1
Dime el nombre de un servicio: ALG
Este proceso se encuentra parado. ¿Desea iniciarlo? Pulsa Y para iniciarlo y N para no iniciarlo: Y
Iniciando programa...
```

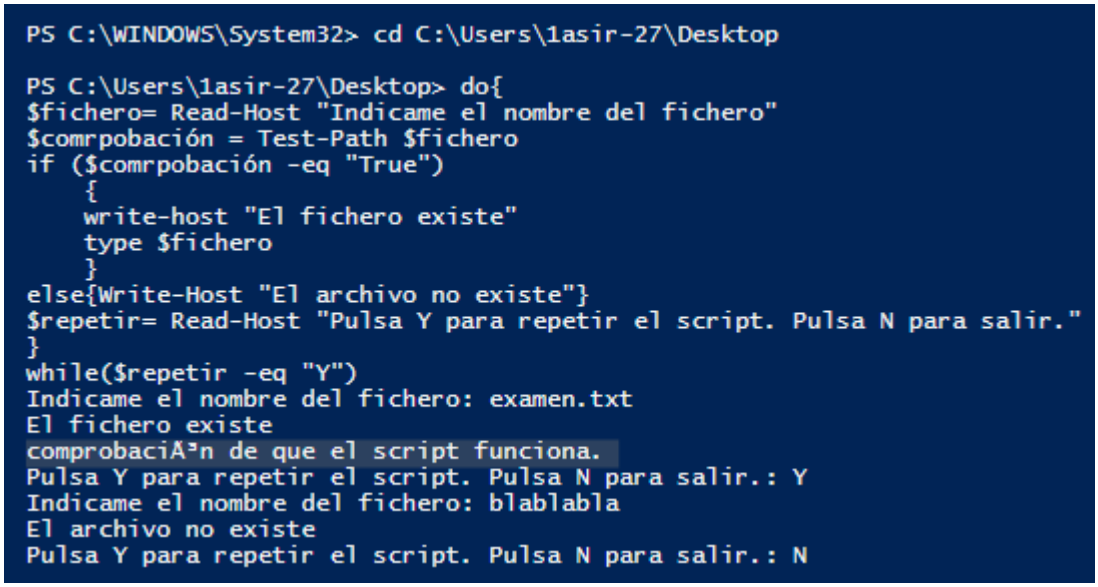
```
PS C:\Windows\system32> get-service

Status   Name               DisplayName
------   ----               -----------
Stopped  AarSvc_10d5dc      Agent Activation Runtime_10d5dc
Stopped  AJRouter           Servicio de enrutador de AllJoyn
Running  ALG                Servicio de puerta de enlace de niv...
```

```
PS C:\Windows\system32> C:\Users\asir27\Desktop\script1.ps1
Dime el nombre de un servicio: ALG
Este proceso se encuentra iniciado. ¿Desea pararlo? Pulsa Y para pararlo y N para no pararlo: Y
Cerrando programa...
```

2.Hacer un script que nos pida el nombre de un fichero y nos muestre el contenido de u fichero en caso de existir o bien nos diga que no existe.Antes de acabar debe pregun tarnos si deseamos volver a ejecutar el script y hacerlo en caso afirmativo.

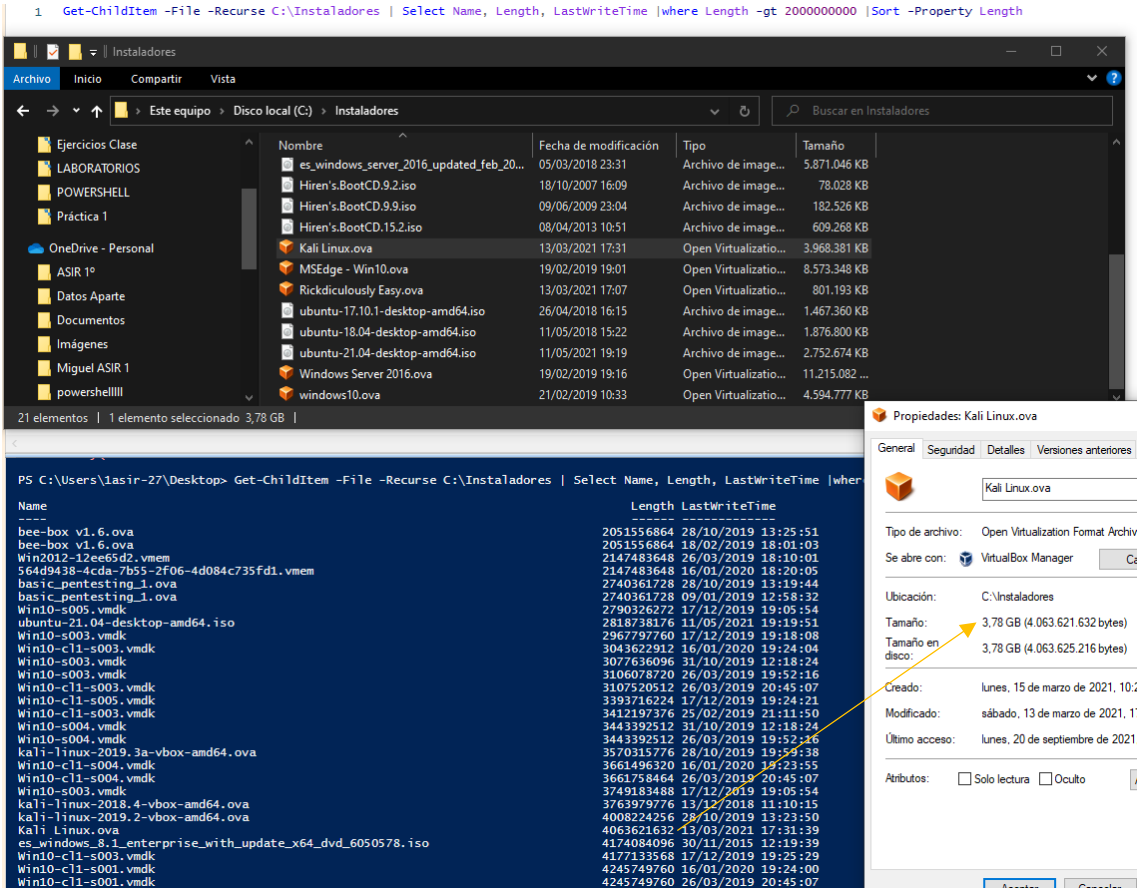
```
do{
$fichero= Read-Host "Indícame el nombre del fichero"
$comrpobación = Test-Path $fichero
if ($comrpobación -eq "True")
    {
    write-host "El fichero existe"
    type $fichero
    }
else{Write-Host "El archivo no existe"}
$repetir= Read-Host "Pulsa Y para repetir el script. Pulsa N para salir."
}
while($repetir -eq "Y")
```



3. Obtener el nombre, tamaño y fecha (en ese orden) de todos los ficheros del directorio “C:\Instaladores” y sus subdirectorios que tengan más de 2GB de ordenados por tamaño.

```
Get-ChildItem -File -Recurse C:\Instaladores | Select Name, Length,
LastWriteTime |where Length -gt 2000000000 |Sort -Property Length
```

Haremos la comprobación de que coincide el tamaño. Usaré “Kali-Linux.ova”



Coincide.

4. Obtén los usuarios del sistema que hayan iniciado sesión alguna vez.

Primero, he realizado un Get-LocalUser| Format-List para ver la propiedad “LastLogon”.

Todos aquellos que tengan una fecha en ese apartado serán los que necesito sacar en el listado.En este caso solo sería:

```
PS C:\Users\1asir-27\Desktop> Get-LocalUser| Format-list


AccountExpires         :
Description            : Cuenta integrada para la administración del equipo o dominio
Enabled                : True
FullName               :
PasswordChangeableDate : 09/05/2018 12:26:09
PasswordExpires        :
UserMayChangePassword  : True
PasswordRequired       : True
PasswordLastSet        : 08/05/2018 12:26:09
LastLogon              : 03/09/2020 10:17:17
Name                   : Administrador
SID                    : S-1-5-21-1125474266-2925866343-2985468450-500
PrincipalSource        : Local
ObjectClass            : Usuario

AccountExpires         :
Description            : Cuenta de usuario administrada por el sistema.
Enabled                : False
FullName               :
PasswordChangeableDate :
PasswordExpires        :
UserMayChangePassword  : True
PasswordRequired       : False
PasswordLastSet        :
LastLogon              :
Name                   : DefaultAccount
SID                    : S-1-5-21-1125474266-2925866343-2985468450-503
PrincipalSource        : Local
ObjectClass            : Usuario

AccountExpires         :
Description            : Cuenta integrada para el acceso como invitado al equipo o dominio
Enabled                : False
FullName               :
PasswordChangeableDate :
PasswordExpires        :
UserMayChangePassword  : False
PasswordRequired       : False
PasswordLastSet        :
LastLogon              :
Name                   : Invitado
SID                    : S-1-5-21-1125474266-2925866343-2985468450-501
PrincipalSource        : Local
ObjectClass            : Usuario

AccountExpires         :
Description            : Una cuenta de usuario que el sistema administra y usa para escenarios de Protección de aplicaciones de Windows Defender.
Enabled                : False
FullName               :
PasswordChangeableDate : 05/04/2018 16:15:52
PasswordExpires        : 01/10/2018 16:15:52
UserMayChangePassword  : True
PasswordRequired       : True
PasswordLastSet        : 04/04/2018 16:15:52
LastLogon              :
Name                   : WDAGUtilityAccount
SID                    : S-1-5-21-1125474266-2925866343-2985468450-504
PrincipalSource        : Local
ObjectClass            : Usuario
```

```
Get-LocalUser|where LastLogon -gt 01/01/1900
```

```
PS C:\Users\1asir-27\Desktop> Get-LocalUser|where lastlogon -gt 01/01/1900

Name           Enabled Description
----           ------- -----------
Administrador True    Cuenta integrada para la administración del equipo o dominio
```