Etat des lieux d'un service Windows

> Listage de l'état d'un service sur l'ensemble des serveurs Windows d'un domaine
> Le compte de la machine ne doit pas être désactivé et il doit répondre au ping
> Dans ce cas, il s'agit du service 'spooler'

```
# Autor : JHAF

# Service à check
$Service = 'spooler'

# Horadatage pour CSV
$DateJour = Get-Date -Uformat %Y%m%d_%H%m

# Initialisation des variables en Array
$Report = @()
$Spoolers = @()

# Liste des serveurs Windows avec une compte actif
$Servers = Get-ADOrganizationalUnit -Filter * | ForEach-Object { Get-ADComputer -Filter 'operatingSystem -like
"*Windows Server*" -and userAccountControl -notlike "4098"' -SearchBase "$_" -SearchScope OneLevel } |
Select-Object DNSHostName, Name, SID
#$Servers | Out-GridView

# Test si les serveurs sont UP
foreach($Server in $Servers){

    $pingtest = Test-Connection -ComputerName $Server.DNSHostName -Quiet -Count 1 -ErrorAction
SilentlyContinue
    if($pingtest){
        #Write-Host $Server.DNSHostName " is reachable"
```

```
        $Spoolers += Get-ADComputer -Identity $Server.Name | Select-Object DNSHostName, Name, SID
    }
    else{
        #Write-Host $Server.DNSHostName " is not reachable"
    }

}
#$Spoolers | Out-GridView

# Récupération des infos du service Spooler pour chaque serveur UP
foreach ($Spooler in $Spoolers) {
    $Status = Get-Service -ComputerName $Spooler.Name -Name $Service | Select-Object MachineName, Name, Status
    $Startup = Get-WmiObject -Computer $Spooler.Name -Class Win32_Service -Property StartMode -Filter "Name='$Service'"
    $Report += [PSCustomObject]@{
        MachineName = $Status.MachineName
        Name        = $Status.Name
        Status      = $Status.Status
        StartMode   = $Startup.StartMode
    }
}
$Report | Out-GridView
#$Report | Export-Csv -Path C:\script\Audit\2022\1032\${DateJour}_Get-Spooler_Status.csv -NoTypeInformation -Encoding UTF8 -Delimiter ';'
```

Arrêt puis désactivation du démarrage auto d'un service sur l'ensemble des machines Windows listé dans un CSV
WinRM doit fonctionner depuis la machine qui lance le script (notamment les flux RPC doivent être ouverts)
Dans ce cas, il s'agit du service 'spooler'

```
# Horadatage pour CSV
$DateJour = Get-Date -Uformat %Y%m%d_%H%m

# Service à stop et check
$Service = 'spooler'
```

```
# Initialisation des variables en Array
$Report = @()

# Fichier CSV à faire à la main pour import
$SpoolersStop = Import-Csv C:\script\Audit\2022\1032\Stop-Spoolers.csv -Delimiter ';'

# Arrêt du service et Désactivation du démarrage auto
foreach ($Spooler in $SpoolersStop) {
    Get-Service -ComputerName $Spooler.MachineName -Name "spooler" | Stop-Service
    Set-Service -Computer $Spooler.MachineName -Name "spooler" -StartupType "Disabled"
}

# Récupération des infos du service Spooler pour chaque serveur UP
foreach ($Spooler in $Spoolers) {
    $Status = Get-Service -ComputerName $Spooler.Name -Name $Service | Select-Object MachineName, Name,
Status
    $Startup = Get-WmiObject -Computer $Spooler.Name -Class Win32_Service -Property StartMode -Filter
"Name='$Service'"
    $Report += [PSCustomObject]@{
        MachineName = $Status.MachineName
        Name        = $Status.Name
        Status      = $Status.Status
        StartMode   = $Startup.StartMode
    }
}
#$Report | Out-GridView
$Report | Export-Csv -Path C:\script\Audit\2022\1032\${DateJour}_Stop-Spoolers_Check.csv -NoTypeInformation
-Encoding UTF8 -Delimiter ';'
```

Revision #4
Created 31 October 2024 16:25:13 by Cavallone
Updated 20 November 2024 19:51:50 by Cavallone