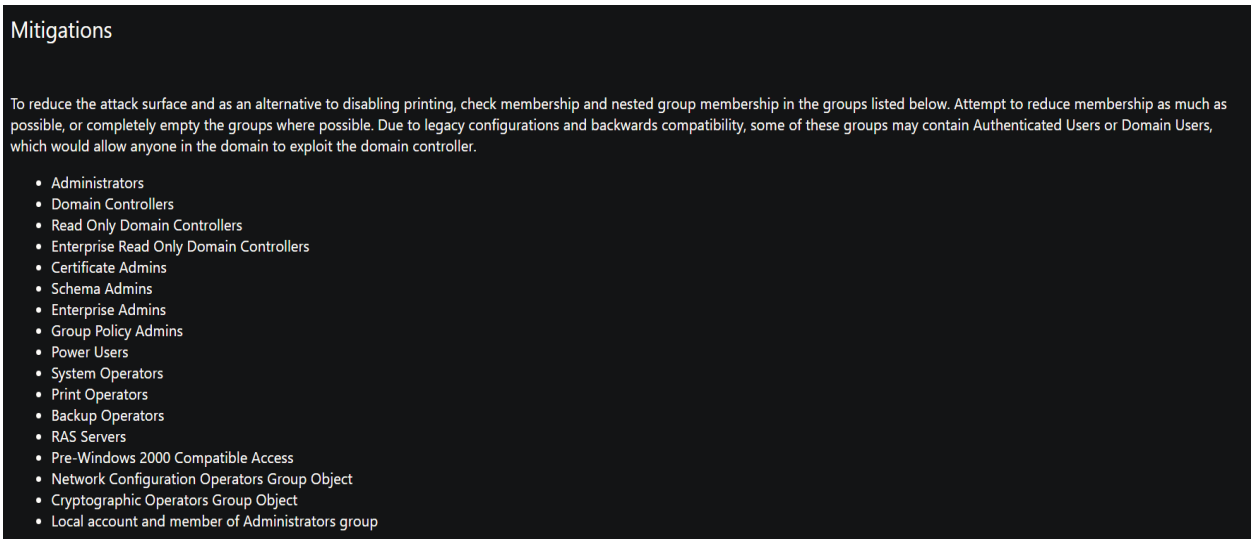
Fix Print Spooler Vulnerability using CB2103

In this post, I am going to use the script shared by MVP to fix above issue with DC and Print Servers within the lab. Microsoft recently shared the info about Print Spooler vulnerability via CVE 2021 34527 – https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527 -



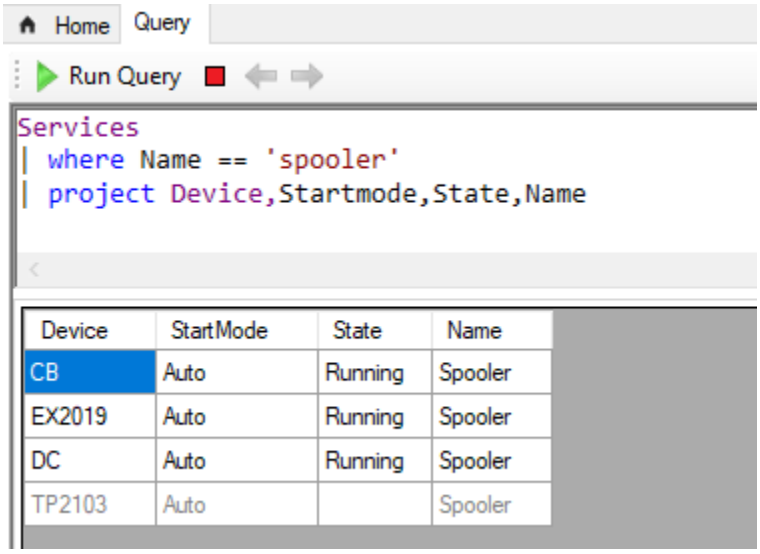
To mitigate, I am going to use the script. Following will the action plan:

1. Identify systems running print spooler using CMPivot
2. Stop and Disable print spooler service using new script
3. Enabling print spooler at Startup – if you need this to be running

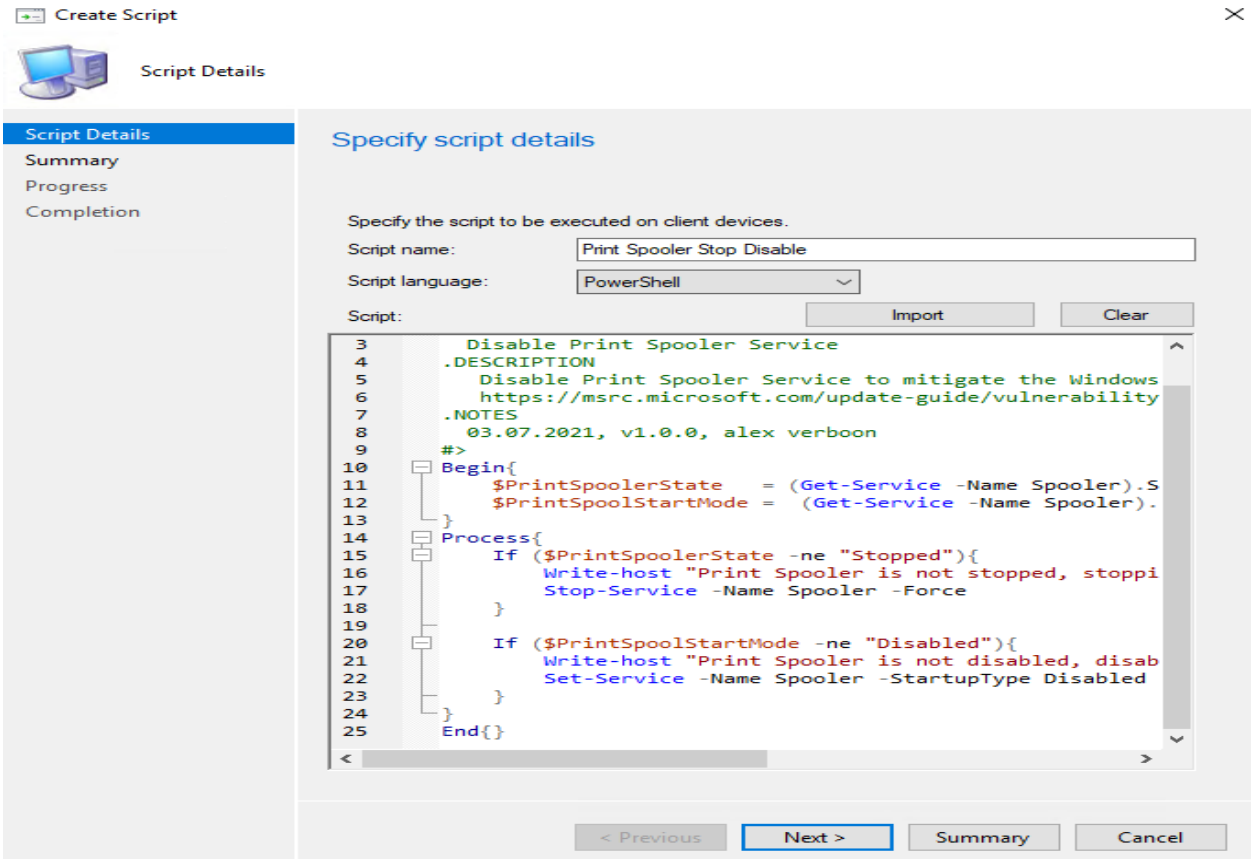
Identify the system running print spooler - Open the Console – Device Collections – Start CMPivot and run this script. I have 4 systems running print spooler service.

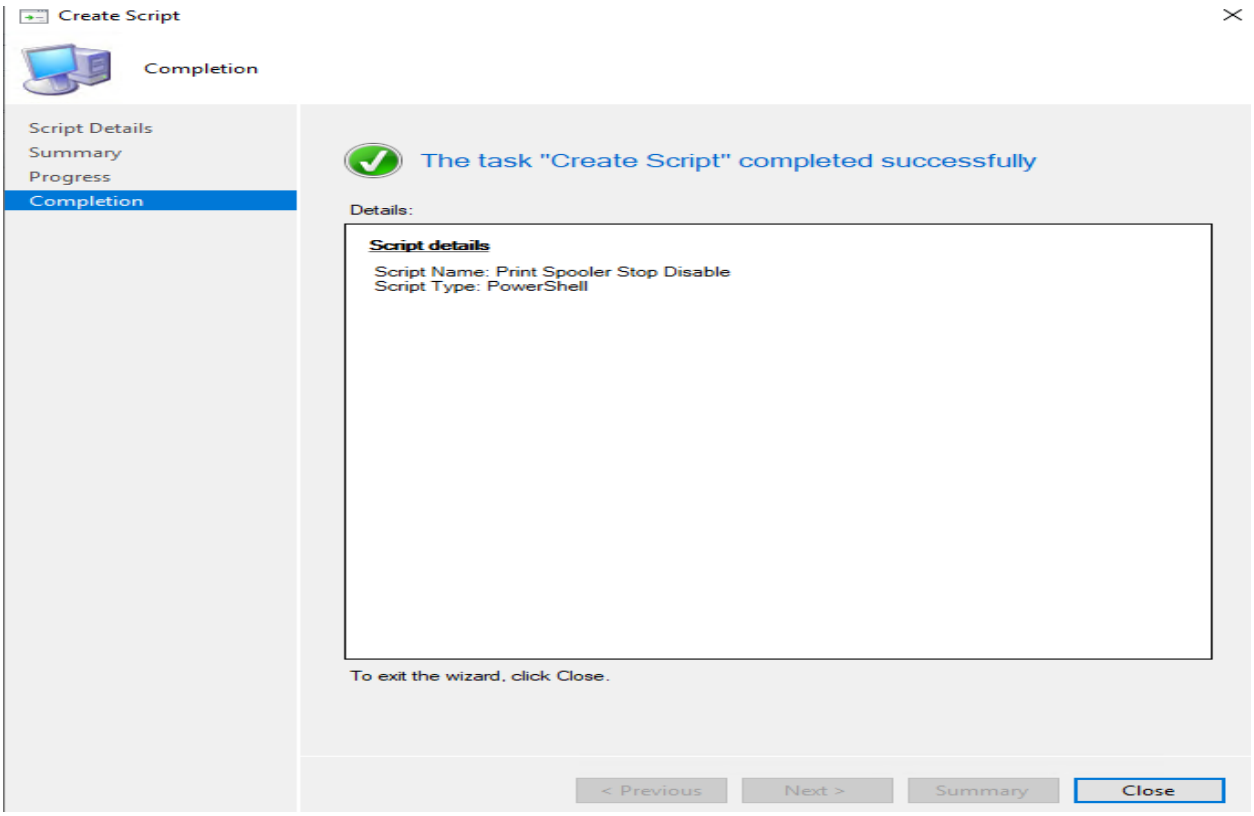
Services

| where Name == 'spooler'
| project Device,Startmode,State,Name

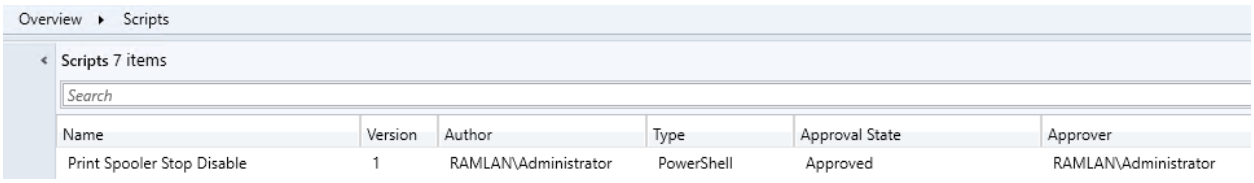


Stop and Disable spooler service – Open Console – Go to Software Library – Scripts – Create Script

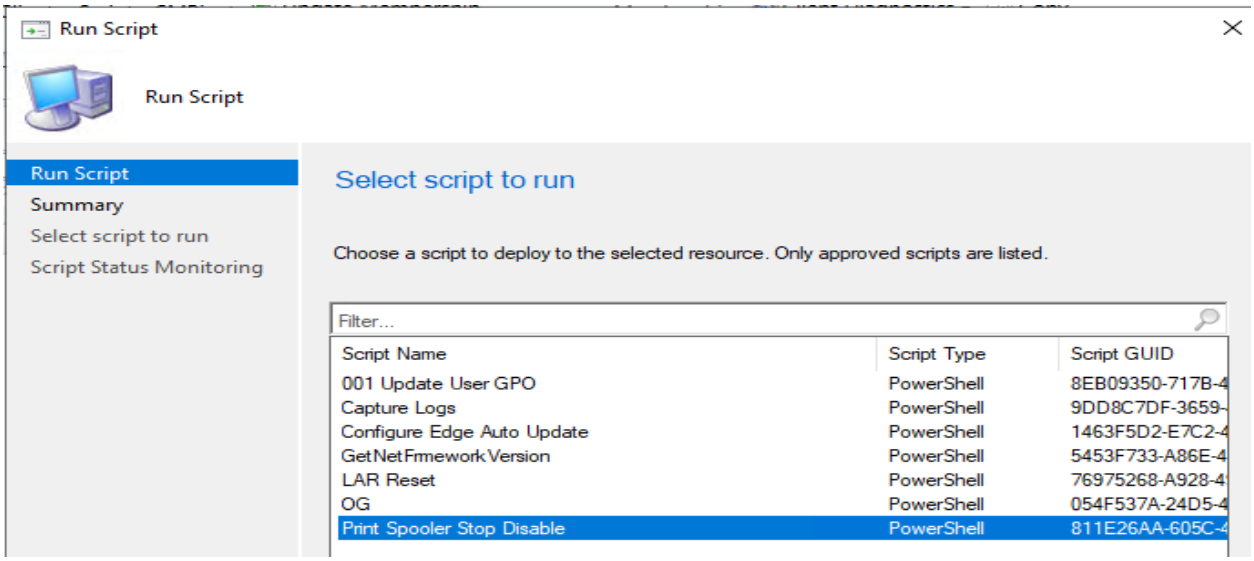


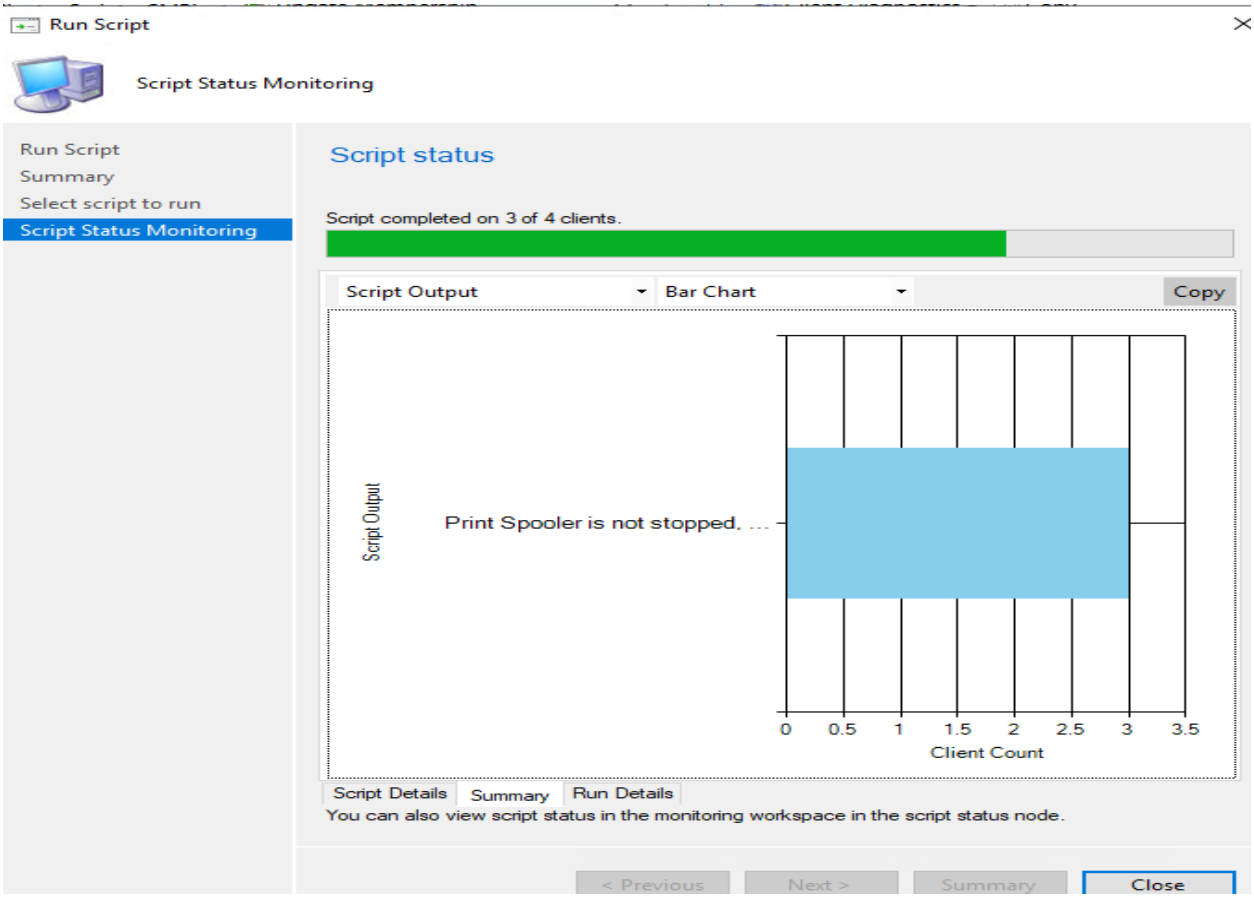


Approve the script and run it.

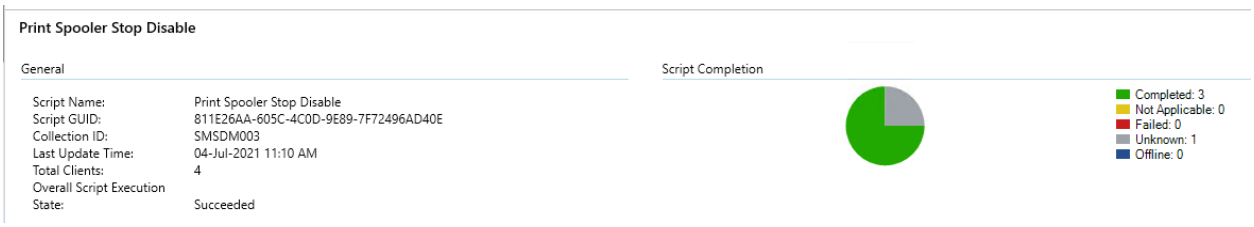


We are ready to run the script for device collections – Go to Device Collections – Run Script

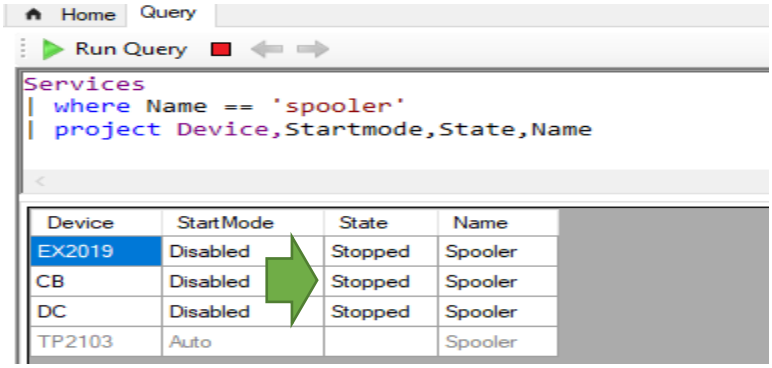




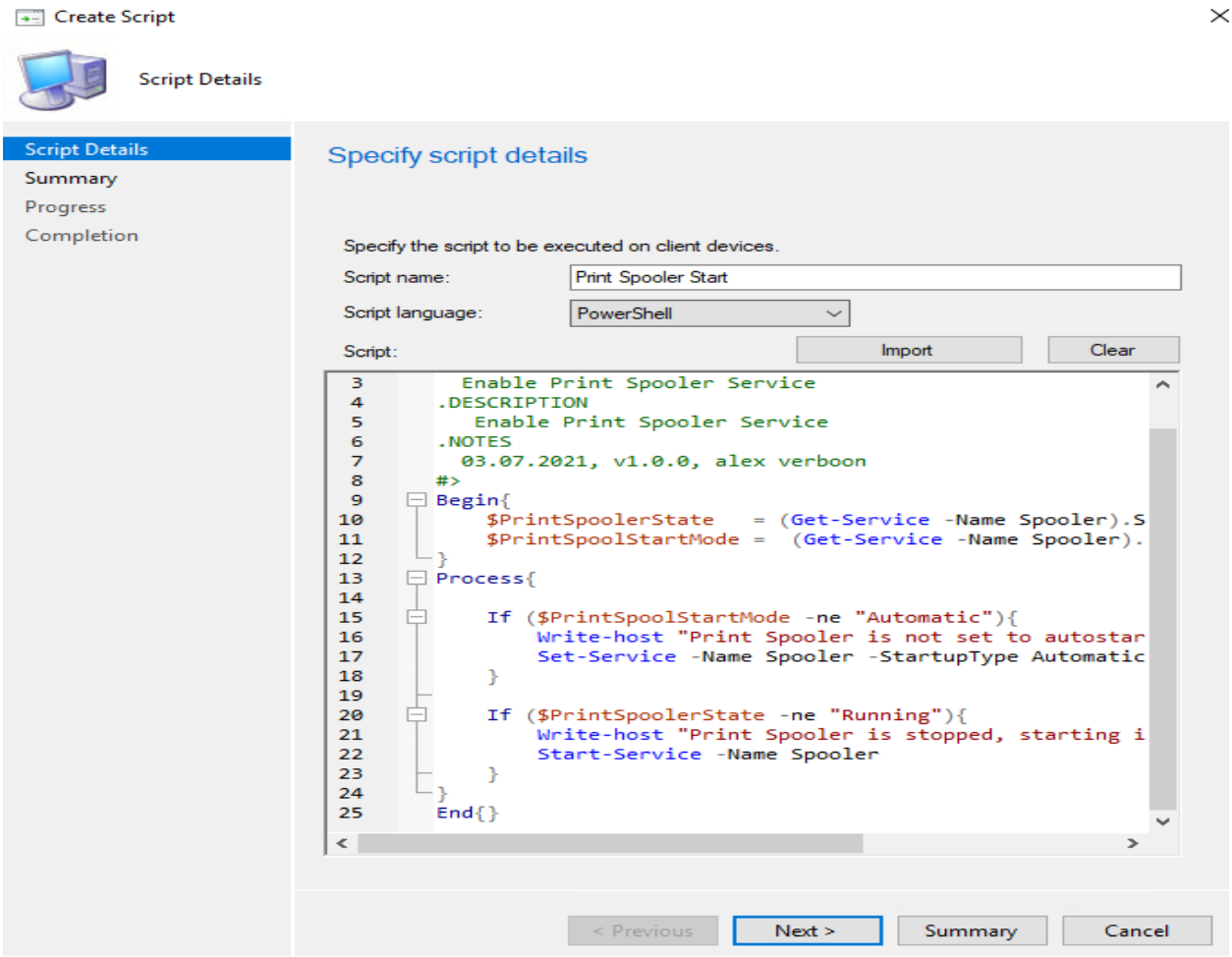
You can check the status under Monitoring – Script Status

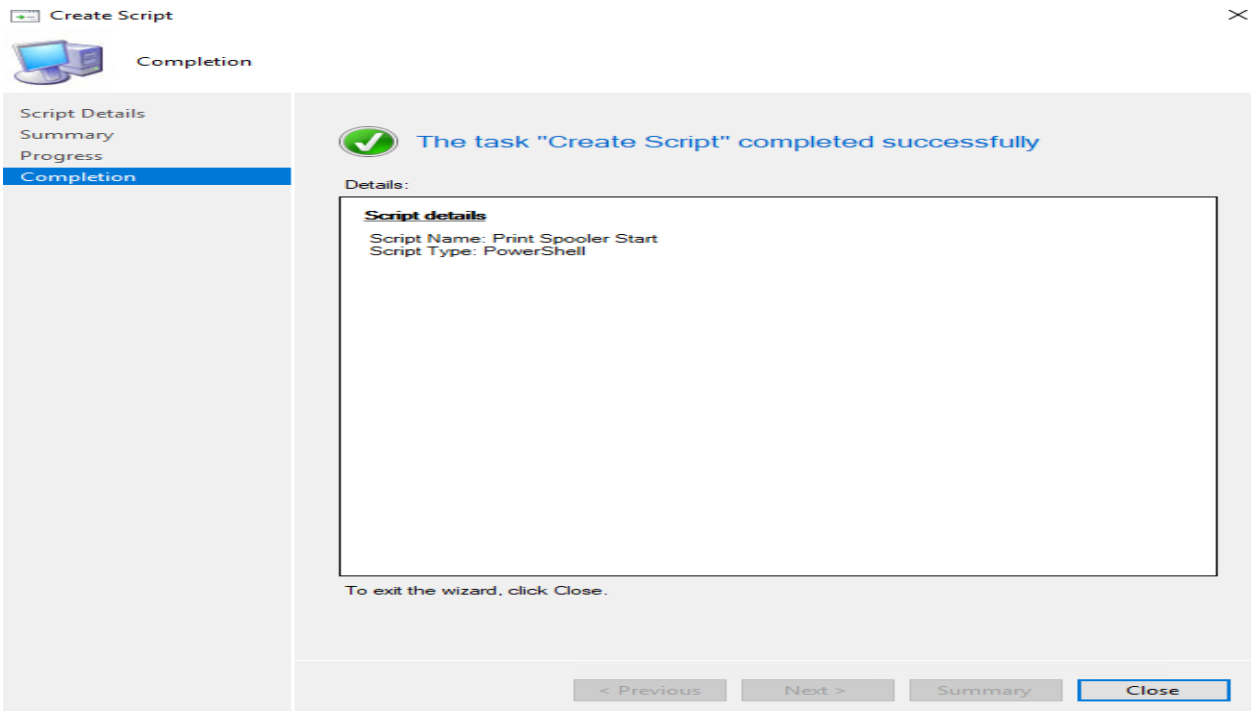


Now check the status again – Device Collection – CMPivot – The spooler is stopped

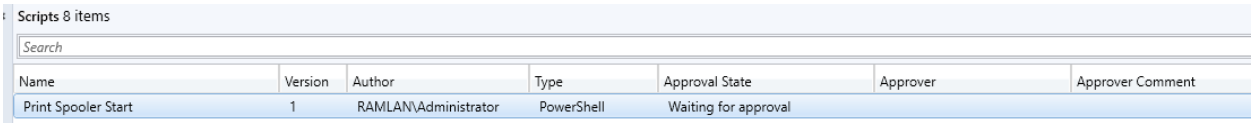


If you want to rollback and want spooler to be running. Use this script

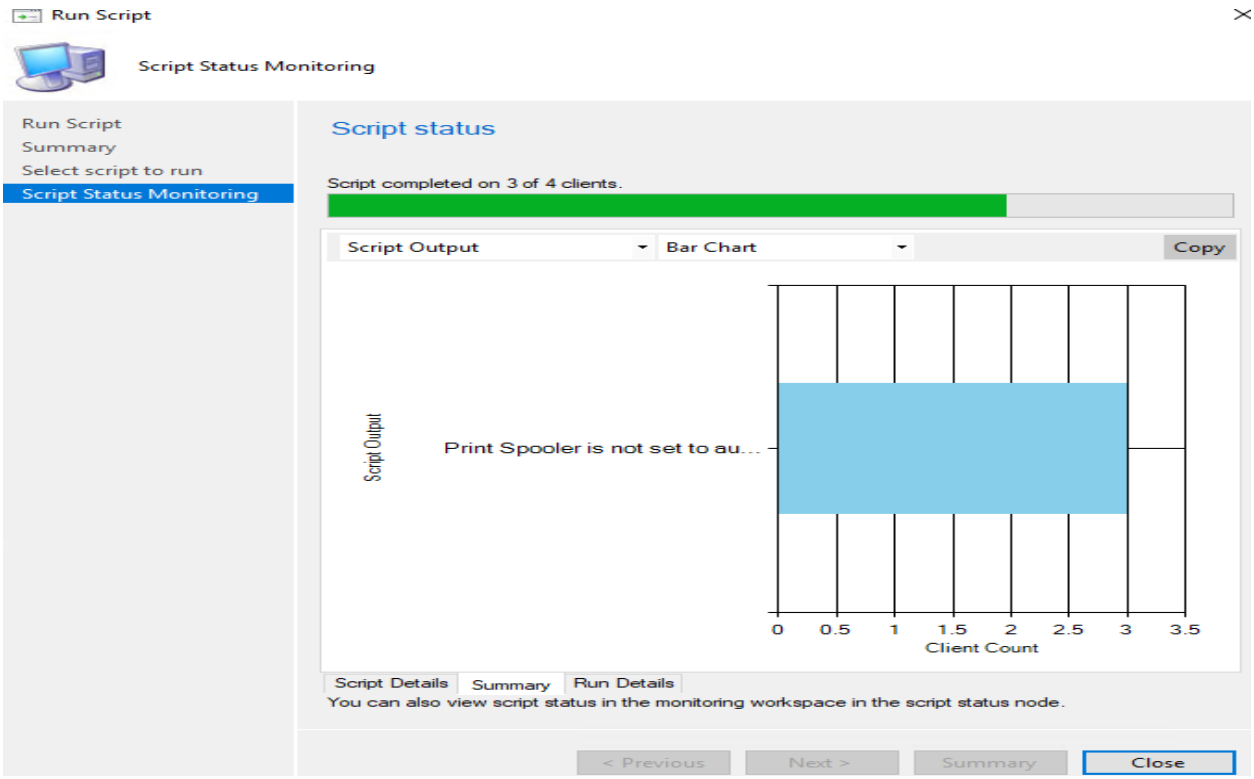


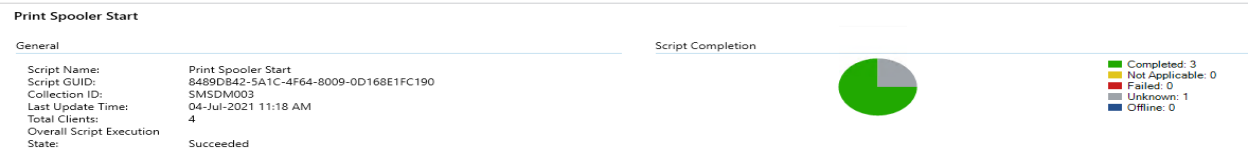


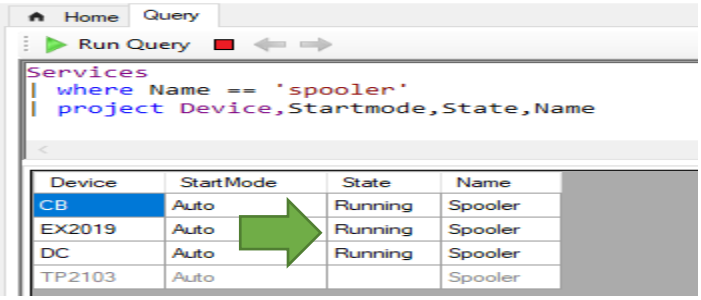
Approve the script and run it.



Back to Device Collection – Run Script – Select Print Spooler Start







Scripts Used Are:

Check Spooler Status - CMPivot

```
Services
| where Name == 'spooler'
| project Device,Startmode,State,Name
```

Stop and Disable Spooler - Script

```
<#

.Synopsis
 Disable Print Spooler Service
.DESCRIPTION
  Disable Print Spooler Service to mitigate the Windows Print Spooler Remote Code Execution
Vulnerability
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
.NOTES
 03.07.2021, v1.0.0, alex verboon
#>
Begin{
   $PrintSpoolerState   = (Get-Service -Name Spooler).Status
   $PrintSpoolStartMode =  (Get-Service -Name Spooler).StartType
}
Process{
   If ($PrintSpoolerState -ne "Stopped"){
      Write-host "Print Spooler is not stopped, stopping it now"
      Stop-Service -Name Spooler -Force
   }

   If ($PrintSpoolStartMode -ne "Disabled"){
      Write-host "Print Spooler is not disabled, disabling it now"
      Set-Service -Name Spooler -StartupType Disabled
   }
}
End{}
```

Start Spooler – Script

```
<#

.Synopsis
  Enable Print Spooler Service
.DESCRIPTION
   Enable Print Spooler Service
.NOTES
  03.07.2021, v1.0.0, alex verboon
#>
Begin{
   $PrintSpoolerState   = (Get-Service -Name Spooler).Status
   $PrintSpoolStartMode =  (Get-Service -Name Spooler).StartType
}
Process{

   If ($PrintSpoolStartMode -ne "Automatic"){
      Write-host "Print Spooler is not set to autostart, configuring that now"
      Set-Service -Name Spooler -StartupType Automatic
   }

   If ($PrintSpoolerState -ne "Running"){
      Write-host "Print Spooler is stopped, starting it now"
      Start-Service -Name Spooler
   }
}
End{}
```