Log Script

**About:**

The PowerShell script auditLogPull.ps1 is meant to be solution for saving and clearing auditing logs on windows system 1803 + without having Splunk or other software installed. Later additions may allow this to work across domains as well.

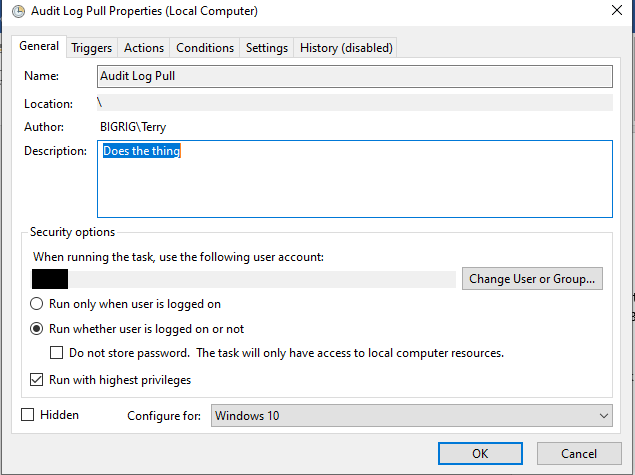
It works by backing up the audit logs to a protected directory. The directory can be hardcoded as is currently. Later releases may include input to have dynamic folder creation.

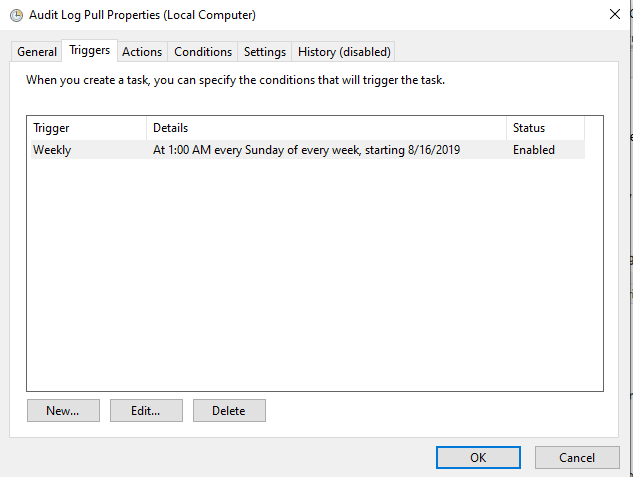
From there it creates the folder of the current date when it backs up logs. The logs are backed up and cleared one by one. After the script is complete the logs can be viewed in the dated folder inside the chosen directory.

**Task Scheduler:**

Create a new task with similar to below:

Give a name to the task as well as a description of what it will do. Make sure to select Logged in or not as well as run with highest privileges. Set for Win 10 compatibility.



In the trigger section, set it for weekly Sunday at 1 am 

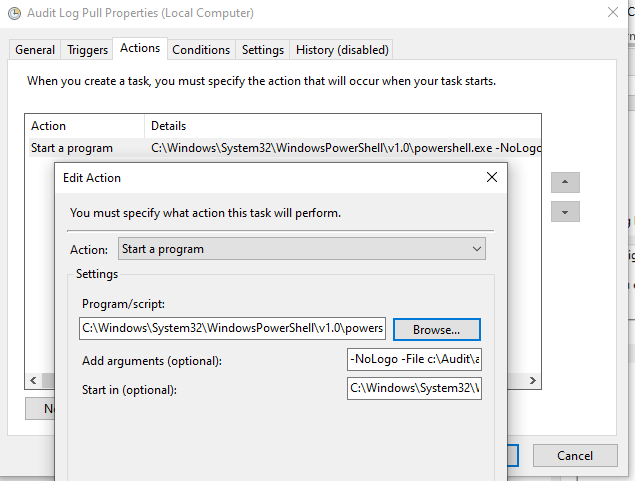
Actions gets a little tricky:

Set Action to start a program

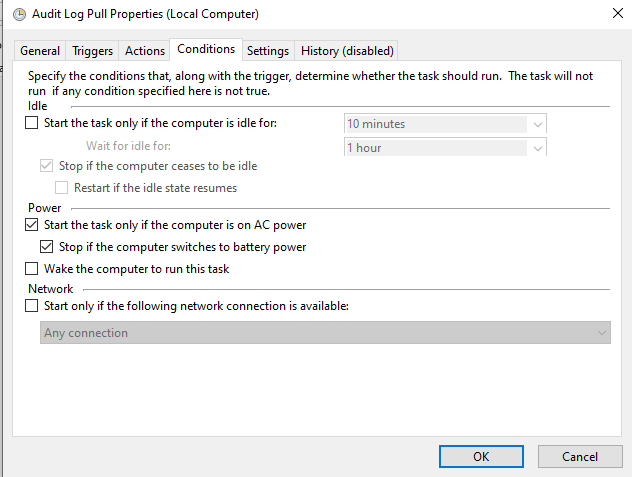
**Program Script:** C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

**Arguments:** -NoLogo -File c:\pathToFolder\auditLogPull.ps1 -ExecutionPolicy RemoteSigned

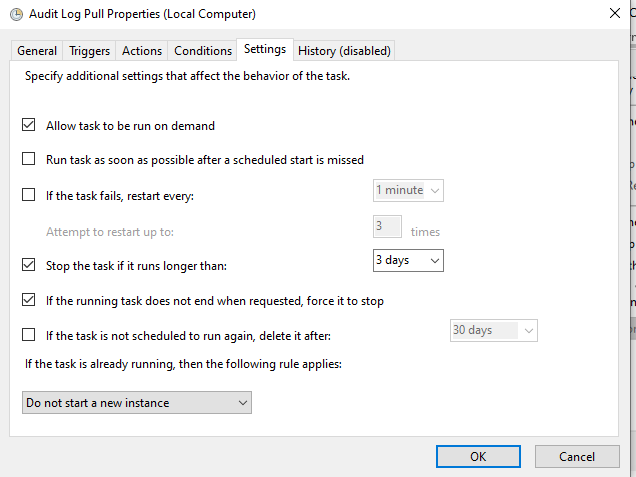
**Start In:** C:\Windows\System32\WindowsPowerShell\v1.0



Conditions can stay standard per below:



Settings can stay standard as well



If you need to make any changes – make sure you use SYSTEMNAME\ACCOUNT when setting the username and password for task updating and setting.

**Per ACCOUNT NEEDS:**

Account: Administrators, log on as batch, log on as service, deny log on locally