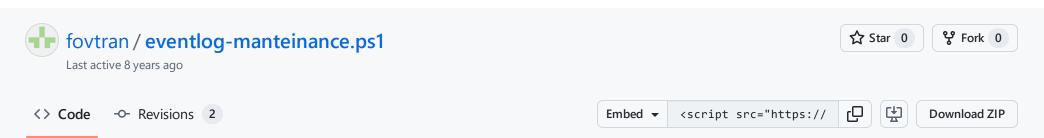


Instantly share code, notes, and snippets.



Cleanup and Relocate EventLog files to other disk

```
  eventlog-manteinance.ps1

                                                                                                                                    Raw
     $evtlist = (.\wevtutil.exe el)
     wevtutil el | Foreach-Object {Write-Host "Clearing $_"; wevtutil cl "$_"}
     wevtutil el | Foreach-Object {Write-Host "Disabled Log: $_"; wevtutil set-log "$_" /e:false /q:true }
 5
     wevtutil set-log Microsoft-Windows-OfflineFiles/Analytic /ms:5000000
 6
 7
     wevtutil cl application
 8
     for /f %x in ('wevtutil el') do wevtutil cl "%x"
 9
     sc stop "Windows Event"
10
11
     Wevtutil sl "Application" /lfn:d:\logs\Application.evtx
12
     Wevtutil sl "Application" /ms:104857600
13
     Wevtutil sl "Security" /lfn:d:\logs\Security.evtx
14
     Wevtutil sl "System" /lfn:d:\logs\System.evtx
15
     Wevtutil sl "Setup" /lfn:d:\logs\Setup.evtx
16
     Wevtutil sl "ForwardedEvents" /lfn:d:\logs\ForwardedEvents.evtx
17
18
     Wevtutil sl "HardwareEvents" /lfn:d:\logs\Hardware.evtx
19
     Wevtutil sl "Internet Explorer" /lfn:d:\logs\Explorer.evtx
20
     Wevtutil sl "Key Management Service" /lfn:d:\logs\Keyserver.evtx
21
     Wevtutil sl "Media Center" /lfn:d:\logs\MediaCenter.evtx
22
     Wevtutil sl "Windows PowerShell" /lfn:d:\logs\Powershell.evtx
23
     Wevtutil sl "Microsoft-Windows-API-Tracing/Operational" /lfn:d:\logs\test.evtx
24
25
     wevtutil set-log "System" /e:true /q:false
26
     wevtutil set-log "Setup" /e:true /q:false
27
     wevtutil set-log "ForwardedEvents" /e:true /q:false
```

Sign up for free to join this conversation on GitHub. Already have an account? Sign in to comment

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information