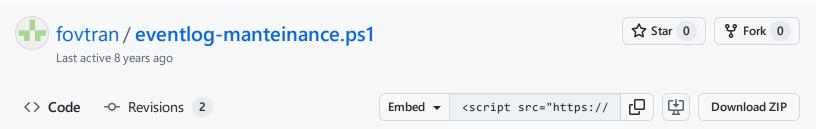


Instantly share code, notes, and snippets.



Cleanup and Relocate EventLog files to other disk

```
⇔ eventlog-manteinance.ps1
                                                                                                        Raw
     $evtlist = (.\wevtutil.exe el)
 2
     wevtutil el | Foreach-Object {Write-Host "Clearing $_"; wevtutil cl "$_"}
 3
     wevtutil el | Foreach-Object {Write-Host "Disabled Log: $_"; wevtutil set-log "$_" /e:false /q:true }
 4
     wevtutil set-log Microsoft-Windows-OfflineFiles/Analytic /ms:5000000
 6
 7
     wevtutil cl application
 8
 9
     for /f %x in ('wevtutil el') do wevtutil cl "%x"
     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
20
     Wevtutil sl "Internet Explorer" /lfn:d:\logs\Explorer.evtx
21
     Wevtutil sl "Key Management Service" /lfn:d:\logs\Keyserver.evtx
     Wevtutil sl "Media Center" /lfn:d:\logs\MediaCenter.evtx
22
     Wevtutil sl "Windows PowerShell" /lfn:d:\logs\Powershell.evtx
23
24
     Wevtutil sl "Microsoft-Windows-API-Tracing/Operational" /lfn:d:\logs\test.evtx
25
     wevtutil set-log "System" /e:true /q:false
26
27
     wevtutil set-log "Setup" /e:true /q:false
```

https://gist.github.com/fovtran/ac0624983c7722e80a8f5a4babb170ee

28 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

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information



© 2024 GitHub, Inc.