fovtran / eventlog-manteinance.ps1

Last active 8 years ago

Cleanup and Relocate EventLog files to other disk

eventlog-manteinance.ps1 Raw

```
1  $evtlist = (.\wevtutil.exe el)
2
3  wevtutil el | Foreach-Object {Write-Host "Clearing $_"; wevtutil cl "$_"}
4  wevtutil el | Foreach-Object {Write-Host "Disabled Log: $_"; wevtutil set-log "$_" /e:false /q:true }
5
6  wevtutil set-log Microsoft-Windows-OfflineFiles/Analytic /ms:5000000
7
8  wevtutil cl application
9  for /f %x in ('wevtutil el') do wevtutil cl "%x"
10 sc stop "Windows Event"
11
12 Wevtutil sl "Application" /lfn:d:\logs\Application.evtx
13 Wevtutil sl "Application" /ms:104857600
14 Wevtutil sl "Security" /lfn:d:\logs\Security.evtx
15 Wevtutil sl "System" /lfn:d:\logs\System.evtx
16 Wevtutil sl "Setup" /lfn:d:\logs\Setup.evtx
17 Wevtutil sl "ForwardedEvents" /lfn:d:\logs\ForwardedEvents.evtx
18
19 Wevtutil sl "HardwareEvents" /lfn:d:\logs\Hardware.evtx
20 Wevtutil sl "Internet Explorer" /lfn:d:\logs\Explorer.evtx
21 Wevtutil sl "Key Management Service" /lfn:d:\logs\Keyserver.evtx
22 Wevtutil sl "Media Center" /lfn:d:\logs\MediaCenter.evtx
23 Wevtutil sl "Windows PowerShell" /lfn:d:\logs\Powershell.evtx
24 Wevtutil sl "Microsoft-Windows-API-Tracing/Operational" /lfn:d:\logs\test.evtx
25
26 wevtutil set-log "System" /e:true /q:false
27 wevtutil set-log "Setup" /e:true /q:false
28 wevtutil set-log "ForwardedEvents" /e:true /q:false
```