Windows

Setting File Auditing Policies using Auditpol.exe, Monitoring File Access and Logon Failures Only

While you can add auditing top level settings via the Group Policy or Local Security Policy this can create a lot of log spam if you are including everything Windows server audits out of the box. In the example below, we are modifying the audit policy to only include only file access and logon failures via auditpol.

```
rem Disable all subcategories
auditpol /set /category:"System" /success:disable
auditpol /set /category:"System" /failure:disable
auditpol /set /category:"Logon/Logoff" /success:disable
auditpol /set /category:"Logon/Logoff" /failure:disable
auditpol /set /category:"Object Access" /success:disable
auditpol /set /category:"Object Access" /failure:disable
auditpol /set /category:"Privilege Use" /success:disable
auditpol /set /category:"Privilege Use" /failure:disable
auditpol /set /category:"Detailed Tracking" /success:disable
auditpol /set /category:"Detailed Tracking" /failure:disable
auditpol /set /category:"Policy Change" /success:disable
auditpol /set /category:"Policy Change" /failure:disable
auditpol /set /category:"Account Management" /success:disable
auditpol /set /category:"Account Management" /failure:disable
auditpol /set /category:"DS Access" /success:disable
auditpol /set /category:"DS Access" /failure:disable
auditpol /set /category:"Account Logon" /success:disable
auditpol /set /category:"Account Logon" /failure:disable
```

```
rem Set new audit sub policy
auditpol /set /subcategory:"File System" /success:enable
auditpol /set /subcategory:"File System" /failure:enable
auditpol /set /subcategory:"Logon" /failure:enable
```

Use the following command to get a list of the policies either after or before you implement the changes. Below is how your policy should look.

```
auditpol /get category:*
```

Results:

```
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
```

IPsec Driver	No Auditing
Other System Events	No Auditing
Security State Change	No Auditing
Logon/Logoff	
Logon	Failure
Logoff	No Auditing
Account Lockout	No Auditing
IPsec Main Mode	No Auditing
IPsec Quick Mode	No Auditing
IPsec Extended Mode	No Auditing
Special Logon	No Auditing
Other Logon/Logoff Events	No Auditing
Network Policy Server	No Auditing
User / Device Claims	No Auditing
Group Membership	No Auditing
Object Access	
File System	Success and Failure
Registry	No Auditing
Kernel Object	No Auditing
SAM	No Auditing
Certification Services	No Auditing
Application Generated	No Auditing
Handle Manipulation	No Auditing
File Share	No Auditing
Filtering Platform Packet Drop	No Auditing
Filtering Platform Connection	No Auditing
Other Object Access Events	No Auditing
Detailed File Share	No Auditing
Removable Storage	No Auditing
Central Policy Staging	No Auditing
Privilege Use	
Non Sensitive Privilege Use	No Auditing
Other Privilege Use Events	No Auditing
Sensitive Privilege Use	No Auditing
Detailed Tracking	
Process Creation	No Auditing
Process Termination	No Auditing
DPAPI Activity	No Auditing
RPC Events	No Auditing
Plug and Play Events	No Auditing
Token Right Adjusted Events	No Auditing
Policy Change	
Audit Policy Change	No Auditing
Authentication Policy Change	No Auditing
Authorization Policy Change	No Auditing
MPSSVC Rule-Level Policy Change	No Auditing
Filtering Platform Policy Change	No Auditing
Other Policy Change Events	No Auditing
Account Management	
Computer Account Management	No Auditing
Security Group Management	No Auditing
Distribution Group Management	No Auditing
Application Group Management	No Auditing
Other Account Management Events	No Auditing
User Account Management	No Auditing
DS Access	
Directory Service Access	No Auditing
Directory Service Changes	No Auditing
Directory Service Replication	No Auditing

```
  Detailed Directory Service Replication  No Auditing
Account Logon
  Kerberos Service Ticket Operations      No Auditing
  Other Account Logon Events              No Auditing
  Kerberos Authentication Service         No Auditing
  Credential Validation                   No Auditing
```

Unique solution ID: #1085

Author: n/a

Last update: 2021-03-30 14:58