Window Audit Setting Config Guide

Wednesday, May 22, 2019 4:49 PM

<u>Modifications / additions to the default Windows Audit Settings:</u>

Force the use of advanced audit policy configuration:

Utilize Group Policy to disable basic auditing force the use of the advanced audit policy configuration. The setting is found under: *Computer Configuration\Policies\Security Settings \Local Policies\Security Options*,
Audit: Force audit policy subcategory settings (Windows Vista or later)

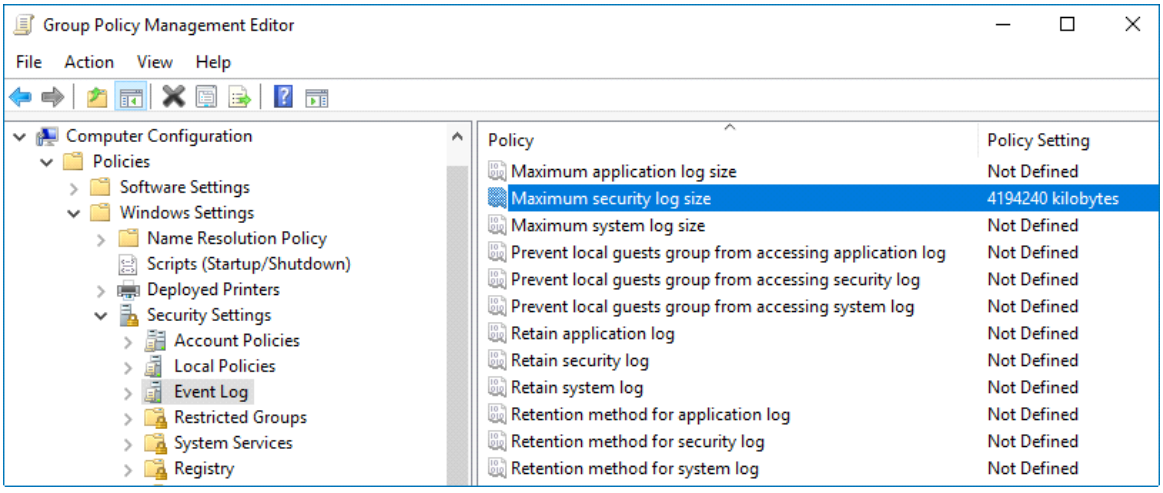
This Group Policy setting enables the *SCENoApplyLegacyAuditPolicy* registry key to prevent basic auditing being applied using Group Policy and the Local Security Policy MMC snap-in

Increase the security log size on servers and workstations:

*Validate risk of increasing log size on servers from current setting of 128 MB or 256 (depending on OS version) to increased size

Group policy setting location

Computer Configuration → Policies → Windows Settings → Security Settings



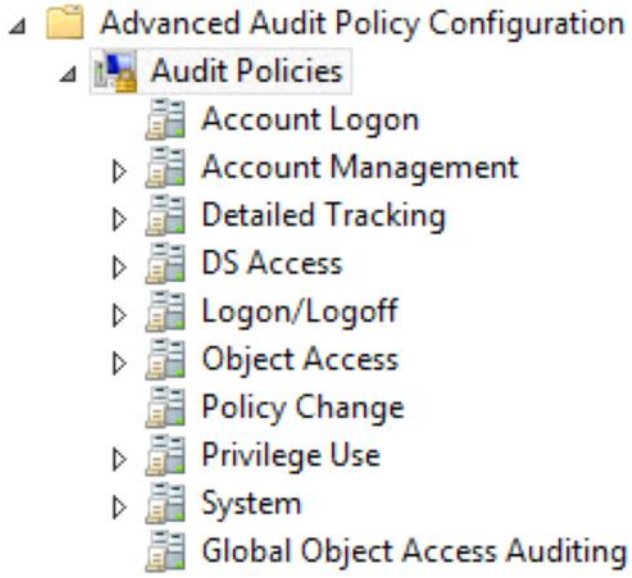
In the Maximum security log size Properties dialog, select Define this policy setting and set maximum security log size to*:*

Servers: 2097120 (2 GB)

Workstations: 1048560 (1 GB)

Advanced Audit Policy:

Group Policy Location:



Domain Controllers:

Account Logon:

Credential Validation:	Success and Failure
Kerberos Authentication Service	Success and Failure
Kerberos Service Ticket Operation	Success and Failure
Other Account Logon Events	Success and Failure

Account Management:

Application Group Management	Success and Failure
Computer Account Management	Success and Failure
Distribution Group Management	Success and Failure
Other Acct Management Events	Success and Failure
Security Group Management	Success and Failure
User Account Management	Success and Failure

Detailed Tracking:

Process Creation	Success and Failure

DS Access:

Directory Service Changes	Success

Logon/Logoff:

Account Lockout	Success and Failure
Group Membership	Success
Logoff	Success
Logon	Success and Failure
Network Policy Server	Success and Failure
Other Logon/Logoff Events	Success and Failure
Special Logon	Success and Failure

Privilege Use:

Sensitive Privilege Use	Success and Failure

Member Servers:

Account Logon:

Credential Validation:	Success and Failure
Kerberos Authentication Service	Success and Failure
Kerberos Service Ticket Operation	Success and Failure
Other Account Logon Events	Success and Failure

Account Management:

Application Group Management	Success and Failure
Computer Account Management	Success and Failure
Distribution Group Management	Success and Failure
Other Acct Management Events	Success and Failure
Security Group Management	Success and Failure
User Account Management	Success and Failure

Logon/Logoff:

Account Lockout	Success and Failure
Group Membership	Success
Logoff	Success
Logon	Success and Failure
Network Policy Server	Success and Failure
Other Logon/Logoff Events	Success and Failure
Special Logon	Success and Failure

Privilege Use:

Sensitive Privilege Use	Success and Failure

Workstations:

Account Logon:

Credential Validation:	Success and Failure
Kerberos Authentication Service	Success and Failure
Kerberos Service Ticket Operation	Success and Failure
Other Account Logon Events	Success and Failure

Account Management:

Application Group Management	Success and Failure
Computer Account Management	Success and Failure
Distribution Group Management	Success and Failure
Other Acct Management Events	Success and Failure
Security Group Management	Success and Failure

User Account Management	Success and Failure

Logon/Logoff:

Account Lockout	Success and Failure
Group Membership	Success
Logoff	Success
Logon	Success and Failure
Network Policy Server	Success and Failure
Other Logon/Logoff Events	Success and Failure
Special Logon	Success and Failure

Privilege Use:

Sensitive Privilege Use	Success and Failure

Object Access:

Removable Storage	Success and Failure