Windows Audit Policies

by Volume and Event ID

Account Logon

Credential Validation

High on domain controllers low on member servers and workstations

- 4774 - An account was mapped for logon.
- 4775 - An account could not be mapped for logon.
- 4776 - The domain controller attempted to validate the cre...
- 4777 - The domain controller failed to validate the creden...
- 4822 - NTLM authentication failed because the account was ...
- 4823 - NTLM authentication failed because access control r...

Kerberos Authentication Service

High on domain controllers

- 4768 - A Kerberos authentication ticket (TGT) was requeste...
- 4771 - Kerberos pre-authentication failed.
- 4772 - A Kerberos authentication ticket request failed.
- 4773 - A Kerberos service ticket request failed.
- 4820 - A Kerberos Ticket-granting-ticket (TGT) was denied ...
- 4824 - Kerberos preauthentication by using DES or RC4 fail...

Kerberos Service Ticket Operations

Very high on domain controllers

- 4769 - A Kerberos service ticket was requested.
- 4770 - A Kerberos service ticket was renewed.
- 4821 - A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.

Detailed Tracking

Process Creation

Medium to high

- 4688 - A new process has been created.
- 4696 - A primary token was assigned to process.

Process Termination

- 4689 - A process has exited.

RPC Events

- 5712 - A Remote Procedure Call (RPC) was attempted.

DS Access

Directory Service Access

High on domain controllers

- 4662 - An operation was performed on an object.
- 5169 - A directory service object was modified.

Directory Service Changes

High on domain controllers

- 5136 - A directory service object was modified.
- 5137 - A directory service object was created.
- 5138 - A directory service object was undeleted.
- 5139 - A directory service object was moved.
- 5141 - A directory service object was deleted.

Logon/Logoff

Group Membership

- 4627 - Group membership information.

Object Access

Certification Services

Medium on AD CS servers

- 4876 - Certificate Services backup started.
- 4877 - Certificate Services backup completed.
- 4886 - Certificate Services received a certificate request...
- 4887 - Certificate Services approved a certificate request...
- 4898 - Certificate Services loaded a template.
- 4899 - A Certificate Services template was updated.
- 4900 - Certificate Services template security was updated.
- <not all shown>

Detailed File Share

- 5145 - A network share object was checked to see whether the client can be granted desired access.

File Share

High on domain controllers & file shares

- 5140 - A network share object was accessed.
- 5142 - A network share object was added.
- 5143 - A network share object was modified.
- 5144 - A network share object was deleted.
- 5168 - Spn check for SMB/SMB2 failed.

Handle Manipulation

- 4656 - A handle to an object was requested.
- 4658 - The handle to an object was closed.
- 4690 - An attempt was made to duplicate a handle to an object.

Other Object Access Events

- 4671 - An application attempted to access a blocked ordina...
- 4691 - Indirect access to an object was requested.
- 4698 - A scheduled task was created.
- 4699 - A scheduled task was deleted.
- 4700 - A scheduled task was enabled.
- 4701 - A scheduled task was disabled.
- 4702 - A scheduled task was updated.
- 5148 - The Windows Filtering Platform has detected a DoS a...
- 5149 - The DoS attack has subsided and normal processing i...
- 5888 - An object in the COM+ Catalog was modified.
- 5889 - An object was deleted from the COM+ Catalog.
- 5890 - An object was added to the COM+ Catalog.

Privilege Use

Registry

- 4657 - A registry value was modified.
- 5039 - A registry key was virtualized.

Sensitive Privilege Use / Non Sensitive Privilege Use

- 4672 - Special privileges assigned to new logon.
- 4673 - A privileged service was called.
- 4674 - An operation was attempted on a privileged object.