# Windows event auditing reference

Author: mdecrevoisier
Version: 2022.07.18
Status: stable

Noisy subcategory
*Disabled event log*

SOURCES:
- NSA guidance: https://apps.nsa.gov/iaarchive/library/ia-guidance/security-configuration/applications/assets/public/upload/Spotting-the-Adversary-with-Windows-Event-Log-Monitoring.pdf
- Notable events: https://github.com/TonyPhipps/SIEM/blob/master/Notable-Event-IDs.md#microsoft-windows-winrmoperational
- Event forwarding guidance: https://github.com/nsacyber/Event-Forwarding-Guidance/blob/master/Events/README.md
- Awesome event IDs: https://github.com/stuhli/awesome-event-ids
- Forensic goodness: https://nasbench.medium.com/finding-forensic-goodness-in-obscure-windows-event-logs-60e978ea45a3
- WDAC/AppLocker/SRP : https://4sysops.com/archives/application-whitelisting-software-restriction-policies-vs-applocker-vs-windows-defender-application-control/
- ANSSI: https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-journalisation-des-systemes-microsoft-windows-en-environnement-active-directory/
- Audit policy auditing and events: https://docs.google.com/spreadsheets/d/e/2PACX-1vSD5-83wlU_Gwl5Vz4cXhiwZr3QBqCh6VZSAigq8vHakf0UN4DF5SCpKXQm9YdGwlz_rNFBgYoMElVl/pubhtml
- Audit policy best practices: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
- Logging essentials: https://github.com/JSCU-NL/logging-essentials/blob/main/WindowsEventLogging.adoc
- Windows 10 event manifest: https://github.com/repnz/etw-providers-docs/tree/master/Manifests-Win10-17134
- https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

## 10-Network related

- Classic event log
  - System
  - Security
  - Application
- SYSMON
  - Microsoft-Windows-Sysmon/Operational → Event log
- SMB share
  - SMB client
    - Event log
      - Microsoft-Windows-SMBClient/Operational
        - ID 30622
        - ID 30624
      - Microsoft-Windows-SMBClient/Security
  - SMB server
    - Event log
      - Microsoft-Windows-SMBServer/Operational
        - Client attempt to use SMBv1 → ID 1001
      - Microsoft-Windows-SMBServer/Audit
        - Client attempt to use SMBv1 → ID 3000
        - Requires auditing activation via PowerShell. Provides more information than ID 1001
      - Microsoft-Windows-SMBServer/Security
  - File Share
    - Event log
      - Security
        - Limited details. Prefer ID 5145
        - Network share object was accessed → ID 5140
        - A network share object was added → ID 5142
        - A network share object was modified → ID 5143
        - A network share object was deleted → ID 5144
        - SPN check for SMB/SMB2 failed → ID 5168
    - Audit policy
      - Audit File Share (S/F)
  - File Share (advanced)
    - Network share object was checked → ID 5145
    - Security → Event log
    - Audit Detailed File Share (S/F) → Audit policy
- Firewall configuration
  - Firewall rules (basic)
    - Security → Event log
      - Events lacking of details. Use instead the "Advanced Security Firewall" event log
      - A rule was added → ID 4946
      - A rule was modified → ID 4947
      - A rule was deleted → ID 4948
    - Audit MPSSVC Rule-Level Policy Change (S/F) → Audit policy
  - Firewall rules (advanced)
    - Microsoft-Windows-Windows Firewall With Advanced Security/Firewall → Event log
      - A rule was added → ID 2004
      - A rule was modified → ID 2005
      - A rule was deleted → ID 2006
  - Configuration changes (advanced)
    - Microsoft-Windows-Windows Firewall With Advanced Security/Firewall → Event log
      - Firewall setting changed → ID 2002
      - Firewall setting changed in profile [X] → ID 2003
  - Configuration changes
    - Security → Event log
      - Mainly about IPsec VPN
      - Audit Filtering Platform Policy Change (S/F)
      - Audit MPSSVC Rule-Level Policy Change (S/F) → Audit policy
- Network flow
  - Flow events
    - Security → Event log
      - Allow
        - A connection was allowed (S) → ID 5156 → Action: connect
        - An application or service has been allowed to listen on a port (S) → ID 5154 → Action: listen
        - A bind to local port has been allowed (S) → ID 5158 → Action: bind
      - Block
        - An application was blocked (F) → ID 5031 → Application
        - A packet was blocked (F) → ID 5146
        - A packet was blocked (restrictive) (F) → ID 5147
        - A packet was blocked (F) → ID 5150
        - A packet was blocked (restrictive) (F) → ID 5151
        - A packet was blocked (F) → ID 5152
        - A packet was blocked (restrictive) (F) → ID 5153
        - A connection was blocked (F) → ID 5157 → Connection
        - Packet → Action: connect
        - An application or service has been blocked to listen on a port (F) → ID 5155 → Action: listen
        - A bind to local port has been blocked (F) → ID 5159 → Action: bind
    - Audit Filtering Platform Packet Drop (S/F)
    - Audit Filtering Platform Connection (S/F) → Audit policy
  - Flow events (TXT)
    - Limited information
    - %systemroot%\system32\LogFiles\Firewall\pfirewall.log → File (TXT)
  - Process connection
    - Network connection → ID 3 → Microsoft-Windows-Sysmon/Operational → Event log
  - RPC traffic
    - zeronetworks / rpcfirewall (3rd party) → Event log
- RDP server activity
  - Event log
    - Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
      - Client timezone is [1] hour from UTC → ID 104
      - The server accepted a new UDP/TCP connection from client [IP]:PORT → ID 131
      - The resolution requested by the client: Monitor 1: [X x Y] → ID 168
      - The client operating system type is (1, 3) > Server [SERVER] → ID 169
    - Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
      - Session logon succeeded → ID 21
      - Session reconnection succeeded → ID 25
    - Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
      - User authentication succeeded → ID 1149
      - Shadow View Session Started → ID 20503
      - Shadow View Session Stopped → ID 20504
      - Shadow View permission granted → ID 20508
- RDP client activity
  - Event log
    - Microsoft-Windows-TerminalServices-RDPClient/Operational
      - RDP ClientActiveX is trying to connect to the server [SERVERX] → ID 1024
      - Base64(SHA1(UserName)) → ID 1029
- DNS client
  - Event log
    - Microsoft-Windows-DNS-Client/Operational
      - Limited information. Prefer to use SYSMON → DNS query complete → ID 3008
      - Limited information. Prefer to use SYSMON → DNS response complete → ID 3020
    - Microsoft-Windows-Sysmon/Operational
      - DNS query → ID 22
- BITS
  - Microsoft-Windows-Bits-Client/Operational → Event log
    - BITS created a task → ID 3
    - BITS transfer completed → ID 4
    - BITS transfer job started with URL [URL] → ID 59
    - BITS transfer job stopped with URL [URL] → ID 60
- OpenSSH
  - OpenSSH/Operational → Event log
    - sshd: [message] → ID 4
- WinRM
  - Microsoft-Windows-WinRM/Operational → Event log
    - WinRM session creation → ID 91
    - User [user]: got authenticated using [auth] → ID 169
- Proxy
  - Microsoft-Windows-WinINet-Config/ProxyConfigChanged → Event log
    - Proxy configuration obtained [Proxy URL] → ID 5600
- DHCP client
  - Microsoft-Windows-Dhcp-Client/Operational → Event log
    - IP conflict detection complete on interface [interface] for IP [IP] → ID 50086
  - Microsoft-Windows-Dhcpv6-Client/Operational → Event log
- Network profiles
  - Microsoft-Windows-NetworkProfile/Operational → Event log
    - Network connected to domain [domain] → ID 10000
- WLAN interface
  - Microsoft-Windows-WLAN-AutoConfig/Operational → Event log
    - Wireless 802.1x authentication started → ID 12011
    - Wireless 802.1x authentication succeeded → ID 12012
    - A client has associated with the hosted network → ID 20019 → Can be Wi-Fi Direct related
    - A client has successfully authenticated with the hosted network → ID 20020 → Can be Wi-Fi Direct related
- Wired interface
  - Microsoft-Windows-Wired-AutoConfig/Operational → Event log
    - A network adapter was added to the system → ID 15510
- WinSock / LSP
  - Microsoft-Windows-Winsock-WS2HELP/Operational → Event log
    - Protocol entry added to Winsock catalog → ID 1
    - Protocol entry removed from Winsock catalog → ID 2
    - Protocol entry disabled from Winsock catalog → ID 3
    - Winsock catalog was reseted → ID 4
- VPN (IPsec)
  - Event log
    - Security
    - Audit Filtering Platform Policy Change (S/F)
  - Audit policy
    - Audit IPsec Main Mode (S/F)
    - Audit IPsec Quick Mode (S)
    - Audit IPsec Extended Mode (S)

## 20-System activity

- System boot
  - Event log
    - System
      - Provider: User32
        - [process] has initiated the restart of [host] on behalf of [user] for the following [reason] → ID 1074
        - Reason supplied by [user] for the last unexpected shutdown is: [reason] → ID 1076
      - Provider: Microsoft-Windows-Kernel-General
        - The operating system started at system time [time] → ID 12
        - The operating system is shutting down at system time [time] → ID 13
      - Provider: Microsoft-Windows-Kernel-Boot
      - Provider: Microsoft-Windows-Kernel-Power
        - The system has rebooted without cleaning shutting down first → ID 41
        - The kernel power manager has initiated a shutdown transition → ID 109
    - Microsoft-Windows-Shell-Core/Operational
      - Boot start: execution for [app -parameter] → ID 9707
- Windows Event Forwarding
  - Event log
    - Microsoft-Windows-Forwarding/Operational → WEF client
    - Microsoft-Windows-EventCollector/Operational → WEC server
- Windows Event log
  - Event log
    - System
      - Provider: EventLog
        - Event log service was started → ID 6005
        - Event log service was stopped → ID 6006
        - Previous system shutdown was not planned → ID 6008
        - System uptime is [seconds] → ID 6013
      - Provider: Microsoft-Windows-Eventlog
        - Event log [log] was cleared → ID 104
    - Security
      - Event logging service has shut down → ID 1100
      - Events have been dropped → ID 1101
      - Audit log was cleared → ID 1102
      - Security log is now full → ID 1104
      - Event log automatic backup → ID 1105
      - Event log service encountered an error → ID 1108
- Group Policy (GPO)
  - Event log
    - Provider: Microsoft-Windows-GroupPolicy → System
    - Microsoft-Windows-GroupPolicy/Operational
    - Microsoft-Windows-Security-Audit-Configuration-Client/Operational
- Time
  - Event log
    - System
      - The system time was changed → ID 1 → Provider: Microsoft-Windows-Kernel-General
      - System was activated with the following settings [year, month, hour, minute] → ID 20000 → Microsoft-Windows-DateTimeControlPanel/Operational
    - Microsoft-Windows-Time-Service/Operational
      - Provider: Microsoft-Windows-Time-Service → System
    - Security
      - The system time was changed → ID 4616
      - Audit Security State Change (S) → Audit policy
- WMI / DCOM
  - Event log
    - Microsoft-Windows-WMI-Activity
      - Noisy events → Provider started → ID 5857
      - Noisy events → Provider error → ID 5858
      - Prefer to use SYSMON events → Registration of Temporary Event Consumer → ID 5860
      - Prefer to use SYSMON events → Registration of Permanent Event Consumer → ID 5861
    - Microsoft-Windows-Sysmon/Operational
      - WmiEventFilter activity → ID 19
      - WmiEventConsumer activity → ID 20
      - WmiEventConsumerToFilter → ID 21
    - Provider: Microsoft-Windows-DistributedCOM → System

## 21-Application & Updates

- Software → Event log
  - Application → Provider: MsiInstaller → ID 11707 → The [product] installation completed successfully.
  - Microsoft-Windows-Application-Experience/Program-Telemetry → ID 500 → Compatibility fix applied to [path.exe]
  - Microsoft-Windows-Application-Experience/Program-Compatibility-Assistant → ID 17 → Program Compatibility Assistant execution
  - Microsoft-Windows-Application-Experience/Program-Inventory
    - ID903/904 → Program installed on the system
    - ID907/908 → Program removed from the system
- Windows Update → Event log
  - Microsoft-Windows-WindowsUpdateClient/Operational → Provides information about update checks and downloads (but no more details)
  - System → Provider: Microsoft-Windows-WindowsUpdateClient → ID 19 → Installation successful: [package]
  - Setup → Provider: Microsoft-Windows-Servicing
    - ID 2 → Package [KBx] was successfully changed to the Installed state.
    - ID 10 → Selectable update [module/feature] was successfully turned off.
- Application crash → Event log
  - Application
    - Provider: Application Error → ID 1000 → Application crash / error
    - Provider: Application Hang → ID 1002 → Application hang
    - Provider: Windows Error Reporting → ID 1001 → WER
  - System → Provider: Microsoft-Windows-WER-SystemErrorReporting → ID 1001 → BSOD
- Default application → Event log → Microsoft-Windows-Shell-Core/AppDefaults → ID 62443 → Association= [pdf], ProgId=[App path], U=[User SID]
- Microsoft Office → Event log → OAlerts → ID 300 → Provides info. about opened files, brutforce, DDE attacks ...

## 22-Task & Service

- Services (life cycle) → Event log → System → Provider: Service Control Manager
  - Start events
    - Installation → ID 7045 → Service installation → Prefer ID 4697
    - ID 7000 → EVENT_SERVICE_START_FAILED
    - ID 7021 → EVENT_SEVERE_SERVICE_FAILED
    - ID 7022 → EVENT_SERVICE_START_HUNG
    - ID 7038 → EVENT_FIRST_LOGON_FAILED_II
    - ID 7041 → EVENT_SERVICE_LOGON_TYPE_NOT_GRANTED
  - Configuration
    - ID 7030 → EVENT_SERVICE_NOT_INTERACTIVE
    - ID 7040 → EVENT_SERVICE_START_TYPE_CHANGED
  - State events
    - ID 7009 → EVENT_CONNECTION_TIMEOUT
    - ID 7011 → EVENT_TRANSACT_TIMEOUT
    - ID 7016 → EVENT_BAD_SERVICE_STATE
    - ID 7035 → EVENT_SERVICE_CONTROL_SUCCESS
    - ID 7036 → EVENT_SERVICE_STATUS_SUCCESS
    - ID 7037 → EVENT_SERVICE_CONFIG_BACKOUT_FAILED
  - Exit events
    - ID 7011 → EVENT_SERVICE_SHUTDOWN_FAILED
    - ID 7023 → EVENT_SERVICE_EXIT_FAILED
    - ID 7024 → EVENT_SERVICE_EXIT_FAILED_SPECIFIC
    - ID 7031 → EVENT_SERVICE_CRASH
    - ID 7032 → EVENT_SERVICE_RECOVERY_FAILED
    - ID 7034 → EVENT_SERVICE_CRASH_NO_ACTION
    - ID 7042 → EVENT_SERVICE_STOP_SUCCESS_WITH_REASON
- Services (advanced) → Event log → Security → ID 4697 → Service installation → Provides more context than ID 7045 regarding user information
  - Audit policy → Audit Security System Extension (S/F)

## 31-System security

- Task Scheduler (life cycle) → Event log → Security
  - ID 4698 → Schedule task created
  - ID 4699 → Schedule task deleted
  - ID 4700 → Schedule task disabled
  - ID 4701 → Schedule task enabled
  - ID 4702 → Schedule task modified
  - Audit policy → Audit Other Object Access Events (S/F)
- Task Scheduler (execution) → Event log → Microsoft-Windows-TaskScheduler/Operational → Noisy, but provides more context about task execution stages
- Windows Defender antivirus → Event log → Microsoft-Windows-Windows Defender/Operational
  - ID 1013 / 1014 → Malware history deletion
  - ID 1116 → Threat detected (no action taken yet)
  - ID 1117 → Threat detected (action taken with success)
  - ID 1118 → Threat detected (action taken failed)
  - ID 1119 → Threat detected (action taken critically failed)
  - ID 1151 → Health report (inc. last update time) → Triggered hourly
  - ID 5007 → Configuration changed (reports exclusions)
- CVE → Event log → System → Provider : Microsoft-Windows-Audit-CVE → ID 1 → Possible detection for [CVE]
- Certificates → Event log → Microsoft-Windows-CAPI2/Operational
  - ID 11 → Certificate build chain
  - ID 30 → Verify certificate chain policy
  - ID 70 → Acquire certificate private key → Relevant to detect software accessing private key (eg: Mimikatz)
  - ID 81 → Verify certificate trust
- Application whitelisting
  - Software Restriction Policies → Event log → Application → Provider: Microsoft-WindowsSoftwareRestrictionPolices
  - AppLocker → Event log
    - Microsoft-Windows-AppLocker/EXE and DLL
      - ID 8002 → [path] was allowed to run
      - ID 8003 → [path] was prevented from running
      - ID 8004 → [path] was not allowed to run.
    - Microsoft-Windows-AppLocker/MSI and Script
      - ID 8005 → [path] was allowed to run
      - ID 8006 → [path] was prevented from running
      - ID 8007 → [path] was not allowed to run.
  - Application Control (WDAC) → Event log → *See AppLocker and Code Integrity event logs*
- Code integrity
  - Event log → Microsoft-Windows-CodeIntegrity/Operational
    - ID 3001 → Unsigned drivers loaded on the system
    - ID 3002 → Unable to verify the image integrity of the [FILE] because the set of per-page image hashes could not be found
    - ID 3003 → Unable to verify the image integrity of the [file] because the set of per-page image hashes could not be found on the system. The image is allowed to load because kernel mode debugger is attached.
    - ID 3004 → Unable to verify the image integrity of the [file] because file hash could not be found on the system.
    - ID 3033/3063 → Code Integrity determined that [process] attempted to load [FILE] that did not meet the signing level requirements → LSA Protection block mode related. Requires registry changes to enable these events
    - ID 3065, 3066 → Code Integrity determined that [process] attempted to load [FILE] that did not meet the signing level requirements → LSA Protection audit mode related. Requires registry changes to enable these events
  - Event log → Security
    - ID 5038 → Invalid image hash of a file
    - ID 6281 → Invalid page hash of an image file
    - ID 6410 → File does not meet requirements to load into a process.
  - Audit policy → Audit Security System Extension (F)
- Local Security Authority → Event log
  - Microsoft-Windows-LSA/Operational → ID 300 → Group Assigned to new Session
  - System → Provider: Microsoft-Windows-Wininit → ID 12 → LSA started as a protected process
  - Security
    - ID 4610 → An authentication package has been loaded by the Local Security Authority.
    - ID 4611 → A trusted logon process has been registered with the Local Security Authority.
    - ID 4622 → A security package has been loaded by the Local Security Authority.
- BitLocker → Event log
  - Microsoft-Windows-BitLocker/BitLocker Management
  - Microsoft-Windows-BitLocker/BitLocker Operational
- Security mitigations → Event log
  - Microsoft-Windows-Security-Mitigations/KernelMode
  - Microsoft-Windows-Security-Mitigations/UserMode
- DLL load → Event log
  - System → Provider: Microsoft-Windows-Wininit → ID 11 → Custom dynamic link libraries are being loaded for every application
  - Sysmon → ID 7 → Image loaded
- Credential Manager → Event log
  - Security → ID 5379 → Credential Manager credentials were read → Available only on recent Windows 10 (confirmed on 20H2)
  - Auditing settings → User account management

## 32-External device

- Device & drivers
  - Log file (TXT) → C:\Windows\INF\SetupAPI.dev.log
  - Eventlog
    - System → Provider: Microsoft-Windows-Kernel-PnP
      - ID 219 → Failed to load driver [driver]
    - Microsoft-Windows-Kernel-PnP/Configuration
      - ID 400 → Device [path] was configured
      - ID 401 → Device [path] failed to be configured
      - ID 410 → Device [path] was initiated
    - Microsoft-Windows-DriverFrameworks-UserMode/Operational
    - Microsoft-Windows-Partition/Diagnostic → ID 1006 → Disk/device informations
- Removable storage → Event log → Security → ID 6416 → New external device was recognised by the System
  - Audit policy → PNP activity (S)
- Printer → Event log
  - Microsoft-Windows-PrintService/Admin
    - ID 354 → Failed to initialize [printer path] from [path.dll]
    - ID 808 → Printer spooler failed to load module [path.dll]
    - ID 823 → Changing default printer to [printer]
  - Microsoft-Windows-PrintService/Operational
    - ID 848 → Printer share created
    - ID 849 → Printer share deleted
- RDP (device activity) → Event log
  - Microsoft-Windows-TerminalServices-ClientUSBDevices/Operational
  - Microsoft-Windows-TerminalServices-PnPDevices/Operational
  - Microsoft-Windows-TerminalServices-ServerUSBDevices/Operational
- ISO/VHD file → Event log → Microsoft-Windows-VHDMP-Operational
  - ID 1 → File is online
  - ID 2 → File is removed

## 40-PowerShell

- Transcript
  - Text file (TXT)
  - Auditing settings → Transcript
- Classic → Event log → Windows PowerShell
  - ID 600 → Less relevant
  - ID 800
- Modern
  - Module logging
    - Event log → Microsoft-Windows-PowerShell/Operational → ID 4103
    - Auditing settings → Module logging
  - Script block
    - Event log → Microsoft-Windows-PowerShell/Operational → ID 4104
    - Auditing settings → Script block logging

## 50-Authentication

- Account logon
  - Event log → Security
    - ID 4624 → Account successfully logged on
    - ID 4625 → Account failed to log on
    - ID 4634 → Account logged off
    - ID 4648 → A logon was attempted using explicit credentials
  - Audit policy → Audit Logon (S/F)
- NTLM authentication
  - Standard
    - Event log → Security
      - ID 4774 → An account was mapped for logon (S/F)
      - ID 4775 → An account could not be mapped for logon
      - ID 4776 → Computer attempted to validate the credentials (S/F)
      - ID 4777 → Domain controller failed to validate the credentials of an account (F) → Event never registered.
      - ID 4823 → NTLM authentication failed because access control restrictions are required
    - Audit policy → Audit Credential Validation (S/F)
  - Advanced
    - Event log → Microsoft-Windows-NTLM/Operational
    - Audit settings
      - Restrict NTLM: Audit NTLM authentication in this domain
      - Restrict NTLM: Audit Outgoing NTLM Traffic to remote servers
      - Restrict NTLM: Audit Incoming NTLM Traffic
      - → Optional. Configured in Group policy preferences
- Privileged logon → Event log → Security → ID 4672 → Special privileges assigned to new logon
  - Audit policy → Audit Special Logon (S)
- Group membership
  - Standard → Event log → Microsoft-Windows-LSA/Operational → ID 300 → Group Assigned to new Session → Prefer ID 4627 as it includes a logon type
  - Standard → Event log → Security → ID 4627 → Group membership information
    - Audit policy → Group Membership (S)
  - Advanced → Event log → Security → ID 4964 → Special groups have been assigned to a new logon → Requires registry settings configuration for auditing the login of provided groups
    - Audit policy → Audit Special Logon (S)
- Azure Active Directory → Event log → Microsoft-Windows-AAD/Operational

## 23-User and group management

- Refer to Active Directory mindmap