Windows event auditing reference

Classic event log

- System
- Security
- Application

SYSMON

- Microsoft-Windows-Sysmon/Operational → Event log

Network related

SMB

- Client (Event log)
  - Microsoft-Windows-SMBClient/Audit
  - Microsoft-Windows-SMBClient/Security
- Server (Event log)
  - Microsoft-Windows-SMBServer/Audit
  - Microsoft-Windows-SMBServer/Security
- File Share (Event log)
  - Security
    - ID 5140 — Network share object was accessed — Limited details. Prefer ID 5145
    - ID 5142 — A network share object was added
    - ID 5143 — A network share object was modified
    - ID 5144 — A network share object was deleted
  - Audit policy
    - Audit File Share (S/F)
- File Share (advanced) (Event log)
  - Security
    - ID 5145 — Network share object was checked — Provides more info. than ID 5140
  - Audit policy
    - Audit Detailed File Share (S/F)

Firewall configuration

- Firewall rules (basic) (Event log)
  - Security
    - ID 4946 — A rule was added
    - ID 4947 — A rule was modified
    - ID 4948 — A rule was deleted
    - Events lacking of details. Use instead the "Advanced Security Firewall" event log
  - Audit policy
    - Audit MPSSVC Rule-Level Policy Change (S/F)
- Firewall rules (advanced) (Event log)
  - Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
    - ID 2004 — A rule was added
    - ID 2005 — A rule was modified
    - ID 2006 — A rule was deleted
- Configuration changes (advanced) (Event log)
  - Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
    - ID 2002 — Firewall setting changed
    - ID 2003 — Firewall setting changed in profile [X]
- Configuration changes (Event log)
  - Security
    - Audit Filtering Platform Policy Change (S/F)
      - ID 5031 — Application — An application was blocked (F)
      - ID 5150 — Packet — A packet was blocked (F)
      - ID 5151 — Packet — A packet was blocked (restrictive) (F)
      - ID 5152 — Packet — A packet was blocked (F)
      - ID 5153 — Packet — A packet was blocked (restrictive) (F)
      - ID 5156 — Connection — A connection was allowed (S)
      - ID 5157 — Connection — A connection was blocked (F)
      - Mainly about IPsec VPN
    - Audit MPSSVC Rule-Level Policy Change (S/F)

Network flow

- Security → Event log
  - Action: connect
    - Application: ID 5031 — An application was blocked (F)
    - Packet: ID 5150 — A packet was blocked (F); ID 5151 — A packet was blocked (restrictive) (F); ID 5152 — A packet was blocked (F); ID 5153 — A packet was blocked (restrictive) (F)
    - Connection: ID 5156 — A connection was allowed (S); ID 5157 — A connection was blocked (F)
  - Action: listen
    - ID 5154 — An application or service has been allowed to listen on a port (S)
    - ID 5155 — An application or service has been blocked to listen on a port (F)
  - Action: bind
    - ID 5158 — A bind to local port has been allowed (S)
    - ID 5159 — A bind to local port has been blocked (F)
- Flow events → Audit policy
  - Audit Filtering Platform Packet Drop (S/F)
  - Audit Filtering Platform Connection (S/F)
- File (TXT) → Flow events (TXT)
  - %systemroot%\system32\LogFiles\Firewall\pfirewall.log — Limited information
- Event log → Process connection
  - Microsoft-Windows-Sysmon/Operational — ID 3 — Network connection
- Event log → RPC traffic
  - zeronetworks / rpcfirewall (3rd party)

RDP server activity

- Event log
  - Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
    - ID 104 — Client timezone is [I] hour from UTC
    - ID 131 — The server accepted a new UDP/TCP connection from client [IP]:PORT
    - ID 168 — The resolution requested by the client: Monitor I: [X x Y]
    - ID 169 — The client operating system type is (1, 3) > Server [SERVER]
  - Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
    - ID 21 — Session logon succeeded
    - ID 25 — Session reconnection succeeded
  - Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational
    - ID 1149 — User authentication succeeded

RDP client activity

- Event log
  - Microsoft-Windows-TerminalServices-RDPClient/Operational
    - ID 1024 — RDP ClientActiveX is trying to connect to the server [SERVERX]
    - ID 1029 — Base64(SHA1(UserName))

DNS client

- Event log
  - Microsoft-Windows-DNS-Client/Operational
    - ID 3008 — DNS query complete — Limited information. Prefer to use SYSMON
    - ID 3020 — DNS response complete — Limited information. Prefer to use SYSMON
  - Microsoft-Windows-Sysmon/Operational
    - ID 22 — DNS query

BITS

- Event log
  - Microsoft-Windows-Bits-Client/Operational
    - ID 3 — BITS created a task
    - ID 4 — BITS transfer completed
    - ID 59 — BITS transfer job started with URL [URL]
    - ID 60 — BITS transfer job stopped with URL [URL]

OpenSSH

- Event log
  - OpenSSH/Operational
    - ID 4 — sshd: [message]

WinRM

- Event log
  - Microsoft-Windows-WinRM/Operational
    - ID 91 — WinRM session creation
    - ID 169 — User [user]: got authenticated using [auth]

Proxy

- Event log
  - Microsoft-Windows-WinINet-Config/ProxyConfigChanged
    - ID 5600 — Proxy configuration obtained [Proxy URL]

DHCP client

- Event log
  - Microsoft-Windows-Dhcp-Client/Operational
    - ID 50086 — IP conflict detection complete on interface [interface] for IP [IP]
  - Microsoft-Windows-Dhcpv6-Client/Operational

Network profiles

- Event log
  - Microsoft-Windows-NetworkProfile/Operational
    - ID 10000 — Network connected to domain [domain]

WLAN interface

- Event log
  - Microsoft-Windows-WLAN-AutoConfig/Operational
    - ID 12011 — Wireless 802.1x authentication started
    - ID 12012 — Wireless 802.1x authentication succeeded
    - ID 20019 — A client has associated with the hosted network — Can be Wi-Fi Direct related
    - ID 20020 — A client has successfully authenticated with the hosted network — Can be Wi-Fi Direct related

Wired interface

- Event log
  - Microsoft-Windows-Wired-AutoConfig/Operational
    - ID 15510 — A network adapter was added to the system

WinSock / LSP

- Event log
  - Microsoft-Windows-Winsock-WS2HELP/Operational
    - ID 1 — Protocol entry added to Winsock catalog
    - ID 2 — Protocol entry removed from Winsock catalog
    - ID 3 — Protocol entry disabled from Winsock catalog
    - ID 4 — Winsock catalog was reseted

VPN (IPsec)

- Event log
  - Security
- Audit policy
  - Audit Filtering Platform Policy Change (S/F)
  - Audit IPsec Main Mode (S/F)
  - Audit IPsec Quick Mode (S)
  - Audit IPsec Extended Mode (S)

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
    - ID 903/904 — Program installed on the system
    - ID 907/908 — 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 ...

Task & Service

- 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
- Services (life cycle) → Event log → System → Provider: Service Control Manager
  - Installation → ID 7045 — Service installation — Prefer ID 4697
  - Start events
    - 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)

Security related

- 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

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

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

System activity

System boot

- Event log
  - System
    - Provider: User32
      - ID 1074 — [process] has initiated the restart of [host] on behalf of [user] for the following [reason]
      - ID 1076 — Reason supplied by [user] for the last unexpected shutdown is: [reason]
    - Provider: Microsoft-Windows-Kernel-General
      - ID 12 — The operating system started at system time [time]
      - ID 13 — The operating system is shutting down at system time [time]
    - Provider: Microsoft-Windows-Kernel-Boot
    - Provider: Microsoft-Windows-Kernel-Power
      - ID 41 — The system has rebooted without cleaning shutting down first
      - ID 109 — The kernel power manager has initiated a shutdown transition
  - Microsoft-Windows-Shell-Core/Operational
    - ID 9707 — Boot start: execution for [app -parameter]

Windows Event Forwarding

- Event log
  - WEF client — Microsoft-Windows-Forwarding/Operational
  - WEC server — Microsoft-Windows-EventCollector/Operational

Windows Event log

- Event log
  - Provider: EventLog
    - System
      - ID 6005 — Event log service was started
      - ID 6006 — Event log service was stopped
      - ID 6008 — Previous system shutdown was not planned
      - ID 6013 — System uptime is [seconds]
    - Provider: Microsoft-Windows-Eventlog
      - ID 104 — Event log [log] was cleared
  - Security
    - ID 1100 — Event logging service has shut down
    - ID 1102 — Audit log was cleared
    - ID 1104 — Security log is now full
    - ID 1105 — Event log automatic backup

Group Policy (GPO)

- Event log
  - System — Provider: Microsoft-Windows-GroupPolicy
  - Microsoft-Windows-GroupPolicy/Operational
  - Microsoft-Windows-Security-Audit-Configuration-Client/Operational

Time

- Event log
  - System
    - Provider: Microsoft-Windows-Kernel-General — ID 1 — The system time was changed
    - Microsoft-Windows-DateTimeControlPanel/Operational — ID 20000 — System was activated with the following settings [year, month, hour, minute]
    - Microsoft-Windows-Time-Service/Operational
    - Provider: Microsoft-Windows-Time-Service
  - Security — ID 4616 — The system time was changed
- Audit policy — Audit Security State Change (S)

WMI / DCOM

- Event log → Microsoft-Windows-WMI-Activity
  - ID 5857 — Provider started — Noisy events
  - ID 5858 — Provider error — Noisy events
  - ID 5860 — Registration of Temporary Event Consumer — Prefer to use SYSMON events
  - ID 5861 — Registration of Permanent Event Consumer — Prefer to use SYSMON events
- Event log → System → Provider: Microsoft-Windows-DistributedCOM

Author: mdecrevoisier
Version: 2022.05.05
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
- WDAC/AppLocker/SRP : https://4sysops.com/archives/application-whitelisting-software-restriction-policies-vs-applocker-vs-windows-defender-application-control/