Windows Server advanced auditing

ADDS server

- See dedicated map

DNS server

- Transaction logs
  - One of them
    - Debug logs (TXT)
    - ETW channel
    - ETL file
- Event log
  - *DNS server*
  - *Microsoft-Windows-Microsoft-Windows-DNSServer/Audit*
- 3rd party
  - Mandiant / SilkETW
  - acalarch / ETL-to-EVTX

IIS webserver

- Transaction logs
  - Format
    - One of them
      - IIS
      - W3C
      - NCSA
      - Custom
    - Log file (TXT)
  - Audit level
    - Server
    - Site
- Event log
  - *Microsoft-IIS-Configuration/Operational*
  - *Microsoft-IIS-Configuration/Admin*
  - System

Exchange Server

- See dedicated map

OCSP responder

- Event log
  - Security
- Audit policy
  - Audit NPS (S/F)
- Audit settings
  - Audit configuration changes
  - Audit security settings changes

ADCS server

- Event log
  - *Security*
- Audit policy
  - Audit Certification Services (S/F)
- Auditing settings
  - Several check boxes

SQL server

- Transaction logs
  - Log file (TXT)
  - Event log
    - One of them
      - Application
      - Security
- Auditing settings
  - Audit object
    - Server
    - Database
  - Specification object

Windows Server Backup

- Event log
  - Microsoft-Windows-Backup

ADFS server

- Event log
  - Security
  - DRS/Admin
  - AD FS/Admin
  - Microsoft-Windows-FederationServices-Deployment/Operational
- Audit policy
  - Audit Application generated (S/F)
- Auditing settings
  - Several check boxes

DHCP server

- Transaction logs
  - Audit log (TXT)
- Event log
  - *Microsoft-Windows-DHCP Server Events/Admin*
  - *Microsoft-Windows-Dhcp-Server/Operational*

Advanced Threat Analytics

- Event log
  - Microsoft ATA
- SYSLOG
  - Better structure

VPN server (RAS / Direct Access / AOVPN / IPSec)

- Event log
  - *Microsoft-Windows-Base-Filtering-Engine-Connections/Operational*
  - *Microsoft-Windows-Base-Filtering-Engine-Resource-Flows/Operational*
  - *Microsoft-Windows-WinNat/Oper*
  - *Microsoft-Windows-Iphlpsvc/Operational*
  - *Security*
- Audit policy
  - Audit IPsec main mode (S/F)
  - Audit IPsec quick mode (S/F)
  - Audit IPsec driver(S/F)

NPS server

- Transaction logs
  - Event log
    - Security
  - SQL server instance
  - Log file (TXT)
  - Can be simultaneous
- Audit policy
  - Audit NPS (S/F)
- Auditing settings
  - Audit rejected requests
  - Audit successful requests

Containers

- Event log
  - Application
    - Source: Docker
  - Microsoft-Windows-Containers-Wcifs/Operational
  - Microsoft-Windows-Containers-Wcnfs/Operational

Terminal Service (RDS)

- Event log
  - Microsoft-Windows-RemoteApp and Desktop Connection Management/Operational
  - Microsoft-Windows-TerminalServices-Licensing/Operational
  - Microsoft-Windows-TerminalServices-SessionBroker/Operational

Disabled event log

Author: mdecrevoisier
Version: 2021.41
Status: stable