Active Directory advanced auditing

Author: mdecrevoisier
Version: 2023.12.01
Status: stable

Disabled event log

SOURCES
- Netlogon audit: https://www.manageengine.com/products/active-directory-audit/how-to/how-to-enable-netlogon-logging.html

60-Domain controller authentication

Kerberos

Kerberos Service Ticket (TGS)

- Event log
  - Security
    - ID 4769 — A Kerberos service ticket was requested
    - ID 4770 — A Kerberos service ticket was renewed
    - ID 4773 — A Kerberos service ticket request failed
    - ID 4821 — A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.
- Audit policy
  - Audit Kerberos Service Ticket Operations (S/F)

Kerberos Granting Ticket (TGT)

- Event log
  - Security
    - ID 4768 — A Kerberos authentication ticket (TGT) was requested
    - ID 4771 — Kerberos preauthentication failed
    - ID 4772 — A Kerberos authentication ticket request failed
    - ID 4820 — Kerberos Ticket granting ticket (TGT) denied (device does not meet access control restrictions)
    - ID 4824 — Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.
- Audit policy
  - Audit Kerberos Authentication Service (S/F)

Authentication / Silo policies

- Event log
  - Microsoft-Windows-Authentication/AuthenticationPolicyFailures-DomainController
    - 101 — An NTLM sign-in failure occurs because access control restrictions are required, and those restrictions cannot be applied to NTLM.
    - 105 — A Kerberos restriction failure occurs because the authentication from a particular device was not permitted.
    - 106 — A Kerberos restriction failure occurs because the user or device was not allowed to authenticate to the server.
    - 305 — A potential Kerberos restriction failure might occur because the authentication from a particular device was not permitted.
    - 306 — A Kerberos restriction failure might occur because the user or device was not allowed to authenticate to the server.

KDC

- Event log
  - Microsoft-Windows-Kerberos-Key-Distribution-Center/Operational
    - 302 — KDC uses the below KDC certificate for smart card or certificate authentication
  - System
    - Provider: Kerberos-Key-Distribution-Center
      - 39 — User certificate valid but could not be mapped to a user in a secure way

Protected users

- See "50-Authentication" in Windows mindmap
- Microsoft-Windows-Authentication/ProtectedUser-Client
- Microsoft-Windows-Authentication/ProtectedUserFailures-DomainController
  - ID 100 — An NTLM sign-in failure occurs for an account that is in the Protected Users security group.
  - ID 104 — DES or RC4 encryption types are used for Kerberos authentication and a sign-in failure occurs for a user in the Protected User security group.
- Microsoft-Windows-Authentication/ProtectedUserSuccess-DomainController
  - ID 303 — A Kerberos ticket-granting-ticket (TGT) was successfully issued for a member of the Protected User group.

LDAP

- Directory Service
  - Event log
    - ID 1138 — Function ldap_search entered
    - ID 1174 — Wrong password
    - ID 1644 — A client issued a search operation with the following options
      - Output full LDAP query
  - Audit activation
    - LDAP debugging requires activation via registry

Netlogon

- Log file
  - %SYSTEMROOT%\debug\netlogon.log
    - Activation via NLTEST command
- Provider: Netlogon
  - System
    - Event log
      - ID 5827 — The Netlogon service denied a vulnerable Netlogon secure channel connection from a machine account.
      - ID 5828 — The Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account.
      - ID 5829 — The Netlogon service allowed a vulnerable Netlogon secure channel connection.
      - ID 5830 — The Netlogon service allowed a vulnerable Netlogon secure channel connection because the machine account is allowed in the "Domain controller
      - ID 5831 — The Netlogon service allowed a vulnerable Netlogon secure channel connection because the trust account is allowed in the " Domain controller
      - ID 5805 — A machine account failed to authenticate

gMSA account

- Directory Service
  - Log file
    - ID 2946 — Call successfully fetched the password of a gMSA account
    - ID 2947 — Call failed fetched the password of a gMSA account

NTLM

- See 50-Authentication in Windows mindmap

61-Directory Services

Access

- Event log
  - Security
    - ID 4661 — A handle to an object was requeste
    - ID 4662 — An operation was performed on an object
- Audit policy
  - Audit Directory Service Access (S/F)
- SACL
  - Requires flag on object(s)

Extended rights usage

- Event log
  - Security
    - ID 4662 — An operation was performed on an object
- Audit policy
  - Audit Directory Service Access (S/F)
- SACL
  - All extended rights on object(s)

Changes

- Event log
  - Security
    - ID 5136 — A directory service object was modified
    - ID 5137 — A directory service object was created
    - ID 5138 — A directory service object was undeleted
    - ID 5139 — A directory service object was moved
    - ID 5141 — A directory service object was deleted
- Audit policy
  - Audit Directory Service Changes (S/F)
- SACL
  - Write all properties
  - Modify owner
  - Modify permissions
    - Provides advanced detection

Replication (basic)

- Event log
  - Security
    - ID 4932 — Synchronization of a replica of an Active Directory naming context has begun
    - ID 4933 — Synchronization of a replica of an Active Directory naming context has begun Success
- Audit policy
  - Audit Directory Service Replication (S/F)

Replication (detailed)

- Event log
  - Security
    - ID 4928 — An Active Directory replica source naming context was established
    - ID 4929 — An Active Directory replica source naming context was removed
    - ID 4930 — An Active Directory replica source naming context was modified
    - ID 4931 — An Active Directory replica destination naming context was modified
    - ID 4934 — Attributes of an Active Directory object were replicated
    - ID 4936 — Replication failure ends
    - ID 4937 — A lingering object was removed from a replica
- Audit policy
  - Audit Detailed Directory Service Replication (S/F)

62-DNS server

- See Server role mindmap

63-AD security related

Attack

- Event log
  - Security
    - ID 4649 — A replay attack was detected
- Audit policy
  - Other Logon/Logoff Events (S/F)

SID / ACL

- Event log
  - Security
    - ID 4765 — SID history added to an account
    - ID 4766 — Attempt to add SID History failed
    - ID 4780 — ACL set on admin account
- Audit policy
  - User account management (S/F)

DSRM

- Event log
  - Security
    - ID 4794 — Attempt to set the DSRM password (S/F)
- Audit policy
  - User account management (S/F)

IFM / NTDS

- Event log
  - Application
    - Provider: ESENT
      - ID 325 — The database engine created a new database
      - ID 326 — The database engine attached a new database
      - ID 327 — The database engine detached a new database

23-User and group management

Users

- Event log
  - Security
- Audit policy
  - Audit User Account Management (S/F)

Computers

- Event log
  - Security
- Audit policy
  - Audit Computer Account Management (S)

Groups

- Event log
  - Security
- Audit policy
  - Audit Security Group Management (S)

Password reset

- Event log
  - Security
    - ID 4723 — Attempt was made to change an account's password
    - ID 4724 — Attempt was made to reset an account's password
- Audit policy
  - Audit User Account Management (S/F)

Password security

- Event log
  - Security
    - ID 4782 — The password hash of an account was accessed
    - ID 4793 — The Password Policy Checking API was called
- Audit policy
  - Audit Other Account Management Events (S)

Lockout

- Event log
  - Security
    - ID 4740 — Account lock-out
- Audit policy
  - Audit User Account Management (S)