CH1 Window Audit Policy

Auditing

=) Each Windows has 9 audit policies / categories
- ↳ Win NT, 2000, XP - all auditing off by default
- ↳ Win 2003, 2008 - some auditing enabled
- ↳ Beginning with Win 2008 each category has sub category
  - → Audit policy can be controlled at category or sub category level

Audit Policy Configuration

=) Windows 2000 & 2003
- ↳ Local Security Policy
- ↳ Group policy (for AD is activate)

=) Window 2003
- ↳ Categories
  - → Local Security Policy
  - → Group Policy (activated AD)
- ↳ Subcategories
  - → Auditpol command
  - → Win2008 R2 (via Group Policy)

Windows will ignore Advanced Audit Policy configuration.

=> Audit policy status
↳ Success
↳ Failure
↳ No auditing.

=> Config subcategories on WM 2008
1. Enable "Audit: Force audit policy subcategory settings (Vista or later) to override audit policy category settings"
2. Configure subcategories
Re R2 -> Use auditpol command
R2 -> Can also use Group policy.

=> Auditpol command
↳ List all categories
auditpol /list /subcategory:*
↳ Turn on "Logon" for success & failure
auditpol /set /subcategory: "Logon" /success: enable /failure: enable
↳ Display current audit policy
auditpol /get /category:*

=) Category vs Subcategory
↳ Don't turn on entire categories in Win2008
→ Too much noise
→ Configure at subcategory level

=) Domain Controller
↳ ensure all DCs configured the same.
↳ Use Default Domain Controllers Policy GPO
↳ Linked to DC OU

=) Workstations & Member Server.
↳ Configure audit policy in GPOs linked to appropriate OUs

Categories
=) Account Logon
↳ Credential Validation
- NTLM events
↳ Kerberos Authentication Service
- Initial authentication
↳ Kerberos Service Ticket Operations
- Subsequent access to servers.

↳ Other Account Logon Events
- Dumping ground

⇒ Account Management
↳ User Account Management
↳ Computer Account Management
↳ Security Group Management
↳ Distribution Group Management
↳ Application Group Management
↳ Other Account Management Events
- Password, lockout policy
- Raising the domain functional level
- Network Security:
• Force logoff when logon hours expire.

⇒ Detailed Tracking
↳ Process Creation
↳ Process Termination
↳ DPAPI Activity
- activity concerning the Data Protection API

↳ RPC events
- events related to Remote Procedure Call security.

=) DS (Directory Service) Access
↳ Directory Service Access
- Access, move
↳ Directory Service Changes
- Create, Modify, Delete, Un delete
↳ Directory Service Replication
- non security
↳ Detailed Directory Service Replication
- non security

=) Logon / Logoff
↳ Logon
↳ Logoff
↳ Account Lockout
↳ IPSec Main Mode
↳ IPSec Quick Mode
↳ IPSec Extended Mode
↳ Special Logon

- Admin-equivalent logons

↳ Other Logon / Logoff Events
- Terminal services, workstation lock, screen saver

↳ Network Policy Server
- Network Access Policy funtionality for Windows networks which includes IPSec, 802.1x, quarantine

=> Object Access
↳ File System
↳ Registry
↳ Kernel Object
↳ SAM (Security Account Manager)
↳ Certification Services
↳ Application Generated
- Authorization Manager
↳ Handle Manipulation
↳ File Share
- share access
↳ Filtering Platform Packet Drop
- Windows Firewall

- MPSSVC (MpsSvc): a process belonging to Microsoft One Care Live which protect computer against Internet-bound threats.

↳ Filtering Platform Connection
- Windows Firewall
↳ Other Object Access Events
- Scheduled Task
- Dumping ground

=) Policy Change
↳ Audit Policy Change
↳ Authentication Policy Change
- Trusts, Kerberos, logon rights
↳ Authorization Policy Change
- user rights
↳ MPSSVC Rule-Level Policy Change
- Documents the current configuration Window Firewall and changes
↳ Filtering Platform Policy Changes
- Current configuration of the Windows Filtering Platform (related for lower level then the Window Firewall)
↳ Other Policy Change Events
- One event that should be in Filtering Platform Policy Change

* Hodgepodge : Confused mixture

=) Privilege Use
↳ Sensitive privilege use
↳ Non sensitive privilege use
- No events observed
↳ Other privilege use events
- No events observed

=) System
↳ Security State Change
- Startup, shutdown, time change
↳ Security System Extension
- Authentication package, logon process, notification package, security load ups
- New service installed
↳ System Integrity
- Crypto ops
↳ IPSec Driver
- operation of the IPSec system service
↳ Other System Events
- Hodgepodge of events dominated by Windows Firewall system service activity.

Per-user selective auditing

- Takes precedence over system level audit policy
- Per user, not user group
- Primarily useful for suppressing noise events from specific users
- Configured by command line
  - Win 2003 : auditusr
  - Win 2008 : auditpol
- List per user audit policy for ____.
  - auditpol /get /user: ____ /category: *
- Exclude success auditing of Logon for ____
  - auditpol /set /subcategory: "Logon" /user: ____ /exclude /success: enable.

Chap 2 Windows Security Logs

Overview

- Each Windows computer has its own security log
- Security events are not replicated between computers
  - Not even domain controllers
- Win 2003
  - binary format
  - C:\WINDOWS\System32\config\SecEvent.Evt
- Win 2008
  - XML format
  - System32\winevt\Logs\Security.evtx
- Location can be changed
- Can be dumped
  - Tab delimited
  - Comma delimited
  - Win 2003
    - Native binary EVT format
  - Win 2008
    - Native EVTX format
    - XML
- Can run into the issues when

viewing logs saved on one version of Windows from a different computer.

- Event Viewer (the only native tool for viewing security log)
  - ⇒ Event Viewer in Win 2008 improve
    - Filtering
    - Searching
    - Custom Views
  - ⇒ Win 2008 Tips
    - ↳ Don't try to filter by categories, use subcategories
      - Set Event Sources to "Microsoft Windows security auditing."
      - Task Category populated with subcategories
    - ↳ Event list shows subcategories as "Task Category"
      - Top level categories not shown

Event forwarding
- MS calls "Quick & Dirty"
- Refers to SCOM as "true enterprise eventing"

New Event Log Features in Win 2008

=) Event forwarding
=) Triggers
=) Custom View

Event forwarding

=) Good points:
→ Standard Based - DMTF WS-Eventing standard - see OpenWSMAN at SourceForge
→ Agentless
→ Down-Level Support - XP SP2+ and Win2003 SP1+
→ Multi-Tier - collectors may forward collectors.
→ Scalable ?
→ Group Policy configurable
→ Pre-Rendering - Events can now be pre-rendered on the Source Computer.
→ Resiliency
- mobile scenarios
- TCP for guaranteed delivery.

⇒ Security - Certificate based, encryption via Kerberos or HTTPS

⇒ Overview
↳ "Source" computers and "collectors"
↳ Options
- Should source or collector initiate?
  - Sources initiated configurable via group policy
- Which source logs
- Which destination log on collector
- Which events
- How often
- http / https

⇒ Event Forwarding Set Up Steps
1. Create Event Forwarding Subscription
↳ On source computer
↳ Open Event Viewer and select Subscription
- Which computer subscription applied to
- Which source logs

- WinRM (Windows Remote Management): Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows hardware and operating system, from different vendors, to interoperate.

- Which destination log on collector
- Which events
- How often
- http or https

2. Enable WinRM via Group Policy (setting)
   - ↳ Win 2008 & Vista (simple group policy)
     - Winrm quickconfig -q
   - ↳ Win 2003 & XP
     - install WS-Management 1.1

3. Configure security log permissions on source computers via Group Policy
   - ↳ XP SP2+
     - Run "Windows Remote Management" service as "Local System"
   - ↳ Win 2003
     - "CustomSD" key need to be set within "HKLM/SYSTEM/CCS/Services/EventLog/Security" to "O:BAG:SYD:(A;;CC;;;NS)"
   - ↳ Win 2008 / Vista
     - Add "Network Service" to the "Event Log Readers" Local Security Group.

4. Configure Event Forwarding via Group Policy
   ↳ Specify Computer (collector) to get subscription from
   ↳ All other settings defined in Subscription.
5. Test / Troubleshoot
   ↳ Events not showing up?
   ↳ has group policy been applied
   ↳ has the source computer registered with collector?
      ⇒ wecutil gr <subscription name>

B. Triggers
   ⇒ Win 2008 / Win Vista
      ↳ Task Scheduler
   ⇒ Win 2003 / Win XP
      ↳ EventTriggers.exe

B. Custom View
   ⇒ Can be saved
   ⇒ Multiple logs

=) Multiple events
=) Beyond filtering by event ID

Bottom line

=) Forwarding
↳ Can't manage entire logs
↳ Could be used for events of interest
=) Triggers
↳ Limited selection criteria
↳ No pre-built actions or workflow
↳ No group policy support
=) No reporting

Event Record Format

=) Standard fields in every event
↳ Event ID
↳ Date
↳ Time
↳ "Keywords"
↳ User
↳ Computer
↳ Source
↳ Task Category

=) Description
↳ Static string with insertion points for each data specific to Event ID
↳ Static data can be lost when viewing logs on different computer
- Computer
- Source DLL not available
- Different version of windows.

=) Changes with each version of Windows
↳ Events IDs
- New events added
- Events discontinued
- Events redefined.
↳ Description fields
- New field added
  - Even in the middle of existing fields

Q. Event ID Schemes in Win 2003 and Win 2008

=) No event IDs shared between pre and post Vista security logs

=) Pre-Vista
- 3 digit event IDs
=) Post-Vista
- 4 digit event IDs
=) Events migrated over.
- Legacy event ID +4096

Migrating / supporting log management for Win 2008
=) 3 pain point.
↳ Updating all
- Alert rules
- Noise filters
- Reporting criteria and columns
↳ Potential doubling of alerts and reports to analyze
↳ Inability to centrally configure audit subcategory policy.

CHAP3 Audit Trail Integrity

Audit Policy Access

=) Methods and authority required to modify audit policy

↳ Group policy
- write access to GPO

↳ Auditpol / local security policy
- Local admin authority
- User right: "Manage auditing and security log"
- Listed in Audit Policy Security descriptor:
  - auditpol /set /sd:D:(A;;DCSWRPDTRC;;;TRC;;;BA)(A;;DCSWRPDTRC;;;SY)
  - Set the security descriptor used to delegate access to the audit policy. The security descriptor must be specified using SDDL

Log handling

- Log file location
- Wrapping
- Rotation
- Dumping
- Access control

Properties

- Max size
  - Don't exceed 199mb on Win 2000, 299mb on 2003
- Wrapping options
  - Auto log rotation available.

Crash On Audit File

- HKLM\SYSTEM\CurrentControlSet\Control\Lsa
- Win 2008
  - auditpol /set /option:CrashOnAuditFail /value:enable

Moving security Log
=) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Security

Automatic Log File Rotation
=) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Security
=) Event 524 1105
↳ The security log file was saved as Security-2003-02-05-22-48-40-0.evt because the current log is full
=) Filename log file name & the date and time (in UTC)
↳ Logname-YYYY-MM-DD-HH-MM-SS-mmm.evt
=) Regular move these files to a secure archive server.

"Manage auditing and security log" user right required to
=) clear
=) change audit policy on specific objects

Viewing or dumping security log governed by:

=) Windows 2000
  ↳ "Manage auditing and security log" right

=) Windows 2003
  ↳ HKLM\System\CurrentControlSet\Services\Eventlog\Security\CustomSD - RegSZ in SDDL format
  ↳ SDDL explained at tinyurl.com/wiygb
  ↳ (A;;0x1;;;[SID])

=) Windows 2008
  ↳ Wevtutil command using the sl switch which means "set log"
  ↳ To get help on this command run "wevtutil sl /?"
  ↳ Look for /ca switch which means "channel access".
  ↳ Also check out "wevtutil gl" where gl means "get log"

Tampering

⇒ Clearing Log
- ↳ Requires Manage Auditing and Security Log right
- ↳ Subsequent event logged identifying clearer

⇒ Tampering requires
- ↳ Physical access
- ↳ Local Administrator membership
- ↳ Write access to GPO applied to computer.

⇒ Winzapper
- ↳ http://ntsecurity.nu/toolbox/winzapper/
- ↳ Requires admin authority
- ↳ Allow to selectively delete events
  - → Crashes the event logging service
  - → Leaves a dummy.dat file in same folder as security log.

⇒ Bottom line
- ↳ Basically a risk from administrators or successful hackers
- ↳ Only solution

→ Get events of monitored system and into a secure database as they occur.

Audit Trail Integrity Events
⇒ Audit Policy
⇒ Security Log

Audit Policy
⇒ 4719 - Audit policy changed
⇒ 4912 - Per user auditing policy set for user
⇒ 4904 - A security event source has attempted to register.
⇒ 4905 - A security event source has attempted to unregister
⇒ 4715 - Audit Policy ACL changed
⇒ 4906 - The CrashOnAuditFail value has changed
⇒ 4907 - Auditing settings on object were changed

B. Security Log

=) 4608 - Windows starting up

=) 4612 - Internal resources allocated for the queuing of audit message have exhausted, leading to the loss of some audits

=) 1101 - Audit events have been dropped by the transport

=) 1102 - The audit log was cleared

=) 1104 - The security Log is now full

=) 1105 - Events log automatic backup

=) 1108 - The event logging service encountered an error.

CH 4 Understanding Authentication & Logons

Logons

- 2 kinds of accounts
  - Local computer SAM
  - AD domain accounts
- 2 kinds of logons
  - Interactive
  - Network (aka remote)
- Credentials entered once
  - But seperate logon for each computer accessed
  - Workstation remembers credentials for each computer accessed.

Logon vs Authentication

- Logon
  - computer where the account gains access to objects can run programs
- Authentication
  - computer that checks the account's credentials
- Same computer for both
  - workstation or member server

↳ User is loggin on to domain controller itself

=) Different computers

↳ User logging onto workstation or member server with domain account

Logon / logoff events

=) Logged whenever an account logs onto the computer

↳ Interactively, network, batch, service, terminals services.

Accounts logon events

=) Logged only when local computer authenticates

↳ Domain controllers
- all domain account logons

↳ Member servers and workstations
- only local SAM accounts

B "Account Logon" useful

1) For centralized monitoring of domain account authentication (all DCs)
2) For detecting local account authentication

B "Logon / Logoff" still has its uses

1) Only way
   - ↳ See when user logged off
   - ↳ link process tracking and object access events to logon sessions.
   - ↳ provides more granular information on type of logon and logon failures
   - ↳ Can detect local account authentication.

Ch 3 Account Logon Events

Account Logons

=) Subcategories

↳ Credential Validation
→ NTLM events

↳ Kerberos Authentication Service
→ Initial Authentication

↳ Kerberos Service Ticket Operations
→ Subsequent access to services

↳ Other Account Logon Events
→ Only one event associated with IIS client certificate based authentication.

2 Authentication Protocols

=) Kerberos

↳ 3 sided protocol based on tickets

↳ Mutual authentication

↳ Better obfuscation

=) NTLM

↳ Based on old proprietary technology

↳ Easy to sniff and crack unless implemented

⇒ Default is Kerberos but Windows will fall back to NTLM

B NTLM

⇒ Used when ...

↳ Any pre-Win 2000 computer involved
- Client
- Server
- Domain Controller.

↳ Local SAM accounts

↳ Between un-trusted domains

⇒ NTLM events

OS	Event ID	Type	Description
2008	4776	Success Failure	Account Used for Logon

⇒ Description & fields

↳ By : Authentication table
↳ Account Name : pre-W2k logon name
↳ Workstation : computer name of workstation
↳ Error code

⇒ NTML Error Codes

Error Code		Error
Decimal	Hex	Description
3221225572	C0000064	user name not exist
3221225578	C000006A	user name correct, password wrong
3221226036	C0000234	user is currently locked out
3221225586	C0000072	account currently disabled.
3221225584	C0000070	work station restriction
3221225875	C0000193	account expiration
3221225585	C0000071	expired password
3221226020	C0000224	user is required to change password at next logon
3221225582	C000006F	user tried to login outside his day of week or time of day restriction.

Kerberos

- 3 principles
  - Client
    - User
  - Service
    - Workstation and each server accessed
  - KDC
    - AD domain controller
- Each principle has key
  - Simply the password of the user or computer.
- 3 sided authentication protocol
- Use tickets
- Time stamped
- Developed by MIT
- Used widely in UNIX
- Very secure except in case of weak passwords
  - Unless using smart cards for Windows interactive logons.

* KDC : Key Distribution Center

Event 4771: Kerberos pre-authentication failed

=) 2 kinds of tickets

↳ Service Ticket

- 1 needed for workstation and each server access
- Encrypted with KDC's key
- Contains:
  - Session key
  - Timestamp

↳ Ticket granting Ticket

- Used by client to obtain service tickets
- Encrypted with Service's key
- Contains:
  - Session key
  - Timestamp

=) Kerberos Process & Events

1. User enters domain credentials
2. Workstation obtain TGT from DC

↳ Fail

- Bad password or clocks out of sync - event 4771

- Event 4768 : A Kerberos authentication ticket was requested

Event 4769 : Kerberos service ticket was requested.

- Other reason - event 4768
  ↳ Succeeds
  - event 4768

3. Workstation uses TGT to obtain 3 service tickets
   ↳ Event 4769
   ↳ "Service" name is event description
   - Computer name of workstation
   - Computer name of domain controller
   - "krbtgt"

4. User tries to access a server
5. Workstation uses TGT to obtain ticket to server
   ↳ Succeeds - event 4769
   - User fields = user's account
   - Service fields = server's computer account
   ↳ Fails - event 4769 failure.
6. Workstation presents ticket to server.

* LDAP : Lightweight Directory Access Protocol

2) Understanding Kerberos Events

↳ Initial logon at workstation
- → 2 events:
  - 1 TGT event
  - 3 Service ticket event

↳ Accesses a server
- → 1 service ticket event

↳ Computers generate many Kerberos events
- → Group policy
- → LDAP queries
- → Can be ignored
- → Recognizable
  - user name and service name (with $)

⇒ Kerberos Events

Scenario	Event ID	Type	Description
Pre-authentication Failure	4771	Failure	Kerberos pre-authentication failed
Authentication	4768	Success Failure	A Kerberos authentication ticket (TGT) was requested
Service Ticket Request	4769	Success Failure	A Kerberos service ticket was requested
	4773	Failure	A Kerberos service ticket request failed Windows does not log this event - see 4769
Service Ticket Renewal	4770	Success	A Kerberos service ticket was renewed.

2) Computer account related Kerberos events

↳ Computer also authenticate and logon to other computers frequency
→ Application of group policy, file replication, etc.

↳ Easily identified
→ User name = computername$

↳ At boot up each computer in the domain obtains
→ TGT - 4768
→ Service ticket to the DC - 4769
→ Service Ticket to "krbtgt" - 4769

↳ Computer remains boots on for extended period

↳ Ticket reaches maximum lifetime

↳ Computer attempts to renew service ticket to "krbtgt"

↳ Similar chain of events for user ticket renewal

↳ Bottom line
→ usually safe to ignore.

2) Kerberos failure code

↳ Kerberos failure code came directly from RFC 1510 - The Kerberos Network Authentication Service (V5)

Failure code		Kerberos RFC description.
Dec	Hex	
1	1	Client's entry in database is expired
2	2	Server's entry in database is expired
3	3	Request protocol version # not supported
4	4	Client's key encrypted in old master key
5	5	Server's key encrypted in old master key
6	6	Client not found in Kerberos database
7	7	Server not found in Kerberos database
8	8	Multiple principal entries in database
9	9	The client or server has a null key
10	A	Ticket not eligible for postdating
11	B	Requested start time is later than end time
12	C	KDC policy rejects request.
13	D	KDC cannot accommodate requested option

41	29	Message stream modified
42	2A	Message out of order
44	2C	Specified version of key is not available
45	2D	Service key no available
46	2E	Mutual authentication failed
47	2F	Incorrect message direction
48	30	Alternative authentication method required
49	31	Incorrect sequence number in message
50	32	Inappropriate type of checksum in message
60	3C	Generic error (description in text)
61	3D	Field is too long for this implementation.

⇒ Common Kerberos event description field

↳ User name
- Pre-win 2000 user logon name

↳ User domain
- Pre-win2000 domain name
- Domain's DNS name
  - ACME.LOCAL

* Realm: a field or domain of activity

↳ User ID
- Pre-w2k domain name \pre-w2k user logon name
- ACME \JSMITH
↳ Supplied Realm Name
- Pre-w2k domain name
- Or domain's DNS name
↳ Service name
- Computername$
- krbtgt
- krbtgt/domain's DNS name
- HOST/ip address
↳ Service ID
- Domain \computername$
↳ Client Address
- IP address of computer initiating Kerberos request
↳ Ticket option
↳ Ticket Encryption
↳ Pre-Authentication

* PADATA => Pre-Authentication DATA

14	E	KDC has no support for encryption type
15	F	KDC has no support for checksum type
16	10	KDC has no support for padata type
17	11	KDC has no support for transited type
18	12	clients credentials has been revoked
19	13	Credential for server has been revoked
20	14	TGT has been revoked
21	15	Client not yet valid - try again later
22	16	Server not yet valid - try again later
23	17	Password has expired
24	18	Pre-authentication information was invalid
25	19	Additional pre-authentication required.
31	1F	Integrity check on decrypted field failed
32	20	Ticket expired
33	21	Ticket not yet valid
34	22	Request is replay
35	23	Ticket isn't for us
36	24	Ticket and authenticator don't match
37	25	Clock skew too great
38	26	Incorrect net address
39	27	Protocol version mismatch
40	28	Invalid msg type.

=) Bottom Line

↳ Kerberos allows to determine
- who is logging on to which workstation
- what servers do they connect to next
- Where are all those password guessing attempts coming from?

Ch 6 Logon / Logoff Events

Logon / Logoff Events and Buttom Line

- Logon
  - Enable for Success, Failure
- Logoff
  - Enable for Success
- Account Lockout
  - Enable for Success
- IPSec Main Mode
  - No auditing unless using IPSec
- IPSec Quick Mode
  - No auditing unless using IPSec
- IPSec Extended Mode
  - No auditing unless using IPSec
- Special Logon
  - Admin-equivalent logons
  - Consider enabling for Success
- Other Logon / Logoff events
  - Terminal services, Workstation lock, screen saver.
  - Optional
- Network Policy Server.

→ Network Access Policy funtionality for Windows networks which includes IPSec, 802.1x, quarantine
→ No auditing unless using NAP.

Success logon and Logoff events

Scenario	Event ID	Type	Description
Logon	4624	Success	An account was successfully logged on
Logoff	4634		An account was logged out
	4647		User initiated logoff

Logon/Logoff description fields.

1) User name
   ↳ pre-W2k login name
2) Domain
   ↳ pre-W2k domain name
3) Login ID
   ↳ Hex number identify logon session
   ↳ can be used to link object access and detailed tracking events.

=) Logon process
↳ Kerberos, user32, NtLmSsp, advapi, etc...
=) Authentication Package
↳ Kerberos, Negotiate, NTLM, etc...
=) Workstation name
↳ Pre-w2k computer name.
=) Logon type

Logon Type	Logon Title	Description
2	Interactive	physical console
3	Network	over network (through drive mapping)
4	Batch	Batch logon (such as scheduled tasks)
5	Service	Service logon
7	Unlock	Workstation unlocked
8	Network-Cleartext	Network logon with plaintext password
9	New-Credentials	Use alternative credential
10	Remote-Interactive	remotely via Terminal Services / Remote Desktop (not for Win2000 & previous)
11	Cached-Interactive	Logon with cached credential

Logon Failure

Event ID	Type	Description
4625	Failure	An account failed to log on

Sub-status code	Description
C0000064	user name does no exists
C000006A	username correct but password is wrong
C0000234	user is currently locked out
C0000072	account is currently disabled
C000006F	user tried logon outside his day of week or time of day restriction
C0000070	Workstation restriction
C0000193	account expiration
C0000071	expired password
C0000133	clocks between DC and other computer too far out of sync
C0000224	user is require to change password next login.

C0000225	evidently a bug in Windows and not a risk
C000015b	The user has not been granted the requested logon type at this machine

Terminal Services Event

Scenario	Event ID	Type	Description
RDP Session Reconnect	4778	Success	A session was reconnected to a Window Station
RDP Session Disconnect	4779		A session was disconnected from a Window Station

Bottom Line

- Identifies actual entries into local computer via
  - ↳ Network
  - ↳ Console
  - ↳ Terminal Services
  - ↳ Service Startup

① Account successfully logon over network on workstation

② Account successfully logon on server via physical console or remotely (via Terminal Service or Remote Desktop)

=) Potentially Suspicious
① ↳ 4624 with logon type 3 on workstation
② ↳ 4624 on server with logon type 2 or 10.

=) Requires monitoring of each computer
↳ Kerberos service ticket requests allow to reconstruct each computer accessed by looking at just DC logs.

Problems with tracking logoffs

=) Network logon sessions are terminated as soon as all open files are closed.
↳ Causing gobs and gobs of 4624/4634 pairs on file servers.

=) Interactive logon sessions
↳ 4634 is usually logged but not always
↳ 4647 is logoff initiated but sometimes the user aborts the logoff.

CH7 Process Tracking Events.

- Subcategories
  1) Process Creation
  2) Process Termination
  3) DPAPI Activity
     - Activity concerning the Data Protect API
  4) RPC Events
     - events related to Remote Procedure Call security

- Allow to track programs executed
  1) By users on their workstation
  2) Executed on Server

- Events can be linked to
  1) Files open by program
  2) Logon session.

- Process tracking

Scenario	Event ID	Type	Description
Process start	4688	Success	A new process has been created
Stop	4689		A process has exited.

* Image File Name can be New Process Name or Process Name

=) Description fields
↳ New Process ID
-> use for linking event ID
↳ Image File Name
-> path to executable
↳ Token Evaluation Type
-> Define how the process under User Account Control (UAC):
- 1: UAC disabled / ran on root
- 2: ran with evaluation
- 3: ran without evaluation
↳ Creator Process ID
=> Define a process ID of the process that started this new process
↳ User Name
↳ Domain
↳ Login ID

Linking
=) Linking process tracking and logon/logoff events
=) Linking parent and child process

2 Service Installation

Event ID	Type	Description
4697	Success	A service was installed in the system

Recommended Baseline Audit Policy

- Process Creation
  - Enabled for success on all computers
- Process Termination
  - Optional
- DPAPI Activity
  - No audit
- RPC events
  - No audit

Review Point

- Allow to track each and every executable run by whom and how long.
- Does not include scripts or batch files
- Can be correlated to logon and object access activity on same computer.
  - not cross system though
- Also provides tracking of scheduled tasks and services.

- SAM = Security Account Manager.

CH 8-1 Object Access Events — Core Concept.

Subcategories & baseline audit policy

⇒ File system
↳ File and folder level access

⇒ Registry
↳ Registry key and value access and changes

⇒ Kernel Object
↳ Present for Common Criteria Certification; not useful

⇒ SAM
↳ Present for Common Criteria Certification; not useful

⇒ Certification Services
↳ Applicable on Certificate Authority servers

⇒ Application Generated
↳ Authorization manager

⇒ Handle Manipulation
↳ Adds tracking of Open/Close events

⇒ File Share
↳ Share access

↳ No coverage of changes to shares until Win 2008 R2

⇒ Detailed File Share
↳ Like Object Open but only via shares (new in R2)

⇒ Filtering Platform Packet Drop
↳ Window Firewall
↳ Very noisy

⇒ Filtering Platform Connection
↳ Window Firewall
↳ Very noisy

⇒ Other Object Access Events.
↳ Scheduled Tasks
↳ Dumping ground.

Object Access

⇒ Can audit access to
↳ Files
↳ Folders
↳ Registry keys and values
↳ Printer
↳ Services

Object Access Audit policy.

=) 2 level activation

↳ System

→ Group policy

→ Auditpol command

↳ Object

→ Properties, Security tab, Advanced, Auditing tab

Object Level Audit Policy

=) Specified similar to file

↳ Auditing must be enabled for

→ Object

→ Success / Failure

→ User or Group

→ Access

- read, write, delete.

=) 2 Types:

↳ File access

↳ Folder access

B. Object access events

=) Access levels to be tracked
- ↳ Read
- ↳ Write
- ↳ New child object
- ↳ Deletions

(like select, update, insert, delete in RDBMS)

=) Track successful and failed access attempts

=) Can be linked to
- ↳ Logon events
- ↳ Process tracking events

=) Event ID ** (next page)

*Important ID in tracking event:

1. Handle ID (In Object)
=) Semi-unique ID (unique between reboots) that identifies all subsequent audited event while the object is open.
2. Process ID (In Process information)
=) Unique number that identifies each running processes in a operating system.

Scenario	Event ID	Type	Description	Audit Policy	
Object Open	4656	Success Failure	A handle to an object was requested	File system, Registry, SAM, or Other Object Access Events	and Handle Manipulation
Accessed	4663	Success	An attempt was made to access an object		
Closed	4658		The handle to an object was closed		and Handle Manipulation

Object access attempt

⇒ Logged

↳ Between Open & Close

↳ Whenever 1 or more access permissions are actually used for the first time
- but subsequently re-used are not re-logged.

↳ only logged on success.

Open and Close Events

⇒ Usually extra noise

↳ Handle open events
- Specifies the permission the user acquired to object when opening it
- NOT - which permission the user actually exercised.

↳ Handle close events

⇒ Track successful access

↳ Track 4663 - Object access

↳ Disable Handle Manipulation subcategory
→ Open and close events not logged

=) Handle Manipulation needed for:
↳ Duration of object open
↳ Tracking access failure

How was the object accessed
=) "Access Request Information" in event description
↳ Specifies types of access user opened object with
↳ Corresponds to low level "special" permissions.

Review
=) Enable the right subcategories
↳ File system
↳ Registry
↳ Kernel Object
↳ SAM
↳ Track
→ Access failures
→ Duration of object was open
→ Enable "Handle Manipulation"

=) Enable auditing at the object level
  ↳ On desired objects
  ↳ For the right people
    → everyone
  ↳ For the right types of access
    → permission
    → Success and/or Failure
=) Track 4633 (access)
  ↳ User
  ↳ Object
  ↳ Type of access
=) If access denied
  ↳ 4656 (object open) - Handle request
  ↳ Logged if failure auditing enabled for that
    → Object
    → Permission
=) Duration for object opened?
  ↳ Compare time of
    - 4656 (open) and 4658 (close)
  ↳ Correlate with Handle ID

Object Deletion

Scenario	Event ID	Type	Description
Object Deleted	4660	Success	An object was deleted.

* Deletions also logged by 4663
4663 : An attempt was made to access an object
In "Accesses" of "Access Request Information", it will show "DELETE".

Tracking other types of objects

1) Registry
   - Keys
   - Values

   } Subcategory: Registry

2) Printer
3) System Services
4) SAM
5) Kernel objects.

} Subcategory: ~~Object~~ Other Object Access Event.

Object access events

- Win 2008 varies audit subcategory according to object type
- Event 4656 (open), 4658 (close), 4663 (access) can show up as
  - File system
  - Registry
  - SAM
  - Other Object Access Events

Event 4657 - A registry value was modified

- Key
- Value
- Operation
  - Created
  - Modified
  - Deleted

  } choose 1
- Value data and type
  - Before
  - After

  } both

Global Object Access Auditing

- New to Win 2008 R2
- Define global audit policy applied to all
  - Files
  - Registry key
- Combined with object's audit policy
- Define users or groups to track across entire computer.
- Specify
  - Users or groups to be tracked
  - Permissions they exercise (Success/failure)
- Applies to all objects on entire system
  - Whether object's audit policy defined or not
- If conflict between global audit policy and the object's audit policy
  - Policies are cumulative
  - If either policy result indicates action should be audited
    - → Event is generated

=) In general, don't use.

Review points

=) 2 level activation

=) Object access primarily provides file system access auditing

=) Events reflect interaction between application and file system - not user and application.

CH 8.2 Object Access Events - Audit Scenarios

Object Access auditing

=) Advantages
- ↳ Detecting changes to fairly static files
- ↳ Detecting permission changes
  - → Caveat: notification on child object
  - → More to come in this chapter
- ↳ Accessed record
- ↳ Providing assurance admin level users have not accessed sensitive information
- ↳ Tracking down file deletions

=) Object Access
- ↳ Auditing modification to Office documents
- ↳ Auditing database files
- ↳ No good for copy
  - → 2 events: read, create
- ↳ No good for moves and deletes
  - → 2 events: delete, create

* Caveat: notice

=) Audit policy tips
↳ Normally audit "EVERYONE"
→ Unless monitoring admin authority
↳ Don't audit Read permission on folders
↳ Becareful about auditing reads access in general
↳ Understand meaning of each permission as it pertains to folders vs. files.

Audit Scenario

=) Attempts to look at unauthorized files
=) Audit trail of information access
=) Audit trail of modification
=) File / Folder creation
=) File / Folder Deletion
=) Permission changes
=) Providing assurance admin level users have not accessed sensitive information.

		Attempts to look at unauthorized files
Audit	Audit Policy	=> Enable File System and Handle Manipulation
		=> Desired folder ↳ Enable Failed Read Data ↳ This folder, subfolder and
	Monitor 4656 (access)	=> Desired folder => Failed => Read Data
Identity	Note subject & object	=> Yes
	Caveats	—

	Audit Trail of Information access	Audit Trail of Modification
	=> Enable File System	
for everyone files	↳ Files only	
	↳ Enabled Successful ReadData for Everyone	↳ Enabled Successful WriteData for Everyone
	=> Successful	
	=> Read Data	=> Write Data
	=> Window Explorer thumbnails and preview	=> Doesn't work for office docs.

	File Creation	Folder Creation
	* Rejected (Poor Implementation)	
Audit Policy	=> Enable File System	
	=> Desired folders ↳ Folder only	
	↳ Enable successful Create file for Everyone	↳ Enable successful create file for Everyone
Monitor Utils	=> Desired folders	
	=> Successful	
	=> Add File	=> Add Subdirectory
Note Subject & object	=> Yes	=> Yes (parent folder)
Caveats	=> Ambiguity between this activity and File Modification => Object may be parent or new file name ↳ From Notepad: Object = new file ↳ From Explorer: Object = parent	=> Ambiguity between this and AppendData to ↳ Object type: File => New subfolder name not specified => New folders from audited but not command.

	File deletion	Folder deletion
	↳ File only	↳ Folder only
	↳ Enable successful delete for Everyone	
	=> Delete	
	=> Yes	
activity file	=> Ignore 4660 (file name omitted)	=> Object type: File
Explorer "md"		

Audit Scenario: Tracking Permission Change

=> 2 Options
- 4663 with WRITE_DAC
- 4670 - Permissions on an object were changed.

=> Event ID 4663 with WRITE_DAC
- Tell changed permission
- Don't tell the changes
- Changing permission on a parent object
  - => Windows logs an event for every child objects
- Thus 4670 is better.

=> Event 4670 - Permissions on an object were changed.
- Shows up as subcategory Authorization Policy Change
- But
  - => Independent of that category
  - => Depends on
    - File system subcat enabled.

- "Change Permission" auditing enabled at the object level

Audit Scenario - Providing assurance admin level users has not accessed sensitive information

⇒ This scenario incompatible with other scenarios requiring any kind of success audit

⇒ Sensitive folder audit policy
  ↳ Administrators (instead of Everyone)
  ↳ ReadData
  ↳ Files only

⇒ Monitor 4663 (access) with
  ↳ Folder name
  ↳ Success
  ↳ ReadData

Review Point

1) Object Access audit is the best for monitoring
   - ↳ Permission Change
   - ↳ Knowing something changed in a folder
     - → Except Office documents
   - ↳ Attempts to access unauthorized data
   - ↳ Providing assurance admin level users have not accessed sensitive information

CH8.3 Object Access Events - Other Sub categories & File Share Sub Categories

⇒ File share
- ↳ Logs whenever share accessed
- ↳ Win2008 R2
  - Finally get share maintainance event.

⇒ Detailed File Share
- ↳ New to Win2008 R2
- ↳ Logs whenever access control decision made on share

⇒ File Share Events

Event	OS	Sub-cat.	Type	Scenario
5140	2008	File Share	Success	First time you access a given network share during a given logon session
5142	2008 R2			Share created
5143				Share modified
5144				Share deleted
5145		Dedicated File Share	Success Failure	Network share object was checked to see whether client can be granted desired access

Certificate Service

=) Useful on Certification Authorities
  ↳ For monitoring PKI administration
  ↳ 2-level activation audit policy
    - This sub categories
    - Auditing tab of the Properties dialog of the CA in the Certification Authority MMC snap-in.

Event	Title
4886	The certificate manager denied a pending certificate request
4887	Certificate Services recieved a resubmitted certificate request
4870	Certificate Service revoked a certificate
4871	Certificate Service recieve a request to publish the certificate revocation list (CRL)
4872	Certificate Services published the certificate revocation list (CRL)
4873	A certificate request extension changed
4875	Certificate Services recieved a request to shutdown.

AD CS = Certificate Service.

Event	Title
4876	CS backup started
4877	CS backup completed
4878	CS restore started
4879	CS restore completed
4880	CS Started
4881	CS stopped
4882	The Security permissions for CS changed
4883	CS retrieved an archived key
4884	CS imported a certificate into its database
4885	The audit filter for CS changed
4886	CS received a certificate request
4887	CS approved a certificate request and issued a certificate
4888	CS denied a certificate request
4889	CS set the status of certificate request to pending
4890	The certificate manager setting for CS changed
4891	A configuration entry changed in CS
4892	A property of CS changed
4893	Certificate Service archive a key

4894	CS imported and archived key
4895	CS published the CA certificate to AD Domain Services
4896	One or more rows have been deleted from the certificate database
4897	Role Separation enabled
4898	CS loaded a template
4899	A CS template was updated
4900	CS template security was updated

Application generated

Event	Title
4665	An attempt was made to create an application client context
4666	An application attempted an operation
4667	An application client context was deleted
4668	An application was initialized.

Other Object Access Events

=) Same events as File system logged but for access to system services.

Event	Title
4656	A handle to an object was requested
4658	The handle to an object was closed.
4659	A handle to an object was requested with intent to delete
4660	An object was deleted
4663	An attempt was made to access an object

Scheduled Task

Event	Type	Description	Scheduled Task Operation
4698			Create
4699			Delete
4700	Success	A scheduled task was_.	Enable
4701			Disable
4702			Update

* WFP = Window Filtering Platform.

Filtering Platform Connection

Event	Title
5031	The Window Firewall Service blocked an application from accepting incoming connection on the network
5154	The WFP has permitted an application or service to listen on a port for incomming connection
5155	The WFP has blocked an application or service to listen on a port for incomming connection
5156	The WFP has allowed a connection
5157	The WFP has blocked a connection
5158	The WFP has permitted a bind to a local port
5159	The WFP has blocked a bind to a local port.

Filtering Platform Packet Drop

Event	Title
5152	The Window Filtering Platform blocked a packet
5153	A more restrictive Window Filtering Platform filter has blocked a packet.

Review Points

=) File Share subcat - Useful in 2008 R2
- must deal with all the instances of 5140

=) Certificate Services & Application Generated very valuable on applicable system

=) Other Object Access useful for tracking changes to system services and scheduled tasks.

=) Disable other subcatagories normally.

CH 9 Account Management

Sub categories & baseline audit policy

=) User Account Management
↳ Enable on DCs & member server

=) Computer Account Management
↳ Enable on DCs only

=) Security Group Management
↳ Enable on DCs & member server

=) Distribution Group Management
↳ Optional on DCs

=) Application Group Management
↳ Optional

=) Other Account Management Events
=> Password, lockout policy
=> Raising the domain functional level
=> Network security: Force logoff when logon hours expire

↳ Enable.

Account management events

- Allow to track administration of
  - Users
  - Groups
  - Computers
- Operations
  - Creation
  - Changes
  - Deletion
  - Group members
    - Additions
    - Removals

Users

- Actual end-users
- Service / application accounts

Computers

- Workstations
- Member servers
- Domain Controller.

Groups

=) Have scope and type

=) Type

↳ Distribution

- cannot be assigned rights or permission
- can only be used as distribution lists in Exchange
- listed as "security disabled" in event

↳ Security

- assigned rights and permission
- used as distribution list in Exchange
- listed as "security enabled" in event

• Indicates events are logged on domain controller only

			Created	Changed	Deleted	Member	
						Added	Removed
User			4720	4738	4726	Not applicable	
Computer			4741	4742	4743		
Groups	Security	Local	4731	4737	4734	4732	4733
		Global	4727	4735	4730	4728	4729
		Universal	4754	4755	4758	4756	4757
	Distribution	Local	4744	4745	4748	4746	4747
		Global	4749	4750	4753	4751	4752
		Universal	4759	4760	4763	4761	4762

Description fields User changes

=) Second line of description sometimes include a description of what was changed

Description fields (Windows 2003) User creation / change operations.

=) Changed Attributes
=) Sam Account Name
=) Display Name
=) User Principal Name
=) Home Directory
=) Home Drive
=) Script Path
=) Profile Path
=) User Workstations
=) Password Last Set
=) Account Expires
=) Primary Group ID
=) Allowed Group ID
=) Old UAC Value
=) New UAC Value
=) User Account Control
=) User Parameters
=) Sid History
=) Logon Hours

Additional user related events

Event	Description
4722	User account enabled
4723	Change password attempt Win 2000: This event is logged for both password changes and reset Win 2003/2008: Only logged for changes
4724	User account password reset Win 2000: Not logged Win 2003/2008:
4725	User account disabled
4740	User account locked out.
4767	User account unlocked

Group related events

=) Create, change, delete, member, change

↳ Description fields

- [type] [scope] Group Created:
- New or Target : Group that was acted on
- Subject : who did it

=) Member change

↳ Description Fields

→ [type] [scope] Group Member [Added / Removed]

→ Member Name : member added or removed

→ Group : from which member added or removed

→ Subject : who do it.

=) Other group related events

Event	Description
4764	Group type changed

↳ Description Fields

→ Subject : who do it

→ Group : that was changed.

=) Other account management event

Event	Type	Description
4739	Success	Domain policy changed.

The Local SAM

=) Detecting Local SAM Account Activity on Member Servers

↳ The Importance of member server security logs

↳ Local SAM on Windows Servers

↳ Key security events for SAM activity.

Member server security logs

=) Reason don't monitor DC security logs only

↳ Logon attempts with local accounts

↳ Logon type and accurate logon failure reasons

↳ Policy changes

↳ File auditing

↳ System events

↳ Program execution

↳ Change to local users and groups.

Local SAM on Servers

1) Computer Management
   ↳ Local Users and Groups
2) Critical Operations
   ↳ New user account
   ↳ Account enabled
   ↳ Password Reset
   ↳ Group member added
3) Monitor member server security logs
4) Alert or review daily.

Event	Operation	Notes
4720	New user account	
4722	Account enabled	*False positive if preceded by 4720 for same user account.
4724	Password reset	
4732	Group member added	

DC vs Member Server event.

=) Events from many computers in one DB.
=) Distinguish DC account management events from Member server events.
=) New / target domain for member server = Computer name

Other important events for Local SAM Security

Event ID	Operation
4725	User account disabled
4726	User account deleted
4733	Group member removed.
4740	User account locked out

Review Points

=) Important category for both DCs and member servers
=) Different event for each object type and action
=) Many events only logged on DCs

CH 10

Directory Service Access Event.

Subcategories with recommended baseline Audit Policy

=) Directory Service Access
- ↳ (Disable)
- ↳ Not useful unless looking for
  - → Access failures
  - → Read activity

=) Directory Service Changes
- ↳ (Enable for success)
- ↳ Provides good coverage of changes to AD objects

=) Directory Service Replication
- ↳ (Disable)

=) Detailed Directory Service Replication
- ↳ (Disable)

Directory Service Changes

=) Track access to AD objects
- ↳ Users
- ↳ Groups
- ↳ Computers
- ↳ Organizational Units
- ↳ Group Policy Objects
- ↳ Domain Object
- ↳ etc.

=) Operations
  ↳ Creation
  ↳ Deletion
  ↳ Property level access
    → User
      - Full name
      - Job title
      - Account Options
      - Telephone numbers.

=) Similar to object access
  ↳ Must enable auditing for specific objects. Before access events are logged
  ↳ Very granular, must refer AD schema
  ↳ Tells
    → What properties changed
    → Before and after data

=) First enable "directory service changes" on each domain controller
=) Then enable auditing for desired AD object (2 level of auditing):
  ↳ Object
  ↳ Property

Event	Title	
5136	A directory service object was ___	modified
5137		create
5138		undeleted
5139		move
5141		deleted

Directory Service Changes vs Account Management events

Account Management events	Directory Service changes
→ Only users, groups, computers	→ All Active Directory classes
→ Specific event IDs for each class of objects and operations	→ 5 events for entire directory service access category
→ Only SAM level attributes ↳ not all X500 properties	→ All properties.

=) Use Account Management where possible
=) Directory Service Changes is needed for:
↳ Tracking user properties not covered by Account Management
↳ Tracking Group Policy related changes
↳ Tracking delegation of admin authority
↳ Tracking moves
↳ Tracking OU deletions

Tracking user properties not covered by Account Management.
=) At root of domain add audit entry
↳ Everyone
↳ On Property tab
- Apply to User objects
- Write access to specific properties
=) Monitor 5136(A directory service object was modified) with property name and object class user.

Tracking Group Policy related changes

⇒ Auditing of GPO create / edit / delete

↳ Add audit entries to System\Policies
→ Create groupPolicyContainer objects
→ Write All Properties of groupPolicyContainer objects on System\Policies
→ Delete groupPolicyContainer

↳ Monitor for 5136, 5137, 5141. (A directory Service object has modified (created/deleted) with
→ groupPolicyContainer

⇒ Group Policy Object (GPO)

↳ Object Type: groupPolicyContainer
↳ GPO edited
→ Accesses : Write Property
→ Properties: versionNumber
↳ GPO permissions changed
→ Accesses: Write Permission

* SDDL → Security Descriptor Definition Language

⇒ Used to define formatting used in expressing a security description, usually as a text string. SDDL is used in the nTSecurityDescriptor attribute for defining an ACL as well as in registry keys and NTFS file

⇒ Auditing Group Policy related changes on container objects

↳ At root of domain add audit entries for

→ domainDNS, organizationalUnit, site

→ Audit entries

- Write access to gPOptions
- Write access to gPLink

↳ Monitor for 5136 (A Directory Service object was modified) with

- domainDNS, organizationalUnit or site
- gPOptions or gPLink.

Tracking delegation of admin authority

⇒ At the root of domain add audit entries for

↳ Everyone

↳ This object and all child objects

↳ Modify Permission

⇒ Monitor 5136 with nTSecurityDescriptor as attribute value name

↳ 2 occurrences = before and after ACL in SDDL

Tracking move

- 5139 only recorded
  - if new Parent OU has Create auditing enabled for All Objects or at least that type of child object
- New and old Distinguished Name (DN) reported

Tracking OU deletions

- Add root of domain, add audit entry
  - Everyone
  - Apply to OUs
  - Delete & Delete subtree
- Monitor 5141 (A directory service object was deleted)

Review Points

- Useful for tracking AD changes not caught by account management
- Allow to track
  - Group policy changes
  - Delegated administrative authority
- Very granular and cryptic
  - Must know AD schema.

CH4 Policy Change Event

Subcategories & Recommended Baseline Audit Policy

=) Audit Policy Change
↳ (enable)

=) Authentication Policy Change
↳ (enable)
↳ Trusts, Kerberos, logon rights

=) Authorization Policy Change
↳ (enable)
↳ User rights

=) MPSSVC Rule-Level Policy Change
↳ (Optional)
↳ Documents the current configuration Window firewall and changes

=) Filtering Platform Policy change
↳ (optional)
↳ Current configuration of the Window Filtering Platform Crelated for lower level than the Window Firewall

=) Other Policy Change Events
↳ (optional)
↳ One event that should be in Filtering Platform Policy Change

Good
=) Windows logs events for most security configuration changes

Bad
=) Windows doesn't log events for most changes under "Security Option".

Ugly
=) Many events fail to identify who made the change.

Format
=) Identify the policy / configuration change
=) Event IDs
=) When does Windows log the event?
  ↳ Real-time?
  ↳ Next refresh of group policy?
=) Does the event identify whodunnit?
=) What does the event leave out?
=) Security policy changes not reported by the security logs.

Kerberos Policy

=) Policies

↳ Computer Configuration\Windows Settings\Security Setting\Account Policies\

→ Kerberos Policy

=) Format

↳ Event IDs : 4713

↳ When does Windows log the event?

- Next refresh group policy

↳ Does the event identify whodunnit?

- No - SYSTEM

↳ What does the event leave out?

- No complaints, all changed Kerberos values documented.

Trust Relationship

=) Format

↳ Event IDs

Event	Title	
4706	A new trust was created to a domain	
4707	A trust to a domain was removed	
4716	Trusted domain information was modified	
4865	A trusted forest	added
4866	information entry was	removed
4867	___.	modified

↳ When does Windows log the events?
→ At time of change
↳ Does the event identify who dunnit?
→ Yes
↳ Complaints
→ Duplicate events, cryptic codes, "trusted/trustng"

Password Policy
=) Not covered by this category
=) See Account Management : Other.

User right assignment

=) Logon right

↳ Logon locally, Access this computer from the network, et al.

↳ Subcategory: Authentication Policy Change

=) User rights

↳ Everything else

↳ Subcategory: Authorization Policy Change

Logon Right

=) Types

↳ Logon locally (aka interactive)

↳ Access this computer from the network

↳ Logon through Remote Desktop

↳ Logon as a server

↳ Logon as a batch job

↳ Deny rights as well.

=) Format

↳ Event ID

→ 4717 (assigned)

→ 4718 (removed)

↳ When does Window log the event?
→ Next time group policy applied.
↳ Does the event identify whodunnit?
→ No - SYSTEM
↳ Complaints?
→ NONE

User Rights Assignment

⇒ Policies
↳ Computer Configuration \ Window Settings \ Security Settings \ Local Policies
→ User Rights Assignment.

⇒ Event IDs
↳ 4704 - assigned
↳ 4705 - removed

⇒ When does Window log the event?
↳ Next refresh of group policy

⇒ Does the event identify whodunnit?
↳ No - SYSTEM

⇒ What does the event leave out?
↳ No complaints, all changed values documented
↳ See xref for translating rights system name
→ Logon rights
→ User rights

IP Security Policies

- Policies
  - Computer Configuration / Windows Settings / Security Settings / IP Security Policies.
  - Event ID
    - 4709 - 4712
    - 5040 - 5049
- When does Windows log the event?
  - Next refresh of group policy
- Does the event identify who dunnit?
  - No - SYSTEM
- What does the event leave out?
  - No complaints

Encrypting File System

- Event ID
  - 4714 - Encrypted data recovery agent changed
- When does Windows log the event?
  - Next refresh of group policy
- Does the event identify who dunnit?
  - No - SYSTEM

=> What does the event leave out?
↳ No complaints

Review Points

=> Provide important policy change notifications
↳ Far from complete though

=> "Who did it" often not reported since changes made indirectly via group policy.

Ch 12 System Events

Sub categories & recommended baseline audit policy

=) Security State Change
↳ (enable)
↳ Startup, shutdown, time change

=) Security System Extension
↳ (enable)
↳ Authentication package, logon process notification package, security package load ups
↳ New service installed

=) System Integrity
↳ (optional)
↳ Crypto ops

=) IPSec Driver
↳ (optional)
↳ operation of the IPSec system service

=) Other System events.
↳ (disable)
↳ Hodge podge of events dominated by Windows Firewall system service activity

Security State Change

Event	Type	Title
4608	Success	Windows NT is starting up
4609	Success	Windows NT is shutting down
4616	success	The system time was changed

Security System Extension

2) Logged at system startup
2) Security value
   ↳ Detect rogue plug-ins

Event	Title
4610	Authentication package has been loaded by the Local Security Authority
4611	Trusted logon process has been registered with the Local Security Authority
4614	Notification package has been loaded by the Local Security Authority
4622	A security package has been loaded by the Local Security Authority
4697	A service was installed in the system

Service Installations

Event	Type	Description
4697	Success	A service was installed in the system

Review Points

⇒ Wide range of events
↳ Some very important such system start and time change
↳ Plenty of noise generated by some sub categories.