

Auditování ve Windows

Lukáš Brázda | MCT, MCSA, MCSE | lukas@brazda.org

OBSAH

- Úvod
- Auditování
- EventLog

Úvod



CO JE AUDITOVÁNÍ VE WINDOWS

- Je to jeden z typů monitorování
- Jde o zaznamenávání událostí o činnosti uživatelů, služeb, systémů atp.
- Díky auditování jsem schopen najít odpovědi na otázky jako:
 - Co se stalo?
 - Kde se to stalo?
 - Kdy se to stalo?
 - Kdo to udělal a odkud?

CHCI AUDITOVAT? A PŘÍPADNĚ CO?

- Zapnout auditování všeho, pro všechny a na všech systémech – je to dobrý nápad?
- Není a to z několika důvodů:
 - Generovalo by to kvanta dat
 - Tato data by bylo třeba někam uložit, kontrolovat a vyznat se v nich
 - Mohlo by to ovlivnit výkon serveru
- Naopak pokud budete auditovat „málo“, můžete přijít o ty události, co vás zajímají
- Cílem tedy je nebýt ani „přeauditovaný“ ani „podauditovaný“

CO VŠECHNO LZE AUDITOVAT?



JEDNODUCHÉ (STARŠÍ) AUDITOVÁNÍ

Local Security Policy

File Action View Help

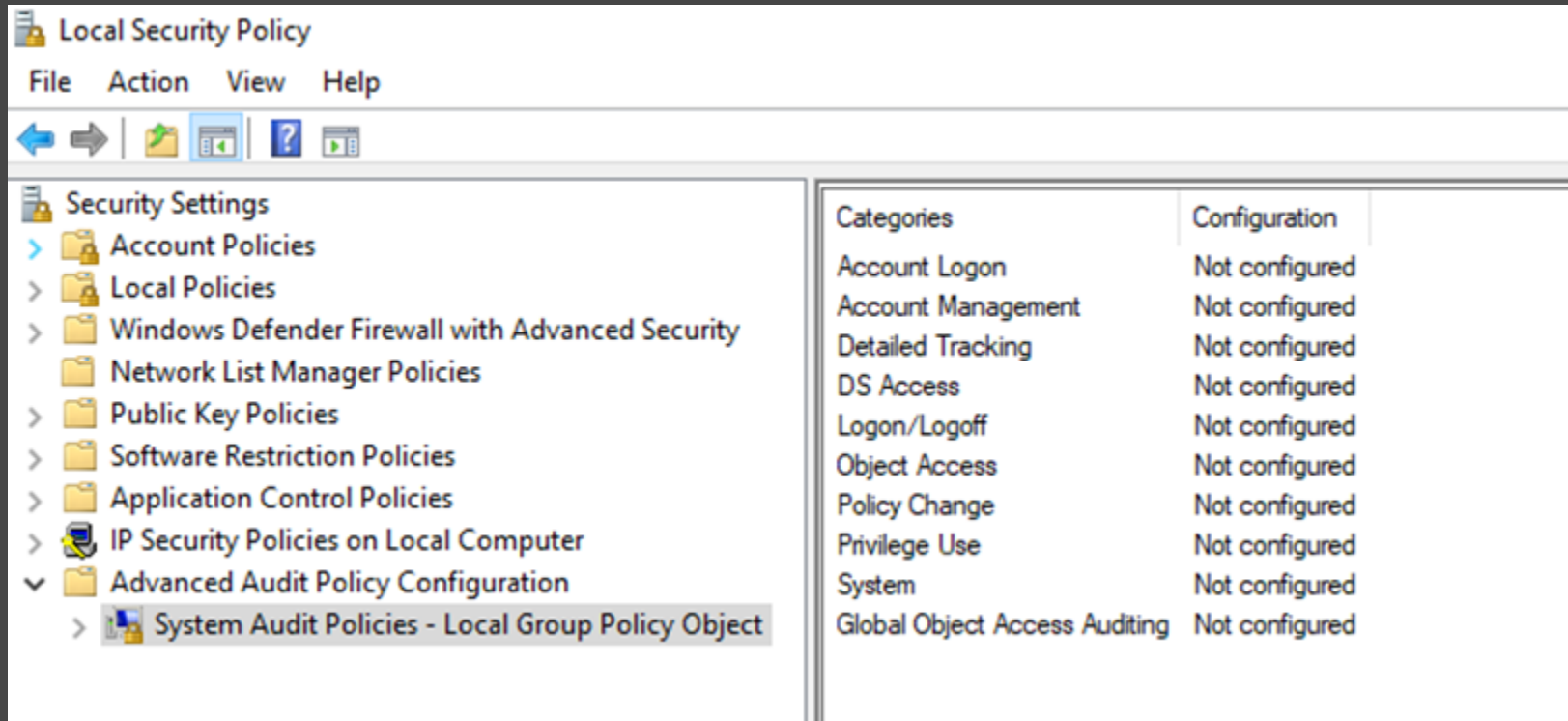
Security Settings

- > Account Policies
- ▼ Local Policies
 - Audit Policy**
 - > User Rights Assignment
 - > Security Options
- > Windows Defender Firewall with Advanced Security
- Network List Manager Policies
- > Public Key Policies
- > Software Restriction Policies
- > Application Control Policies
- > IP Security Policies on Local Computer
- > Advanced Audit Policy Configuration

Policy

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

GRANULÁRNÍ (NOVĚJŠÍ) AUDITOVÁNÍ



The screenshot displays the Windows Local Security Policy console. The left pane shows a tree view of Security Settings, with 'System Audit Policies - Local Group Policy Object' selected. The right pane shows a list of audit categories and their configuration status.

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

C:\>auditpol /get /category:*

Account Logon

Kerberos Service Ticket Operations
Other Account Logon Events
Kerberos Authentication Service
Credential Validation

Account Management

Computer Account Management
Security Group Management
Distribution Group Management
Application Group Management
Other Account Management Events
User Account Management

Detailed Tracking

Process Creation
Process Termination
DPAPI Activity
RPC Events
Plug and Play Events
Token Right Adjusted Events

DS Access

Directory Service Access
Directory Service Changes
Directory Service Replication
Detailed Directory Service Replication

Logon/Logoff

Logon
Logoff
Account Lockout
IPsec Main Mode
IPsec Quick Mode
IPsec Extended Mode
Special Logon
Other Logon/Logoff Events
Network Policy Server
User / Device Claims
Group Membership

Object Access

File System
Registry
Kernel Object
SAM
Certification Services
Application Generated
Handle Manipulation
File Share
Filtering Platform Packet Drop
Filtering Platform Connection
Other Object Access Events

Detailed File Share
Removable Storage
Central Policy Staging
Policy Change
Audit Policy Change
Authentication Policy Change
Authorization Policy Change
MPSSVC Rule-Level Policy Change
Filtering Platform Policy Change
Other Policy Change Events
Privilege Use
Non Sensitive Privilege Use
Other Privilege Use Events
Sensitive Privilege Use
System
Security System Extension
System Integrity
IPsec Driver
Other System Events
Security State Change

NEJZAJÍMAVĚJŠÍ KATEGORIE AUDITOVÁNÍ

- Account Logon
- Logon/Logoff
- DS Access
- Account Management
- Object Access

JAK AUDITOVÁNÍ NASTAVIT?

- SecPol.msc / GPEdit.msc
- GPO
- Auditpol.exe:
 - `Auditpol.exe /get /Category:"Object Access" /Success:Disable /Failure:Enable`
 - `Auditpol.exe /set /Subcategory:"File System" /Success:Enable /Failure:Enable`
 - `Auditpol.exe /set /Category:"Object Access" /Success:Disable /Failure:Disable`

AUDITUJE SE NĚCO SAMO OD SEBE?

- Windows Server i Client mají ve výchozím stavu nějaké auditování nastaveno
- Server i Client se trochu liší
- Aktuální nastavení lze zjistit pomocí:
 - `Auditpol.exe /get /category:*`
 - `Auditpol.exe /get /category:* /r`

DEFAULT: WINDOWS 10

- Windows 10 Enterprise Build 1803

Subcategory	Settings
Account Lockout	Success
Audit Policy Change	Success
Authentication Policy Change	Success
Logoff	Success
Logon	Success
Network Policy Server	Success and Failure
Other System Events	Success and Failure
Security Group Management	Success
Security State Change	Success
Special Logon	Success
System Integrity	Success and Failure
User Account Management	Success

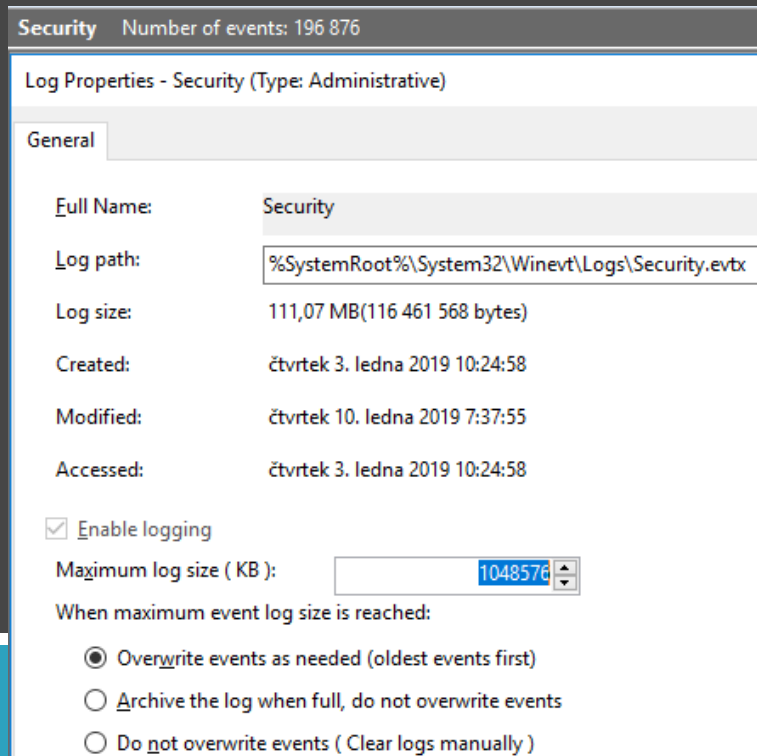
DEFAULT: WINDOWS SERVER

- Windows Server 2016 DTC RTM
- Windows Server 2019 DTC RTM

Subcategory	Settings
Account Lockout	Success
Audit Policy Change	Success
Authentication Policy Change	Success
Computer Account Management	Success
Credential Validation	Success
Directory Service Access	Success
Kerberos Authentication Service	Success
Kerberos Service Ticket Operations	Success
Logoff	Success
Logon	Success and Failure
Network Policy Server	Success and Failure
Other System Events	Success and Failure
Security Group Management	Success
Security State Change	Success
Special Logon	Success
System Integrity	Success and Failure
User Account Management	Success

KAM SE AUDITOVÁNÍ ZAPISUJE?

- Všechny auditovací události se zapisují do EventLogu, konkrétně do Security logu
- Vždy na tom stroji, kde událost vznikne
- Výchozí nastavení Security EventLogu:
 - Velikost 20 MB
 - Přepisovat od nejstarších událostí







The screenshot shows the 'Log Properties - Security (Type: Administrative)' dialog box in Windows. The 'General' tab is selected, displaying the following information:

- Full Name:** Security
- Log path:** %SystemRoot%\System32\Winevt\Logs\Security.evtx
- Log size:** 111,07 MB(116 461 568 bytes)
- Created:** čtvrtek 3. ledna 2019 10:24:58
- Modified:** čtvrtek 10. ledna 2019 7:37:55
- Accessed:** čtvrtek 3. ledna 2019 10:24:58

Below the properties, the 'Enable logging' checkbox is checked. The 'Maximum log size (KB)' is set to 1048576. Under the heading 'When maximum event log size is reached:', the 'Overwrite events as needed (oldest events first)' radio button is selected.

NASTAVENÍ PRO SECURITY EVENTLOG

- Doporučená nastavení pro velikosti EventLogu (KB957662)
- Přepisovat, archivovat nebo co?
- GPO: Computer\Windows Settings\Security Settings\Local Policies\Security Options

 Audit: Audit the access of global system objects	Disabled
 Audit: Audit the use of Backup and Restore privilege	Disabled
 Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined
 Audit: Shut down system immediately if unable to log security audits	Disabled

OS	Recommended maximum size for each log (kB)	Recommended maximum total size for all logs (kB)	Approximate maximum logging rate (events/s)	Recommended maximum log size to view (kB)
WS2008, 32bit	4,194,240	16,776,960	2000	4,194,240
WS2008+, 64bit	4,194,240	16,776,960	5000	4,194,240
Vista+, 32bit	4,194,240	16,776,960	2000	4,194,240
Vista+, 64bit	4,194,240	16,776,960	5000	4,194,240

CrashOnAuditFail

- Audit: Shut down system immediately if unable to log security audits
- Naplnění SecurityLogu a nemožnosti dalšího auditování = BSOD
- STOP: C0000244 {Audit Failed}
- Ve výchozím stavu zakázáno resp. nenakonfigurováno



For more information about this issue and possible fixes, visit <http://windows.com/stopcode>

If you call a support person, give them this info:

Stop code: 0xc0000244

Auditování



NEJZAJÍMAVĚJŠÍ KATEGORIE AUDITOVÁNÍ

- Account Logon
- Logon/Logoff
- DS Access + Account Management
- Object Access

Account Logon + Logon/Logoff

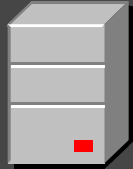


ACCOUNT LOGON vs. LOGON

- Account Logon – ověření identity uživatele, počítače atp.
- Logon – vlastní přihlášení nebo zalogování

ACCOUNT LOGON vs. LOGON

- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?



DC

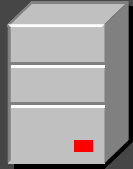


CLIENT



ACCOUNT LOGON vs. LOGON

- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?



DC

Logon

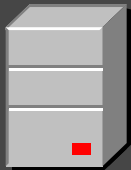


CLIENT

ACCOUNT LOGON vs. LOGON

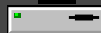
- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?

Account Logon



DC

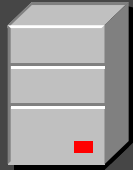
Logon



CLIENT

ACCOUNT LOGON vs. LOGON

- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?



DC

Account Logon

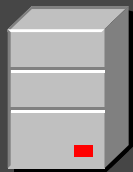
Logon



CLIENT

ACCOUNT LOGON vs. LOGON

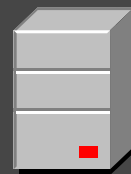
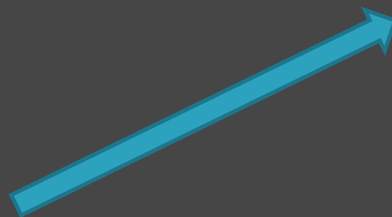
- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?



DC



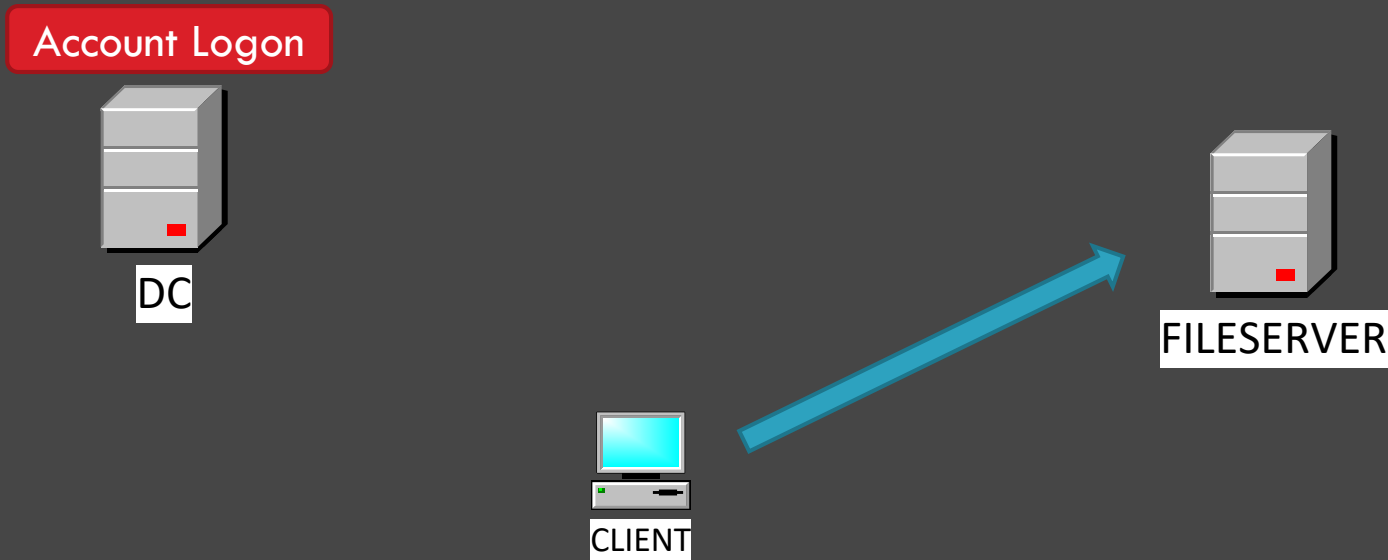
CLIENT



FILESERVER

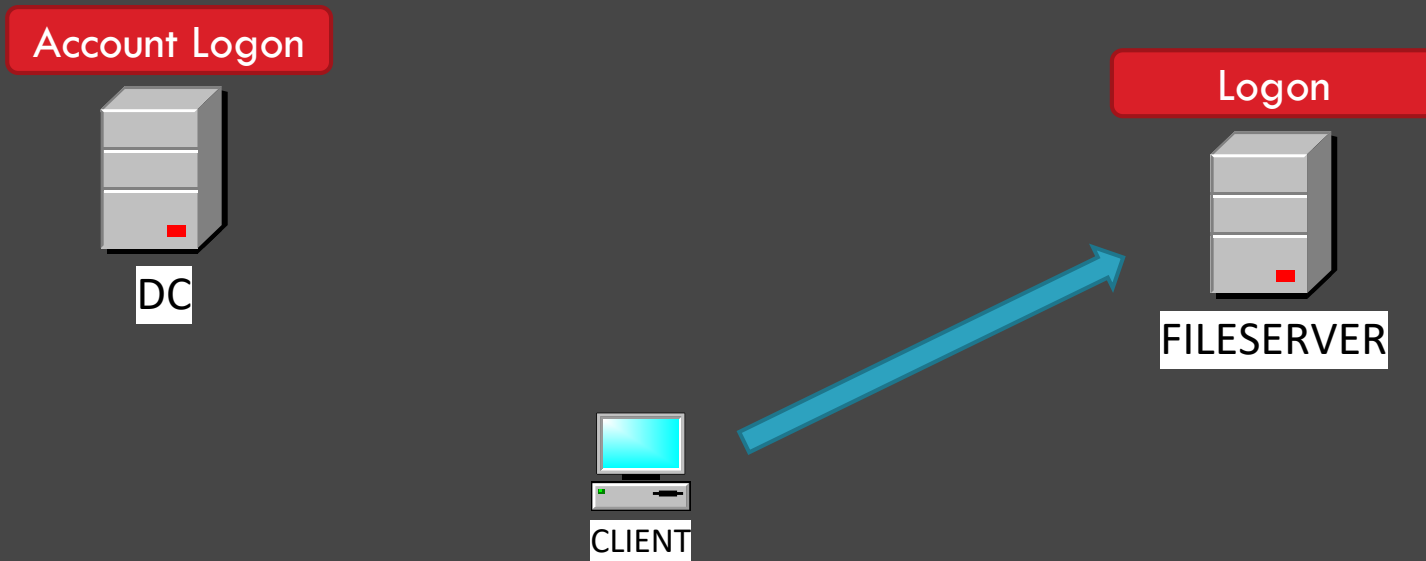
ACCOUNT LOGON vs. LOGON

- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?



ACCOUNT LOGON vs. LOGON

- Uvažujme zapnuté auditování všeho a všude... Kde vzniknou jaké eventy?



ACCOUNT LOGON

Account Logon

Kerberos Service Ticket Operations
Other Account Logon Events
Kerberos Authentication Service
Credential Validation

- Ověření identity
- Podkategorie:
 - Credential Validation – podkategorie obsahuje úspěšné a neúspěšné události týkající se ověření pomocí protokolů Lan Manager. Jde tedy o LM, NTLM a NTLMv2. EventID 4776.
 - Kerberos Authentication Service – podkategorie obsahuje úspěšné a neúspěšné události týkající se žádostí o vystavení Kerberos Ticket-granting Tickets (KRB-TGT). EventID 4768, 4771.
 - Kerberos Service Ticket Operations – podkategorie obsahuje úspěšné a neúspěšné události týkající se žádostí o vystavení Kerberos TGS ticketů. EventID 4769.
 - Other Account Logon Events – v současné době tato podkategorie negeneruje žádné eventy.

ID4776

- NTLM ověření
- Na DC
- Audit Success

Event Properties - Event 4776, Microsoft Windows security auditing.

General Details

The computer attempted to validate the credentials for an account.

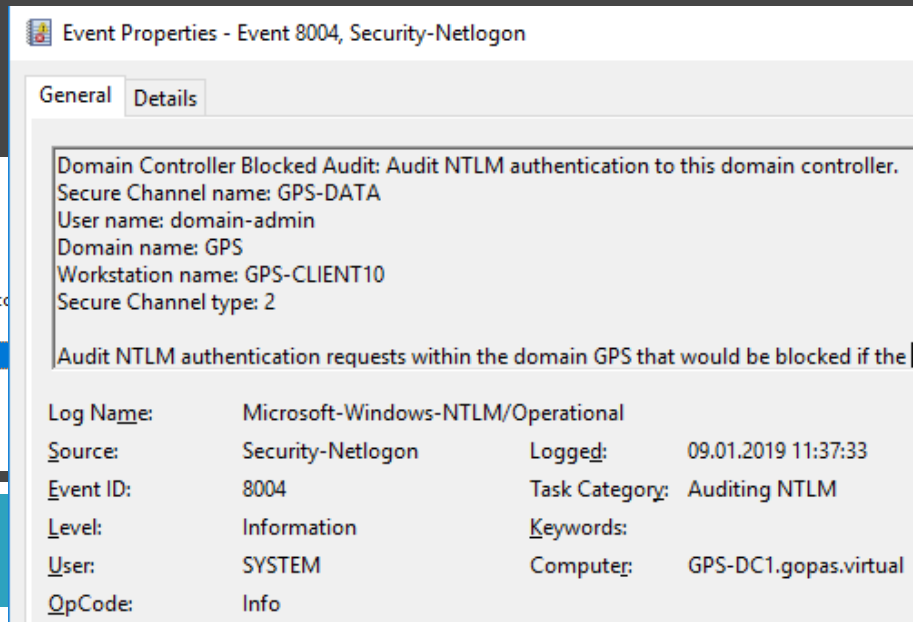
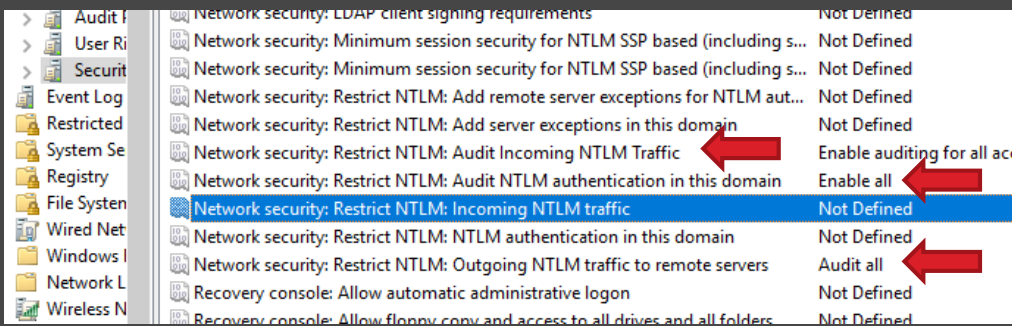
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: Admin
Source Workstation: CL1
Error Code: 0x0

Log Name: Security
Source: Microsoft Windows security Logged: 1/6/2019 10:39:14 AM
Event ID: 4776 Task Category: Credential Validation
Level: Information Keywords: Audit Success
User: N/A Computer: DC1.GOPAS.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

ODBOČKA K AUDITOVÁNÍ NTLM

- Auditování NTLM ověření v kategorii Credential Validation není moc detailní
- Dá se zapnout detailní audit v GPO
- Computer\Windows Settings\Security Settings\Local Policies\Security Options



ID4768

- Úspěšná žádost o TGT
- Na DC
- Audit Success

Event Properties - Event 4768, Microsoft Windows security auditing.

General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	Admin
Supplied Realm Name:	GOPAS
User ID:	GOPAS\Admin

Service Information:

Service Name:	krbtgt
Service ID:	GOPAS\krbtgt

Network Information:

Client Address:	::ffff:10.1.0.51
Client Port:	50541

Additional Information:

Ticket Options:	0x40810010
Result Code:	0x0

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/6/2019 10:38:42 AM
Event ID:	4768	Task Category:	Kerberos Authentication Service
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4771

- Chybná žádost o TGT
- Špatné heslo
- Na DC
- Audit Failure

Event Properties - Event 4771, Microsoft Windows security auditing.

General Details

Kerberos pre-authentication failed.

Account Information:
Security ID: GOPAS\Admin
Account Name: Admin

Service Information:
Service Name: krbtgt/GOPAS

Network Information:
Client Address: ::ffff:10.1.0.51
Client Port: 50539

Additional Information:
Ticket Options: 0x40810010
Failure Code: 0x18
Pre-Authentication Type: 2

Log Name: Security

Source: Microsoft Windows security Logged: 1/6/2019 10:38:37 AM

Event ID: 4771 Task Category: Kerberos Authentication Service

Level: Information Keywords: Audit Failure

User: N/A Computer: DC1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

ID4769

- Žádost o TGS
- Na DC
- Audit Success

Event Properties - Event 4769, Microsoft Windows security auditing.

General Details

A Kerberos service ticket was requested.

Account Information:
Account Name: Admin@GOPAS.LOCAL
Account Domain: GOPAS.LOCAL
Logon GUID: {0ffd79e4-6413-51df-47e0-787594701952}

Service Information:
Service Name: CL1\$
Service ID: GOPAS\CL1\$

Network Information:
Client Address: ::ffff:10.1.0.51
Client Port: 50617

Additional Information:
Ticket Options: 0x40810000
Ticket Encryption Type: 0x12

Log Name: Security

Source: Microsoft Windows security Logged: 1/6/2019 11:07:21 AM

Event ID: 4769 Task Category: Kerberos Service Ticket Operations

Level: Information Keywords: Audit Success

User: N/A Computer: DC1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

LOGON/LOGOFF

- Vlastní přihlášení
- Některé podkategorie:
 - Logon – podkategorie oznamující úspěšný nebo neúspěšný pokus o přihlášení. EventID 4624, 4625.
 - Logoff – podkategorie oznamující odhlášení identity. Jen úspěšné události. Dá se použít pro zjištění délky přihlášení. EventID 4634.
 - Account Lockout – podkategorie informuje o uzamčení účtu po x špatných pokusech přihlášení. Paradoxně se nastavuje auditování neúspěšných událostí. EventID 4625.
 - Group Membership – nová podkategorie na W10. Pro každý account logon zobrazuje událost obsahující členství identity ve skupinách. EventID 4627. Jen úspěšné události.

Logon/Logoff

Logon

Logoff

Account Lockout

IPsec Main Mode

IPsec Quick Mode

IPsec Extended Mode

Special Logon

Other Logon/Logoff Events

Network Policy Server

User / Device Claims

Group Membership

LOGON TYPES

Logon type	Logon title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).
9	NewCredentials	A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections.
10	RemoteInteractive	A user logged on to this computer remotely using Terminal Services or Remote Desktop.
11	CachedInteractive	A user logged on to this computer with network credentials that were stored locally on the computer. The domain controller was not contacted to verify the credentials.
12	CachedRemoteInteractive	
13	CachedUnlock	

ID4624

- Přihlášení na CL1
- Audit Success

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	CL1\$
Account Domain:	GOPAS
Logon ID:	0x3E7

Logon Information:

Logon Type:	10
Restricted Admin Mode:	No
Virtual Account:	No
Elevated Token:	Yes

Impersonation Level: Impersonation

New Logon:

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	1/6/2019 10:38:42 AM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	CL1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4625

- Přihlášení na CL1
- Audit Failure

Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

Security ID:	SYSTEM
Account Name:	CL1\$
Account Domain:	GOPAS
Logon ID:	0x3E7

Logon Type: 10

Account For Which Logon Failed:

Security ID:	NULL SID
Account Name:	Admin
Account Domain:	GOPAS

Failure Information:

Failure Reason:	Unknown user name or bad password.
-----------------	------------------------------------

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/6/2019 10:38:18 AM
Event ID:	4625	Task Category:	Logon
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	CL1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4625

- Zamknutí účtu Admin
- Audit Failure

Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

Security ID:	SYSTEM
Account Name:	CL1\$
Account Domain:	GOPAS
Logon ID:	0x3E7

Logon Type: 10

Account For Which Logon Failed:

Security ID:	NULL SID
Account Name:	Admin
Account Domain:	GOPAS

Failure Information:

Failure Reason:	Account locked out.
-----------------	---------------------

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/6/2019 10:38:26 AM
Event ID:	4625	Task Category:	Account Lockout
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	CL1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4627

- Výpis členství
- Audit Success

Event Properties - Event 4627, Microsoft Windows security auditing.

General Details

Group Membership:

- GOPAS\Domain Users
- Everyone
- BUILTIN\Users
- BUILTIN\Administrators
- NT AUTHORITY\REMOTE INTERACTIVE LOGON
- NT AUTHORITY\INTERACTIVE
- NT AUTHORITY\Authenticated Users
- NT AUTHORITY\This Organization
- LOCAL
- GOPAS\Domain Admins
- GOPAS\Group Policy Creator Owners
- GOPAS\Schema Admins
- GOPAS\Enterprise Admins
- Authentication authority asserted identity
- GOPAS\Denied RODC Password Replication Group
- Mandatory Label\Medium Mandatory Level

Log Name: Security

Source: Microsoft Windows security Logged: 1/6/2019 10:38:42 AM

Event ID: 4627 Task Category: Group Membership

Level: Information Keywords: Audit Success

User: N/A Computer: CL1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

DS Access + Account Management



ACCOUNT MANAGEMENT

- Auditování správy uživatelů, počítačů, skupin atp.
- Vybrané podkategorie:
 - User Account Management
 - Computer Account Management
 - Security Group Management
 - Distribution Group Management
- Nevyžaduje nastavení SACL na objektech
- Loguje vytvoření, smazání, některé úpravy (např. změnu loginu, reset hesla)
- Neloguje ale všechny operace nad objekty (např. změna telefonního čísla)

Account Management

Computer Account Management

Security Group Management

Distribution Group Management

Application Group Management

Other Account Management Events

User Account Management

ID4720

- Vytvoření uživatele
- Uživatel Lukas
- Vytvořil ho domain-admin
- Audit Success

Event Properties - Event 4720, Microsoft Windows security auditing.

General Details

A user account was created.

Subject:

Security ID:	GPS\domain-admin
Account Name:	domain-admin
Account Domain:	GPS
Logon ID:	0x39D36

New Account:

Security ID:	GPS\lukas
Account Name:	lukas
Account Domain:	GPS

Attributes:

SAM Account Name:	lukas
Display Name:	Lukas
User Principal Name:	lukas@gopas.virtual
Home Directory:	-

Log Name: Security

Source:	Microsoft Windows security	Logged:	10.01.2019 15:22:14
Event ID:	4720	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	GPS-DC1.gopas.virtual

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

ID4781

- Změna loginu uživatele
- Uživatel Lukas
- Změna na Karel
- Změnil ho domain-admin
- Audit Success

Event Properties - Event 4781, Microsoft Windows security auditing.

General Details

The name of an account was changed:

Subject:

Security ID:	GPS\domain-admin
Account Name:	domain-admin
Account Domain:	GPS
Logon ID:	0x39D36

Target Account:

Security ID:	GPS\lukas
Account Domain:	GPS
Old Account Name:	lukas
New Account Name:	karel

Additional Information:

Privileges:	-
-------------	---

Log Name: Security

Source:	Microsoft Windows security	Logged:	10.01.2019 15:24:12
Event ID:	4781	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	GPS-DC1.gopas.virtual
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4726

- Smazání uživatele
- Uživatel Lukas (Karel)
- Smazal ho domain-admin
- Audit Success

Event Properties - Event 4726, Microsoft Windows security auditing.

General Details

A user account was deleted.

Subject:

Security ID:	GPS\domain-admin
Account Name:	domain-admin
Account Domain:	GPS
Logon ID:	0x39D36

Target Account:

Security ID:	GPS\lukas
Account Name:	karel
Account Domain:	GPS

Additional Information:

Privileges	-
------------	---

Log Name: Security

Source:	Microsoft Windows security	Logged:	10.01.2019 15:25:29
Event ID:	4726	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	GPS-DC1.gopas.virtual
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4741

- Vytvoření počítače
- Počítač PC28
- Vytvořil ho domain-admin
- Audit Success

Event Properties - Event 4741, Microsoft Windows security auditing.

General Details

A computer account was created.

Subject:

Security ID:	GPS\domain-admin
Account Name:	domain-admin
Account Domain:	GPS
Logon ID:	0x39D36

New Computer Account:

Security ID:	GPS\PC28\$
Account Name:	PC28\$
Account Domain:	GPS

Attributes:

SAM Account Name:	PC28\$
Display Name:	-
User Principal Name:	-
Home Directory:	-

Log Name: Security

Source:	Microsoft Windows security	Logged:	10.01.2019 15:26:52
Event ID:	4741	Task Category:	Computer Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	GPS-DC1.gopas.virtual
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4743

- Smazání počítače
- Počítač PC28
- Smazal ho domain-admin
- Audit Success

Event Properties - Event 4743, Microsoft Windows security auditing.

General Details

A computer account was deleted.

Subject:

Security ID:	GPS\domain-admin
Account Name:	domain-admin
Account Domain:	GPS
Logon ID:	0x39D36

Target Computer:

Security ID:	GPS\PC28\$
Account Name:	PC28\$
Account Domain:	GPS

Additional Information:

Privileges:	-
-------------	---

Log Name: Security

Source:	Microsoft Windows security	Logged:	10.01.2019 15:27:54
Event ID:	4743	Task Category:	Computer Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	GPS-DC1.gopas.virtual
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

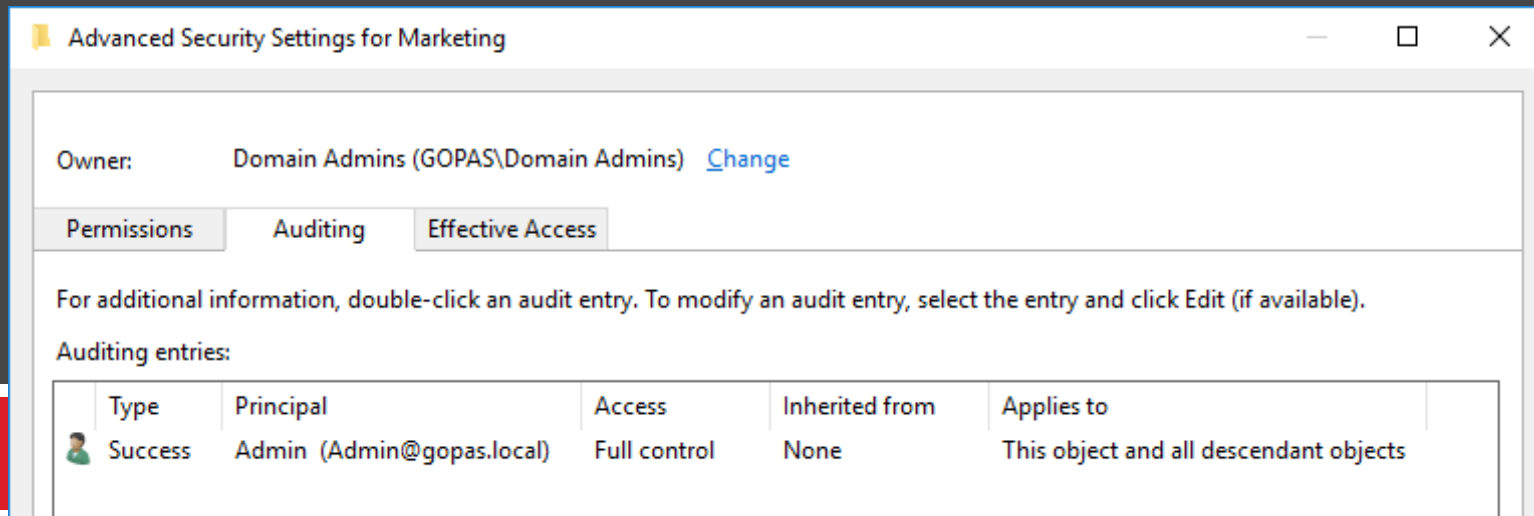
DS ACCESS

```
DS Access
Directory Service Access
Directory Service Changes
Directory Service Replication
Detailed Directory Service Replication
```

- Přístup ke službám Active Directory
- Podkategorie:
 - Directory Service Access – subkategorie informuje o úspěšných či neúspěšných operacích nad AD objekty. Dokáže auditovat i čtení vlastností nebo DACL. Pouze pro DC. EventID 4662.
 - Directory Service Changes – subkategorie informuje o změnách nad AD objekty. Dokáže zaznamenávat změny atributů, včetně původní a nové hodnoty. Pouze na DC.
 - Directory Service Replication – subkategorie je vhodná pro monitorování a řešení potíží s replikacemi AD. Pouze na DC.
 - Detailed Directory Service Replication – subkategorie je vhodná pro monitorování a řešení potíží s replikacemi AD. Pouze na DC.

NASTAVENÍ AUDITOVÁNÍ DS ACCESS

- Zatím stačilo auditování nastavit pouze v lokální / doménové politice
- Některé kategorie auditu ale vyžadují nastavení SACL i na auditovaných objektech
- SACL je obdoba nastavení oprávnění (DACL)
- SACL se používá na definování toho, jaké operace a pro koho chceme auditovat




Advanced Security Settings for Marketing

Owner: Domain Admins (GOPAS\Domain Admins) [Change](#)

Permissions Auditing **Effective Access**

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
 Success	Admin (Admin@gopas.local)	Full control	None	This object and all descendant objects

ID4662

- Přístup k AD objektu
- Uživatel Derek Brown
- Read Property
- Audit Success

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

Security ID:	GOPAS\Admin
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x136539

Object:

Object Server:	DS
Object Type:	user
Object Name:	CN=Derek

Brown,OU=Marketing,OU=Users,OU=GOPAS,DC=GOPAS,DC=local

Handle ID:	0x0
------------	-----

Operation:

Operation Type:	Object Access
Accesses:	Read Property

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/6/2019 11:59:15 AM
Event ID:	4662	Task Category:	Directory Service Access
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID5137

- Úspěšné vytvoření AD objektu
- Uživatel Admin vyrobil účet počítače
- PC2
- Audit Success

The screenshot shows the Windows Event Viewer window for Event ID 5137. The window title is "Event Properties - Event 5137, Microsoft Windows security auditing." It has two tabs: "General" and "Details". The "Details" tab is active, showing the following information:

A directory service object was created.

Subject:
Security ID: GOPAS\Admin
Account Name: Admin
Account Domain: GOPAS
Logon ID: 0x5FD08

Directory Service:
Name: GOPAS.local
Type: Active Directory Domain Services

Object:
DN: cn=PC2,OU=TEST,OU=GOPAS,DC=GOPAS,DC=local
GUID: CN=PC2,OU=TEST,OU=GOPAS,DC=GOPAS,DC=local
Class: computer

Operation:
Correlation ID: {ff14f25b-5d25-4239-87bd-0038837f9871}
Application Correlation ID: -

Log Name: Security
Source: Microsoft Windows security
Event ID: 5137
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 1/9/2019 11:49:32 PM
Task Category: Directory Service Changes
Keywords: Audit Success
Computer: DC1.GOPAS.local

At the bottom of the window, there are "Copy" and "Close" buttons. On the right side of the main content area, there are two arrow buttons (up and down).

ID4662

- Neúspěšné vytvoření AD objektu
- Uživatelka Eva chtěla účet počítače
- CL4
- Audit Failure

Event Properties - Event 4662, Microsoft Windows security auditing.

General Details

An operation was performed on an object.

Subject:

Security ID:	GOPAS\Eva
Account Name:	Eva
Account Domain:	GOPAS
Logon ID:	0x1483EF

Object:

Object Server:	DS
Object Type:	container
Object Name:	CN= Computers,DC=GOPAS,DC=local
Handle ID:	0x0

Operation:

Operation Type:	Object Access
Accesses:	Create Child
Access Mask:	0x1
Properties:	---
	{bf967a86-0de6-11d0-a285-00aa003049e2}

Additional Information:

Parameter 1:	CN= CL4,CN= Computers,DC=GOPAS,DC=local
Parameter 2:	{3673afc8-5187-41b3-9293-7bb6d8739c90}

Log Name: Security

Source: Microsoft Windows security Logged: 1/9/2019 11:52:03 PM

Event ID: 4662 Task Category: Directory Service Access

Level: Information Keywords: Audit Failure

User: N/A Computer: DC1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

ID5136

- Změna na AD objektu
- Uživatel Derek Brown
- Měnil uživatel Admin
- Změna telefonního čísla
- Původní hodnota
- Audit Success

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

A directory service object was modified.

Subject:
Security ID: GOPAS\Admin
Account Name: Admin
Account Domain: GOPAS
Logon ID: 0x136539

Directory Service:
Name: GOPAS.local
Type: Active Directory Domain Services

Object:
DN: CN=Derek Brown,OU=Marketing,OU=Users,OU=GOPAS,DC=GOPAS,DC=local
GUID: CN=Derek Brown,OU=Marketing,OU=Users,OU=GOPAS,DC=GOPAS,DC=local
Class: user

Attribute:
LDAP Display Name: givenName
Syntax (OID): 2.5.5.12
Value: Derek

Operation:
Type: Value Deleted
Completion ID: {554-8404-3303-4020-0664-40143-570657}

Log Name: Security

Source: Microsoft Windows security **Logged:** 1/6/2019 11:59:15 AM

Event ID: 5136 **Task Category:** Directory Service Changes

Level: Information **Keywords:** Audit Success

User: N/A **Computer:** DC1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

ID 5136

- Změna na AD objektu
- Uživatel Derek Brown
- Měnil uživatel Admin
- Změna telefonního čísla
- Nová hodnota
- Audit Success

Event Properties - Event 5136, Microsoft Windows security auditing.

General Details

A directory service object was modified.

Subject:

Security ID:	GOPAS\Admin
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x136539

Directory Service:

Name:	GOPAS.local
Type:	Active Directory Domain Services

Object:

DN:	CN=Derek Brown,OU=Marketing,OU=Users,OU=GOPAS,DC=GOPAS,DC=local
GUID:	CN=Derek Brown,OU=Marketing,OU=Users,OU=GOPAS,DC=GOPAS,DC=local
Class:	user

Attribute:

LDAP Display Name:	givenName
Syntax (OID):	2.5.5.12
Value:	Karel

Operation:

Type:	Value Added
-------	-------------

Log Name: Security

Source: Microsoft Windows security Logged: 1/6/2019 11:59:15 AM

Event ID: 5136 Task Category: Directory Service Changes

Level: Information Keywords: Audit Success

User: N/A Computer: DC1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

Object Access



OBJECT ACCESS

- Auditování CA, FW, souborů, sdílených dat, DAC atp.
- Některé podkategorie:
 - Certification Services – auditování ADCS (nutno nastavit i v ADCS)
 - File Share – generuje úspěšné i neúspěšné události o správě sdílených složek a přístupech do nich. Není detailní.
 - Detailed File Share – generuje detailní úspěšné i neúspěšné události při přístupu k adresáři nebo souboru po síti. Může generovat hodně událostí na file serverech. EventID 5145.
 - File System – generuje úspěšné i neúspěšné události při přístupu k souborům a adresářům, jako modifikace, mazání, změnu oprávnění atp.
 - Filtering Platform Connection – generuje události týkající se WFP, např. WF
 - Filtering Platform Packet Drop – generuje události týkající se WFP, např. WF, EventID 5152

Object Access
File System
Registry
Kernel Object
SAM
Certification Services
Application Generated
Handle Manipulation
File Share
Filtering Platform Packet Drop
Filtering Platform Connection
Other Object Access Events
Detailed File Share
Removable Storage
Central Policy Staging

ID 5152

- Filtering Platform Packet Drop
- Zablokovaný packet na FW
- Ping (ICMP)
- Audit Failure

Event Properties - Event 5152, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has blocked a packet.

Application Information:

Process ID:	4
Application Name:	System

Network Information:

Direction:	Inbound
Source Address:	10.1.0.11
Source Port:	0
Destination Address:	10.1.0.21
Destination Port:	8
Protocol:	1

Filter Information:

Filter Run-Time ID:	67974
Layer Name:	Receive/Accept
Layer Run-Time ID:	44

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 8:13:08 AM
Event ID:	5152	Task Category:	Filtering Platform Packet Drop
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID 5152

- Filtering Platform Packet Drop
- Zablokovaný packet na FW
- SMB
- Audit Failure

Event Properties - Event 5152, Microsoft Windows security auditing.

General Details

The Windows Filtering Platform has blocked a packet.

Application Information:

Process ID:	4
Application Name:	System

Network Information:

Direction:	Inbound
Source Address:	10.1.0.11
Source Port:	64958
Destination Address:	10.1.0.21
Destination Port:	445
Protocol:	6

Filter Information:

Filter Run-Time ID:	67974
Layer Name:	Receive/Accept
Layer Run-Time ID:	44

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 8:15:46 AM
Event ID:	5152	Task Category:	Filtering Platform Packet Drop
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID 5142

- File Share
- Vytvoření sdíleného adresáře
- Audit Success

Event Properties - Event 5142, Microsoft Windows security auditing.

General Details

A network share object was added.

Subject:

Security ID:	GOPAS\Admin\
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x8E118

Share Information:

Share Name:	*\UserData
Share Path:	C:\UserData

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 8:19:00 AM
Event ID:	5142	Task Category:	File Share
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID5140

- File Share
- Otevření sdíleného adresáře
- Není detailní
- Nejsou vidět otevřené soubory
- Audit Success

Event Properties - Event 5140, Microsoft Windows security auditing.

General Details

A network share object was accessed.

Subject:

Security ID:	GOPAS\Admin
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x15CF29

Network Information:

Object Type:	File
Source Address:	10.1.0.11
Source Port:	65001

Share Information:

Share Name:	*\UserData
Share Path:	\\?.\C:\UserData

Access Request Information:

Access Mask:	0x1
Accesses:	ReadData (or ListDirectory)

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 8:30:16 AM
Event ID:	5140	Task Category:	File Share
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID5145

- Detailed File Share
- Otevření souboru z \\SRV1\
- Soubor TEST.txt
- Audit Success

Event Properties - Event 5145, Microsoft Windows security auditing.

General Details

A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:	GOPAS\Admin
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x15CF29

Network Information:

Object Type:	File
Source Address:	10.1.0.11
Source Port:	65002

Share Information:

Share Name:	*\UserData
Share Path:	\\?.C:\UserData
Relative Target Name:	TEST.txt

Access Request Information:

Access Mask:	0x120089
Accesses:	READ_CONTROL SYNCHRONIZE

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 8:37:36 AM
Event ID:	5145	Task Category:	Detailed File Share
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID5145

- Detailed File Share
- Pokus o smazání souboru z \\SRV1\
- Soubor TEST2.txt
- Audit Failure

Event Properties - Event 5145, Microsoft Windows security auditing.

General Details

A network share object was checked to see whether client can be granted desired access.

Subject:

Security ID:	GOPAS\Admin
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x15CF29

Network Information:

Object Type:	File
Source Address:	10.1.0.11
Source Port:	65000

Share Information:

Share Name:	*\UserData
Share Path:	\\?.\C:\UserData
Relative Target Name:	TEST2.txt

Access Request Information:

Access Mask:	0x110080
Accesses:	DELETE SYNCHRONIZE ReadAttributes

Access Check Results:

DELETE: Not granted

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 8:44:41 AM
Event ID:	5145	Task Category:	Detailed File Share
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

AUDIT FILE SYSTEM OBECNĚ

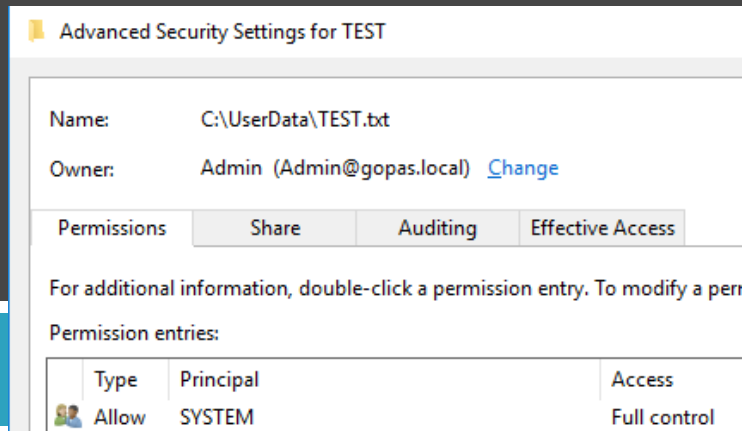
- Asi jedno z nejzajímavějších auditování vůbec (zdánlivě)
- Řeší odpovědi na klasické otázky jako:
 - Kdo a kdy smazal soubor?
 - Kdo a kdy změnil soubor?
 - Kdo otevírá nebo se snaží otevírat jaké soubory?
 - Atp.
- Podobně jako u auditování objektů v AD bude i u souborů a adresářů třeba konfigurovat nejen vlastní auditování v politice, ale navíc i SACL

AUDIT FILE SYSTEM – KOMPLIKACE

- Množství generovaných událostí – např. CMD.exe vs. EXPLORER.exe
- Matoucí nebo zavádějící události:
 - Otevření souboru vs. výpis adresáře vs. zobrazení náhledu / miniatury?
 - Mazání souboru vs. přejmenování vs. přesunutí souboru vs. autoukládání Wordu
- Asi jediná událost, která různými událostmi nemáte, je zápis

CO JE SACL?

- Každý soubor a adresář na NTFS má vlastní security descriptor obsahující tři části:
 - Object owner – vlastník souboru nebo sdresáře
 - Discretionary Access Control Lists (DACL) – nastavuje oprávnění
 - System Access Control Lists (SACL) – nastavuje auditování
- Vlastník, DACL i SACL se konfiguruje na rozšířeném dialogu oprávnění
- Jediný rozdíl mezi DACL a SACL je sloupec type:
 - DACL – Allow a Deny
 - SACL – Success, Fail, All



ID4656

- Úspěšné smazání souboru
- TEST.txt
- Cmd.exe
- GOPAS\Admin
- Audit Success

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID:	GOPAS\Admin
Account Name:	Admin
Account Domain:	GOPAS
Logon ID:	0x8E155

Object:

Object Server:	Security
Object Type:	File
Object Name:	C:\UserData\TEST.txt
Handle ID:	0xa0
Resource Attributes:	-

Process Information:

Process ID:	0x9ac
Process Name:	C:\Windows\System32\cmd.exe

Access Request Information:

Transaction ID:	{00000000-0000-0000-0000-000000000000}
Accesses:	DELETE

Access Reasons: DELETE: Granted by D:(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)

Log Name: Security

Source:	Microsoft Windows security	Logged:	1/7/2019 11:00:03 AM
Event ID:	4656	Task Category:	File System
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	SRV1.GOPAS.local
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

ID4656

- Neúspěšné smazání souboru
- TEST.txt
- Cmd.exe
- GOPAS\Adam
- Audit Failure

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:
Security ID: GOPAS\adam
Account Name: adam
Account Domain: GOPAS
Logon ID: 0x23EAAF

Object:
Object Server: Security
Object Type: File
Object Name: C:\UserData\TEST.txt
Handle ID: 0x0
Resource Attributes: -

Process Information:
Process ID: 0xa38
Process Name: C:\Windows\System32\cmd.exe

Access Request Information:
Transaction ID: {00000000-0000-0000-0000-000000000000}
Accesses: DELETE
Access Reasons: DELETE: Not granted
Access Mask: 0x10000

Log Name: Security
Source: Microsoft Windows security
Event ID: 4656
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 1/7/2019 10:54:40 AM
Task Category: File System
Keywords: Audit Failure
Computer: SRV1.GOPAS.local

Copy Close

ID4670

- Úspěšná změna vlastníka souboru
- TEST.txt
- GOPAS\Admin ⇒ SYSTEM
- Audit Success

Admin Properties

Published Certificates	Member Of	Password Replication	Dial-in	Object	
Security	Environment	Sessions	Remote control		
General	Address	Account	Profile	Telephones	Organization
Remote Desktop Services Profile	COM+	Attribute Editor			

Attributes:

Attribute	Value
o	<not set>
objectCat...	CN=Person,CN=Schema,CN=Configuration,DC=GOPAS
objectClass	top; person; organizationalPerson; user
objectGUID	49e1f3a5-6659-4fad-9c9d-eff5019491be
objectSid	S-1-5-21-4000008492-1298714939-3727512976-1487

Event Properties - Event 4670, Microsoft Windows security auditing.

General Details

Permissions on an object were changed.

Subject:

Security ID: GOPAS\Admin
Account Name: Admin
Account Domain: GOPAS
Logon ID: 0x8E118

Object:

Object Server: Security
Object Type: File
Object Name: C:\UserData\TEST.txt
Handle ID: 0x538

Process:

Process ID: 0x6c0
Process Name: C:\Windows\System32\dlhhost.exe

Permissions Change:

Original Security Descriptor: O:S-1-5-21-4000008492-1298714939-3727512976-1487
New Security Descriptor: O:SY|

Log Name: Security
Source: Microsoft Windows security
Event ID: 4670
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 1/7/2019 11:35:50 AM
Task Category: Authorization Policy Change
Keywords: Audit Success
Computer: SRV1.GOPAS.local

Copy Close

ID4670

- Úspěšná změna oprávnění
- TEST.txt
- Audit Success

Event Properties - Event 4670, Microsoft Windows security auditing.

General Details

Permissions on an object were changed.

Subject:
Security ID: GOPAS\Admin
Account Name: Admin
Account Domain: GOPAS
Logon ID: 0x8E155

Object:
Object Server: Security
Object Type: File
Object Name: C:\UserData\TEST.txt
Handle ID: 0x2bc

Process:
Process ID: 0x5b8
Process Name: C:\Windows\System32\dlhhost.exe

Permissions Change:
Original Security Descriptor: D:AI(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)
New Security Descriptor: D:ARAI(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)(A;ID;FA;;;WD)

Log Name: Security
Source: Microsoft Windows security
Event ID: 4670
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

Logged: 1/7/2019 11:41:41 AM
Task Category: Authorization Policy Change
Keywords: Audit Success
Computer: SRV1.GOPAS.local

Copy Close

SDDL

- Security Descriptor Definition Language
- Je to textový zápis popisovačů zabezpečení
- Obecný formát:
 - O:<vlastník>
 - D:P<oprávnění>
 - S:P<auditování>

Permissions Change:

Original Security Descriptor: D:AI(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)
New Security Descriptor: D:ARAI(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)(A;ID;FA;;;WD)

Permissions Change:

Original Security Descriptor: O:S-1-5-21-4000008492-1298714939-3727512976-1487
New Security Descriptor: O:SY|

SDDL

- SDDL obsahuje ACE. Každý ACE obsahuje 6 částí, tyto části odděluje středník:
 - ACE type (allow/deny/audit)
 - ACE flags (inheritance and audit settings)
 - Permissions (list of incremental permissions)
 - ObjectType (GUID)
 - Inherited Object Type (GUID)
 - Trustee (SID)

ACE Type	
A	ACCESS ALLOWED
D	ACCESS DENIED
OA	OBJECT ACCESS ALLOWED: ONLY APPLIES TO A SUBSET OF THE OBJECT(S).
OD	OBJECT ACCESS DENIED: ONLY APPLIES TO A SUBSET OF THE OBJECT(S).
AU	SYSTEM AUDIT
A	SYSTEM ALARM
OU	OBJECT SYSTEM AUDIT
OL	OBJECT SYSTEM ALARM

Directory service access rights	
RC	Read Permissions
SD	Delete
WD	Modify Permissions
WO	Modify Owner
RP	Read All Properties
WP	Write All Properties
CC	Create All Child Objects
DC	Delete All Child Objects
LC	List Contents
SW	All Validated Writes
LO	List Object
DT	Delete Subtree
CR	All Extended Rights

Generic access rights		File access rights	
GA	GENERIC ALL	FA	FILE ALL ACCESS
GR	GENERIC READ	FR	FILE GENERIC READ
GW	GENERIC WRITE	FW	FILE GENERIC WRITE
GX	GENERIC EXECUTE	FX	FILE GENERIC EXECUTE

P	SDDL_PROTECTED	Inheritance from containers that are higher in the folder hierarchy are blocked.
AI	SDDL_AUTO_INHERITED	Inheritance is allowed, assuming that "P" is not also set.
AR	SDDL_AUTO_INHERIT_REQ	Child objects inherit permissions from this object.

Trustee	
AU	Authenticated users
BA	Built-in administrators
BU	Built-in users
CO	Creator owner
DA	Domain administrators
DU	Domain users
EA	Enterprise administrators
WD	Everyone
IU	Interactively logged-on user
LA	Local administrator
LS	Local service account
SY	Local system
RD	Terminal server users
SA	Schema administrators

ACE Flags	
CI	CONTAINER INHERIT: Child objects that are containers, such as directories, inherit the ACE as an explicit ACE.
OI	OBJECT INHERIT: Child objects that are not containers inherit the ACE as an explicit ACE.
NP	NO PROPAGATE: ONLY IMMEDIATE CHILDREN INHERIT THIS ACE.
IO	INHERITANCE ONLY: ACE DOESN'T APPLY TO THIS OBJECT, BUT MAY AFFECT CHILDREN VIA INHERITANCE.
ID	ACE IS INHERITED
SA	SUCCESSFUL ACCESS AUDIT
FA	FAILED ACCESS AUDIT

Original Security Descriptor: D:AI(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)

New Security Descriptor: D:ARAI(A;ID;FA;;;S-1-5-21-4000008492-1298714939-3727512976-1487)(A;ID;FA;;;WD)

EventLog



EVENTLOG

- Už víme, že auditování se zapisuje do Security EventLogu
- Komplikace:
 - Záznamů v logu bude hodně
 - V některých případech nevíme, na kterém serveru je událost generována (např. u ověření) a tak musíme prohledávat logy na více serverech
 - Použití vestavěných nástrojů na vyhledávání či filtrování logů není úplně snadné

EVENT SUBSCRIPTION

- Události v EventLogu vznikají lokálně na serverech – nutno sledovat lokálně
- Lze vyrobiť subscripci, která shromažďuje logy na centrálním místě
- Lolekce logů může být:
 - Inicializovaná „sběračem“
 - Inicializovaná „sbíraným“
- Sbírat lze logy všechny nebo jen dle parametrického filtru
- Vytvoření custom EventLogu
 - <https://blogs.technet.microsoft.com/russell/2016/05/18/creating-custom-windows-event-forwarding-logs/>

EVENT SUBSCRIPTION – NASTAVENÍ

- Abyste mohli vzdáleně „vytahovat“ logy, musíte na to mít oprávnění
- Na běžné logy jako Application nebo System „stačí“ být lokálním Administrátorem
- Security EventLog je na nastavení trochu složitější
 - Viz chyba 0x138C
 - <https://support.microsoft.com/en-us/help/4047777/security-event-log-forwarding-fails-with-error-0x138c-and-5004>

FILTROVÁNÍ

- Každá událost má dvě části:
 - System – obecnosti
 - EventData – podrobnosti

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID: SYSTEM
Account Name: DC1\$
Account Domain: GOPAS
Logon ID: 0x3E7

Logon Information:

Logon Type: 2
Restricted Admin Mode: -
Virtual Account: No
Elevated Token: No

Impersonation Level:

Impersonation

New Logon:

Security ID: GOPAS\Admin
Account Name: Admin
Account Domain: GOPAS
Logon ID: 0x17A58B

Log Name: Security

Source: Microsoft Windows security Logged: 1/8/2019 11:52:29 AM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: DC1.GOPAS.local

OpCode: Info

More Information: [Event Log Online Help](#)

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

Friendly View XML View

```
- <Event
  xmlns="http://schemas.microsoft.com/win/2004/08/
+ <System>
+ <EventData>
</Event>
```

FILTROVÁNÍ EVENTLOGU POMOCÍ XML

Event Properties - Event 4768, Microsoft Windows security auditing.

General Details

Friendly View XML View

```
<?xml version="1.0" encoding="UTF-16" xmlns="http://schemas.microsoft.com/win/2004/08/events/event" xmlns:system="http://schemas.microsoft.com/win/2004/08/events/system" xmlns:security="http://schemas.microsoft.com/win/2004/08/events/security" >
<System>
  <Provider Name="Microsoft-Windows-Security-Auditing"
    Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4768</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>14339</Task>
  <Opcode>0</Opcode>
  <Keywords>0x8020000000000000</Keywords>
  <TimeCreated SystemTime="2019-01-09T22:08:31.507881100Z" />
  <EventRecordID>22537</EventRecordID>
  <Correlation />
  <Execution ProcessID="592" ThreadID="1920" />
  <Channel>Security</Channel>
  <Computer>DC1.GOPAS.local</Computer>
  <Security />
</System>
<EventData>
  <Data Name="TargetUserName">Admin</Data>
  <Data Name="TargetDomainName">GOPAS</Data>
  <Data Name="TargetSid">S-1-5-21-4000008492-1298714939-3727512976-1487</Data>
  <Data Name="ServiceName">krbtgt</Data>
</EventData>
</event>
```

Copy Close

Filter Current Custom View

Filter XML

To provide an event filter in XPath form, click the "Edit query manually" checkbox below.

```
<QueryList>
  <Query Id="0" Path="ForwardedEvents">
    <Select Path="ForwardedEvents">
      *[
        EventData[Data[@Name='PreAuthType']='2']
        and
        EventData[Data[@Name='TargetUserName']='Admin']
        and
        System[(EventID='4768')]
      ]
    </Select>
  </Query>
</QueryList>
```

Edit query manually

OK Cancel

POWERSHELL

```
1 Get-WinEvent -ComputerName DC1 -FilterHashtable @{Logname='Security';ID=4768;Data='Admin'} |
2 Select-Object -Last 1 -Property Timecreated,
3 @{{label='Hodnota0';expression={$_.properties[0].value}},
4 @{{label='Hodnota1';expression={$_.properties[1].value}},
5 @{{label='Hodnota2';expression={$_.properties[2].value}},
6 @{{label='Hodnota3';expression={$_.properties[3].value}},
7 @{{label='Hodnota4';expression={$_.properties[4].value}},
8 @{{label='Hodnota5';expression={$_.properties[5].value}},
9 @{{label='Hodnota6';expression={$_.properties[6].value}},
10 @{{label='Hodnota7';expression={$_.properties[7].value}},
11 @{{label='Hodnota8';expression={$_.properties[8].value}},
12 @{{label='Hodnota9';expression={$_.properties[9].value}}
```

```
TimeCreated : 1/8/2019 11:52:29 AM
Hodnota0    : Admin
Hodnota1    : GOPAS
Hodnota2    : S-1-5-21-4000008492-1298714939-3727512976-1487
Hodnota3    : krbtgt
Hodnota4    : S-1-5-21-4000008492-1298714939-3727512976-502
Hodnota5    : 1082195984
Hodnota6    : 0
Hodnota7    : 18
Hodnota8    : 2
Hodnota9    : ::1
```

IP ADDRESS MANAGEMENT

- Technologie Windows Serveru 2012+
- Primárně určená pro správu IP adres v síti
- IPAM má vlastní databázi (WID nebo SQL)
- IPAM komunikuje s DHCP, DNS, DC
- Z DC si vytahuje auditovací security logy a dává si je k sobě do databáze
- Nad databází pak umožňuje vyhledávat

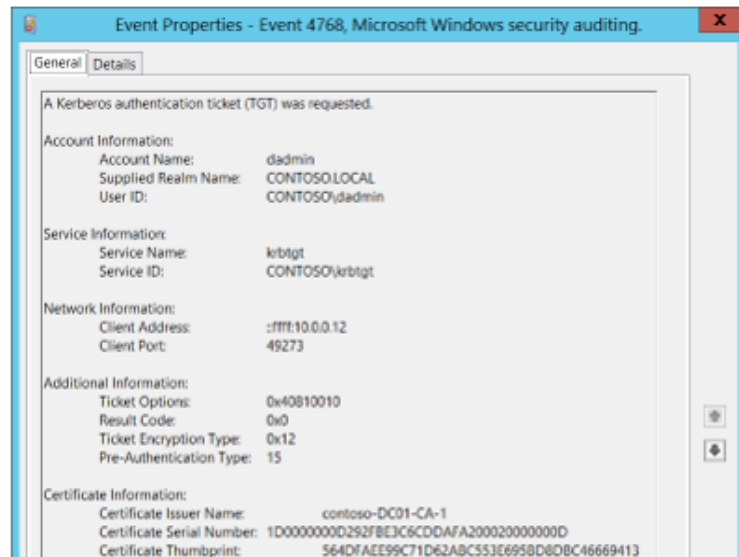
EVENTLOG REFERENCE GUIDE

- <https://www.microsoft.com/en-us/download/details.aspx?id=52630> (754 stran)

Events List:

- [4768](#)(S, F): A Kerberos authentication ticket (TGT) was requested.
- [4771](#)(F): Kerberos pre-authentication failed.
- [4772](#)(F): A Kerberos authentication ticket request failed.

4768(S, F): A Kerberos authentication ticket (TGT) was requested.



Event Properties - Event 4768, Microsoft Windows security auditing

General Details

A Kerberos authentication ticket (TGT) was requested.

Account Information:

Account Name:	dadmin
Supplied Realm Name:	CONTOSO.LOCAL
User ID:	CONTOSO\dadmin

Service Information:

Service Name:	krbtgt
Service ID:	CONTOSO\krbtgt

Network Information:

Client Address:	::ffff:10.0.0.12
Client Port:	49273

Additional Information:

Ticket Options:	0x40810010
Result Code:	0x0
Ticket Encryption Type:	0x12
Pre-Authentication Type:	15

Certificate Information:

Certificate Issuer Name:	contoso-DC01-CA-1
Certificate Serial Number:	1D0000000D292FBE3C6CDDAFA200020000000D
Certificate Thumbprint:	564DFAEE99C71D62A8C553E6958D80BC46669413

Event Description:

This event generates every time Key Distribution Center issues a Kerberos Ticket Granting Ticket (TGT). This event generates only on domain controllers.

If TGT issue fails then you will see Failure event with **Result Code** field not equal to "0x0".

This event doesn't generate for **Result Codes**: 0x10, 0x17 and 0x18. Event "[4771](#): Kerberos pre-authentication failed." generates instead.

Note For recommendations, see [Security Monitoring Recommendations](#) for this event.

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
  <EventID>4768</EventID>
  <Version>0</Version>
  <Level>0</Level>
  <Task>14339</Task>
```

Auditování ve Windows

Lukáš Brázda | MCT, MCSA, MCSE | lukas@brazda.org