Auditování ve Windows

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

OBSAH

- Úvod
- Auditování
- EventLog

Úvod

CO JE AUDITOVÁNÍ VE WINDOWS

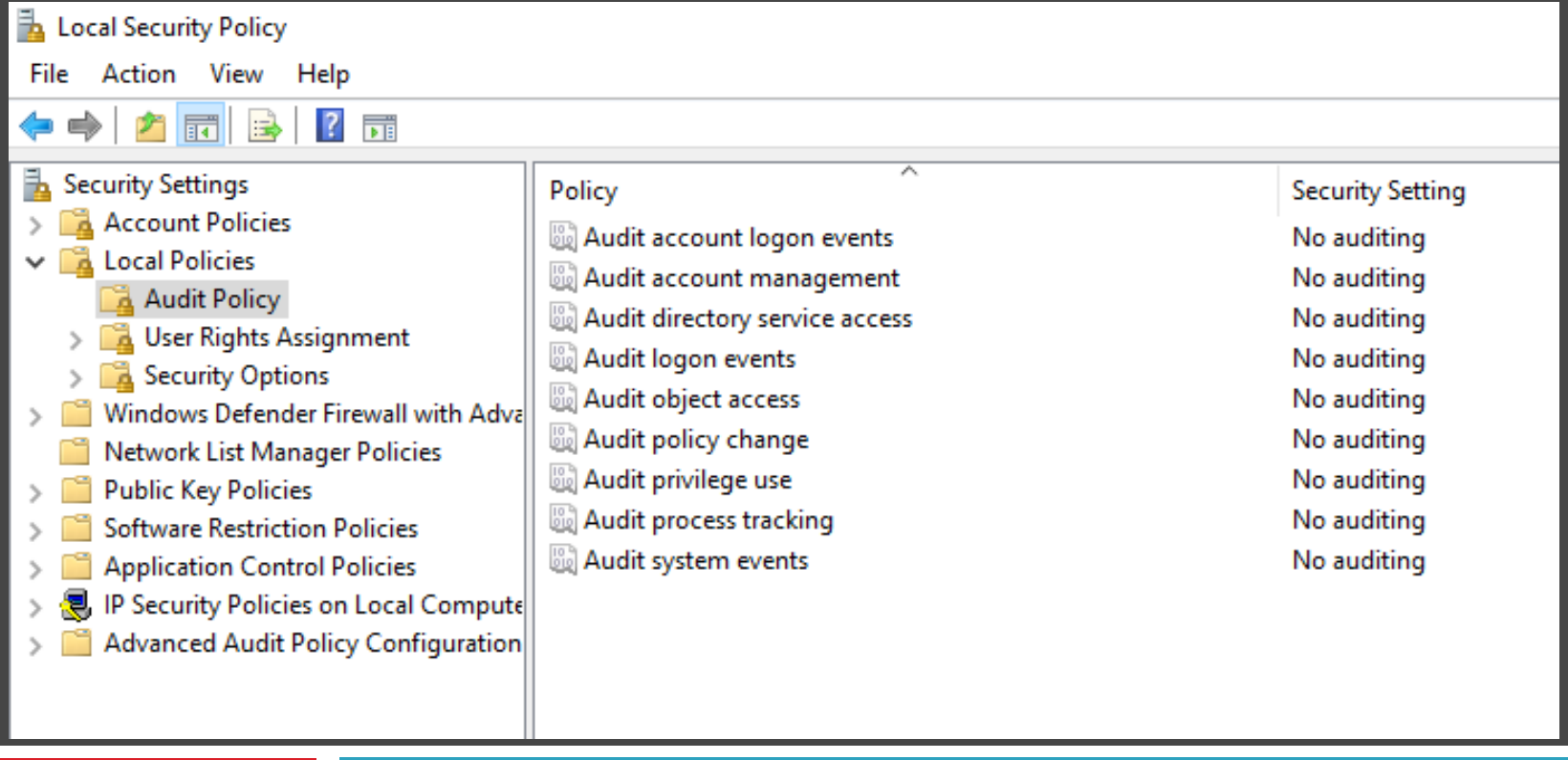
- Je to jeden z typů monitorování
- Jde o zaznamenávání událostí o činnosti uživatelů, služeb, systémů atp.
- Díky auditování jsem schopen najít odpovědi na otázky jako:
  - Co se stalo?
  - Kde se to stalo?
  - Kdy se to stalo?
  - Kdo to udělal a odkud?

CHCI AUDITOVAT? A PŘÍPADNĚ CO?

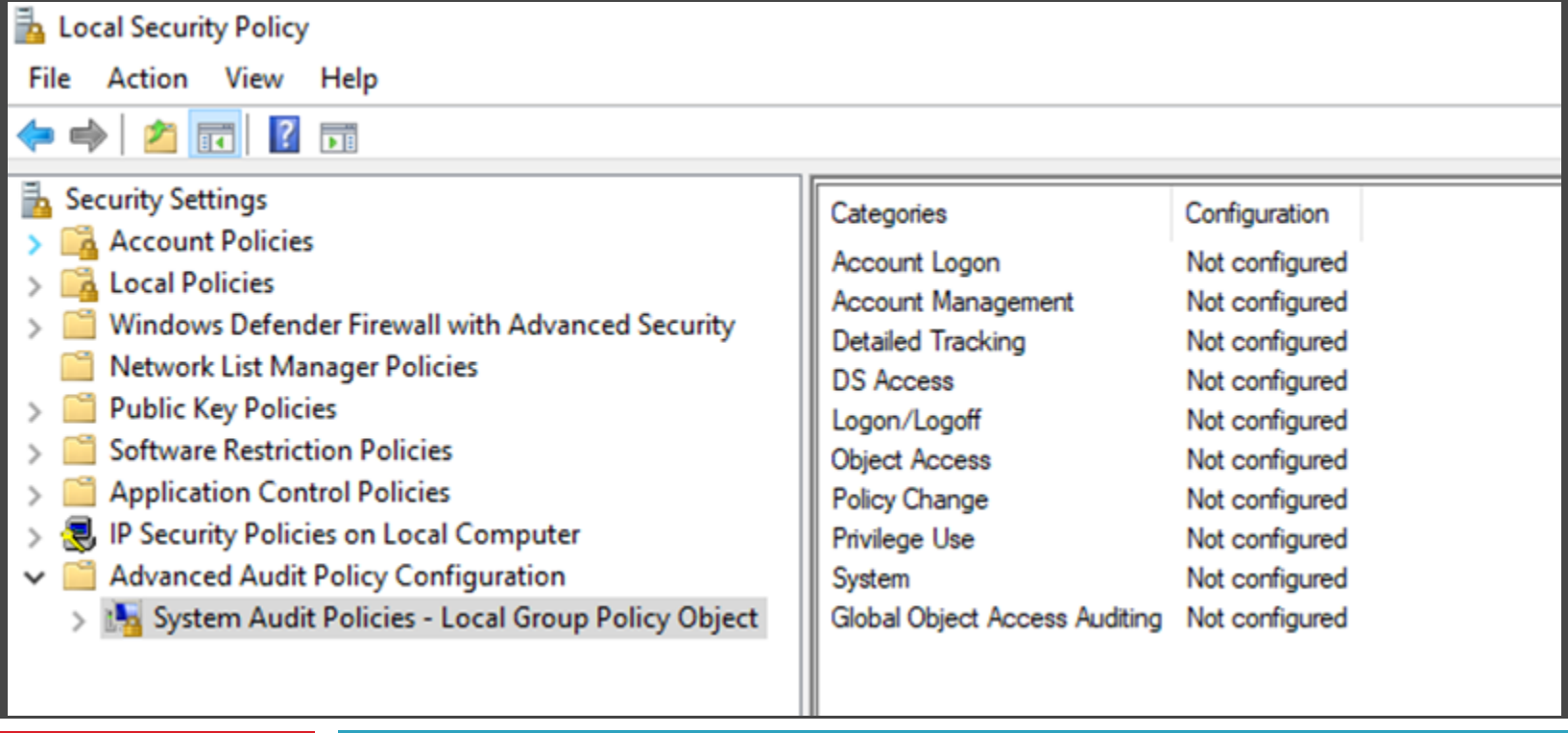
- Zapnout auditování všeho, pro všechny a na všech systémech – je to dobrý nápad?
- Není a to z několika důvodů:
  - Generovalo by to kvanta dat
  - Tato data by bylo třeba někam uložit, kontrolovat a vyznat se v nich
  - Mohlo by to ovlivnit výkon serveru
- Naopak pokud budete auditovat „málo“, můžete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

CO VŠECHNO LZE AUDITOVAT?

JEDNODUCHÉ (STARŠÍ) AUDITOVÁNÍ



GRANULÁRNÍ (NOVĚJŠÍ) AUDITOVÁNÍ



```
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

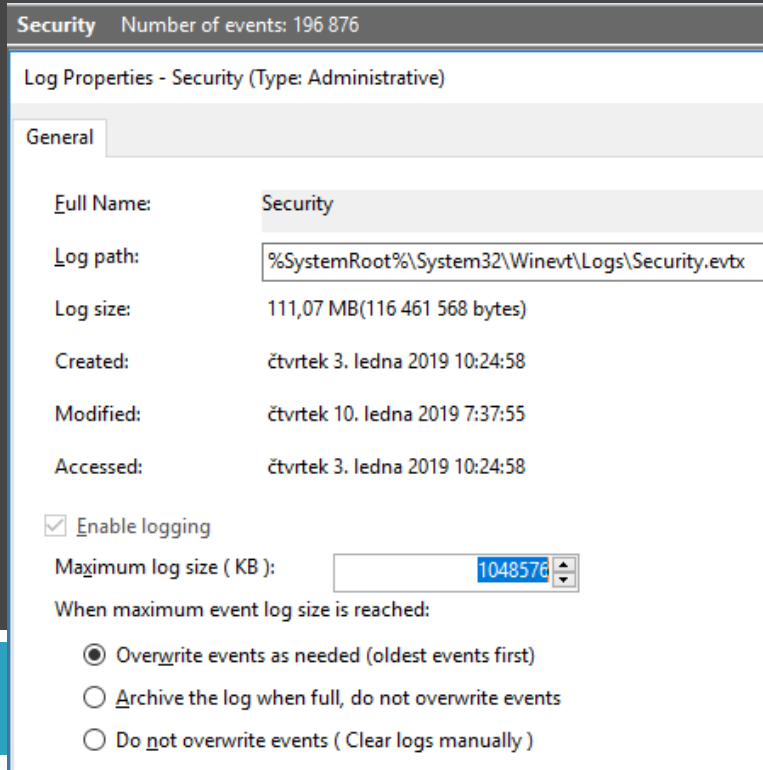
DEFAULT: WINDOWS SERVER

- 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

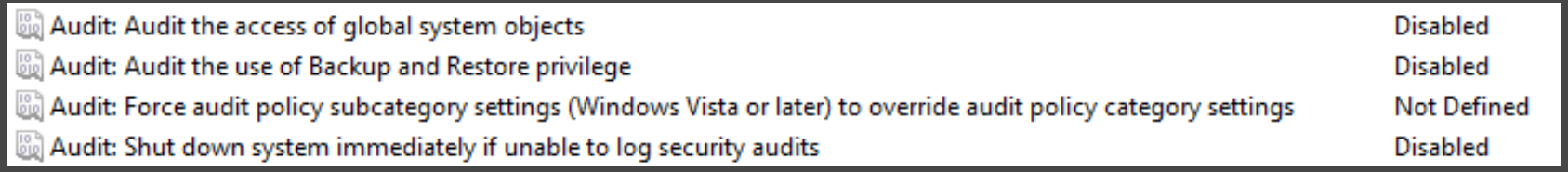
KAM SE AUDITOVÁNÍ ZAPISUJE?

- 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



NASTAVENÍ PRO SECURITY EVENTLOG

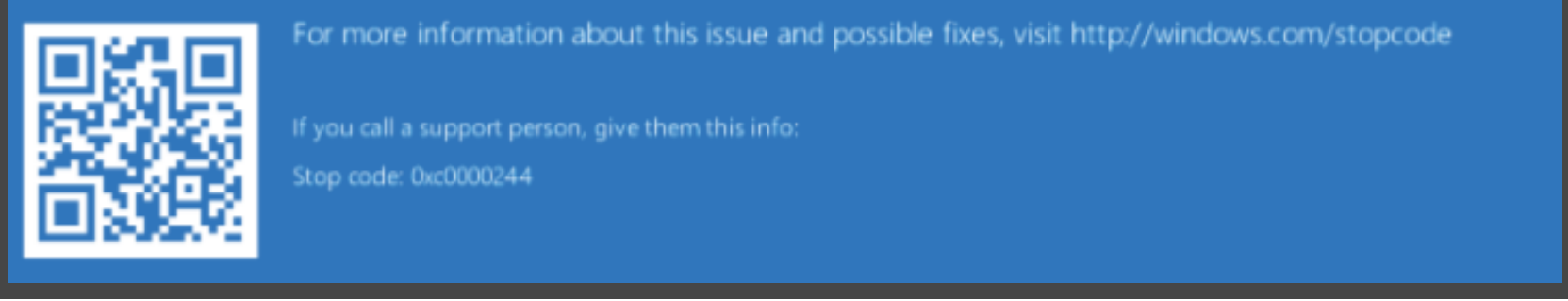
- Doporučená nastavení pro velikosti EventLogu (KB957662)
- Přepisovat, archivovat nebo co?
- GPO: Computer\Windows Settings\Security Settings\Local Policies\Security Options



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



Auditování

NEJZAJÍMAVĚJŠÍ KATEGORIE AUDITOVÁNÍ

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

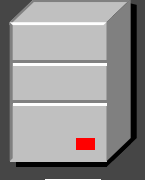
Account Logon + Logon/Logoff

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?

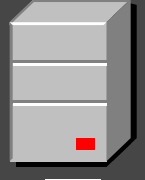


DC

CLIENT

ACCOUNT LOGON vs. LOGON

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



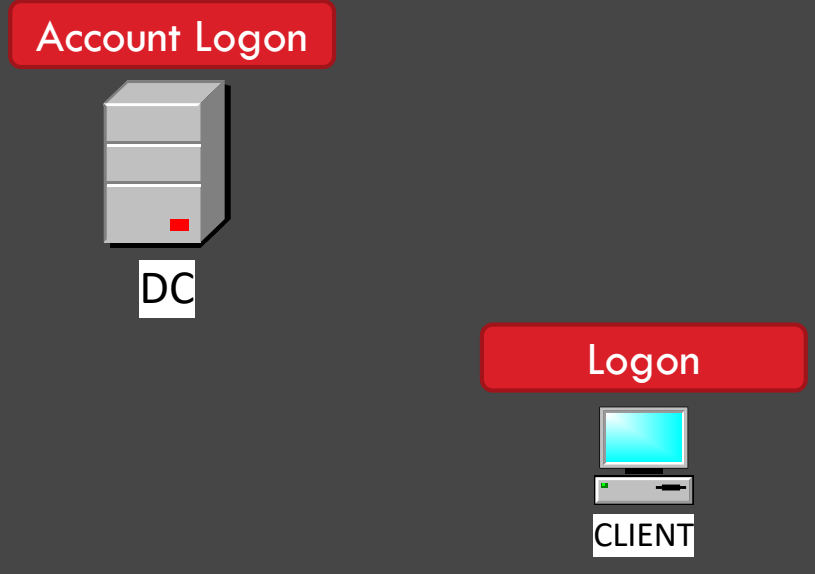
DC

Logon

CLIENT

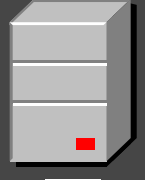
ACCOUNT LOGON vs. LOGON

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



ACCOUNT LOGON vs. LOGON

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



DC

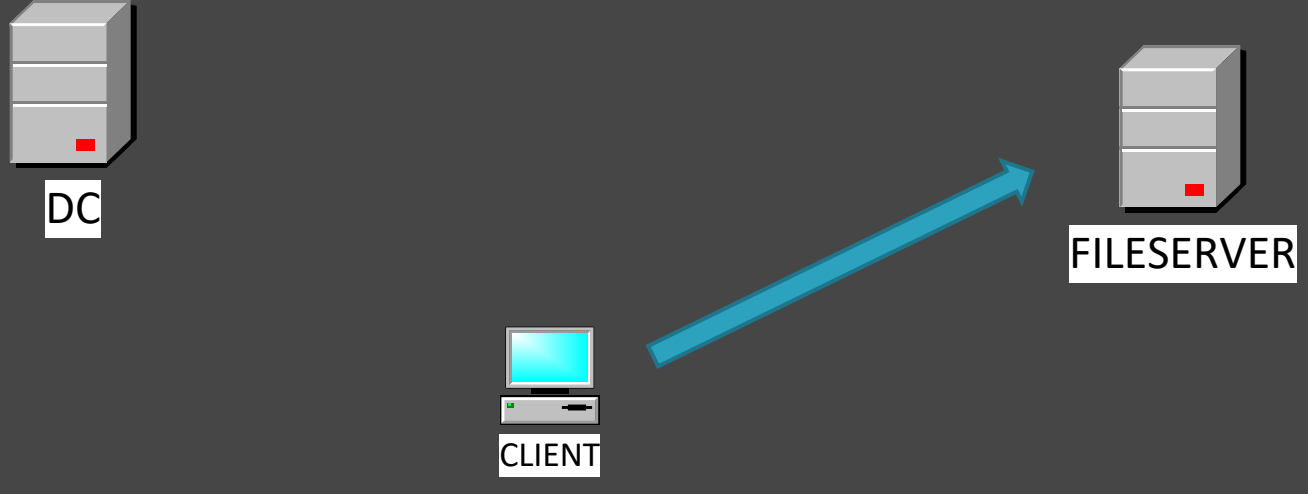
Account Logon

Logon

CLIENT

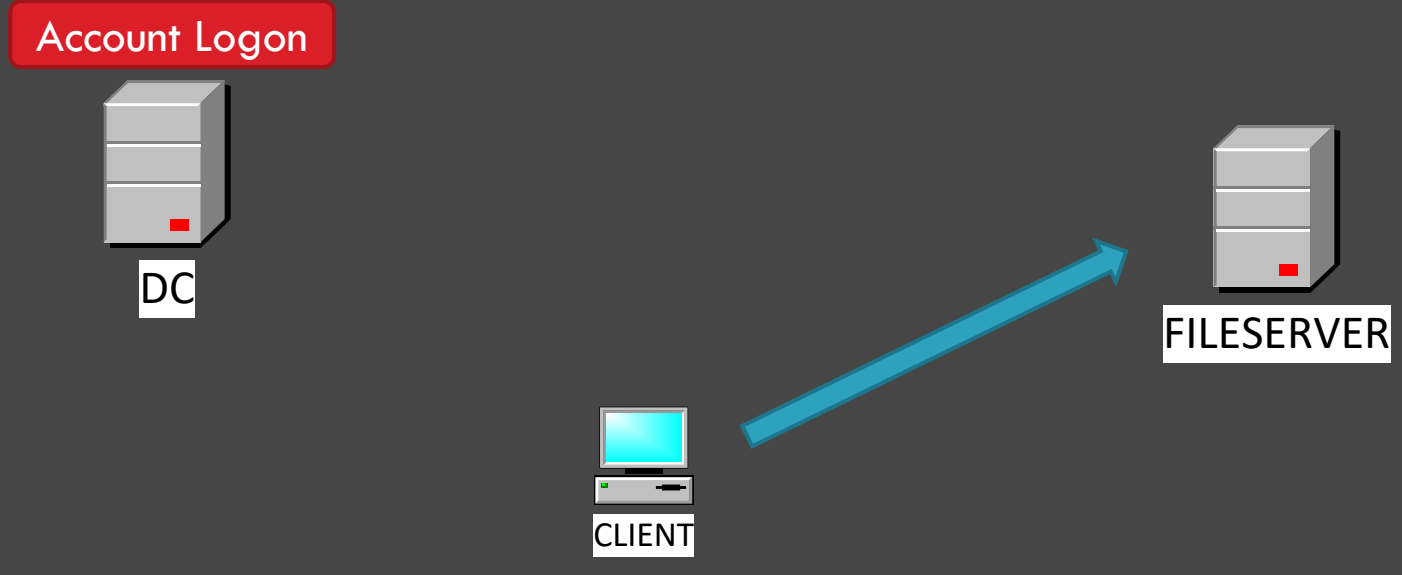
ACCOUNT LOGON vs. LOGON

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



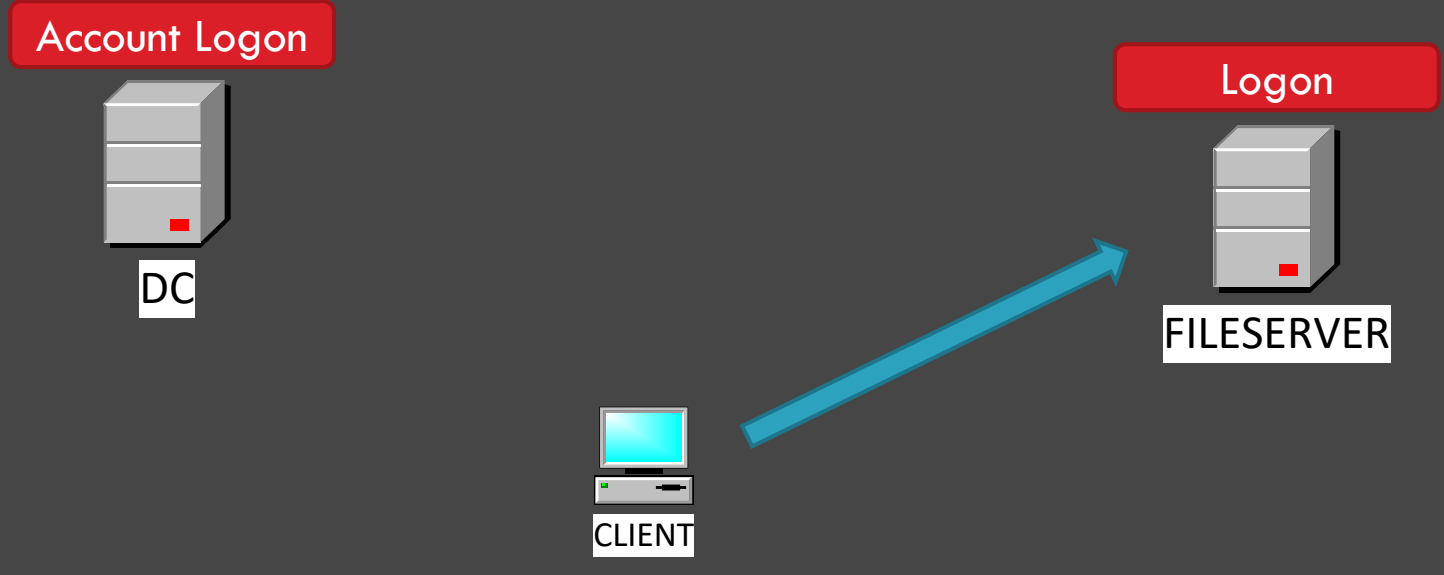
ACCOUNT LOGON vs. LOGON

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



ACCOUNT LOGON vs. LOGON

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



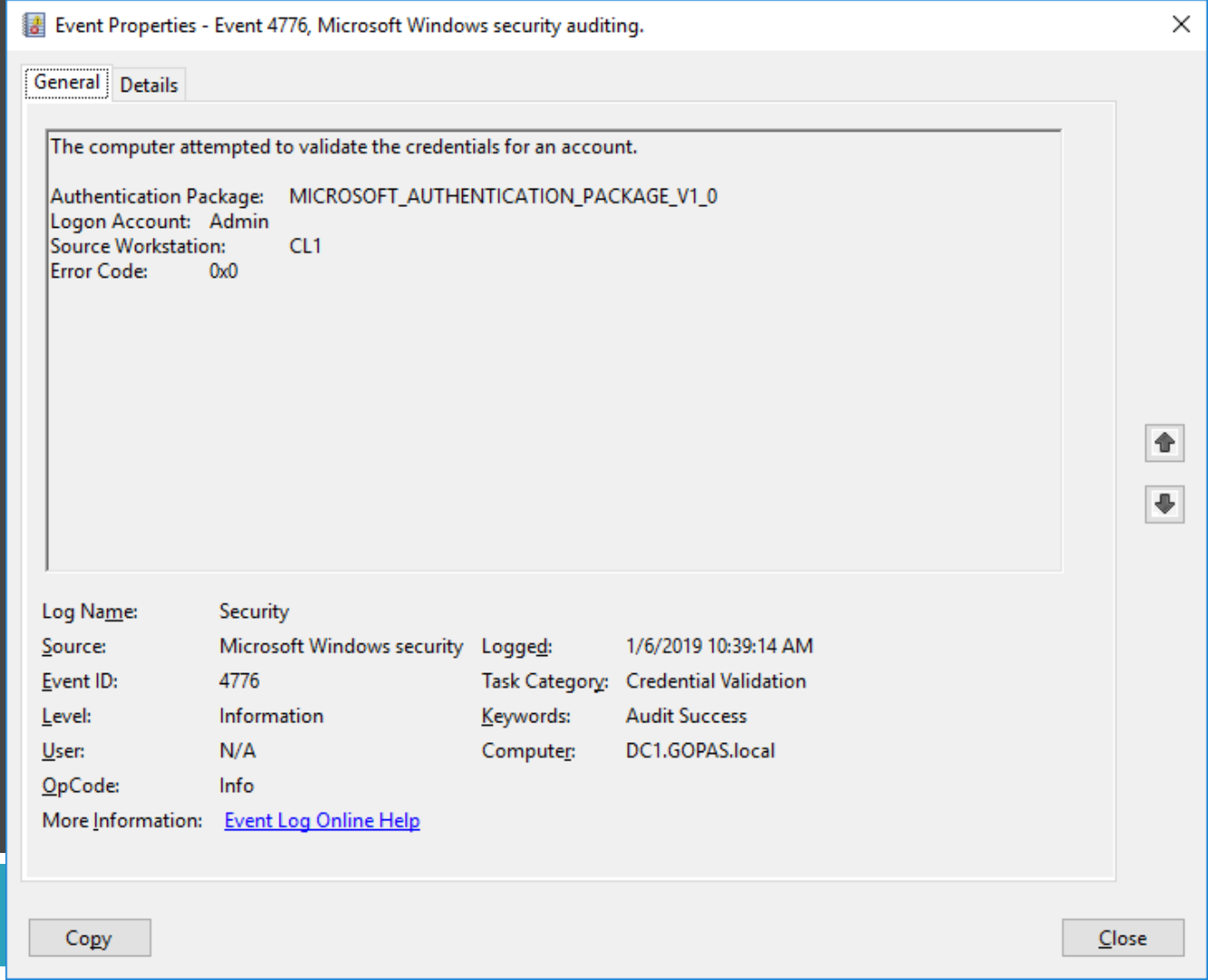
ACCOUNT LOGON

```
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.

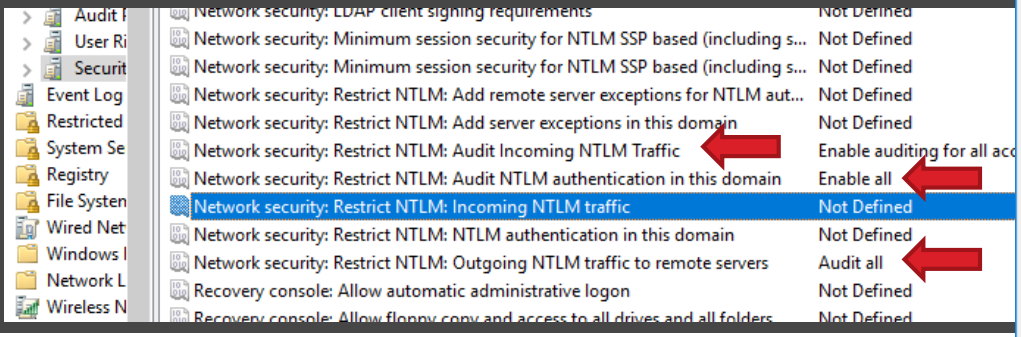
ID4776

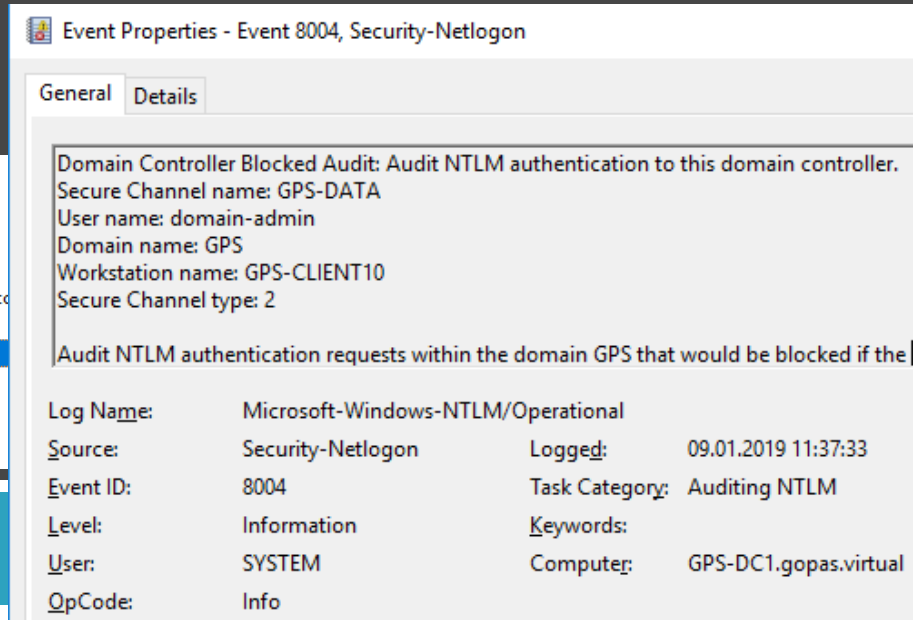
- NTLM ověření
- Na DC
- Audit Success



ODBOČKA K AUDITOVÁNÍ NTLM

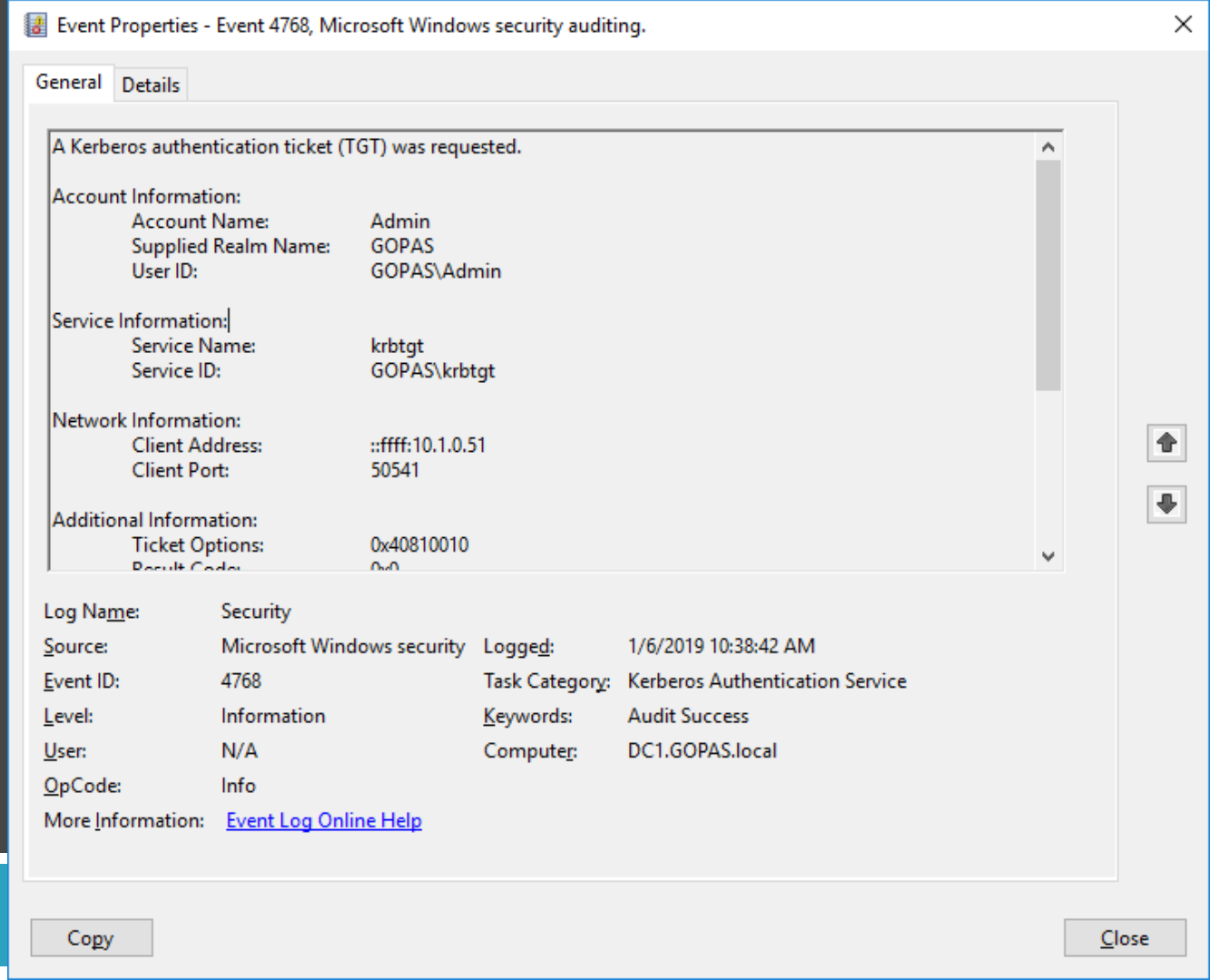
- Auditování NTLM ověření v kategorii Credential Validation není moc detailní
- Dá se zapnout detailní audit v GPO
- Computer\Windows Settings\Security Settings\Local Policies\Security Options





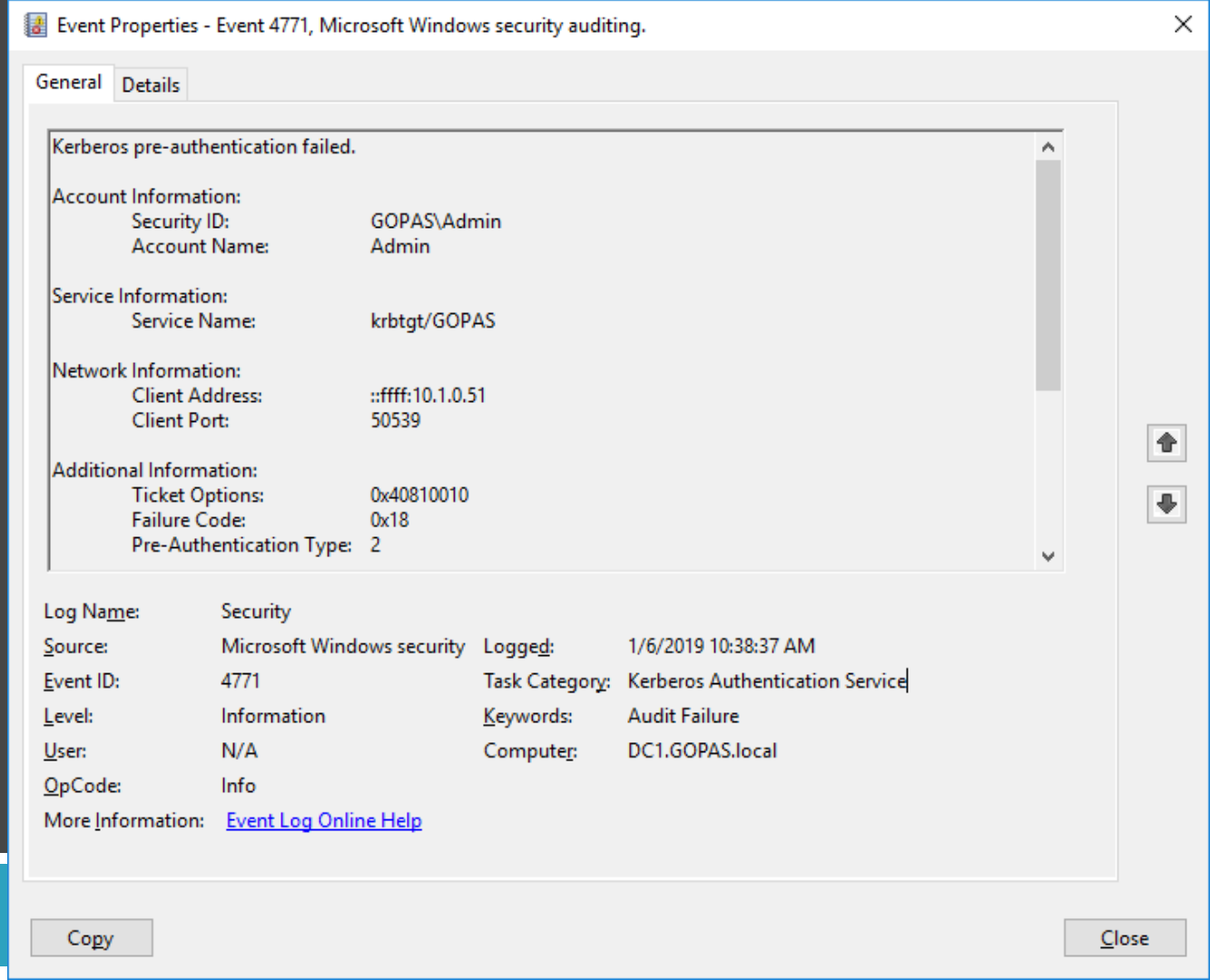
ID4768

- Úspěšná žádost o TGT
- Na DC
- Audit Success



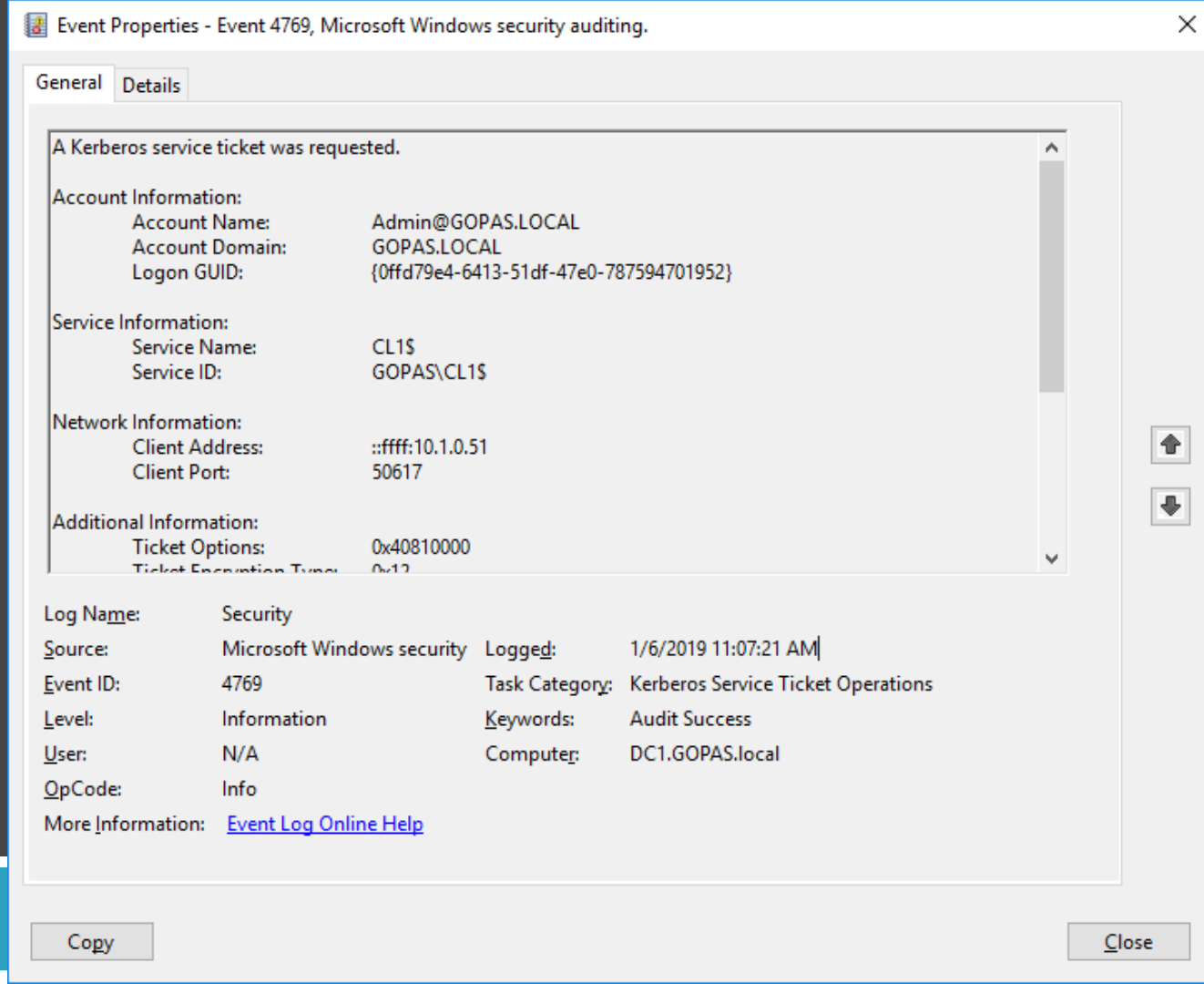
ID4771

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



ID4769

- Žádost o TGS
- Na DC
- Audit Success



LOGON/LOGOFF

```
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
```

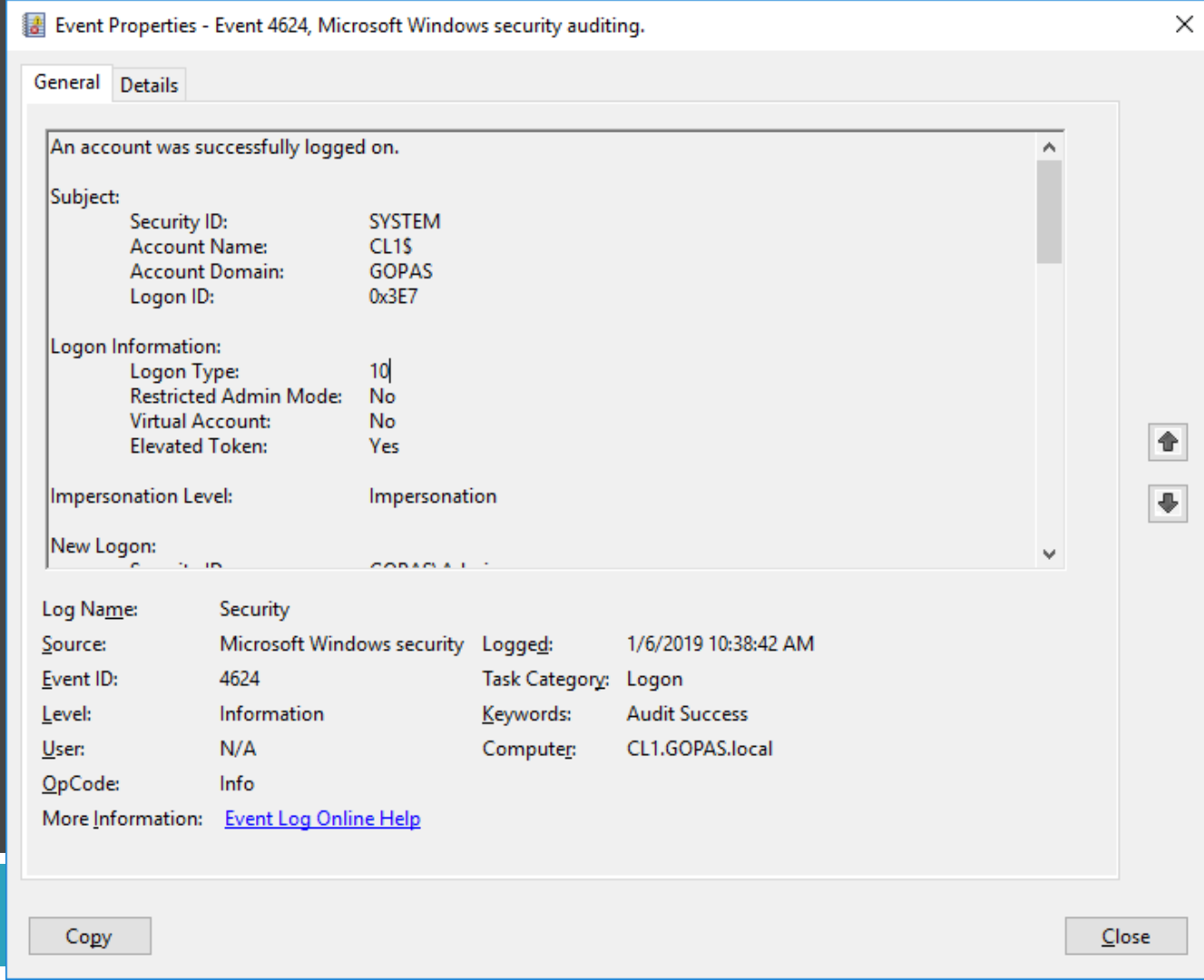
- Vlastní přihlášení
- Některé podkategorie:
  - Logon – podkategorie oznamující úspěšný nebo neúspěšný pokus o přihlášení. EventID 4624, 4625.
  - Logoff – podkategorie oznamující odhlášení identity. Jen úspěšné události. Dá se použít pro zjištění délky přihlášení. EventID 4634.
  - Account Lockout – podkategorie informuje o uzamčení účtu po x špatných pokusech příhlášení. 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 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	

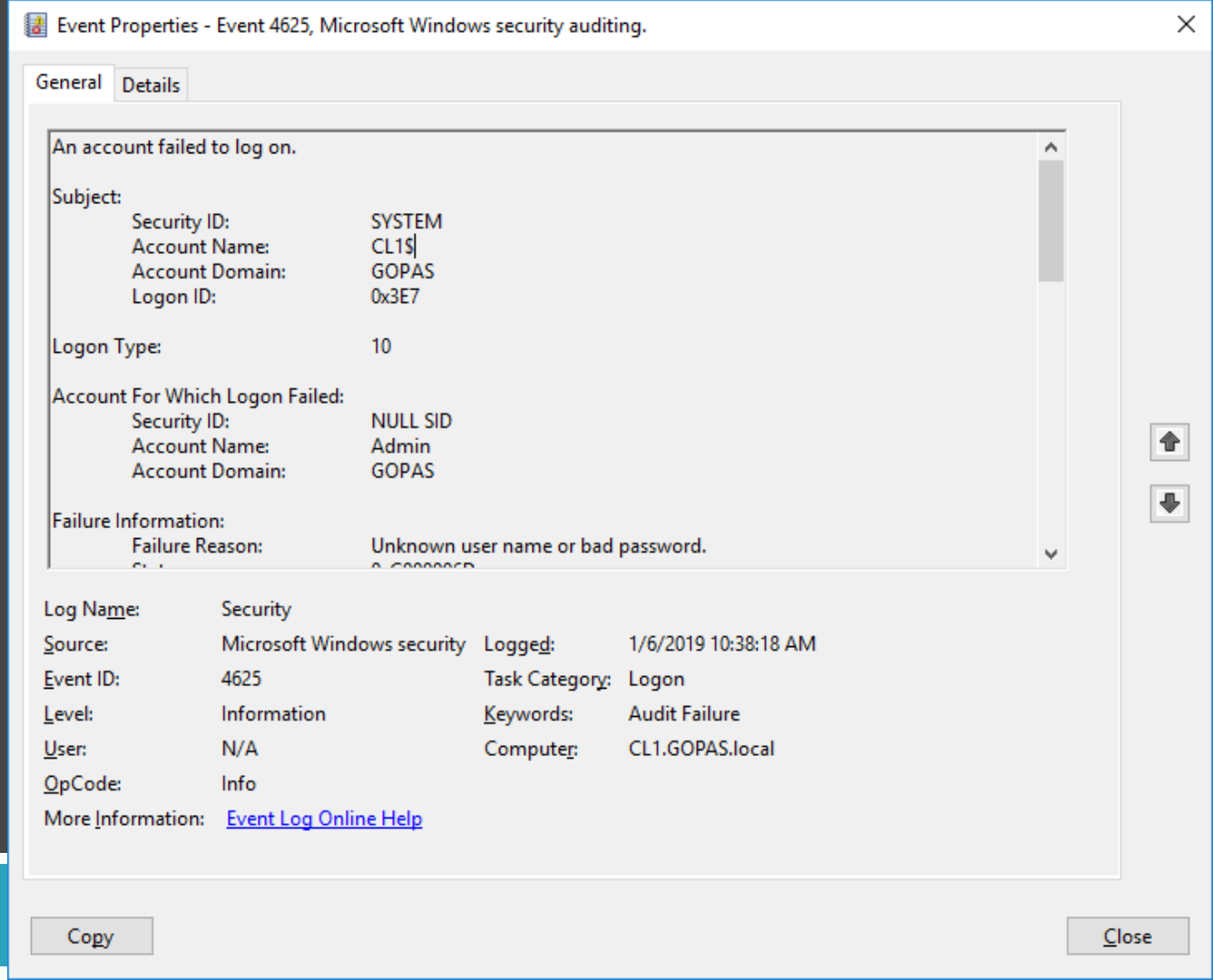
ID4624

- Přihlášení na CL1
- Audit Success



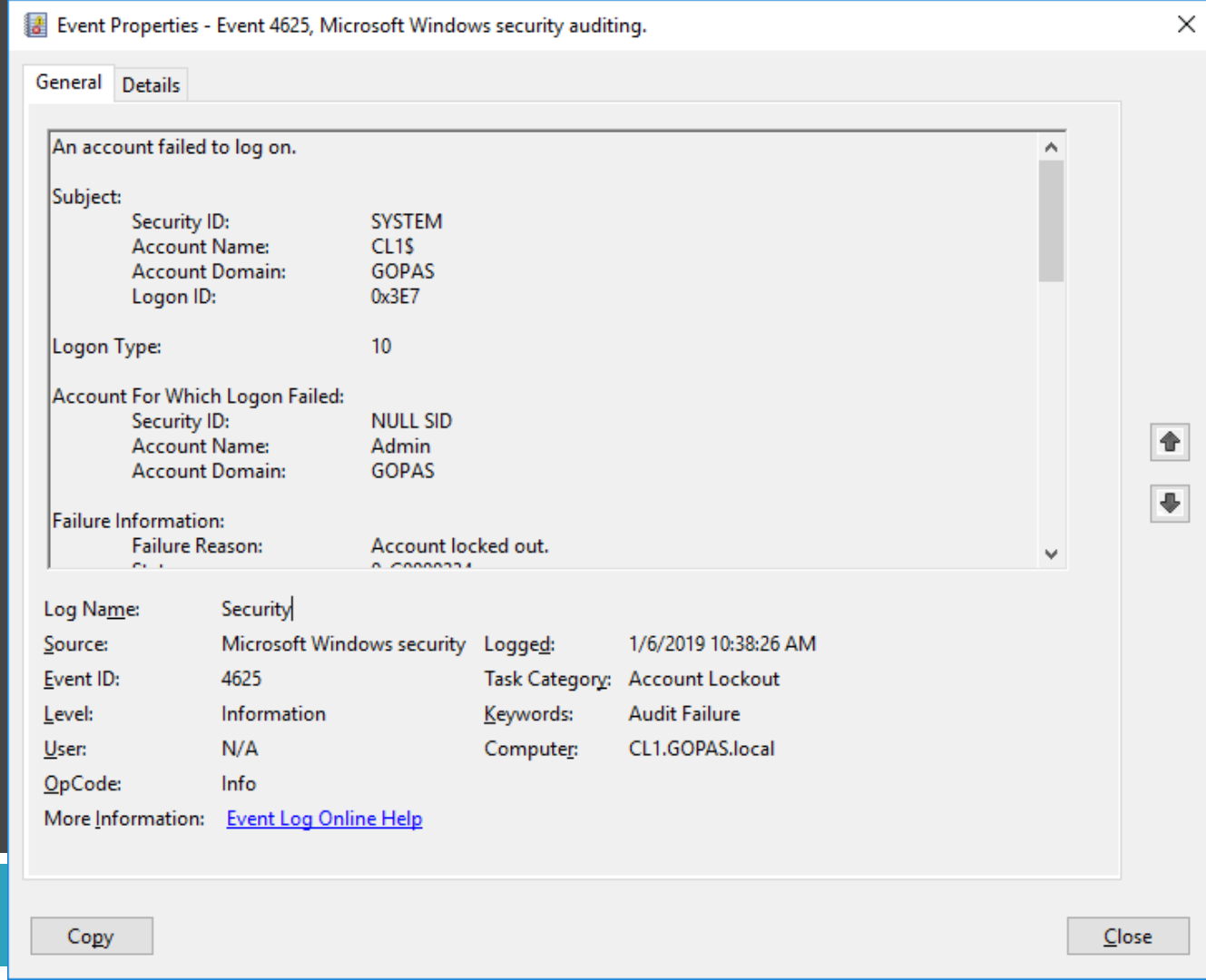
ID4625

- Přihlášení na CL1
- Audit Failure



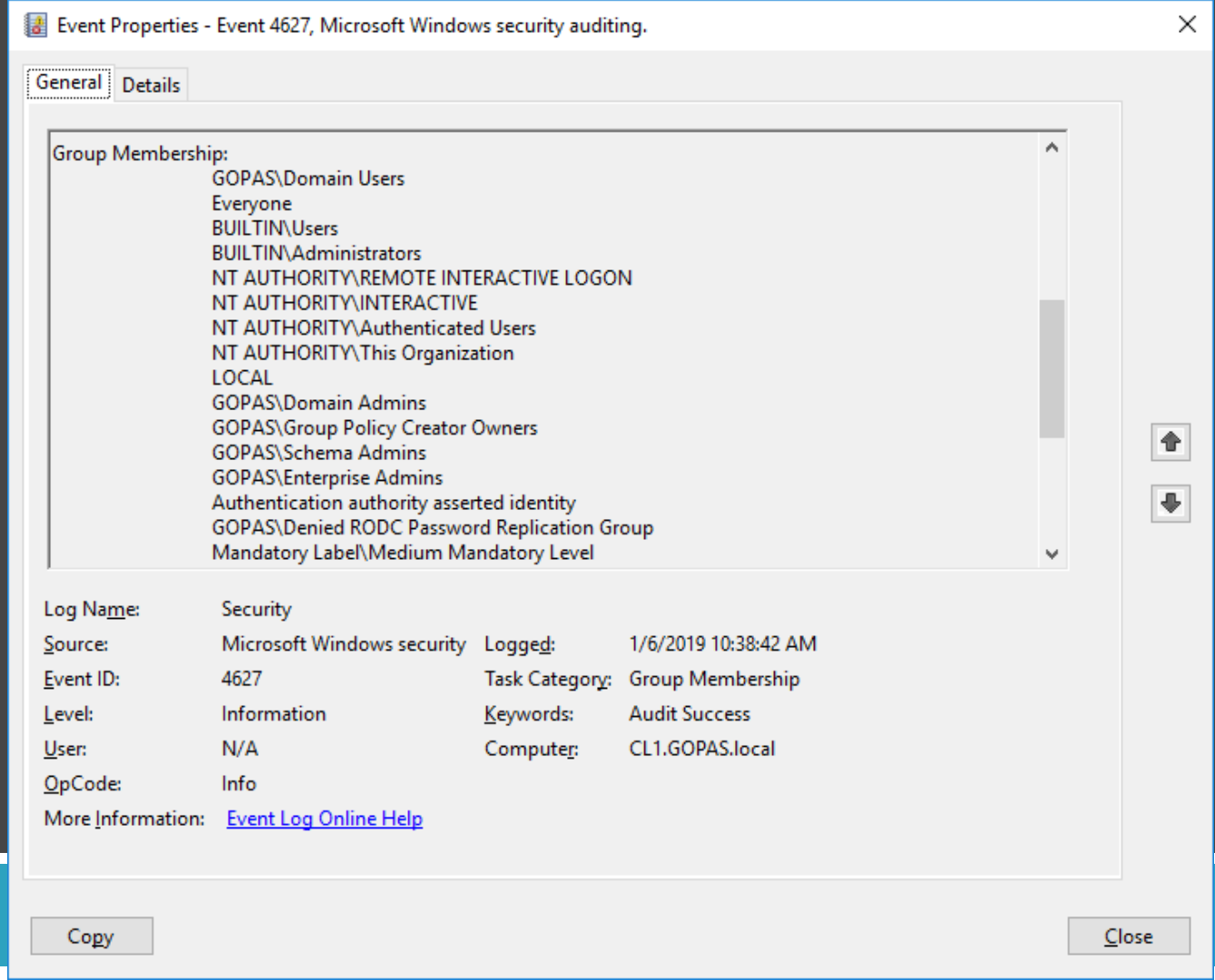
ID4625

- Zamknutí účtu Admin
- Audit Failure



ID4627

- Výpis členství
- Audit Success



DS Access + Account Management

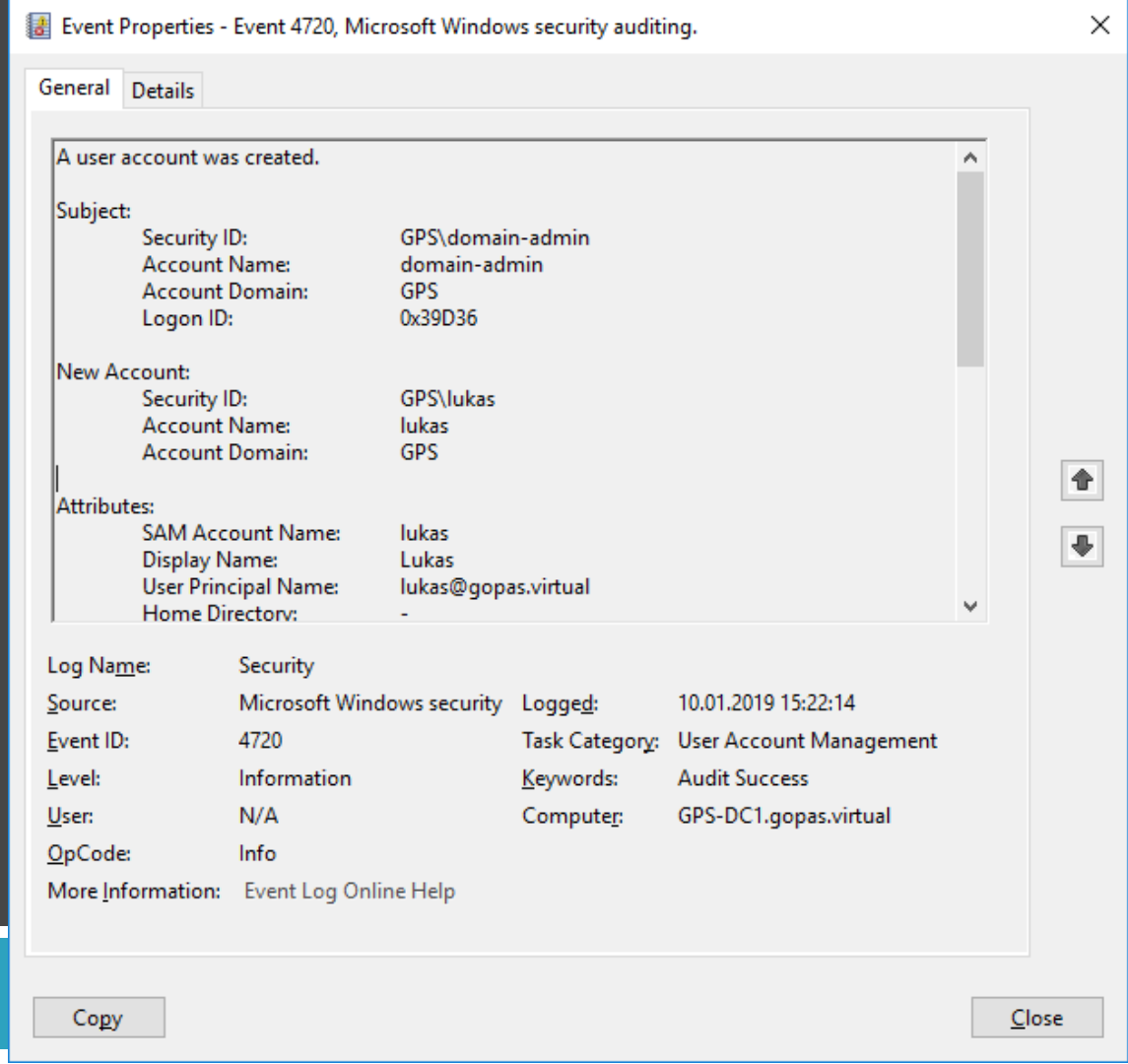
ACCOUNT MANAGEMENT

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

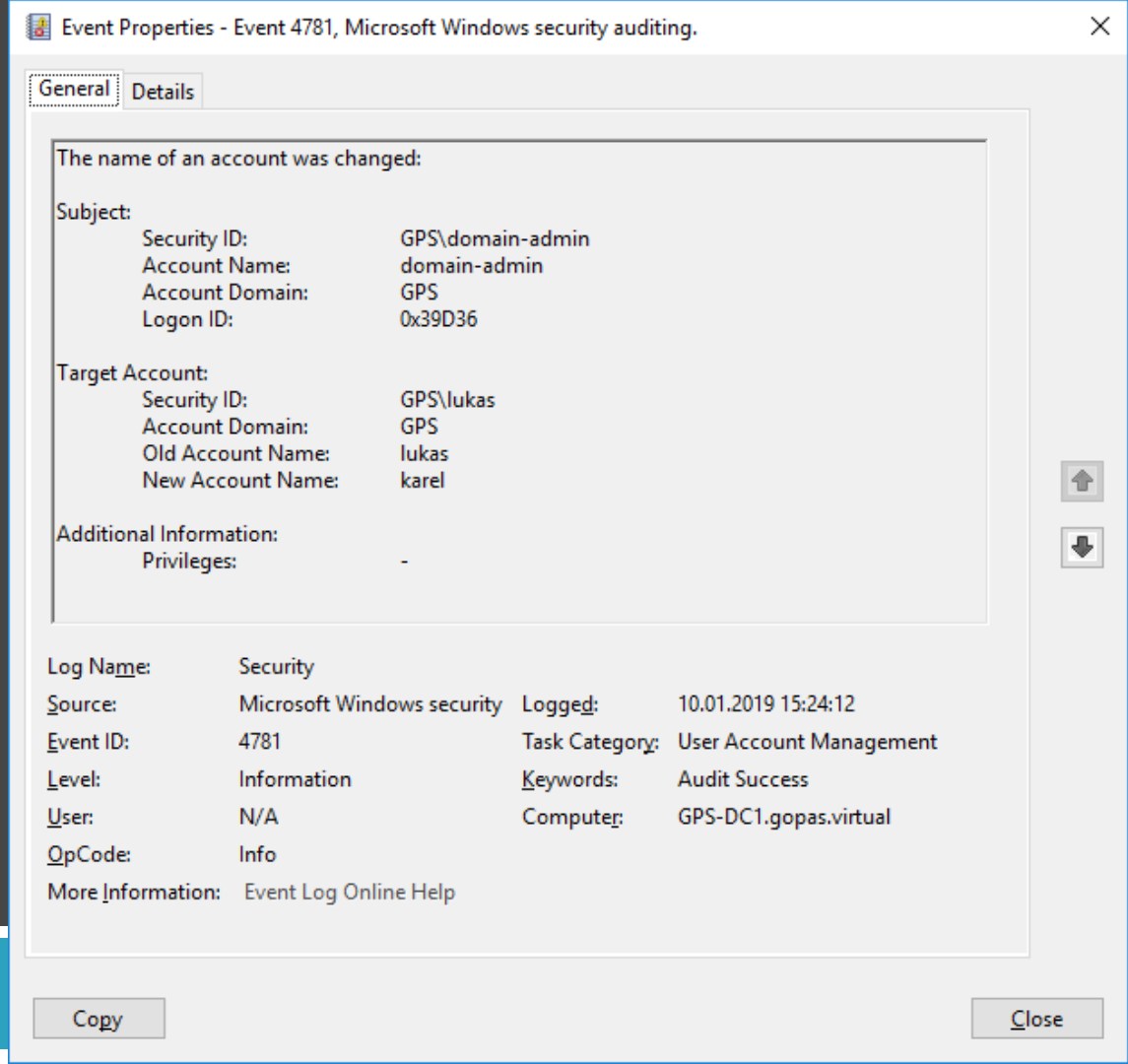
ID4720

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



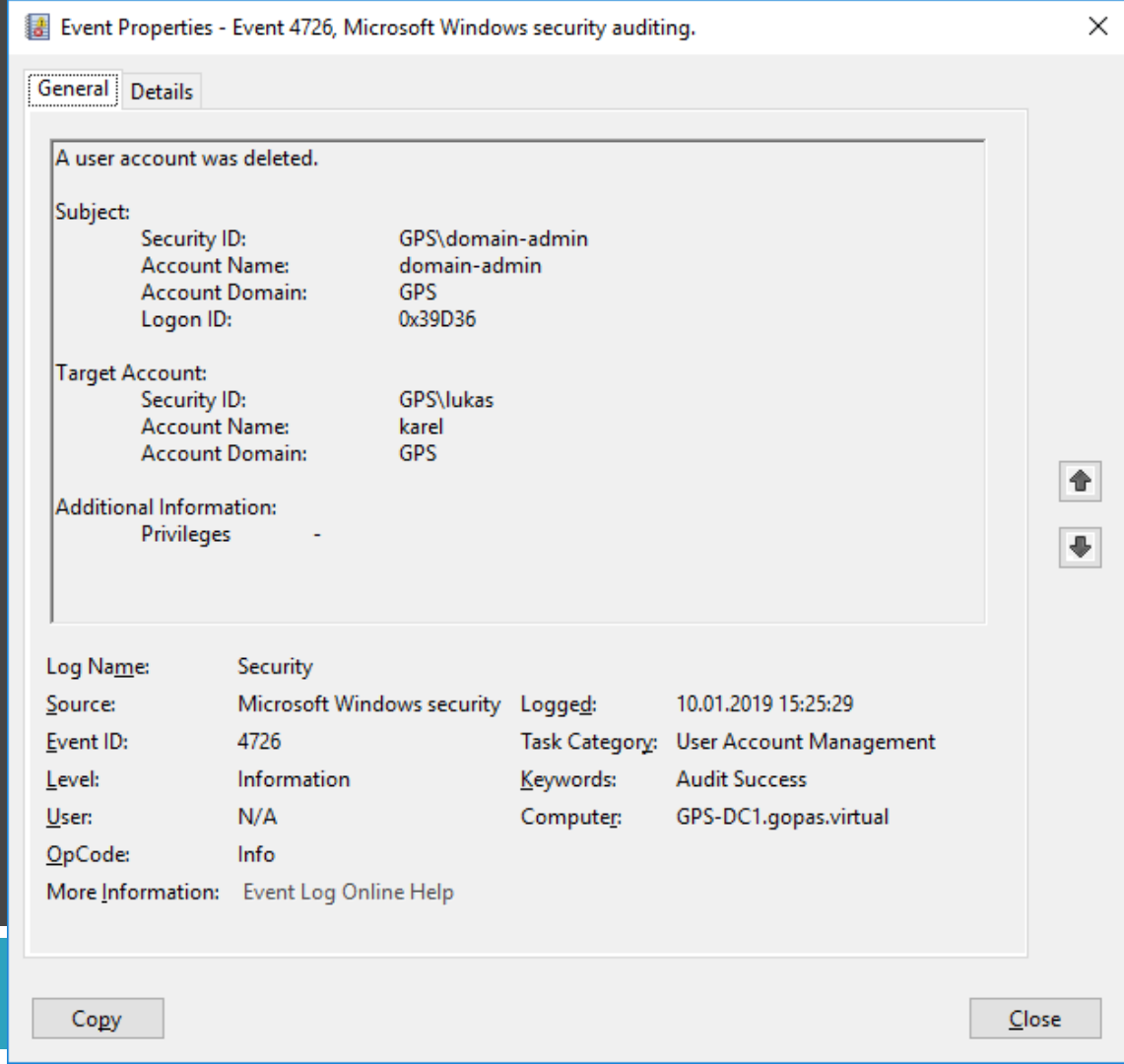
ID4781

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



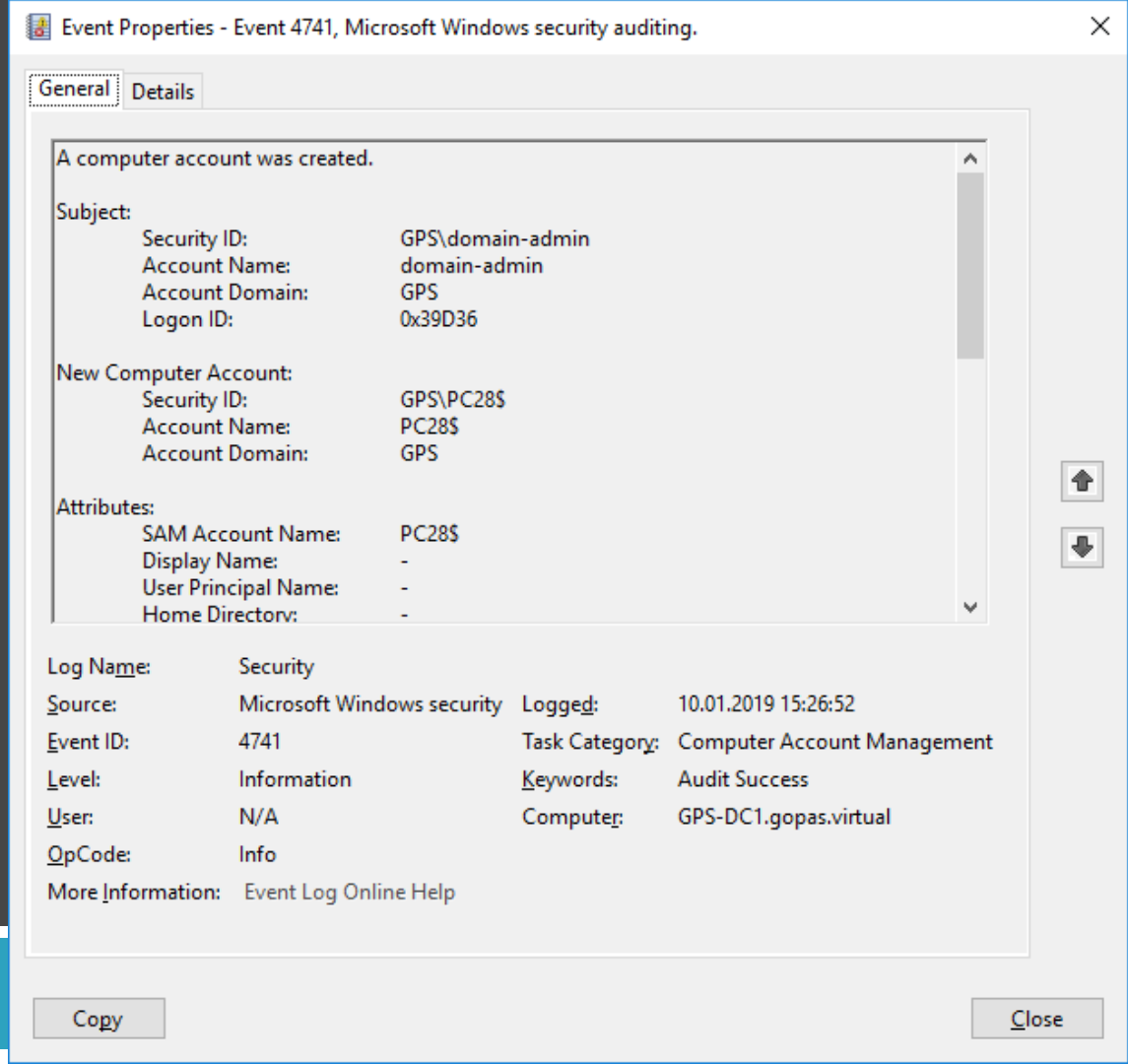
ID4726

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



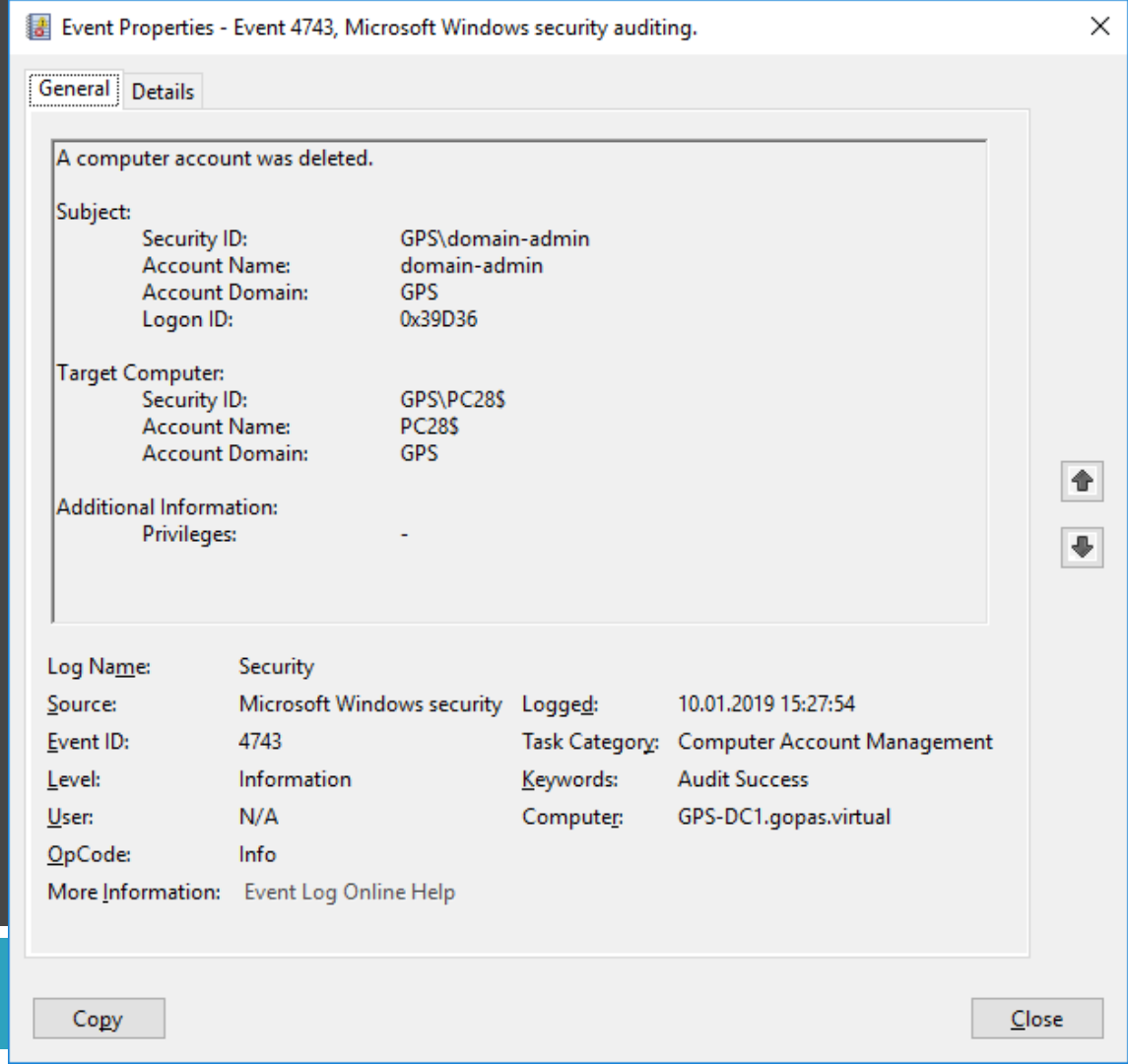
ID4741

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

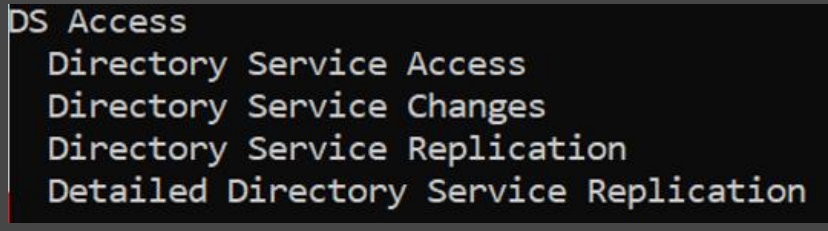


ID4743

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



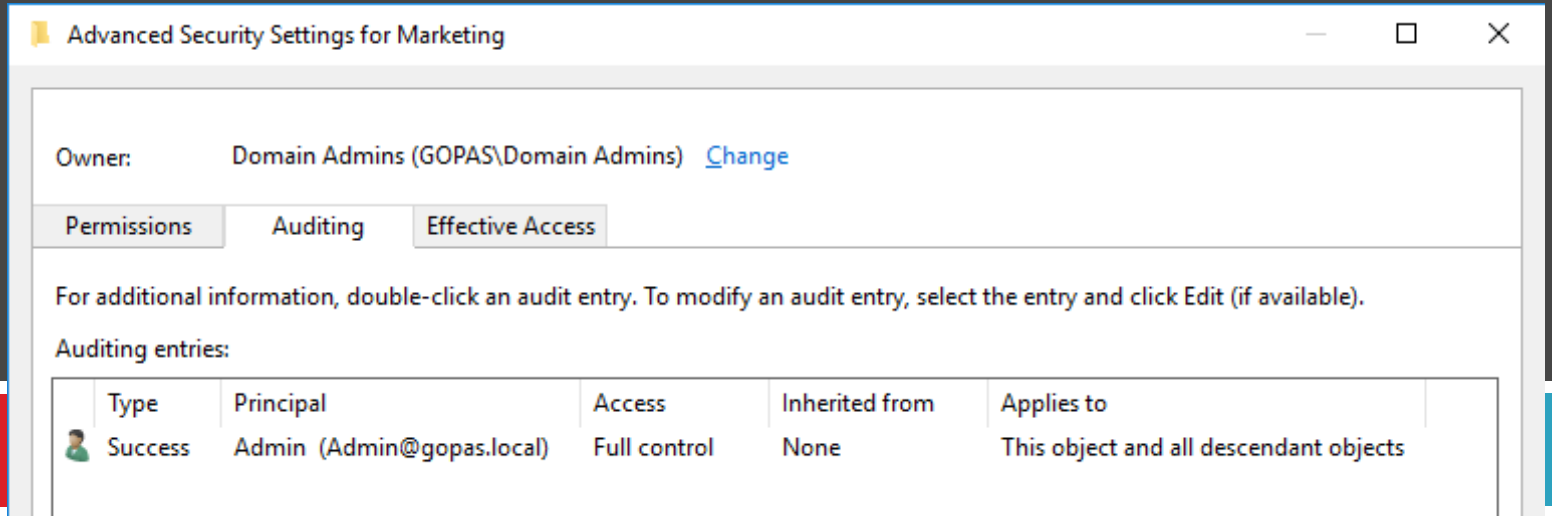
DS ACCESS



- 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.

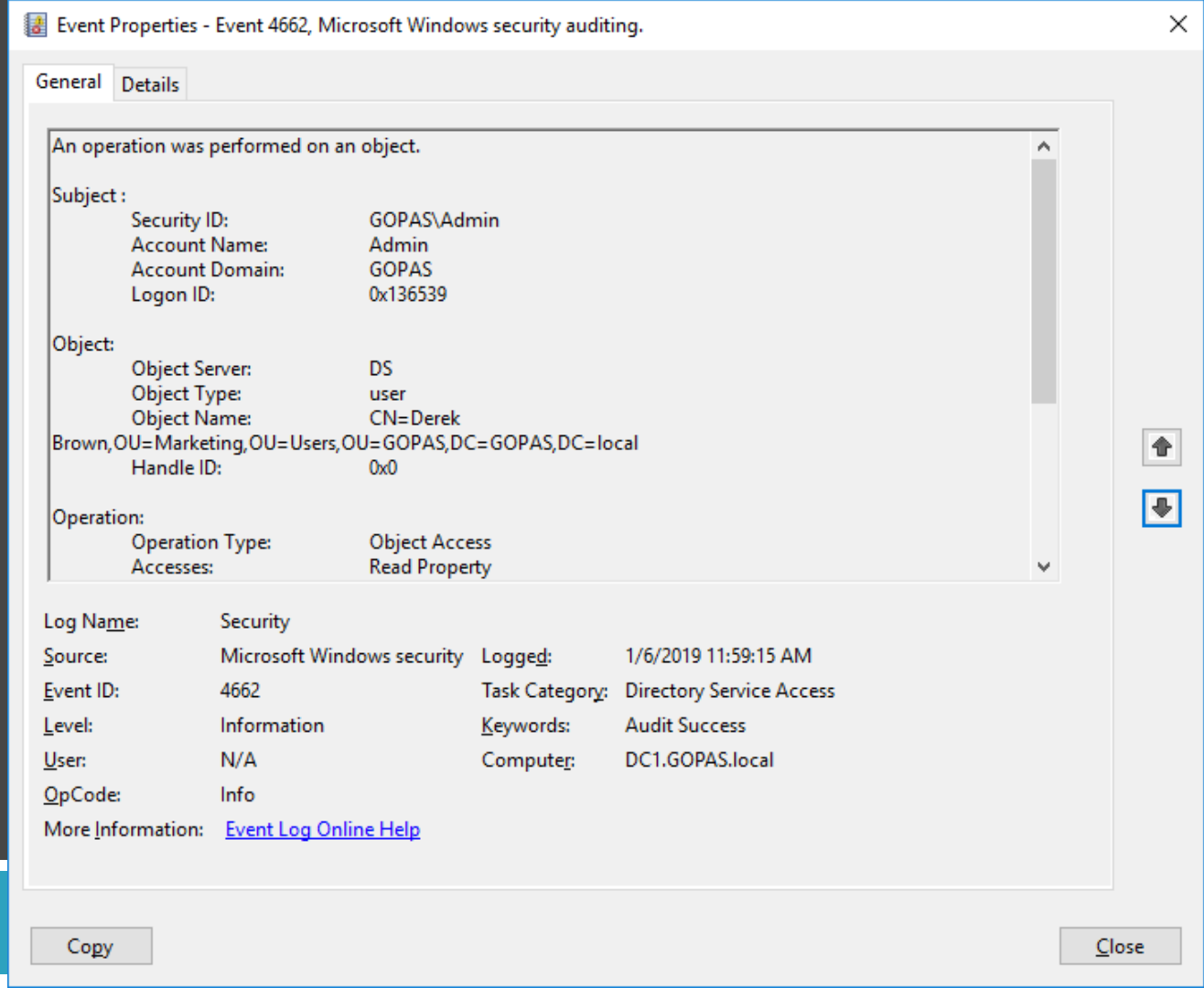
NASTAVENÍ AUDITOVÁNÍ DS ACCESS

- 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



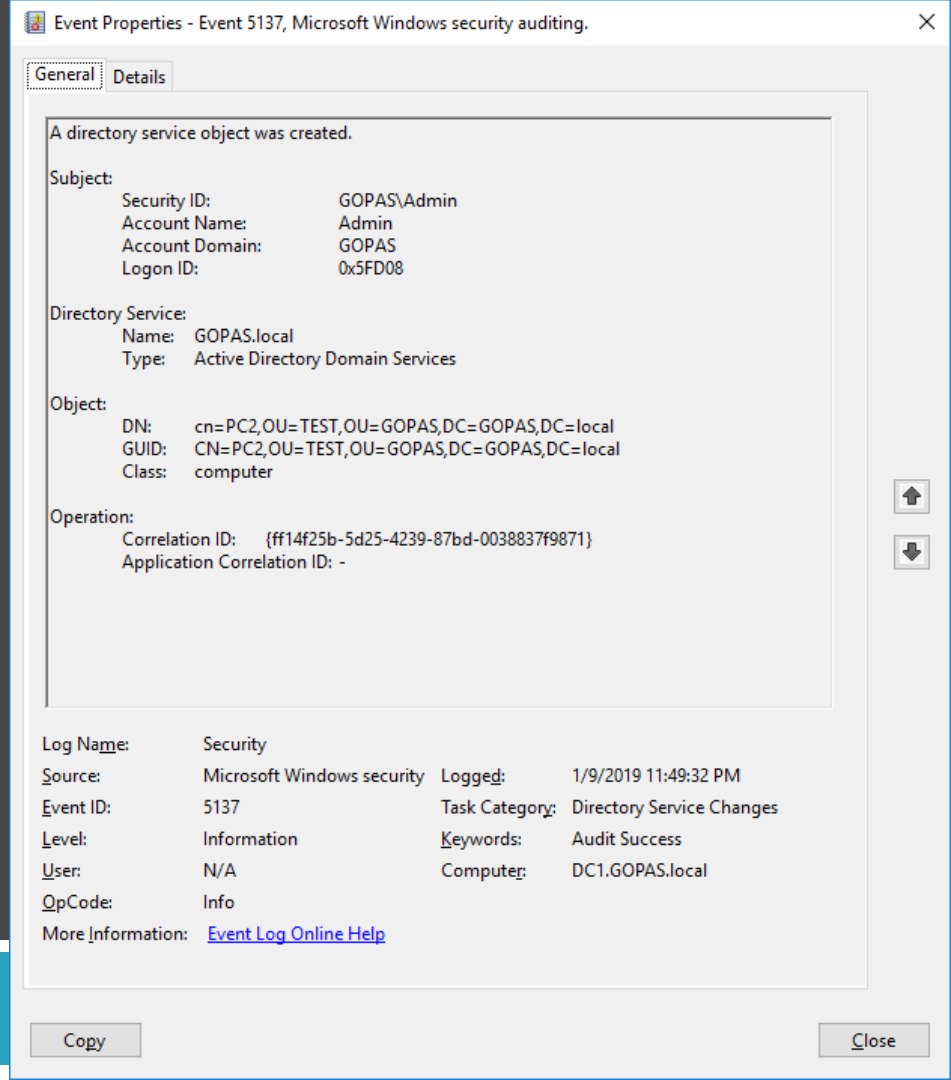
ID4662

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



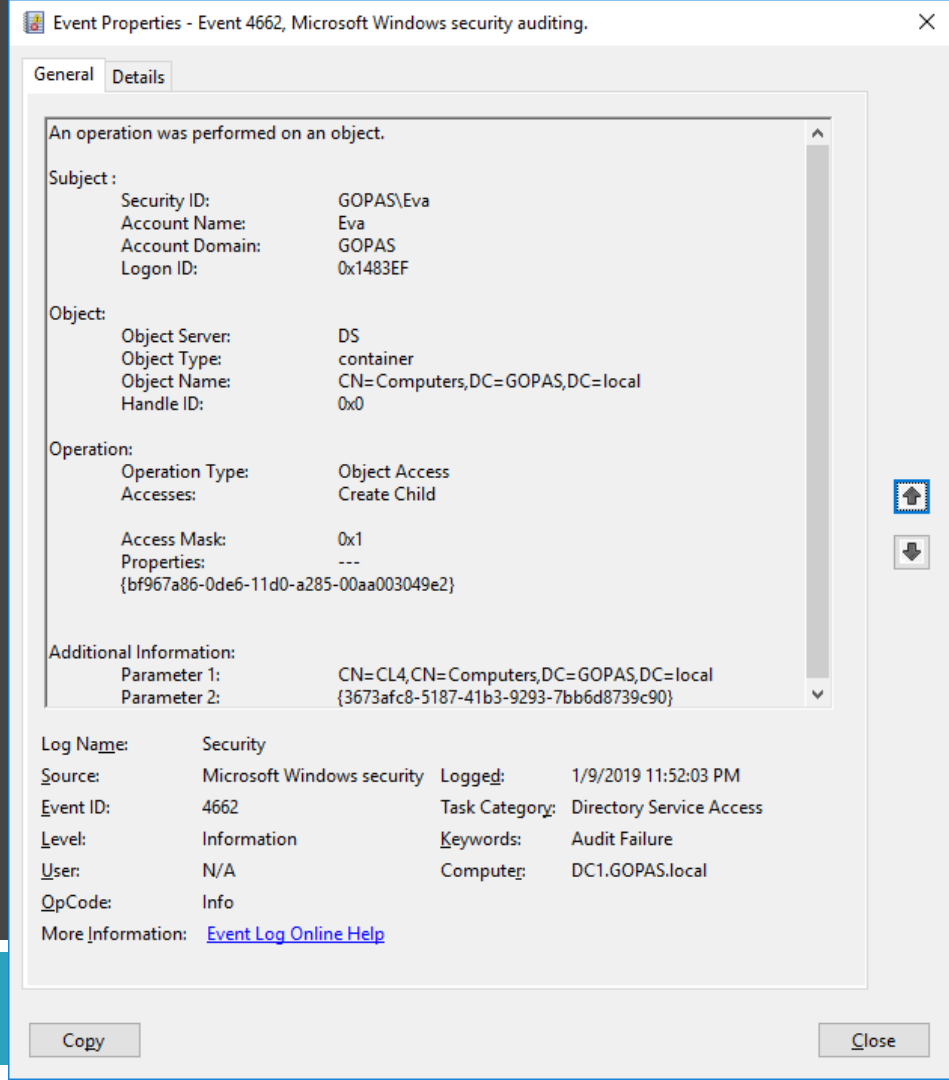
ID5137

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



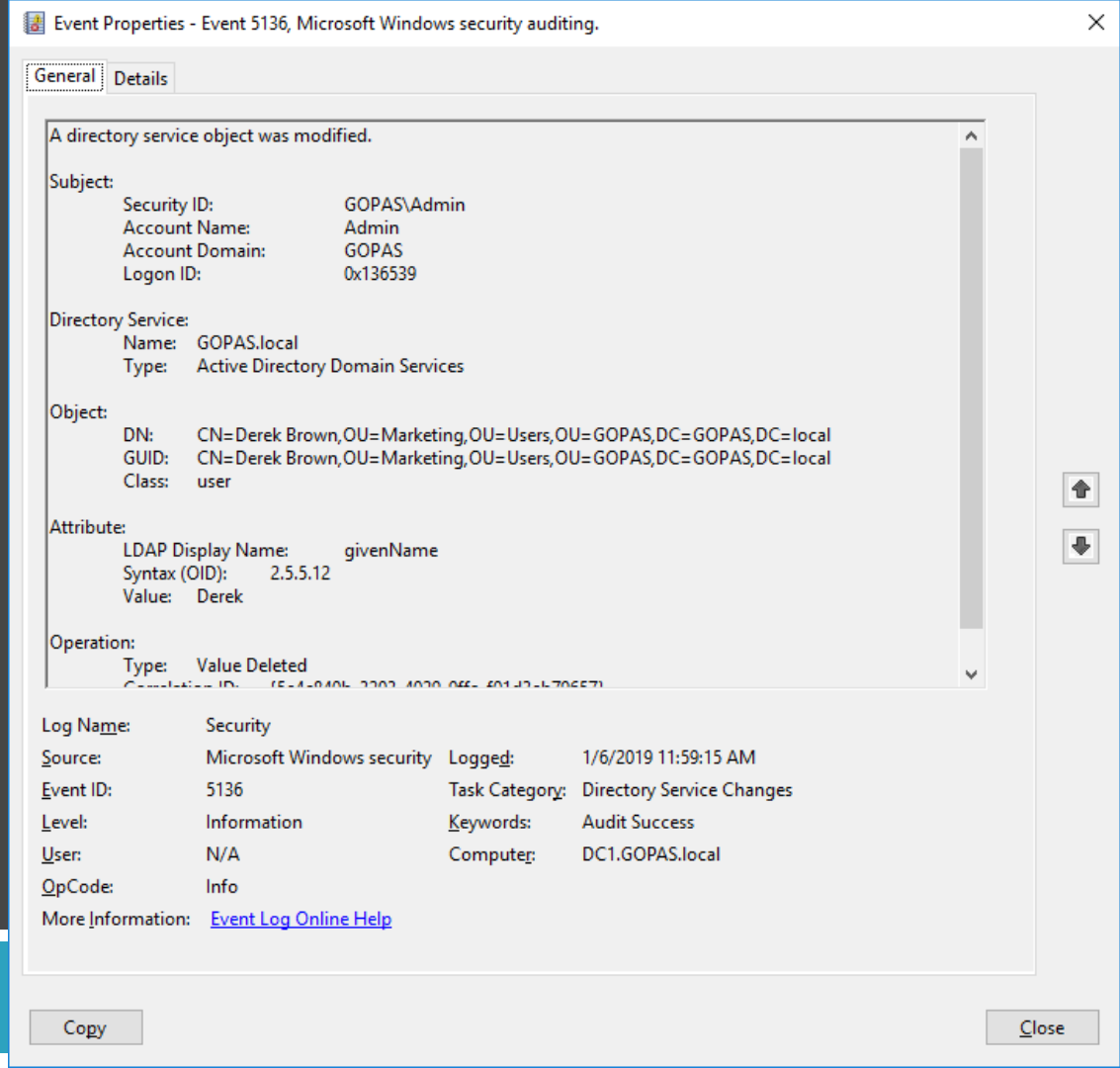
ID4662

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



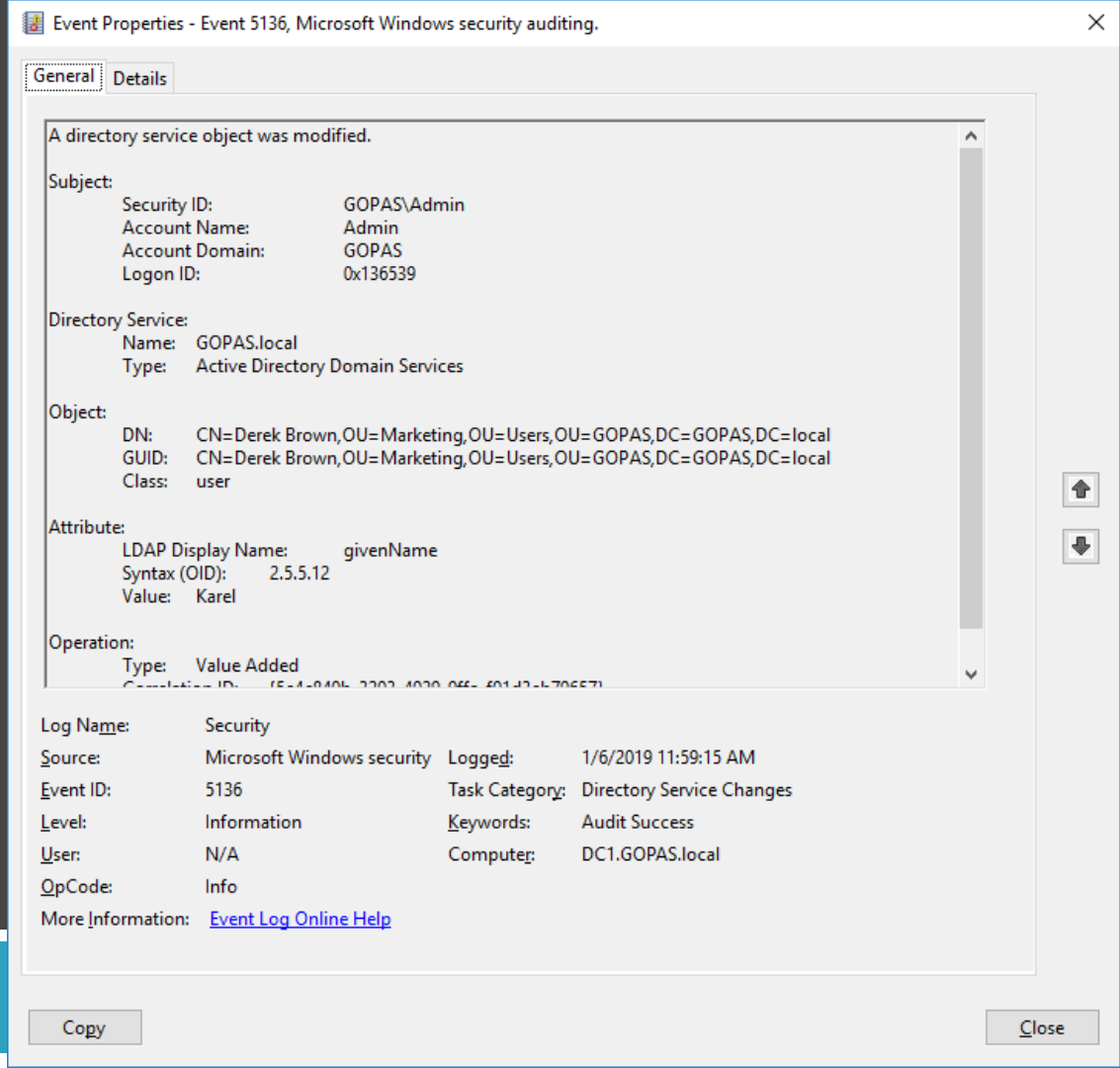
ID5136

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



ID5136

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



Object Access

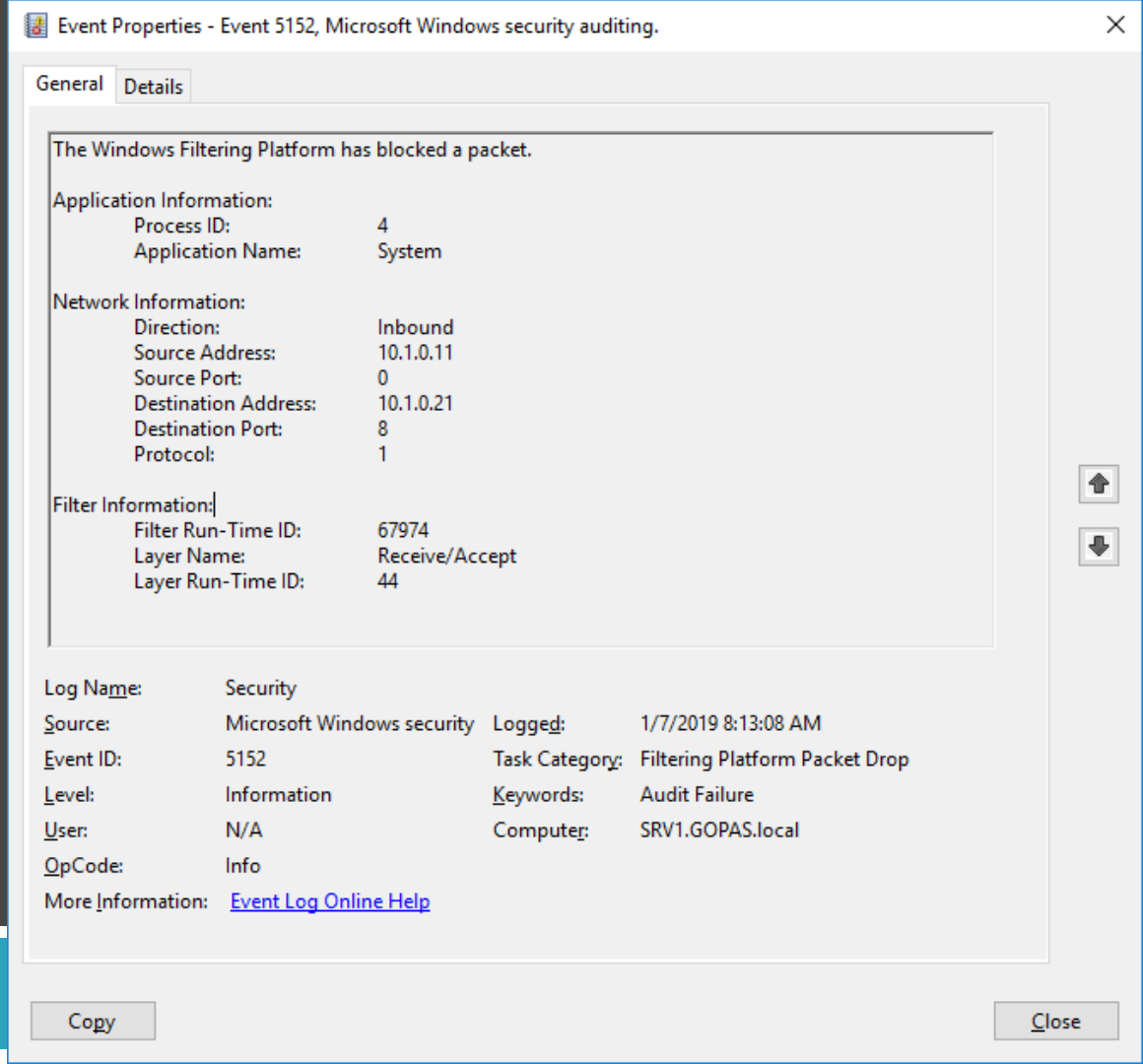
OBJECT ACCESS

```
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
```

- Auditování CA, FW, souborů, sdílených dat, DAC atp.
- Některé podkategorie:
  - Cetification 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

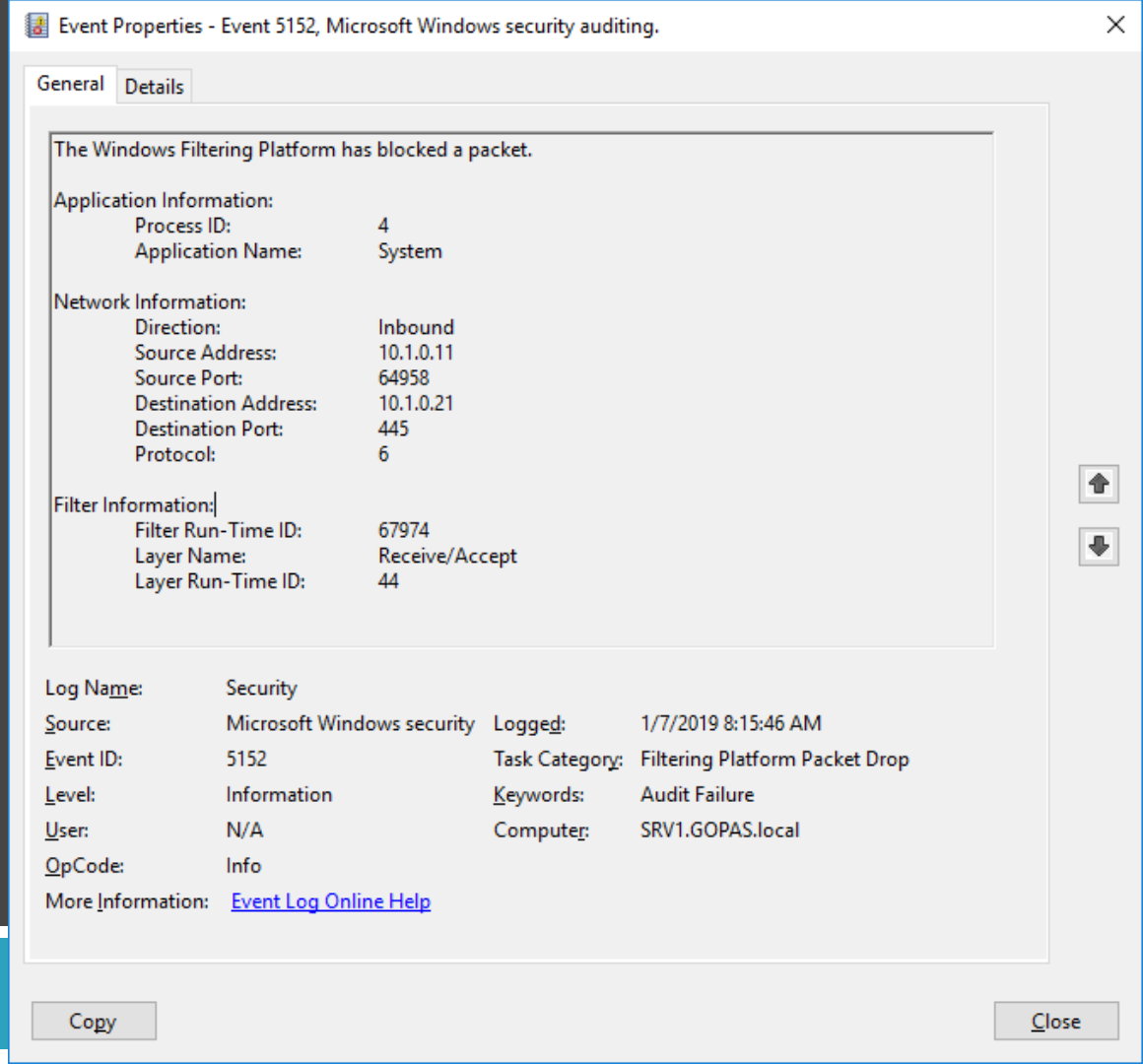
ID5152

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



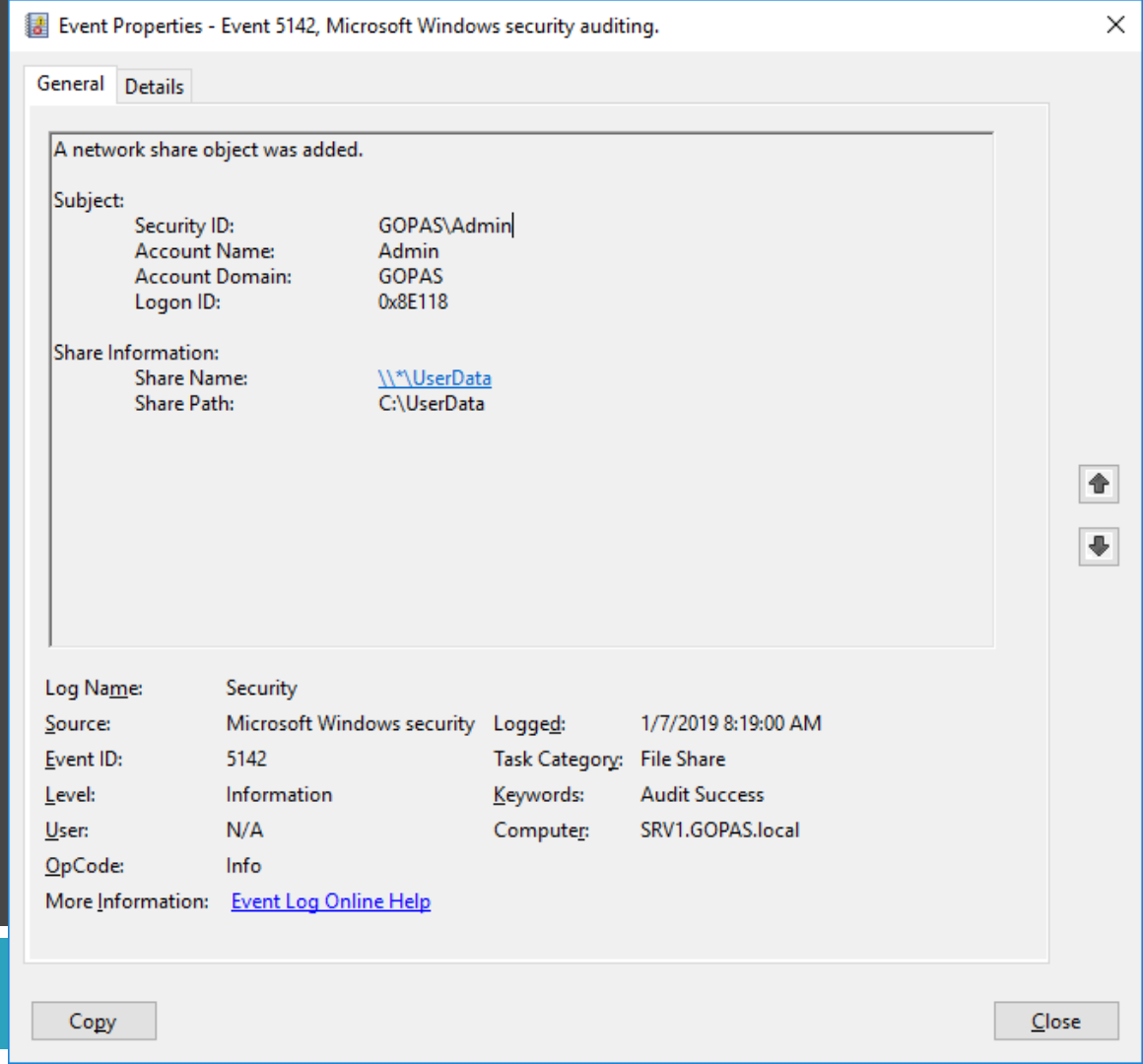
ID5152

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



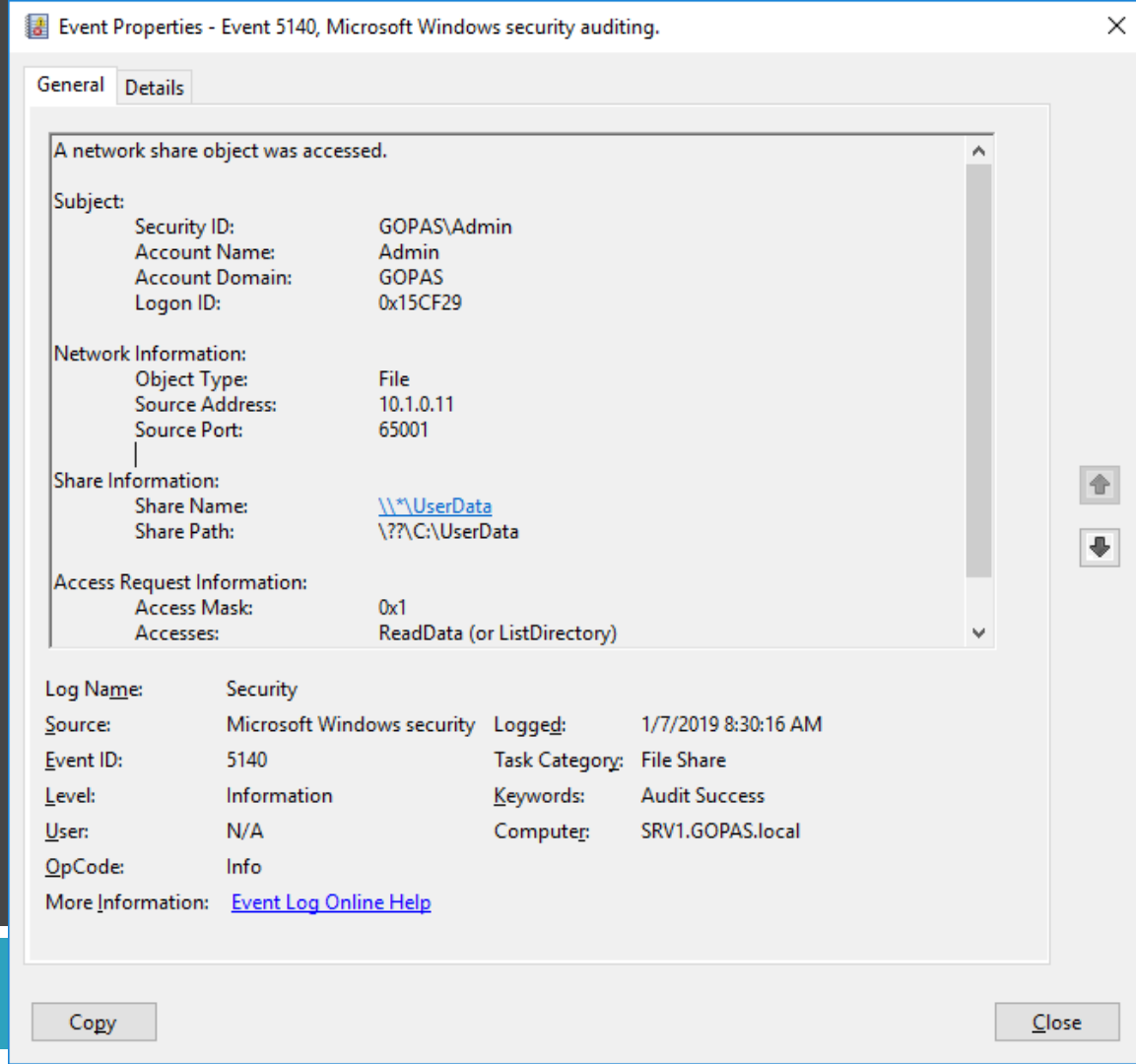
ID5142

- File Share
- Vytvoření sdíleného adresáře
- Audit Success



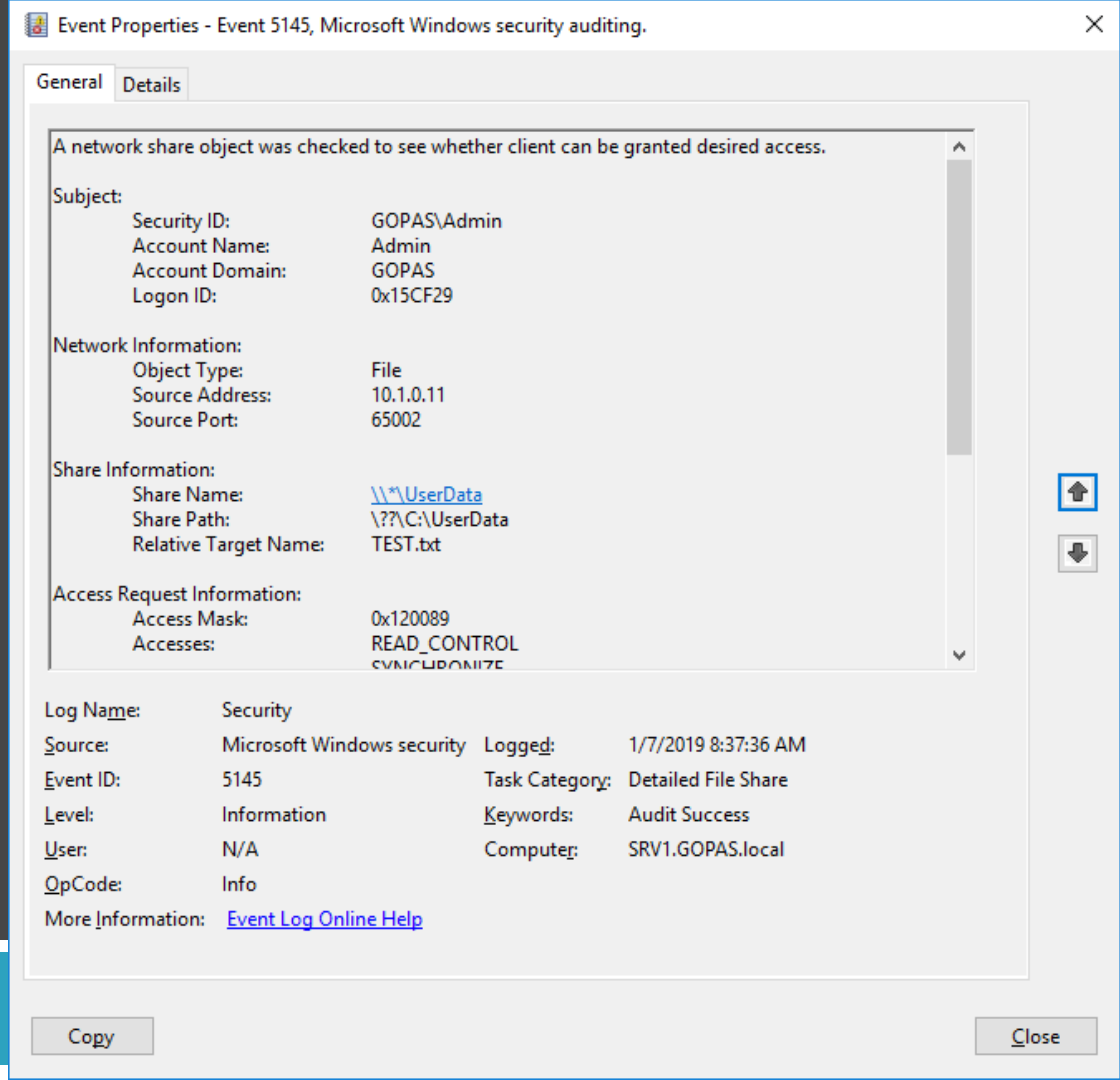
ID5140

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



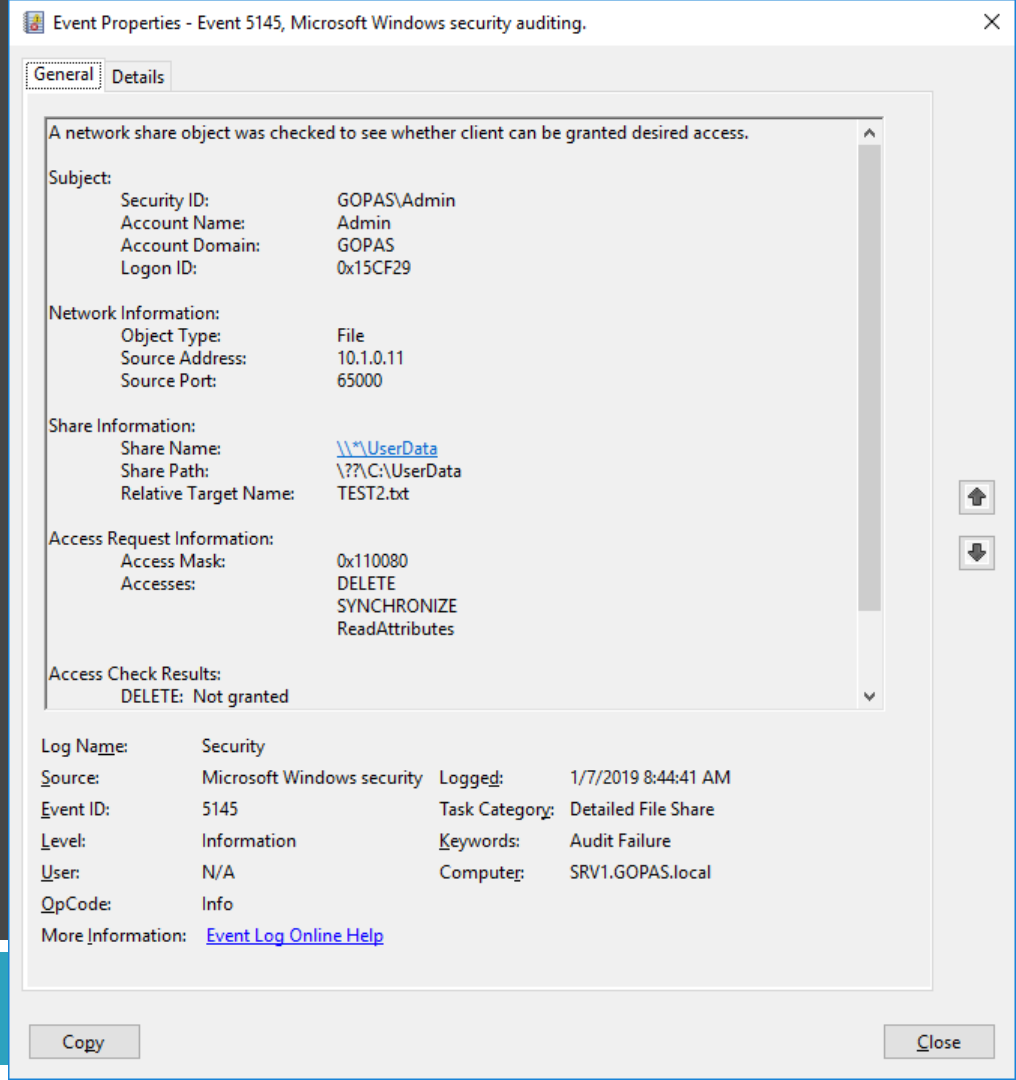
ID5145

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



ID5145

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



AUDIT FILE SYSTEM OBECNĚ

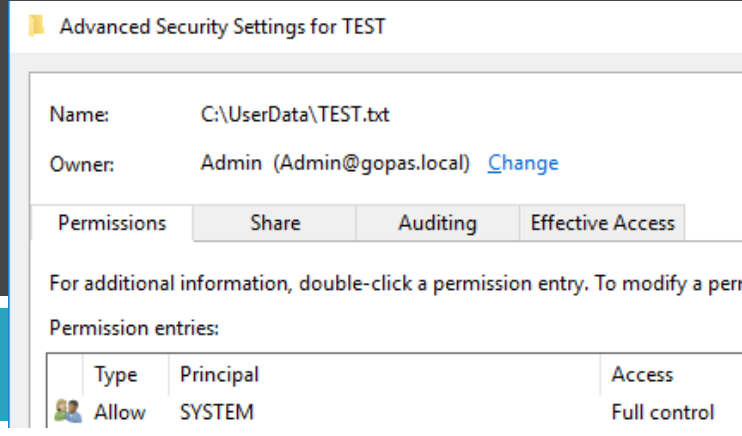
- Asi jedno z nejzajímavějších auditování vůbec (zdánlivě)
- Řeší odpovědi na klasické otázky jako:
  - Kdo a kdy smazal soubor?
  - Kdo a kdy změnil soubor?
  - Kdo otevírá nebo se snaží otevírat jaké soubory?
  - Atp.
- Podobně jako u auditování objektů v AD bude i u souborů a adresářů třeba konfigurovat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

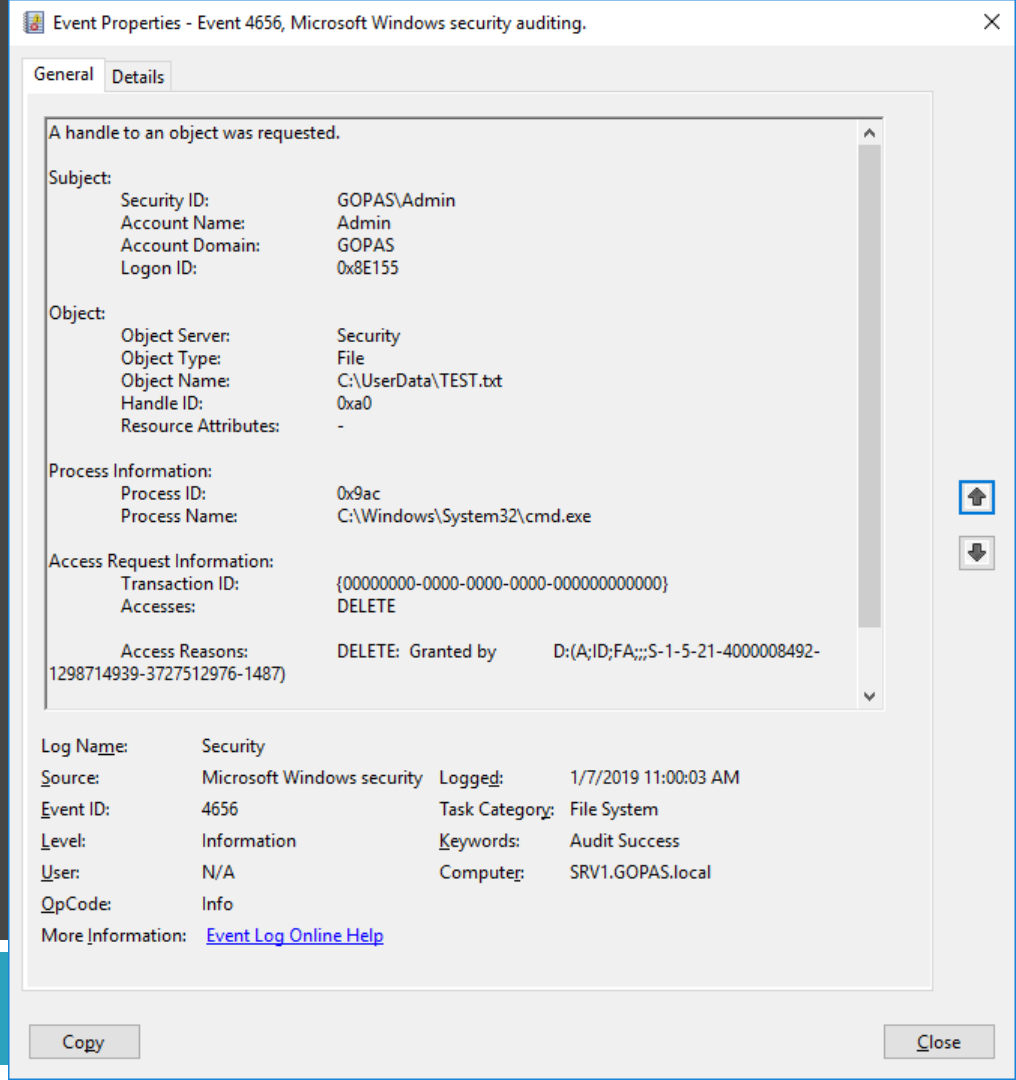
CO JE SACL?

- 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 konfigurují na rozšířeném dialogu oprávnění
- Jediný rozdíl mezi DACL a SACL je sloupec type:
  - DACL – Allow a Deny
  - SACL – Success, Fail, All



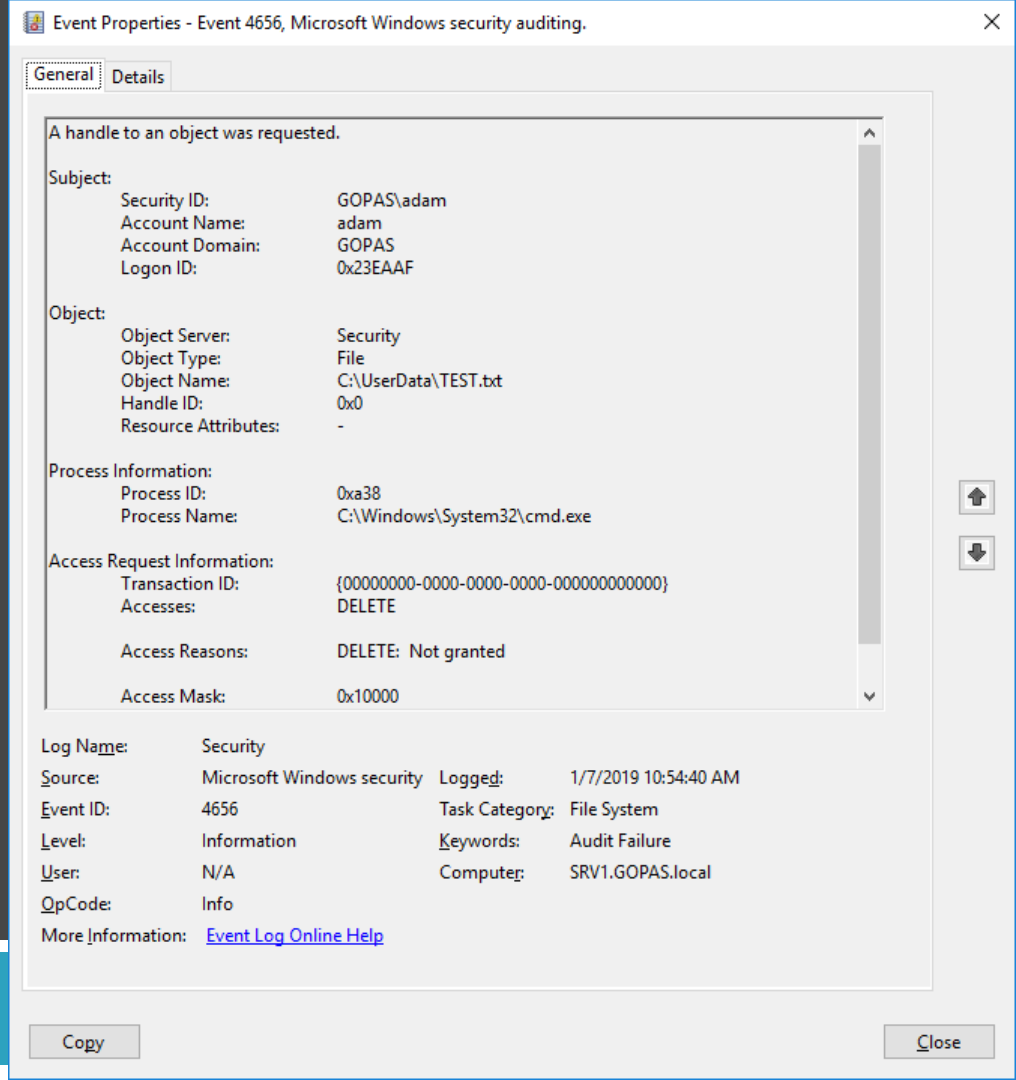
ID4656

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



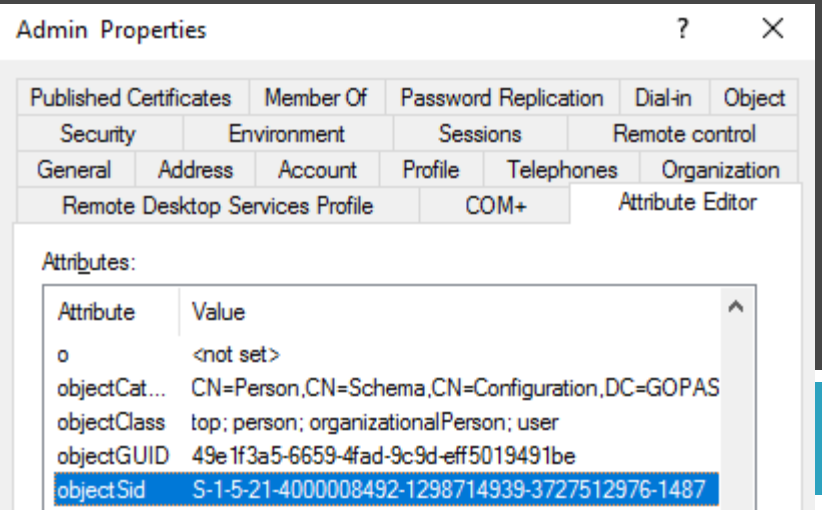
ID4656

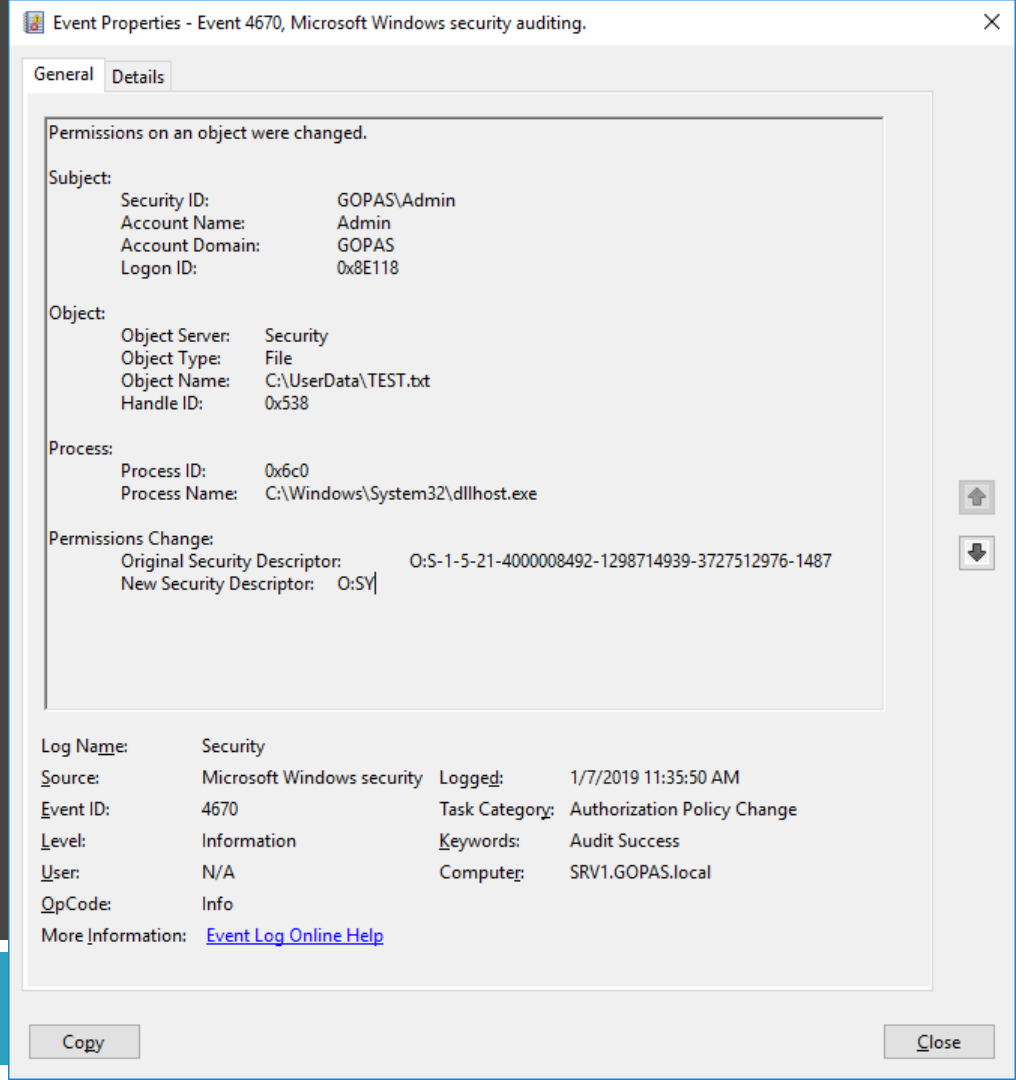
- Neúspěšné smazání souboru
- TEST.txt
- Cmd.exe
- GOPAS\Adam
- Audit Failure



ID4670

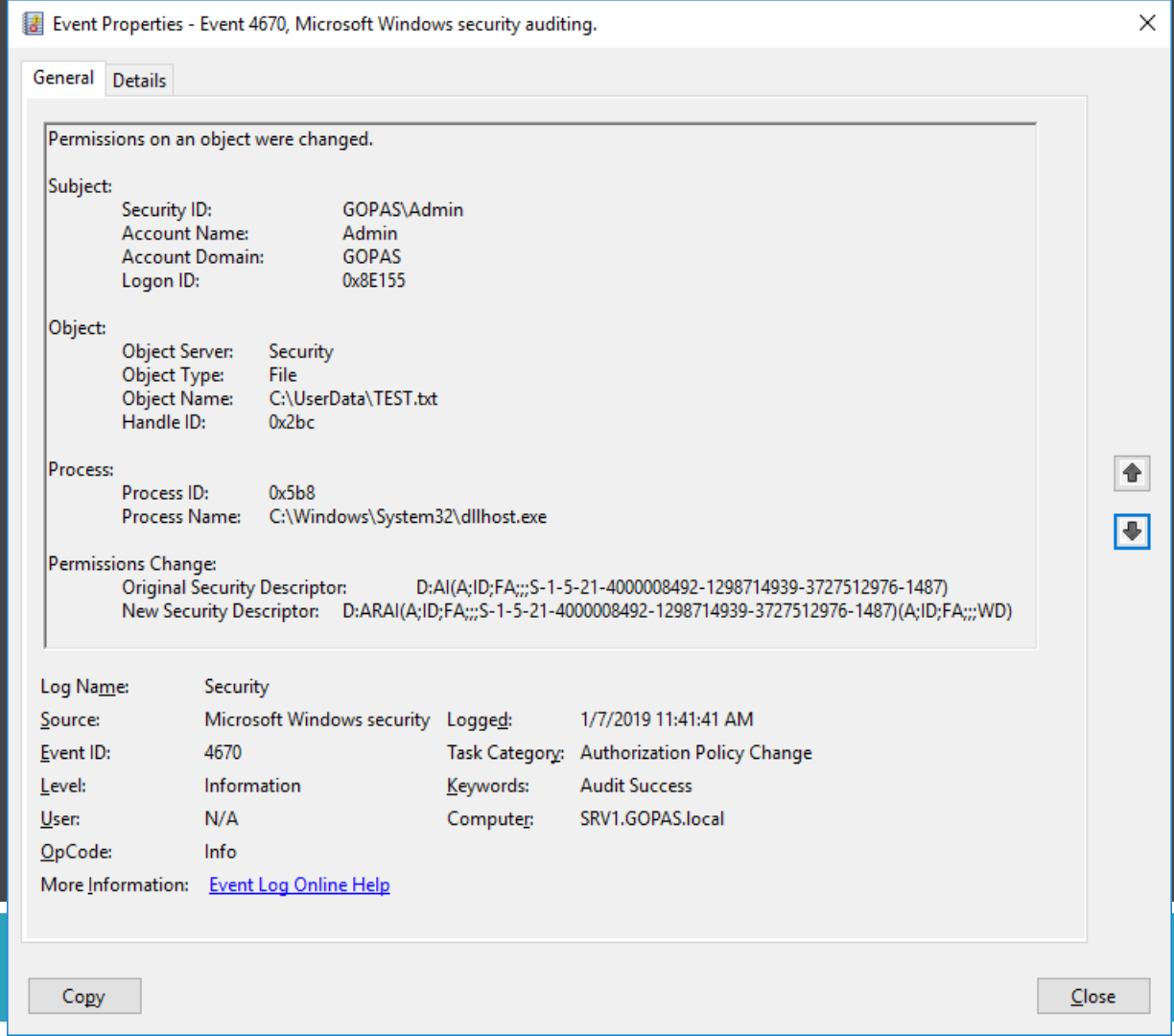
- Úspěšná změna vlastníka souboru
- TEST.txt
- GOPAS\Admin ⇒ SYSTEM
- Audit Success





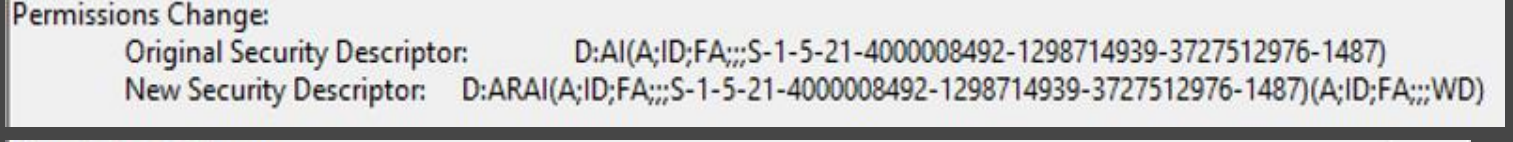
ID4670

- Úspěšná změna oprávnění
- TEST.txt
- Audit Success



SDDL

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



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

Generic access rights	
GA	GENERIC ALL
GR	GENERIC READ
GW	GENERIC WRITE
GX	GENERIC EXECUTE

File access rights	
FA	FILE ALL ACCESS
FR	FILE GENERIC READ
FW	FILE GENERIC WRITE
FX	FILE GENERIC EXECUTE

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

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.

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

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

```
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

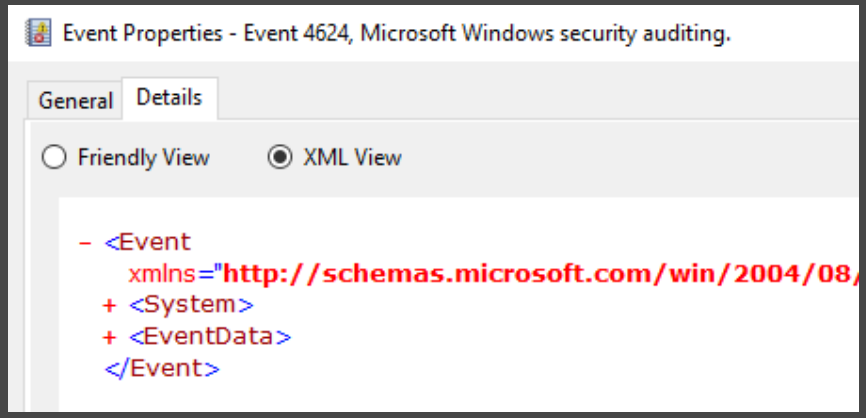
- Události v EventLogu vznikají lokálně na serverech – nutno sledovat lokálně
- Lze vyrobit subscripci, která shromažďuje logy na centrálním místě
- Lolekce logů může být:
  - Inicializovaná „sběračem“
  - Inicializovaná „sbíraným“
- Sbírat lze logy všechny nebo jen dle parametrického filtru
- Vytvoření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

EVENT SUBSCRIPTION – NASTAVENÍ

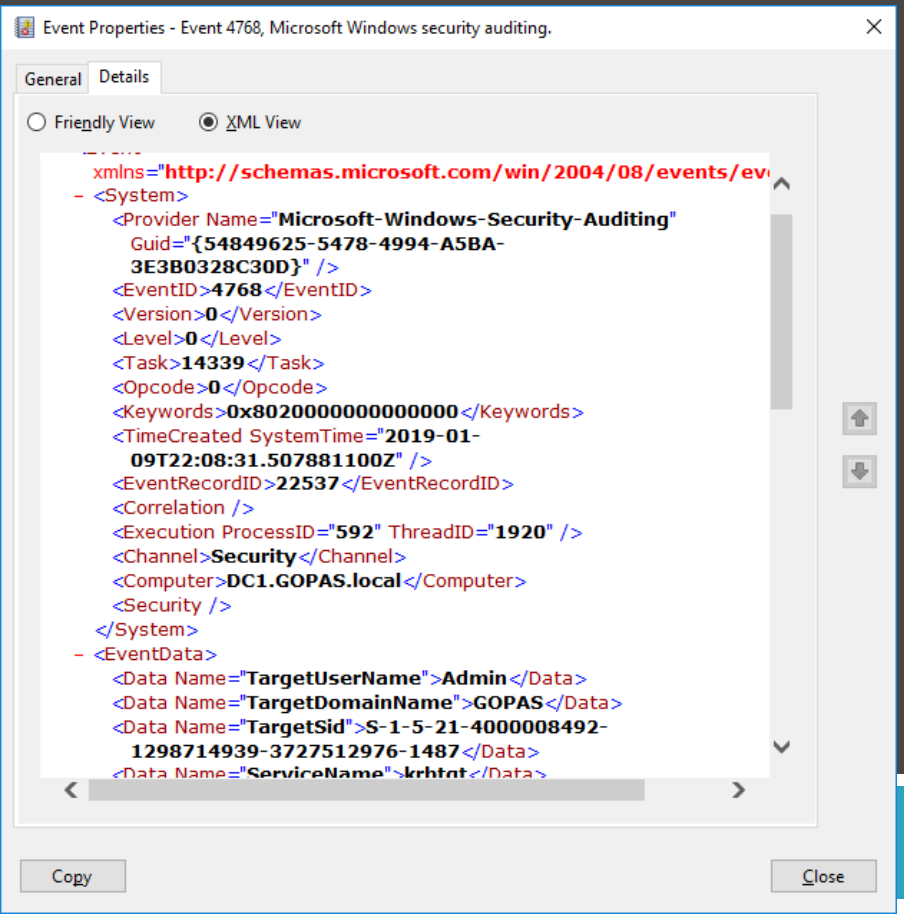
- Abyste mohli vzdáleně „vytahovat“ logy, musíte na to mít oprávnění
- Na běžné logy jako Application nebo System „stačí“ být lokálním Administrátorem
- Security EventLog je na nastavení trochu složitější
  - Viz chyba 0x138C
  - https://support.microsoft.com/en-us/help/4047777/security-event-log-forwarding-fails-with-error-0x138c-and-5004

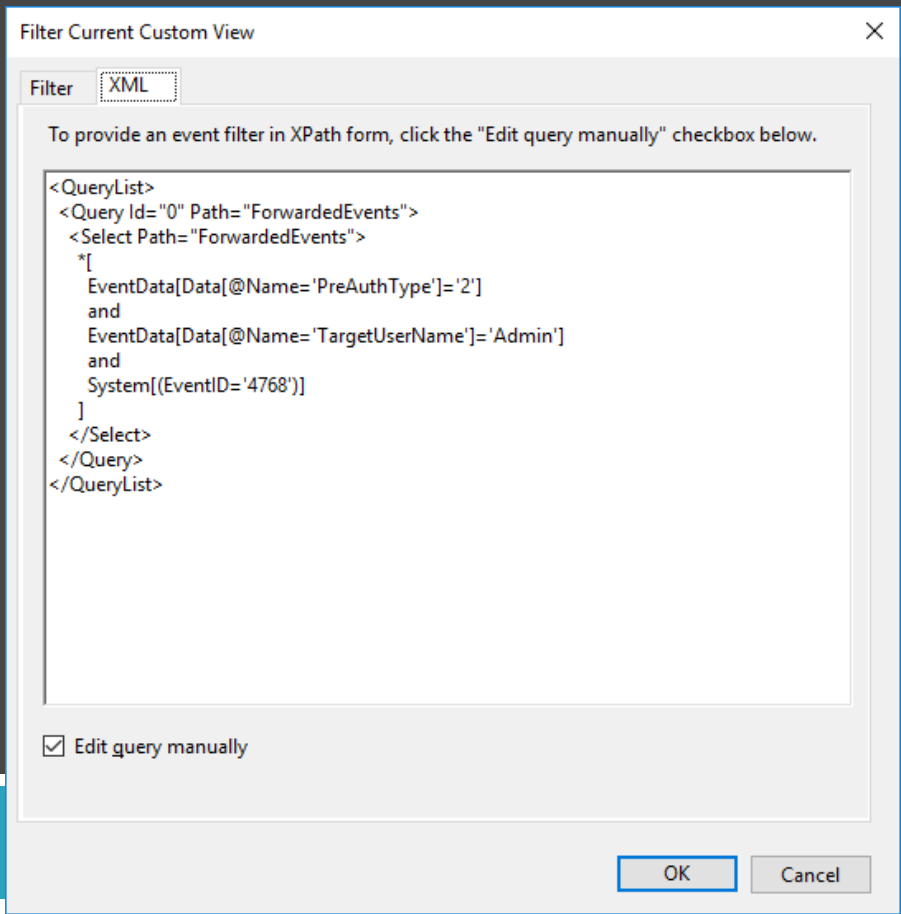
FILTROVÁNÍ

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



FILTROVÁNÍ EVENTLOGU POMOCÍ XML





POWERSHELL

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

SERVER INVEN...
IP ADDRESS SP...
IP Address Bl...
IP Address In...
IP Address R...
VIRTUALIZED I...
MONITOR AN...
DNS and DH...
DHCP Scopes
DNS Zones
Server Groups
EVENT CATALOG

IPAM Configurati...
DHCP Configurati...
IP Address Tracking
By IP Address
By Client ID
By Host Name
By User Name

By User Name

Filtered | 33 items returned

TASKS

Admin Search

and user logon events between these dates: 1/8/2019 1/10/2019

Time of Event	IP Address	Client ID	Host Name	User Name	User Domain Name	User Forest Name	Event Type	Source Server
1/9/2019 8:41:40 AM	10.1.0.51			Admin	GOPAS.LOCAL	GOPAS.local	DCAuthentication	DC1.GOPAS.local
1/9/2019 8:41:49 AM	10.1.0.52			Admin	GOPAS.LOCAL	GOPAS.local	DCAuthentication	DC1.GOPAS.local
1/9/2019 8:41:50 AM	10.1.0.52			Admin	GOPAS.LOCAL	GOPAS.local	DCAuthentication	DC1.GOPAS.local

Details View

10.1.0.51

Details

Description:
A Kerberos authentication ticket (TGT) was requested.

Time of Event: 1/9/2019 8:41:40 AM
IP Address: 10.1.0.51
Client ID:
Host Name:
User Forest Name: GOPAS.local

User Name: Admin
User Domain: GOPAS.LOCAL
Event Type: DCAuthentication
Source Server: DC1.GOPAS.local

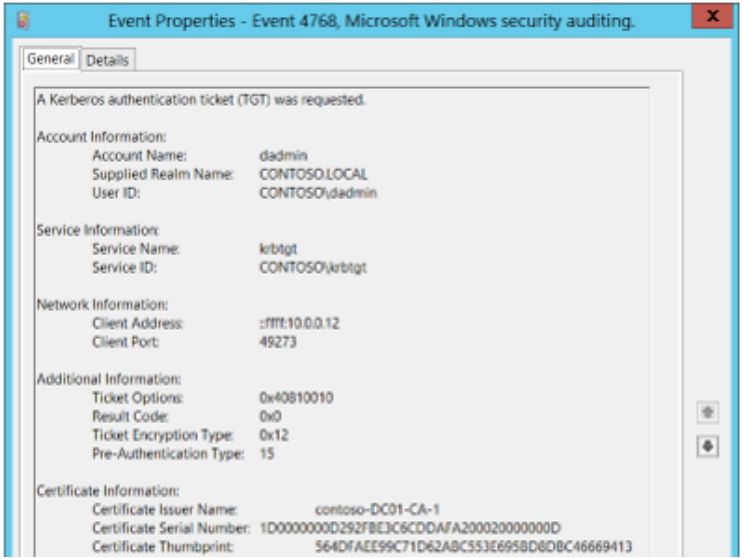
EVENTLOG REFERENCE GUIDE

- 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 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