Rekomendācijas auditēšanas iestatījumiem Windows domēna infrastruktūrā

(Materiāls paredzēts MS Windows domēnu administratoriem)

CERT.LV pastāvēšanas laikā esam novērojuši, ka situācijās, kad organizācijām / uzņēmumiem ir nācies saskarties ar reālu IT drošības incidentu, nereti pietrūkst informācijas to risināšanā.

Viens no pamatuzdevumiem, drošības incidentu risināšanā ir auditācijas pierakstu analīze. Diemžēl jāatdzīst, ka bieži vien iestādei / uzņēmumam ieraksti ir, bet tie ir nepilnīgi t.i. svarīgākās komponentes, kas varētu palīdzēt saprast, kad un kas ir noticis, un, kā tieši notikumi ir attīstījušies, netiek žurnalētas (jāpiemin, ka pēc noklusējuma Microsoft Windows daļu no ļoti kritiskām auditācijas komponentēm ir izslēdzis). Tāpēc CERT.LV ir izstrādājusi minimālās ieteicamās prasības auditācijas iestatījumiem – balstoties gan uz pašu pieredzi, risinot incidentus, gan ņemot vērā padomus no citu valstu CERTu kopienām, gan paša Microsoft rekomendācijām.

==========

Sagatavošanās un izpēte

! PĒC NOKLUSĒJUMA WINDOWS ŽURLNĀLFAILU IZMĒRI NEPĀRSNIEDZ 20MB. BRĪDĪ, KAD IR JĀVEIC INCIDENTA IZMEKLĒŠANA AR ŠO APJOMU NEPIETIEK, JO VĒSTURISKIE NOTIKUMI JAU IR PĀRRAKSTĪTI AR JAUNIEM, KĀ REZULTĀTĀ PILNVĒRTĪGI IZMEKLĒT INCIDENTU IR ĻOTI APGRŪTINOŠI VAI PAT NEIESPĒJAMI. IZŅĒMUMS IR GADĪJUMI, KAD ŽŪRNĀLFAILI TIEK PĀRSŪTĪTI UZ ATSEVIŠĶU SERVERI JEB AUDITĀCIJAS IERAKSTU KOLEKTORU/SIEM RISINĀJUMU, TAD VAR ATSTĀT ARĪ NOKLUSĒJUMA VĒRTĪBAS.

1.) Ieteicami sekojoši lokālo žurnālfailu izmēri (kā minimums):

Application – 256 MB

System – 256 MB

PowerShell – 1 GB

Security – 1 GB darbstacijās un 2 GB serveros

Sysmon – 1 GB (Sysmon jeb System Monitor ir Microsoft izstrādāts rīks, kas nodrošina lielāku redzamību par Windows iekārtā notikušajām darbībām nekā noklusētie Windows auditēšanas ieraksti. Stingri aicinām uzņēmumus un organizācijas ieviest šī rīka izmantošanu. Sysmon auditācijas pierakstus saglabā `Applications and Services Logs/Microsoft/Windows/Sysmon/Operational` jeb "SYSTEMDRIVE\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx")

Application, *System* un *Security* žurnālfailu izmērus var konfigurēt ar šādām grupu politikām:

Application

Group Policy Management Editor ---> Computer Configuration -> Policies -> Administrative Templates -> Windows Components-> Event Log Service-> Application -> Specify the maximum log file size (KB) - > Enabled

Options: Maximum Log Size (KB): **262144**

System

Group Policy Management Editor ---> Computer Configuration -> Policies -> Administrative Templates -> Windows Components-> Event Log Service-> System -> Specify the maximum log file size (KB) - > Enabled

Options: Maximum Log Size (KB): **262144**

Security

Group Policy Management Editor ---> Computer Configuration -> Policies -> Administrative Templates -> Windows Components-> Event Log Service-> Security -> Specify the maximum log file size (KB) - > Enabled

Options: Maximum Log Size (KB): **1048576** vai serveros **2097152**

P.s. Pārējiem žurnālfailiem nevar nomainīt izmēru ar standarta grupu politiku *templates*, to ir iespējams izdarīt, bet nepieciešams uzstādīt papildus *Adminsitrative Templates* vai izveidot jaunas Windows reģistra vērtības. Vēl kā variants var būt *bat* vai Powershell skripta palaišana pie sistēmas iestartēšanās vai ar plānoto uzdevumu, kas izmanto Windows iebūvēto komandu `wevtutil`.

Piemēram:

Komanda, kas definē, ka Powershell žurnālfaila maksimālais izmērs ir 1GB

```
wevtutil sl Microsoft-Windows-PowerShell/Operational /ms:1073741824
```

Komanda, kas definē, ka Sysmon žurnālfaila maksimālais izmērs ir 1GB

```
wevtutil sl Microsoft-Windows-Sysmon/Operational /ms:1073741824
```

2.) Windows žurnālfailu arhivēšana

Žurnālfailus nepieciešams arhivēt, ja vien tie netiek sūtīti uz iekārtu, kas tos uzglabā un apstrādā centralizēti. Kad iepriekš definētais žurnālfaila izmērs būs sasniegts, visi tajā reģistrētie ieraksti, sākot ar senākajiem, tiks pakāpeniski pārrakstīti ar jauniem, tā rezultātā, iespējams, svarīga informācija, kas var noderēt incidenta izmeklēšanā, tiks zaudēta. Lai no šādām situācijām izvairītos, ir iespējams veidot žurnālfaila arhīvu. Maksimālo izmēru sasniegušie faili tiks pārsaukti par Archive-[kanālanosakums]-[datums] un to dati nepazudīs. Tomēr jāņem vērā, ka šie arhīvi automātiski netiek dzēsti vai pārrakstīti, tāpēc jau laikus

nepieciešams padomāt par pietiekamu cietā diska ietilpību (tas varētu būt arī ārējs datu nesējs).
Arhivēšanu var konfigurēt ar grupu politiku palīdzību sekojoši (nepieciešams iespējot divas politikas un katram žurnālfailam atsevišķi):
Group Policy Management Editor -> Computer Configuration -> Policies -> Administrative Templates -> Windows Components-> Event Log Service-> Security -> Backup log automatically when full -> Enabled

Group Policy Management Editor -> Computer Configuration -> Policies -> Administrative Templates -> Windows Components-> Event Log Service-> Security -> **Control Event Log behavior when the log file reaches its maximum size -> Enabled**

Var izmantot arī komandrindas rīku `wevtutil`:

```
wevtutil sl Security /rt:true /ab:true
```

!! MINISTRU KABINETA NOTEIKUMI NR. 397 NOSAKA, KA SISTĒMAS AUDITĀCIJAS PIERAKSTU VEIDOŠANA UN UZGLABĀŠANA IR JĀNODROŠINA VISMAZ SEŠUS MĒNEŠUS PĒC IERAKSTA IZDARĪŠANAS, VAI, PAAUGSTINĀTAS DROŠĪBAS SISTĒMĀM 18 MĒNEŠUS PĒC IERAKSTA IZDARĪŠANAS.

3.) Pārliecināmies, ka domēnā ir iespējota politika, kas nepārrakstīs paplašinātās auditācijas pierakstu vērtības (vērtības ir norādītas dokumenta turpinājumā)**:**
Group Policy Management Editor ---> Computer Configuration -> Policies -> Windows Settings -> SecuritySettings -> Local Policies ->Security Options ->
" Audit:Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" -> **Enabled.**

Vairāk par šīs politikas nozīmi un kā to iespējot var lasīt šeit: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing#to-ensure-that-advanced-audit-policy-configuration-settings-are-not-overwritten

4.) Komandrindas notikumu auditēšana:
Group Policy Management Editor ---> Computer Configuration -> Policies -> Administrative Templates -> System->Audit Process Creation -> **Include command line in process creation events -> Enabled**

5.) PowerShell notikumu auditēšana:
Group Policy Editor ---> Computer Configuration -> Administrative Templates -> Windows Components- > Windows PowerShell -> **Turn on PowerShell Script Block Logging -> Enabled**

- Turn on Powershell Script Block Logging*

- Turn on Module Logging*
- Turn on Powershell Transcription – pēc noklusējuma dati glabāsies lietotāja “My Documents” mapē, bet ir iespējams norādīt pašu izvēlētu direktoriju. Šos datus ieteicams monitorēt centralizēti.

6.) Noderīgas utilītprogrammas (iebūvētas MS OS un kuras var palaist no komandrindas interpretatora jeb cmd.exe):

AUDITPOL.exe: Lietojam šo utilītprogrammu, lai pārskatītu pašreizējos žurnalēšanas uzstādījumus. Piemēram, lai apskatītu, kāds ir esošais stāvoklis visās audita kategorijās un to apakškategorijās:

```
AuditPol /get /category:*
```

REG.exe: Lietojam šo utilītprogrammu, lai veiktu dažādus vaicājumus reģistrā – šeit pieminētie reģistru ceļi ir labs sākums, lai saprastu, ko tieši monitorēt no reģistra (populāras vietas, kur „dzīvo” ļaunatūra).

Piemēram:

Izmaiņas AppInit_Dlls –

```
reg query "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit_Dlls
```

Izmaiņas Servisos –

```
reg query "HKLM\System\CurrentControlSet\Services"
```

Izmaiņas Machine Run atlēgā –

```
reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run”
```

Izmaiņas Machine RunOnce atslēgā –

```
reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce”
```

Izmaiņas User Run atslēgā -

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\Run”
```

Izmaiņas User RunOnce atslēgā –

```
reg query "HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce”
```

P.S. `Run` un `RunOnce` reģistra atslēgas – programma tiek palaista ikreiz, kad lietotājs piesakās sistēmā (log on)

SC.exe: Lietojam šo utilītprogrammu, lai pārskatītu servisus. Piemēram:

Atgriež visus servisus jebkurā stāvoklī –

```
sc.exe query state= all (Jāatceras par atstarpi aiz = zīmes)
```

Atgriež konkrētu servisu –

```
sc.exe query state= all | find /I "telnet"
```

Paplašinātā auditācijas konfigurācija Windows domēna kontrollerī

Group Policy Management Editor -> Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Audit Category	Audit Subcategory	Success	Failure
Account Logon	Credential Validation*	+	+
	Kerberos Authentication Service*	+	+
	Kerberos Service Ticket Operations*	+	+
	Other Account Logon Events	+	+
Account Management	Computer Account Management	+	
	Distribution Group Management	+	
	Other Account Management Events	+	
	Security Group Management	+	
	User Account Management	+	+
Detailed Tracking	DPAPI Activity	+	+
	PNP Activity	+	
	Process Creation (var aizvietot ar Sysmon**)	+	
DS Access	Directory Service Access*	+	+
	Directory Service Changes*	+	+
Logon/Logoff	Account Lockout	+	
	Group Membership	+	
	Logoff	+	
	Logon	+	+
	Other Logon/Logoff Events	+	+
	Special Logon	+	
Object Access	Audit Registry (var aizvietot ar Sysmon**) – vēlams monitored konkrētas reģistra atslēgas citādi būs grūti atrast vertigo info.	+	
	Audit Detailed File Share		+
	File Share*	+	+
	Audit Sam*	+	
	Audit Other Object Access Events	+	+
Policy Change	Audit Policy Change	+	
	Authentication Policy Change	+	
	Authorization Policy Change	+	
	MPSSVC Rule-Level Policy Change	+	
Privilege Use	Sensitive Privilege Use*	+	+
System	Other System Events	+	+
	Security State Change	+	
	Security System Extension	+	
	System Integrity	+	+

Paplašinātā auditācijas konfigurācija Windows serveriem

Group Policy Management Editor -> Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Audit Category	Audit Subcategory	Success	Failure
Account Logon	Credential Validation	+	+
	Other Account Logon Events	+	+
	Other Account Management Events	+	
	Security Group Management	+	
	User Account Management	+	+
Detailed Tracking	DPAPI Activity	+	+
	PNP Activity	+	
	Process Creation (var aizvietot ar Sysmon**)	+	
Logon/Logoff	Account Lockout	+	
	Group Membership	+	
	Logoff	+	
	Logon	+	+
	Other Logon/Logoff Events	+	+
	Special Logon	+	
Object Access	Audit Detailed File Share (failu serverī *)		+
	File Share (failu serverī*)	+	+
	Audit Other Object Access Events	+	+
	Audit Registry (var aizvietot ar Sysmon**) – vēlams monitored konkrētas reģistra atslēgas citādi būs grūti atrast vertigo info.	+	
	Audit Sam	+	
Policy Change	Authentication Policy Change	+	
	Audit Policy Change	+	
	MPSSVC Rule-Level Policy Change	+	
Privilege Use	Sensitive Privilege Use*	+	+
System	Security State Change	+	
	Other System Events	+	+
	Security System Extension	+	
	System Integrity	+	+

Paplašinātā auditācijas konfigurācija darbstacijām (Windows 7, Windows 8, Windows 10, Windows 11)

Group Policy Management Editor -> Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies

Audit Category	Audit Subcategory	Success	Failure
Account Logon	Credential Validation	+	+
	Other Account Logon Events	+	+
	Other Account Management Events	+	
	Security Group Management	+	
	User Account Management	+	+
Detailed Tracking	DPAPI Activity	+	+
	PNP Activity	+	
	Process Creation (var aizvietot ar Sysmon** un ir pat ieteicams, jo Sysmon reģistrē vairāk detaļu, piemēram, palaistā procesa HASH vērtību)	+	
Logon/Logoff	Account Lockout	+	
	Group Membership	+	
	Logoff	+	
	Logon	+	+
	Other Logon/Logoff Events	+	+
	Special Logon	+	
Object Access	Audit Detailed File Share		+
	File Share	+	+
	Audit Other Object Access Events	+	+
	Audit Registry (var aizvietot ar Sysmon**) – vēlams monitored konkrētas reģistra atslēgas citādi būs grūti atrast vertīgo info.	+	
	Audit Sam	+	
Policy Change	Audit Policy Change	+	

	Authentication Policy Change	+	
	MPSSVC Rule-Level Policy Change	+	
Privilege Use	Sensitive Privilege Use*	+	+
System	Other System Events	+	+
	Security State Change	+	
	Security System Extension	+	
	System Integrity	+	+

* izveidos apjomīgu ierakstu skaitu

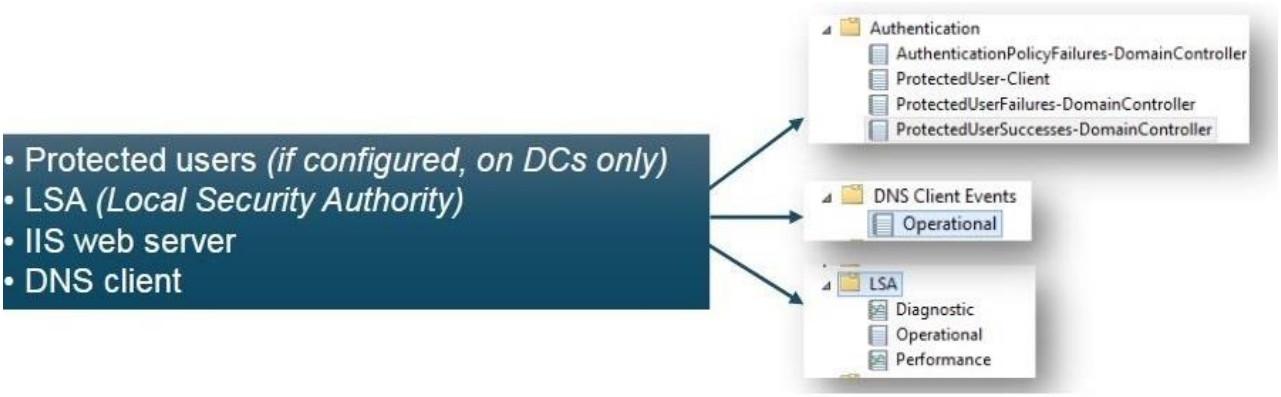
** https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

Sysmon iesakām izmantot kopā ar šo konfigurācijas failu, kas būs kā labs sākums, bet laika gaitā to noteikti var papildināt pēc konkrētās organizācijas vajadzībām - https://github.com/SwiftOnSecurity/sysmon-config

!!! JĀUZSVER, KA KATRA INFRASTRUKTŪRA IR INDIVIDUĀLA UN NOTEIKTI, JA NE PĒC KATRAS APAKŠKATEGORIJAS IESLĒGŠANAS, TAD VISMAZ TĀS KURAS IR ATZĪMĒTAS AR *, IR RŪPĪGI JĀIZVĒRTĒ ĢENERĒTAIS IERAKSTU APJOMS UN PIEEJAMIE RESURSI – ŠEIT VAR NĀKT TALKĀ SYSMON AR KONFIGURĀCIJAS FAILU, KURĀ VAR PIEVIENOT DAŽĀDUS IZŅĒMUMUS, LAI APJOMU SAMAZINĀTU.

Noderīgas piezīmes:

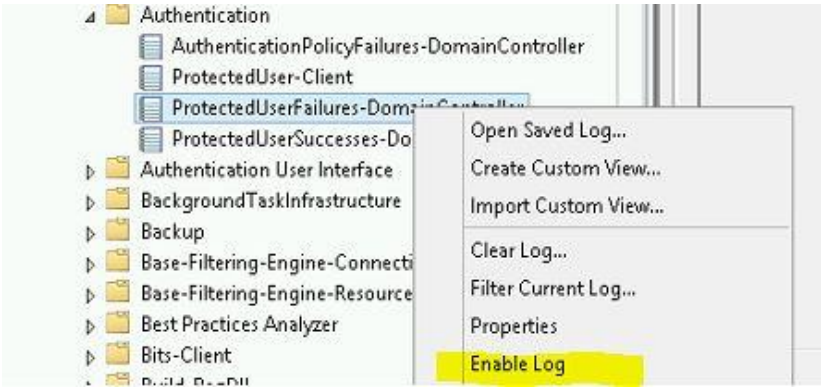
1.) Pēc noklusējuma daži no žurnālfailiem neuzrāda nekādus notikumus, jo tie ir izslēgti. Svarīgākie no tiem ir uzskaitīti zemāk redzamajā attēlā.



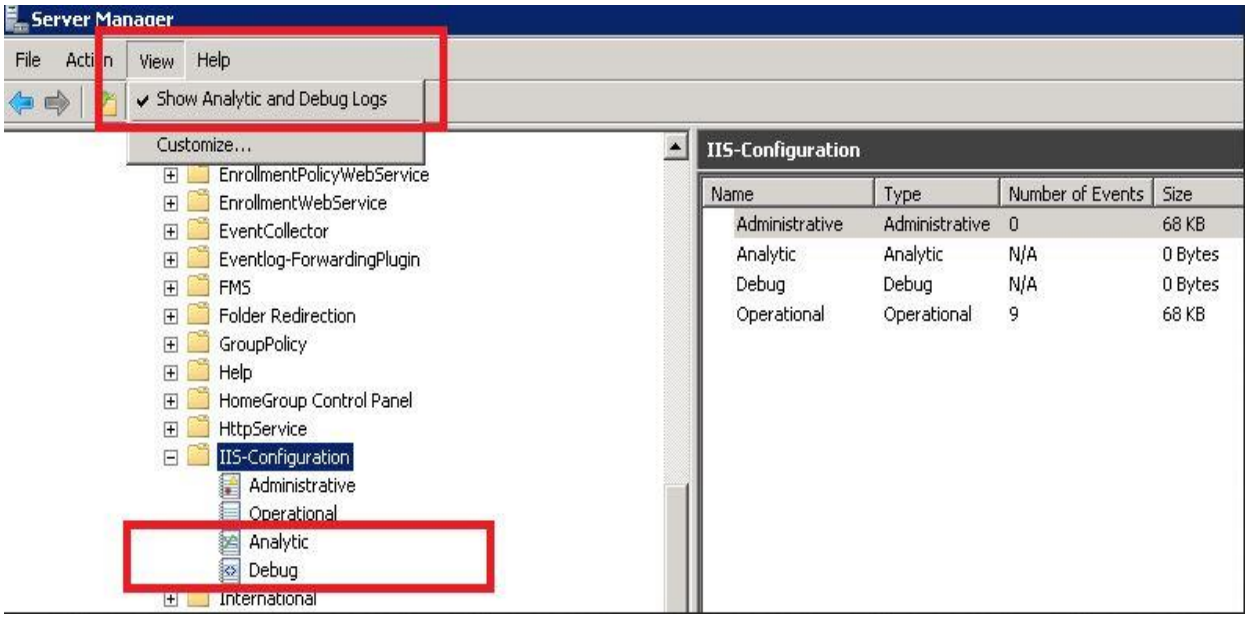
Lai notikumu reģistrēšanu iespējotu, var izmantot komandrindas rīku `wevtutil`:

```
wevtutil sl Microsoft-Windows-LSA/Operational /e:true
```

Tomēr, ja ērtāk ir izmantot Windows OS grafisko interfeisu, tad ir jāatver Event Viewer un ar labo peles klikšķi uz izvēlētās apakškategorijas ir jāuzspiež „Enable Log".



Reizēm noderīga informācija ir pieejama Analytic, Debug vai Trace ierakstos, bet, lai tie būtu pieejami, tos ir speciāli jāatzīmē pie Event Viewer vai Server Manager ar View-> „**Show Analytic and Debug Logs**" opciju: Tāpat tagad redzamās sadaļām ir vēl papildus jāiespējo (iepriekš aprakstīts kā Enable Log). Pēc noklusējuma Analytic, Debug un Trace notikumi ir paslēpti un izslēgti.



2.) Ieslēgt MS Windows DNS servera *debug logging*. Šie auditācijas pieraksti var būtiski palīdzēt noskaidrot, no kuras domēna iekārtas ir noticis konkrēts DNS pieprasījums un, tas ir svarīgi, jo CERT.LV

regulāri izsūta brīdinājumus par kiberdrošības apdraudējumiem un šis brīdinājums var būt par jūsu organizācijas/uzņēmuma IP adresi, kā rezultāta ir jānoskaidro gala iekārta, kura, iespējams, ir inficēta ar datorvīrusu. Jāpiezīmē, ka šo ierakstu ieslēgšana var būtiski ietekmēt servera resursu noslodzi un aizņemt papildu atmiņu, tāpēc par šo jau iepriekš ir jāpadomā un jāpārbauda ietekme uz serveri.

3.) Citi noderīgi Windows auditācijas pieraksti. Ieteicamais apjoms vismaz **128MB**, bet, ja resursi atļauj, tad noteikti var saglabāt lielākā apjomā:

```
Microsoft-Windows-Windows Defender/Operational
Microsoft-Windows-Bits-Client/Operational
Microsoft-Windows-Windows Firewall With Advanced Security/Firewall
Microsoft-Windows-NTLM/Operational
Microsoft-Windows-Security-Mitigations/KernelMode
Microsoft-Windows-Security-Mitigations/UserMode
Microsoft-Windows-PrintService/Admin
Microsoft-Windows-PrintService/Operational (pēc noklusējuma izslēgts)
Microsoft-Windows-Security-Mitigations/UserMode (pēc noklusējuma izslēgts)
Microsoft-Windows-PrintService/Operational
Microsoft-Windows-SmbClient/Security
Microsoft-Windows-AppLocker/MSI and Script
Microsoft-Windows-AppLocker/EXE and DLL
Microsoft-Windows-AppLocker/Packaged app-Deployment
Microsoft-Windows-AppLocker/Packaged app-Execution
Microsoft-Windows-CodeIntegrity/Operational
Microsoft-Windows-Diagnosis-Scripted/Operational
Microsoft-Windows-DriverFrameworks-UserMode/Operational
Microsoft-Windows-WMI-Activity/Operational
Microsoft-Windows-TerminalServices-LocalSessionManager/Operational
Microsoft-Windows-TaskScheduler/Operational (pēc noklusējuma izslēgts)
```

Neskaidrību gadījumā papildu informācija pieejama šeit:

1. **Detalizētāk par paplašinātās auditācijas iestatījumiem, to nozīmi** - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings
2. **Jautājumi un atbildes par paplašināto auditācijas konfigurāciju** - https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq
3. **Utilītprogramma Wevtutil.exe** - https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil
4. **Utilītprogramma Auditpol.exe** - https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/auditpol
5. **Utilītprogramma Reg .exe** - https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/reg
6. **Utilītprogramma Sc.exe** - https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/cc754599(v=ws.11)
7. **Komandrindas notikumu auditēšana** - https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/command-line-process-auditing
8. **PowerShell notikumu auditēšana** - https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
9. **Informācija par to, kā veidot atsevišķu serveri (kolektoru) auditācijas ierakstu uzglabāšanai ar Windows iebūvēto funkcionalitāti Event Forwarding:** https://docs.microsoft.com/en-au/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection