jamk

Labra 2

Ryhmä 3

Antti Tammelin

Tero Räsänen

Elmeri Söderholm

Eliel Taskinen

Raportti
Lokakuu 2022
Tieto-ja viestintätekniikan tutkinto-ohjelma
Koventaminen TTC6050-3001
12.10.2022

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Labra 2 on osa Koventaminen-kurssia. Labrassa tutustutaan Windows 11:n koventamiseen. Kovennuksia tehdään Group Policy Objecteille (GPO) Active Directory (AD)-ympäristössä. Group Policyn avulla voidaan hallita keskitetysti käyttöjärjestelmiä, sovelluksia sekä käyttäjiä. Koventamista voidaan tehdä joko manuaalisesti tai erilaisilla sitä varten tehdyillä ohjelmilla, kuten Windows 11 Security Baselinen avulla. Koventamista voidaan tehdä koko domainin laajuudella tai paikallisesti tietokonekohtaisesti.

1.1 Tehtävänanto

Labrassa piti koventaa Windows 11 workstation. Labran ajaksi ryhmä sai itse päättää mitä kovennusohjetta käyttää. Lisäksi ryhmä sai valita tavan, jolla vertailee labran alku- ja lopputilannetta. Ryhmän valitsemalla ohjeella piti tehdä GPO-kovennukset ja muut ohjeen kehottamat kovennukset. Security Compliance Toolkittiä käytettäessä piti tehdä ainakin yksi lisäkovennus manuaalisesti. Jos kovennukset tehtiin automaattisesti, tuli ryhmän esimerkin omaisesti näyttää muutaman kovennuksen kohdalla, miten sama olisi tehty manuaalisesti. Tässä labrassa tehtävät muutosten tuli olla konekohtaisia, eikä domain kohtaisia (Lab 4 ohjeet. N.d.).

1.2 Labrassa käytetyn ympäristön kuvaus

Labrassa käytetään Windows 11 järjestelmällä varustettua konetta VLE-ympäristössä, eli WS01 WS-Netissä. GPO-kovennukset tehdään Windows 11 koneen Active Directoryssa, eli Servers-Netin DC01 koneella. Muita osia Labraympäristöstä emme käyttäneet. Liitteenä raportissa löytyy kuva labraympäristöstä (ks. liite 1).

2 Teoria

2.1 Windows 11

Windows 11 on Microsoftin uusin käyttöjärjestelmä. Windows 10:n julkaisun yhteydessä Microsoft kertoi luopuvansa Windowsin uusista järjestelmänumeroista, mutta tähän tuli muutos. Windows

11 uudet ominaisuudet on suurilta osin otettu aikaisemmin työn alla olleelta, mutta sittemmin peruutetulta Windows 10X-käyttöjärjestelmästä. Windows 11 on suunniteltu Windows 10 päälle, kun taas 10X olisi ollut suurimmilta osin kokonaan uusi järjestelmä (Petteri Pyyny. 2021.).

2.2 Microsoft Security Baselines

Eri organisaatioilla, esimerkiksi verkkokaupalla tai sairaalalla, ja tuotteilla on erilaisia turvallisuus uhkia. Sen takia eri tuotteille ja organisaatioilla on omat Security Baselinet. Microsoftin Security baselineen on koottu tietoturva-asetuksia samaan ryhmään eri tarpeita varten. Näin on helpompi valita tietyt asetukset käyttöön yli 3000 group policyn joukosta. Security baselinet on koottu Microsoftin työntekijöiden, partnerien ja asiakkaiden palautteen perusteella ja ne voi ladata Security Compliance Toolkitin kautta (Security baselines. 2022).

2.2.1 Windows 11, version 22H2 Security baseline

Microsofin uusin security baseline Windows 11 käyttöjärjestelmälle.

Windowsin Security Baselineja on monia eri versioita, Windows Server 2012 versiosta Windows 11 versioon. Tämä johtuu siitä, että eri versioilla on eri vaatimuksia, ja uudemmilla käyttöjärjestelmillä on featureita, mitä vanhemmilla ei ole. Jos uusia featureita pitää koventaa tai tarvittavat asennukset ovat eri paikassa, ei vanhan Security Baselinen käyttäminen toimi. Käytimme tässä Windows 11, version 22H2 Security Baselinea, koska labran aikana kovensimme Windows 11 konetta, ja tämä oli uusin kaikista Baselineista (Munck R. 2022).

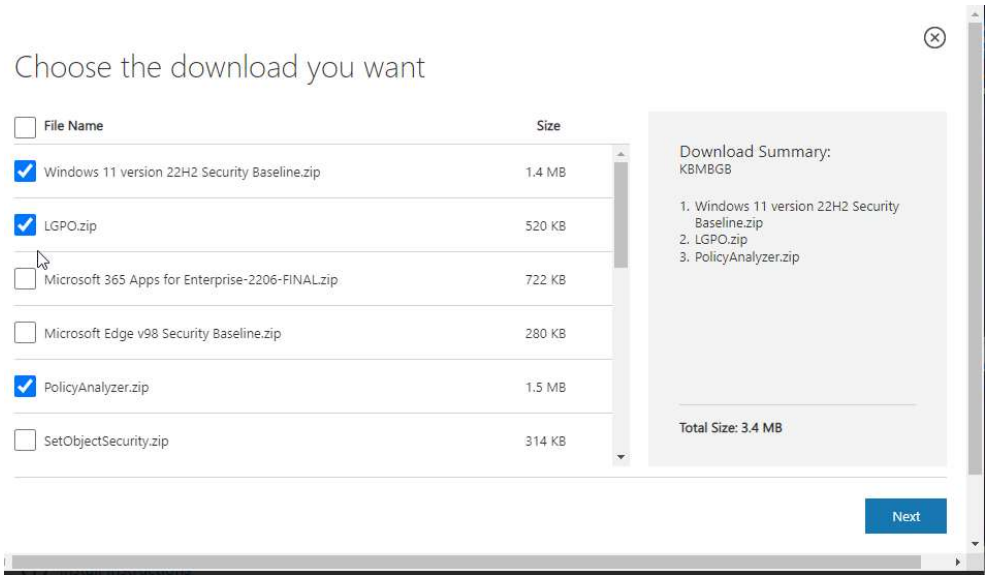
2.3 Windows Active Directory

Windows Active Directory on domainin käyttäjätietokanta sekä hakemistopalvelu. Domain tarkoittaa verkkoa, jota hallitaan keskitetysti. Active Directoryn avulla tämän verkon hallinta on helpompaa, koska voidaan yhdellä komennolla/muutoksella vaikuttaa koko verkon käyttäjiin ja laitteisiin. Admin-rooleja domainissa voi olla myöskin eri tasoja, esimerkiksi domain admin sekä local admin. Domain adminilla on oikeudet tehdä muutoksia koko verkkoon, kun taas local adminin oikeudet koskevat vain tiettyä tietokonetta (Active Directory Domain Services Overview. 2022).

Domainin käyttäjätilien hallinta on tärkeää siksi, koska hyökkääjät voivat yrittää esimerkiksi yksinkertaisia salasanoja tai vanhaa poistamatonta käyttäjätiliä kirjautuakseen domainiin. Siksi käyttäjätilit täytyisi pitää ajan tasalla sekä asettaa salasanoille tietty vaatimus, koska liian yksinkertainen salasana on helppo arvata (esim. admin123). Pääkäyttäjän oikeuksia ei saisi myöskään jaella ylimääräisille henkilöille (Active Directory Domain Services Overview. 2022).

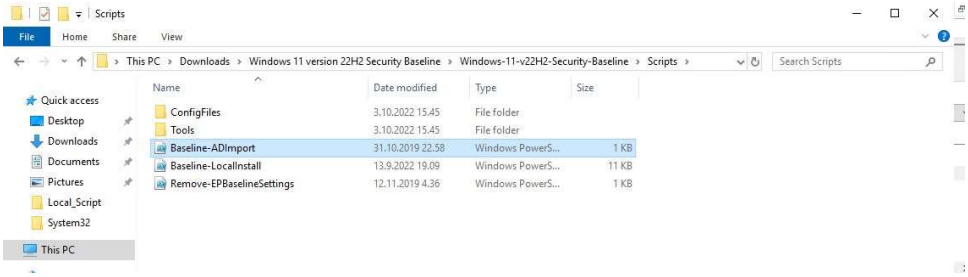
3 Windows 11 Security Baseline kovennus

Aloitimme Windows 11 koventamisen lataamalla `**Microsoft Security Compliance Toolkit 1.0**` tarvittavat tiedostot. Toolkitistä löytyy monia tiedostoja, mutta tähän labraan tarpeelliset olivat `**Policy Analyzerin**`, `**LGPO:n**`, ja labran aikana käytettyä Security Baselinea `**Windows 11 version 22H2 Security Baseline**`. Policy Analyzerin avulla pystyy vertailemaan Baseline asetuksia tällä hetkellä käytössä oleviin asetuksiin, LGPO eli Local Group Policy Object on työkalu, millä pystyy automatisoida policyjen muuttamisen, ja Security Baseline on kaikki muutokset ja Group Policyt, mitä jollekin koneelle pitää tehdä, jotta se olisi Security Baselinejen mukainen. Kaikista näistä löytyy .zip tiedostot Microsoftin sivuilta (ks. kuvio 1) (Microsoft Security Compliance Toolkit 1.0. N.d.).



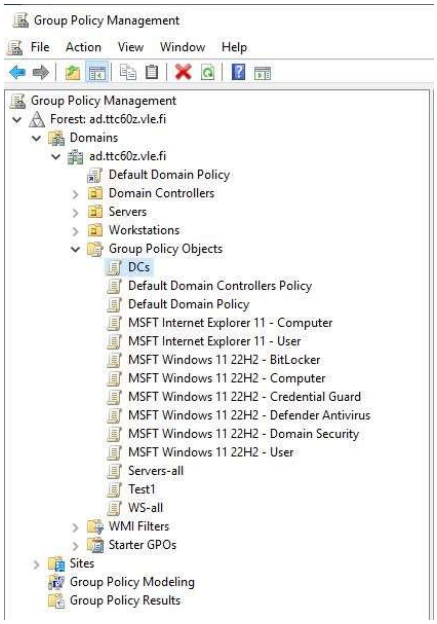
Kuvio 1. Microsoft Security Compliance Toolkit 1.0 Download.

Lataamisen jälkeen asennettiin Windows 11 Security Baseline Active Directoryyn (AD), missä Policy Analyzer ja LGPO oli jo asennettuna. Nämä asennettiin AD:hen sen takia, että pystyisimme kaikille workstationille päivittämään Security Baselinen mukaiset konfiguraatiot, eikä meidän tarvitsisi tehdä niitä yksi kerrallaan. AD:n sisällä piti ajaa `**ADImport**` skripti, joka asensi Group ja Security Policyt Active Directoryyn. ADImport skripti löytyy ladatusta Windows 11 Security Baseline kansiosta `**Scripts**` kansion alta (ks. kuvio 2).

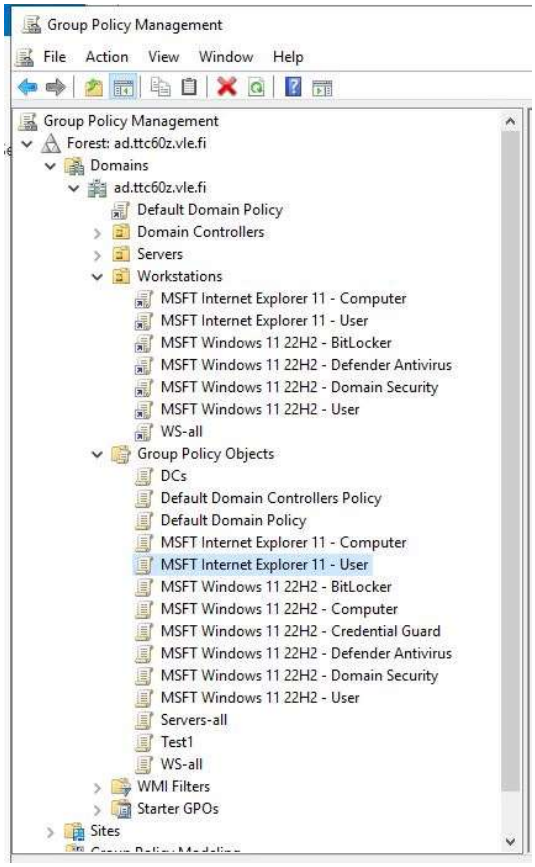


Kuvio 2. Windows security baseline asennusskripti.

Skriptin ADImport ajamisen jälkeen DC01:ssä Group Policyt asentuvat automaattisesti AD:hen. Tämän voi todentaa, kun menee `**Server Manager**` olevassa `**Tools**` kohdasta `**Group Policy Management**` kohtaan. Group Policy Managementista pitäisi löytyä `**Group Policy Objects**` kansiosta juuri asennetut Policyt, ja kun Policyt siirtää `**Workstations**` kansioon, ne vaikuttavat jokaiseen workstationiksi määritellyksi laitteessa (ks. kuvio 3 ja 4).

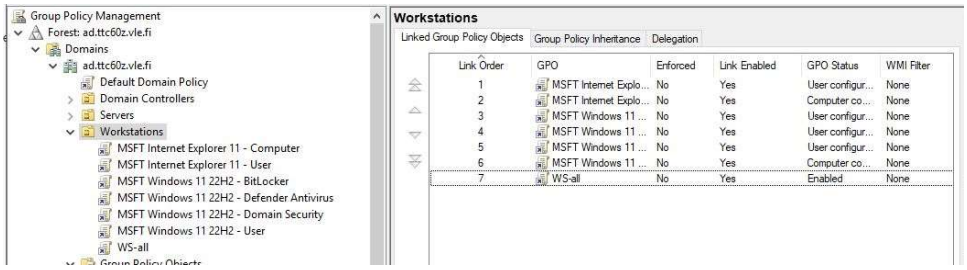


Kuvio 3. Ladatut Windows 11 security baselinet.



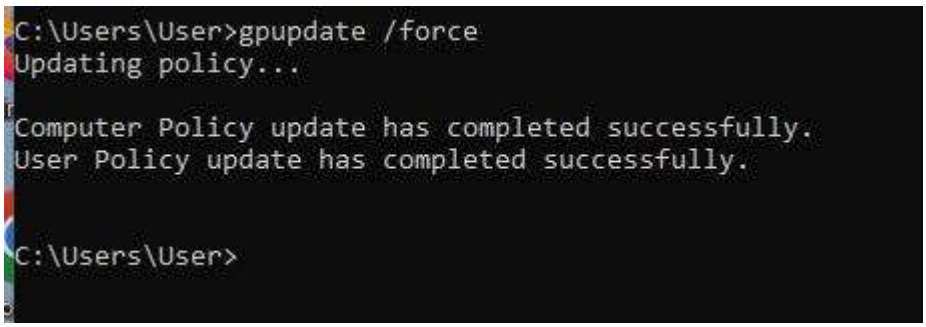
Kuvio 4. Siirretty Workstations kansioon.

Workstationin Link Orderia eli ns. tärkeysjärjestystä pitää muuttaa ennen kuin policyt tulevat voimaan. Kun klikkaa Group Policy Managementissa Workstations kohdalta, aukeaa workstationsin asetukset. Sieltä `**Linked Group Policy Objects**` alta pystyy vaikuttamaan Link Orderiin. Policy nimeltä `**WS-all**` pitää siirtää Link Order listan alimmaksi (ks. kuvio 5).



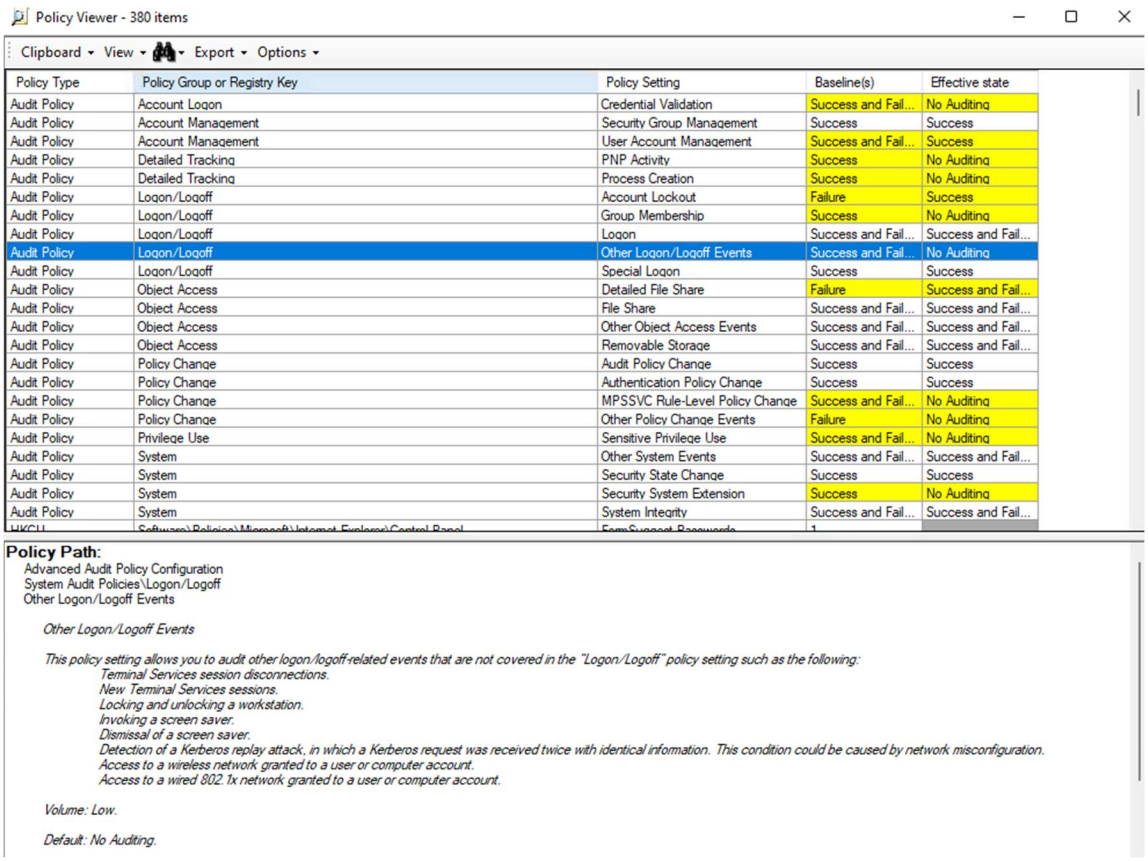
Kuvio 5. Muutettu policyjen Link Order järjestystä.

Kun Workstationsin policyt on konfiguroitu AD:n puolella oikein, pitää ajaa workstationsin puolella, eli WS01:ssä, gpupdate. Sen pystyy ajamaan menemällä WS01 sisälle, painamalla `**WIN+R**`, kirjoittamalla `**cmd**`, ja painamalla Enter. kun terminaali on auki, kirjoittamalla `**gpupdate /force**` pakottaa päivittämään Workstationin Group Policyt (ks. kuvio 6).



Kuvio 6. WS01 gpupdate.

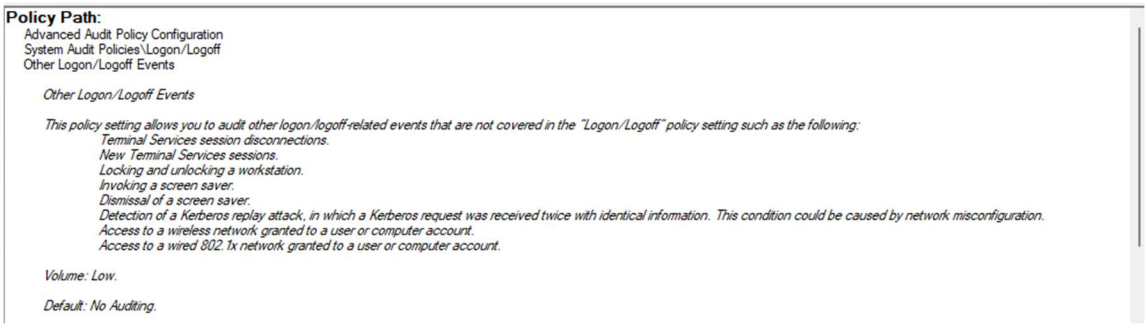
Policy Analyzerissa näkyy nyt muuttuneet policyt, ja miten niiden päivittäminen vaikutti. Vaikka baseline muutti monia sääntöjä Security Baselinen mukaiseksi, näkyy Policy Analyzerista, miten se ei todellakaan korjannut kaikkia konflikteja (ks. kuvio 7).



Kuvio 7. Policy Analyzer puuttuvia konflikteja

4 Policy Analyzerin konfliktien manuaalinen kovennus

Koska suoritimme suurimman osan labrasta automaattisesti, demonstroimme muutamalla Policy Analyzeriin jääneestä konfliktista, miten ne pystyy koventamaan manuaalisesti Security Baselinen mukaiseksi käyttämällä Group Policy Managementtia, ja siihen liittyviä editoreita. Kun näitä alkaa etsimään manuaalisesti, kannattaa käyttää hyväksi Policy Analyzerissa olevaa `**Policy Path**` informaatiota, mikä kertoo missä policy sijaitsee, niin navigointi on helpompaa (ks. kuvio 8).



Policy Path:
Advanced Audit Policy Configuration
System Audit Policies\Logon/Logoff
Other Logon/Logoff Events

Other Logon/Logoff Events

This policy setting allows you to audit other logon/logoff-related events that are not covered in the "Logon/Logoff" policy setting such as the following:
Terminal Services session disconnections.
New Terminal Services sessions.
Locking and unlocking a workstation.
Invoking a screen saver.
Dismissal of a screen saver.
Detection of a Kerberos replay attack, in which a Kerberos request was received twice with identical information. This condition could be caused by network misconfiguration.
Access to a wireless network granted to a user or computer account.
Access to a wired 802.1x network granted to a user or computer account.

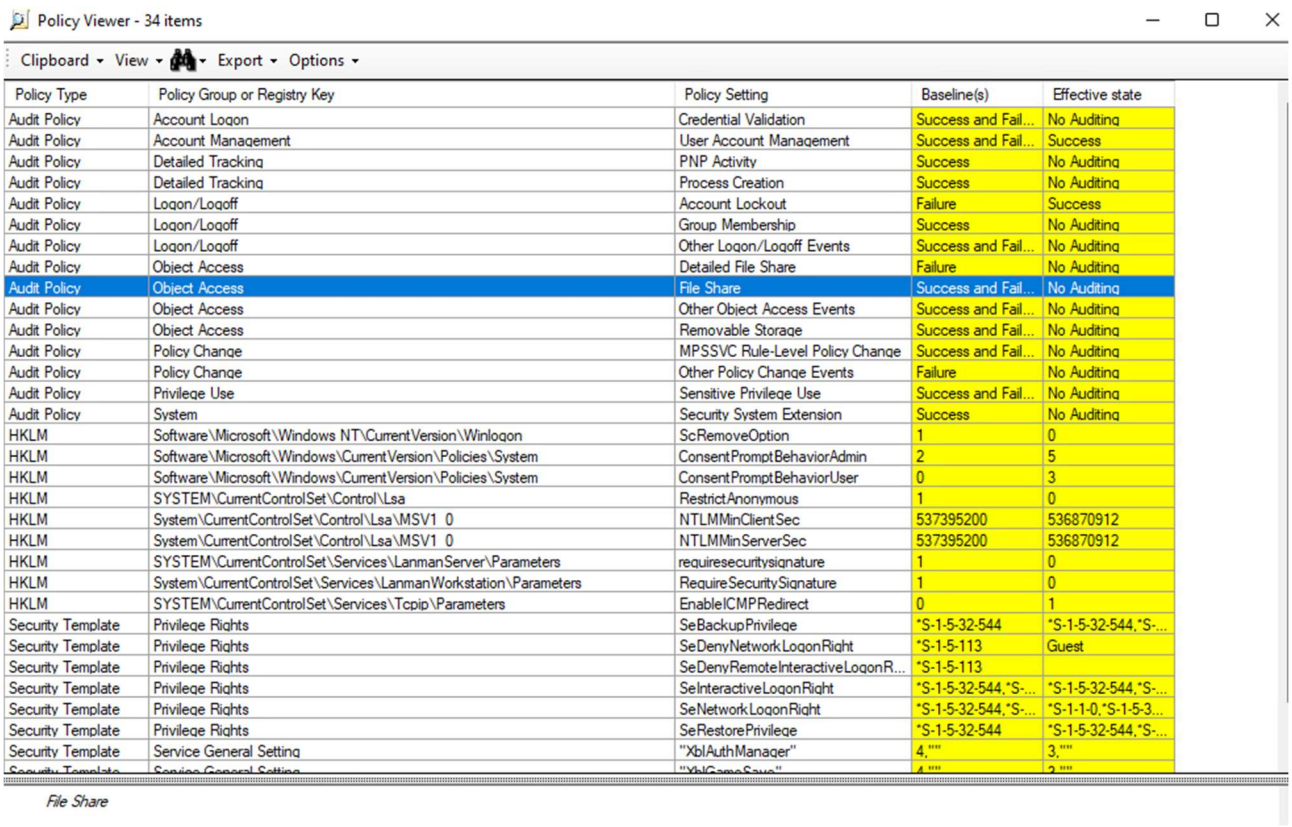
Volume: Low.

Default: No Auditing.

Kuvio 8. Policy Path informaatio Policy Analyzerissa.

4.1 File Share konflikti konfigurointi

Ensimmäinen Group Policy mitä konfiguroimme manuaalisesti, on `**File Share**`. Tällä Audit Policylla pitäisi olla `**Success and Failure**` auditointi päällä, mutta tällä hetkellä siinä ei ole mitään, eli `**No Auditing**` (ks. kuvio 9).



Policy Viewer - 34 items

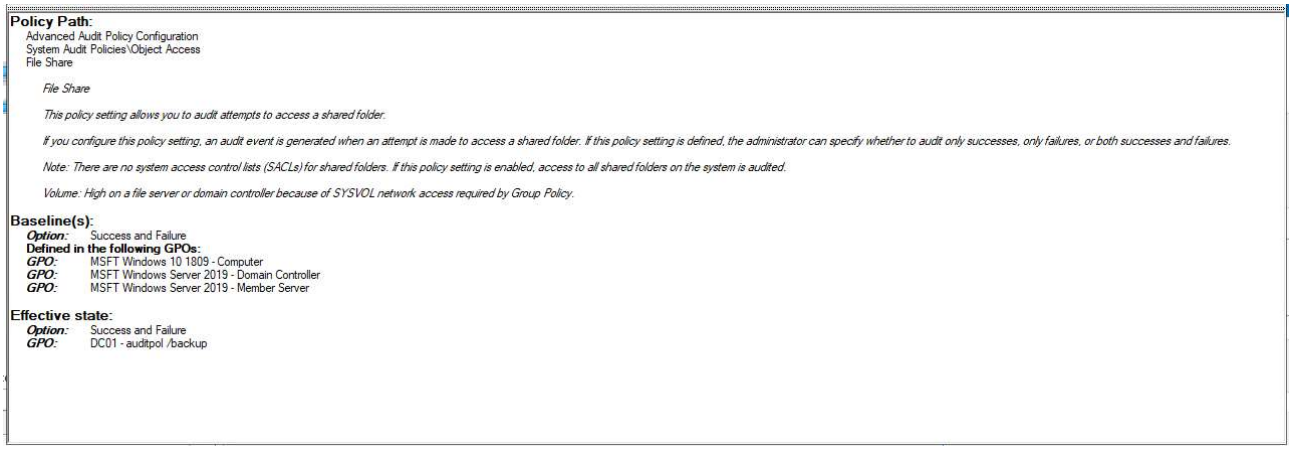
Clipboard ▾ View ▾ Export ▾ Options ▾

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	No Auditing
Audit Policy	Account Management	User Account Management	Success and Fail...	Success
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	Failure	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	No Auditing
Audit Policy	System	Security System Extension	Success	No Auditing
HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ScRemoveOption	1	0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorAdmin	2	5
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorUser	0	3
HKLM	SYSTEM\CurrentControlSet\Control\Lsa	RestrictAnonymous	1	0
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinClientSec	537395200	536870912
HKLM	System\CurrentControlSet\Control\Lsa\MSV1_0	NTLMMinServerSec	537395200	536870912
HKLM	SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters	requiresecuritysignature	1	0
HKLM	System\CurrentControlSet\Services\LanmanWorkstation\Parameters	RequireSecuritySignature	1	0
HKLM	SYSTEM\CurrentControlSet\Services\Tcpip\Parameters	EnableICMPRedirect	0	1
Security Template	Privilege Rights	SeBackupPrivilege	*S-1-5-32-544	*S-1-5-32-544,*S-...
Security Template	Privilege Rights	SeDenyNetworkLogonRight	*S-1-5-113	Guest
Security Template	Privilege Rights	SeDenyRemoteInteractiveLogonR...	*S-1-5-113	
Security Template	Privilege Rights	SeInteractiveLogonRight	*S-1-5-32-544,*S-...	*S-1-5-32-544,*S-...
Security Template	Privilege Rights	SeNetworkLogonRight	*S-1-5-32-544,*S-...	*S-1-1-0,*S-1-5-3...
Security Template	Privilege Rights	SeRestorePrivilege	*S-1-5-32-544	*S-1-5-32-544,*S-...
Security Template	Service General Setting	"XblAuthManager"	4,""	3,""
Security Template	Service General Setting	"XblGameSave"	4,""	3,""

File Share

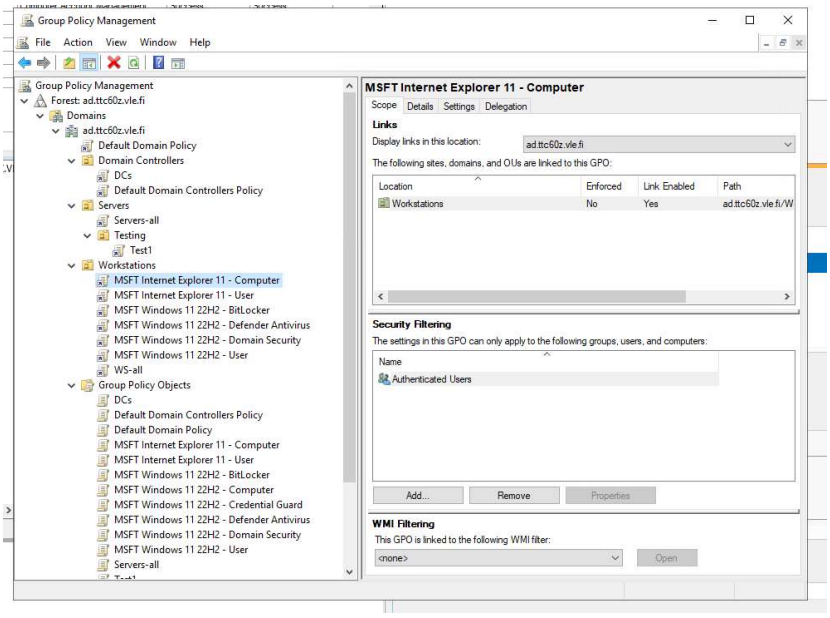
Kuvio 9. "File Share" konflikti

Success and Failure auditointi tarkoittaa, että kun joku lataa tai muokkaa, tai tekee mitään yhteissessä kansiossa, siitä tulee lokitiedosto. Policy Analyzerin mukaan tämä löytyy `**Computer**` puolelta, ja Policy Pathiä seuraamalla pystymme löytämään mistä sen pystyy konfiguroimaan (ks. kuvio 10).



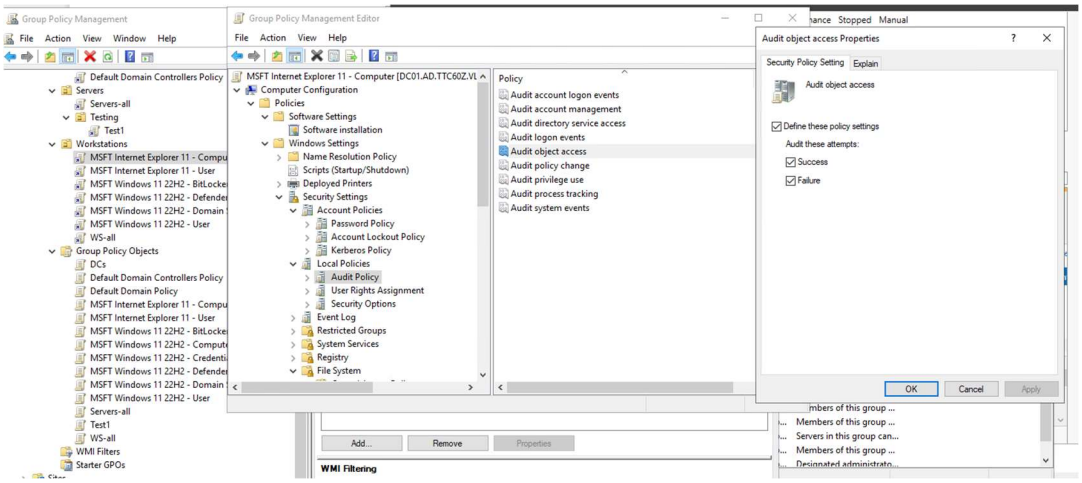
Kuvio 10. Policy Path, informaation File Share Group Policystä.

Computer Group Policyn pystyy löytämään `**Group Policy Management**` kohdasta `**Workstations**`. Kun rightklikkaa `**MSFT Internet Explorer 11 - Computer**` kohtaa ja valitsee `**Edit**`, pääsee `**Group Policy Management Editoriin**` (ks. kuvio 11).



Kuvio 11. Group Policy Management, Computer.

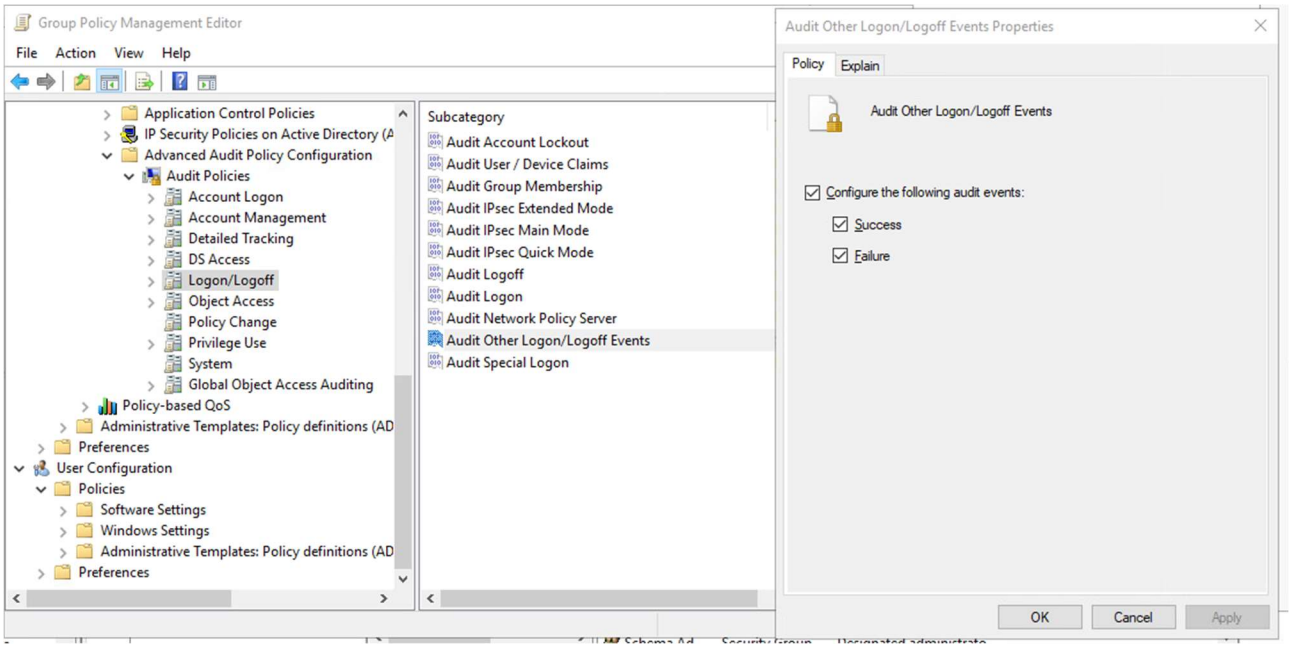
Group Policy Management Editorista polusta `**Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy**` avautuu vaihtoehdot erilaisille Audit Policyille. `**Audit Object Accessia**` klikkaamalla pystyy avaamaan uuden valikon, mistä voimme valita Security Baselinen mukaiset asetukset, eli ensin pitää laittaa `**Define these policy settings päälle**`, minkä jälkeen voimme valita kummatkin `**Success**` ja `**Failure**` (ks. kuvio 12).



Kuvio 12. Audit object access Properties polku

4.2 Logon/Logoff Events konflikti konfigurointi

Kokeilimme muuttaa vielä toisenkin Group Policyn asetuksia Security Baselinen mukaiseksi. Valitsimme `**Logon/Logoff**` policyista `**Other Logon/Logoff Events**` policyn konfiguroitavaksi. Tähän tarvitsi laittaa samat asetukset kuin edelliseen, eli `**Success and Failure**`. Tämäkin näkyy edellisessä kuviossa vähän `**File Sharea**` ylempänä (ks. kuvio 9). Nämä Logon/Logoff asetukset löytyivät hiukan eri paikasta, kuin edellisessä policyn konfiguroinnissa. Kuitenkin olemme konfiguroimassa `**Group Policy Management Editorin**` sisällä. Sieltä polku tähän Logon/Logoff tapahtumiin on `**Computer Configuration/Policies/Windows Settings/Security Settings/Advanced Audit Policy Configuration/Audit Policies/Logon/Logoff**`. Tästä aukeaa samankaltainen valikko, mikä edellisessäkin näkyi, valitaan `**Audit Other Logon/Logoff Events**` ja vaihdetaan siitä asetukset Security Baselinen mukaiseksi, eli laitetaan päälle `**Configure the following audit events**`, ja sen jälkeen klikataan kummatkin `**Success**` ja `**Failure**` päälle (ks. kuvio 13).



Kuvio 13 Audit Other Logon/Logoff Events Properties polku

5 Pohdinta

Tämän labran tehtävänanto oli selkeä ja helppo tehdä samalta pohjalta kuin aikaisempi labra. Selkeiden ohjeiden ja aikaisemman labran kokemuksen avulla labran tekeminen sujui suhteellisen helposti ja nopeasti. Labrassa haaste oli suunnitella mitä koventaa, meillä ei ole simuloitua tilannetta, johon voisimme perustaa erilaiset kovennukset. Hieman haastetta tuotti myös Windows 11 käyttöjärjestelmä, josta meillä ei ollut aiempaa kokemusta. Tämän takia päätimme tehdä koventamisen samalta pohjalta kuin Active Directoryn koventamisen. Latasimme Microsoftin baselinet ja ajoimme ne skriptillä. Automaattisen konfiguroinnin lisäksi kovensimme myös manuaalisesti. Sen lisäksi näiden kahden labran jälkeen on käynyt todella selväksi, miten paljon vaikeampaa koventaminen on manuaalisesti, ja miksi sitä koko ajan automatisoidaan enemmän ja enemmän.

Labrassa opimme käyttämään ja koventamaan Windows 11 käyttöjärjestelmää ja lisää Active Directoryn ominaisuuksia ja kuinka käyttää niitä. Käsitys Active Directoryn tärkeydestä organisaatioille ja varsinkin organisaation laitteiden hallinnasta parani todella paljon. Turvallisuusasetusten lataus AD:lle ja sitä kautta kaikille päätelaitteille vaihtamisesta oli todella helppo ja nopea.

Lähteet

Active Directory Domain Services Overview. 17.8.2022. Viitattu 10.10.2022. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview 20.9.

Lab 4 ohjeet. N.d. Viitattu 10.10.2022. https://moodle.jamk.fi/pluginfile.php/790775/course/section/81509/LAB1-koventaminen.pdf

Microsoft Security Compliance Toolkit 1.0. N.d. Viitattu 10.10.2022. https://www.microsoft.com/en-us/download/details.aspx?id=55319

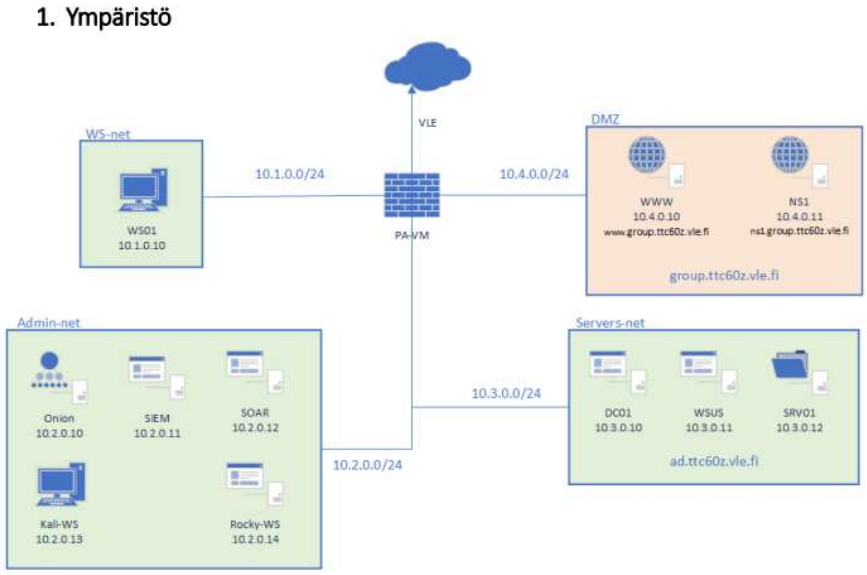
Microsoft. Security baselines. 1.8.2022. Viitattu 7.10.2022. https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines

Munck R. Windows 11, version 22H2 Security baseline 20.09.2022 Viitattu 7.10.2022 https://techcommunity.microsoft.com/t5/microsoft-security-baselines/windows-11-version-22h2-security-baseline/ba-p/3632520

Petteri Pyyny. Laaja katsaus windows-11 saloihin uusi kayttoliittyma paljon vanhaa. 16.6.2021. Viitattu 6.10.2022. https://www.hardware.fi/uutiset/artikkeli.cfm/2021/06/16/laaja-katsaus-windows-11-saloihin-uusi-kayttoliittyma-paljon-vanhaa

Liitteet

Liite 1. Labraympäristö



Kuvio 1 Laboratorio ympäristö