



## Koventaminen - Labra 1

### Ryhmä 3

Juha-Matti Hietala

Topi Liljeqvist

Markus Pollari

Maija Virta

Harjoitustehtävä

Tammikuu 2023

Tieto- ja viestintätetekniikan tutkinto-ohjelma (AMK)

## Sisältö

<b>1</b>	<b>Johdanto.....</b>	<b>4</b>
<b>2</b>	<b>TEORIA .....</b>	<b>5</b>
2.1	Koventaminen .....	5
2.2	Windows AD (Active Directory) .....	5
2.3	Microsoft Best Practices Analyzer (MS BPA).....	5
2.4	PIM & PAM.....	7
2.5	JIT & JEA .....	7
<b>3</b>	<b>DC01 - KOVENNUKSET .....</b>	<b>8</b>
3.1	Windows päivityksen kovennukset .....	8
3.2	Salasanan kesto .....	12
3.3	Estetään suojaamaton vieraskirjautuminen - Disable insecure guest logons .....	14
3.4	Skannaa irrotettavat asemat - Scan removable drives .....	16
3.5	Käyttäytymisen seuranta - Behavior monitoring .....	17
<b>4</b>	<b>FILE SERVERIN (SRV01) - KOHTALO .....</b>	<b>19</b>
<b>5</b>	<b>FILE SERVER (SRV01) - KOVENNUKSET .....</b>	<b>25</b>
5.1	Sisäänkirjautuminen .....	25
5.2	Yhteys verkon kautta .....	28
5.3	Tilien kirjautumisten tarkkailu .....	29
5.4	Tilin lukituskynnys .....	33
<b>6</b>	<b>POHDINTA .....</b>	<b>37</b>
	Lähteet .....	38

## Kuvat

Kuva 1 VLE ympäristö.....	4
Kuva 2 BPA_scan1 .....	6
Kuva 3 BPA_scan2 .....	7
Kuva 4 Greate a GPO .....	8
Kuva 5 Edit Windows Update Settings .....	9
Kuva 6 Reitti kovennuksen tekemiseen.....	9
Kuva 7 Päivityksien ajan automatisointi.....	10
Kuva 8 Uusien päivityksien tarkastus .....	10
Kuva 9 Päivityksien estämisen poisto normaalista käyttäjiltä .....	11

Kuva 10 Enabloinnit .....	11
Kuva 11 Muutosten pakotus .....	11
Kuva 12 Muutosten tarkistus .....	12
Kuva 13 Maximum password age.....	13
Kuva 14 Salasanan keston pituus .....	13
Kuva 15 Muutosten pakotus .....	14
Kuva 16 Muutosten tarkistus .....	14
Kuva 17 Scan - Scan removable drives .....	17
Kuva 18 Enabled - Scan removable drivers .....	17
Kuva 19 Insecure guest access – Lanman Workstation .....	18
Kuva 20 Enable insecure guest logons – Disabled .....	18
Kuva 21 Kirjautuminen SRV01.....	19
Kuva 22 Roles and Features – avaaminen .....	19
Kuva 23 Poistetaan turhat.....	20
Kuva 24 Poisto käynnissä .....	20
Kuva 25 PowerShell asennus.....	21
Kuva 26 File Server - Asetuksien tarkistus uudestaan .....	22
Kuva 27 .Net asetuksien tarkastus .....	22
Kuva 28 File Storage Services asennus .....	23
Kuva 29 Disks .....	23
Kuva 30 SMB Share luontia .....	24
Kuva 31 Share nimi – Labra1_share .....	24
Kuva 32 Valittujen tietojen vahvistus .....	25
Kuva 33 Luotu Labra1_share .....	25
Kuva 34. Local Security Policy löytyy Windowsin Etsi-toiminnolla. ....	26
Kuva 35. Local Security Policy oletusikkuna. ....	26
Kuva 36. Local Policiesin alta Security Options ja tämän alta Interactive logon: Don't display last signed-in. ....	27
Kuva 37. Muutetaan asetus Enabled – tilaan .....	27
Kuva 38. "User Rights Assignment" ja tämän alta "Access this computer from the network" ..	28
Kuva 39. Käyttäjät joilla oletuksena oikeudet. ....	28
Kuva 40. Lisätään sallituksi käyttäjäksi "Authenticated Users". .....	29
Kuva 41. Poistetaan sallituista käyttäjistä "Everyone" ja "Users". .....	29
Kuva 42. Audit Logon Policyn käyttöönotto. ....	30
Kuva 43. Ajettiin gpupdate /force jotta policy tulee voimaan.....	31

Kuva 44. Tili kirjautumisten tarkkailu .....	31
Kuva 45. Tapahtumien filtteröinti .....	32
Kuva 46. Filtteröity näkymä .....	32
Kuva 47. Account lockout määritys .....	33
Kuva 48. Account lockout threshold määritys .....	33
Kuva 49. Reset account lockout counter after määritys.....	34
Kuva 50. Group Domain Policy Account lockout määritykset .....	34
Kuva 51. Account lockout policy workstation domainiin.....	35
Kuva 52. User1 Account locked WS domainissa.....	36

## 1 Johdanto

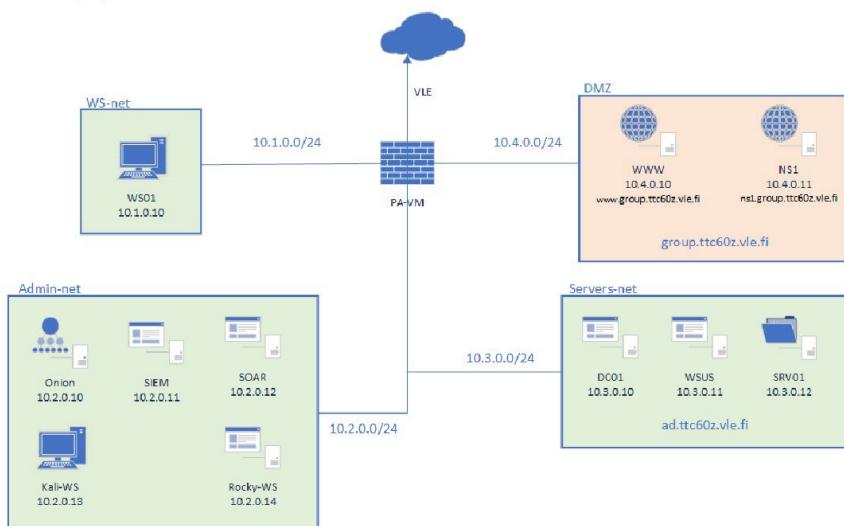
Dokumentaatio on osana koventamisen kurssin (TTC6050-3002) laboratorioharjoituksia. Ensimmäisen LAB1 harjoituksen tavoitteena on Active Directoryn (AD) koventaminen. Ryhmä saa valita itse kovennusohjeen ja mitä kovennuksia toteuttaa VLE ympäristössä oleville DC01 (IP 10.3.0.10) ja SRV01 (IP 10.3.0.12) koneille. VLE ympäristö esitetty kuvassa 1. Kovennuksia tehdään yhteenä noin kymmenen kappaletta ja tavoitteena on, että jokainen ryhmän jäsen toteuttaa vähintään kaksi kovennusta.

AD kovennuksien todentamiseen käytetään Microsoft Best Practices Analyzeria (MS BPA). Kovennukset dokumentoidaan kuvankaappauksilla sekä havainnollistetaan, miten kovennus tehdään ja miksi. Analyzer ajetaan harjoitusta aloittaessa sekä lopuksi tehtyjen kovennuksien jälkeen, jotta voidaan vertailla mitä muutoksia saatiin aikaan ja miten Analyzer arvioi ympäristön turvallisuutta koventamisen jälkeen.

Teorialla ja koventamisen harjoituksilla ryhmän jäsenet saavat taidot ja ymmärryksen Active Directoryn koventamiseen. Lisäksi dokumentoinnissa käydään läpi teoriaa koventamisesta sekä Microsoft Best Practices Analyzerista.

Harjoituksessa tullaan lisäksi dokumentoimaan File Serverin kohtalo (ympäristössä SRV01). SRV01 on jätetty siihen tilaan, ettei se ole turvallinen, koska siinä ajetaan paljon erilaisia rooleja. Koventamisen näkökulmasta palvelimella tulee ajaa mahdollisimman vähän eri rooleja, joten SRV01 tyhjennetään ja jatkossa se toimii vain fileserverinä.

### 1. Ympäristö



Kuva 1 VLE ympäristö

## 2 TEORIA

### 2.1 Koventaminen

Koventamisella tarkoitetaan järjestelmän asetusten muuttamista niin, että haavoittuvuuspinta-ala (Attack surface) järjestelmässä saadaan pienennettyä. Riskien pienentämiseksi järjestelmissä otetaan käyttöön vain käyttövaatimusten kannalta olennaiset toiminnot, palvelut ja laitteet, sekä esimerkiksi palvelujen näkyvyys tulee rajata mahdollisimman pieneksi, joka vähentää hyökkäysvektoreita (Attack vectors). Mitä enemmän tilaa on, sitä helpompi hyökkääjän on päästä laitteelle tai ympäristöön koska silloin hyökkäystapoja on enemmän. Kun toimintoja rajoitetaan, käytettävissä olevat hyökkäystavat vähenevät. (Katakri 2020, 80)

Koventamisen toimenpiteitä ovat esimerkiksi oletussalasanojen vaihtaminen organisaation salasanapolitiikan mukaisiin laadukkaisiin salasanoihin sekä pakottaa salasanalla vaihto sopivin määräajoin, käyttöoikeuksien rajaaminen ja ryhmittely, tarpeettomien ohjelmistojen poistaminen, tarpeettomien käyttäjätunnuksien poisto ja tarpeettomien palveluiden poistaminen käytöstä. Lisäksi turhien tietokantojen, skriptien poisto sekä ohjelmistojen pito ajantasalla. Kovennusten voimassaolosta ja vaikuttavuudesta lisäksi huolehditaan koko tietojärjestelmälinkaaren ajan. (Katakri 2020, 78).

### 2.2 Windows AD (Active Directory)

Active Directory on Microsoftin suunnittelema Windows toimialueen aktiivihakemisto eli hakemistopalvelu sekä käyttäjätietokanta. Se mahdollistaa tietokonaisuksien keskitetyn hallinnan ja jakelun käyttäjille ja sovelluksille. Active Directoryyn voidaan lisätä tietoa domainiin kuuluvista resursseista kuten laitteista, esimerkiksi tulostimia, tietokoneita, palvelimia, ohjaimia sekä tietoa käyttäjistä (roolit, oikeudet) sekä tiedot käyttäjien ryhmistä. (Keski-Simonen 2016, 3.)

### 2.3 Microsoft Best Practices Analyzer (MS BPA)

Microsoft Best Practice Analyzer (BPA) on palvelimen hallintatyökalu, joka skannaa palvelimen roolit mahdollisten puutteiden osalta. Puutteiksi todetaan löydökset, jotka eivät ole parhaiden

käytänteiden (Best Practices) mukaisia, jotka Microsoftin asiantuntijat ovat määritelleet. BPA käytön hyötyjä ovat esimerkiksi turvallisuustason ja toimintavarmuuden nouseminen, sekä mahdollisten konfiguraatio-ongelmien löytäminen. (Allen 2022)

Skannatessaan BPA arvioi kuinka hyvin roolien konfiguraatiot ovat parhaiden käytänteiden mukaisia. Arvio tehdään kahdeksan eri kategorian perusteella, jotka viittaavat tehokkuuteen, luotettavuuteen ja toimintavarmuuteen. Nämä kahdeksan kategoriaa ovat security, performance, configuration, policy, operation, predeployment, postdeployment ja prerequisites. (Run Best Practices Analyzer Scans and Manage Scan Results 2023)

Skannauksen tulokset voivat saada vakavuusasteen kolmessa eri tasossa, jotka ovat error, information ja warning. Error tarkoittaa, että skannattu rooli ei täytä parhaiden käytänteiden ehtoja ja toiminnallisia ongelmia on odotettavissa. Information palautetaan, jos rooli täyttää parhaiden käytänteiden ehdot. Warning tarkoittaa, että ehtojen noudattamatta jättäminen saattaa aiheuttaa ongelmia, vaikka tällä hetkellä ongelmia ei ilmene. Esimerkiksi asetus, joka tulee käyttöön vasta, kun yritetään muodostaa etäyhteyttä. (Run Best Practices Analyzer Scans and Manage Scan Results 2023)

Ennen kovennuksien aloittamista ajoimme BPA skannauksen. Sieltä tuli 8/42 varoitusta. (1 Error ja 7 varoitusta) Esitetty kuvassa 2.

Server Name	Severity	Title	Category
DC01	Error	The PDC emulator master DC01.ad.ttc60z.vle.fi in this forest should be configured to correctly synchronize time from a valid time source	Configuration
DC01	Warning	All domains should have at least two domain controllers for redundancy	Operation
DC01	Warning	All OUs in this domain should be protected from accidental deletion	Configuration
DC01	Warning	The directory partition DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition CN=Configuration,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
<b>Problem:</b> The primary domain controller (PDC) emulator operations master in this forest is not configured to correctly synchronize time from a valid time source.			
<b>Impact:</b> If the PDC emulator master in this forest is not configured to correctly synchronize time from a valid time source, it might use its internal clock for time synchronization. If the PDC emulator master in this forest fails or otherwise becomes unavailable (and if you have not configured a reliable time server (GTIMESERV) in the forest root domain), other member computers and domain controllers in the forest will not be able to synchronize their time. <a href="#">More information about this best practice and detailed resolution procedures</a>			

Kuva 2 BPA\_scan1

Kovennuksien jälkeen ajoimme uudestaan skannauksen ja tuli samat 8/42 varoitusta. Tekemämme kovennukset eivät vaikuttaneet varoituksiin. Esitetty kuvassa 3.

The screenshot shows the Windows Server Manager interface. On the left, there's a navigation pane with links like Dashboard, Local Server, All Servers, AD DS (which is selected), DNS, and File and Storage Services. The main area displays service status for DC01 (Server, LanmanServer, Running, Automatic (Triggered)), File Replication (Ntfrs, Stopped, Disabled), and Kerberos Key Distribution Center (Kdc, Running, Automatic). Below this is the 'BEST PRACTICES ANALYZER' section, which shows 8 of 42 total warnings or errors. A table lists these findings, including issues related to time synchronization, backup schedules, and domain controller protection.

Server Name	Severity	Title	Category
DC01	Error	The PDC emulator master DC01.ad.ttc60z.vle.fi in this forest should be configured to correctly synchronize time from a valid time source	Configuration
DC01	Warning	The directory partition CN=Configuration,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition DC=DomainDnsZones,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition DC=ForestDnsZones,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition CN=Schema,CN=Configuration,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	All OUs in this domain should be protected from accidental deletion	Configuration
DC01	Warning	All domains should have at least two domain controllers for redundancy	Operation

Kuva 3 BPA\_scan2

## 2.4 PIM & PAM

PIM (Privileged Identity Management) ja PAM (Privileged Access Management) tarkoitetaan käyttäjiä, joilla on vähiten rajoittavat oikeudet järjestelmiin tai resursseihin. Etuoikeus (Privileged) tulee laajoista oikeuksista tehdä verkkoon tai tietokoneeseen muutoksia. Oikeudet voivat olla ihmillisillä tai tileillä, joilla molemmissa voi olla eri tasoisia etuoikeuksia. Esimerkiksi senior IT administration tai "superkäyttäjä" voivat pystyä määrittelemään palvelimia, palomuureja, pilvitalennustilaa korkeammalla käyttöoikeudella kuin tavallinen käyttäjä. (Kuokkanen 2020, 23.)

Tavallisilla käyttäjillä tai tileillä, joissa ei ole etuoikeutta, voivat kirjautua yrityksen tietokoneelle, ja käyttää erilaisia ohjelmia, mutta eivät voi muuttaa verkkoasetuksia tai käyttöoikeuksia sekä eivät voi ladata ohjelmistoja, jos ne eivät ole hyväksyttyjen listalla (Kuokkanen 2020, 23).

Etuoikeutettuja käyttövaltuuksien tilejä ja tunnuksia voidaan hallita PAM työkaluilla ja prosesseilla. PAM viittaa siis enemmän järjestelmiin kuin taas PIM sisältää sen hallinnan, mihin resursseihin ne, joilla on oikeudet muuttaa tärkeitä tiedostoja, pääsevät käsiksi.

## 2.5 JIT & JEA

JIT (Just-In-Time Admin) käyttöoikeusmalli on perusturvakäytäntö, jossa järjestelmille tai sovelluksille myönnetyt käyttöoikeudet on rajoitettu etukäteen määrätyksi ajaksi ja tarpeen mukaan. Tämä

minimoi pysyvien oikeuksien riskejä, joita hyökkääjät voivat yrittää hyödyntää (Simos & Davies 2022).

JEA (Just-Enough-Admin) on taas tietoturvateknikka, joka mahdollistaa PowerShellin hallinnoiman delegoidun hallinnan. Tämän avulla voidaan vähentää koneiden järjestelmävalvojen määrää käytäväällä virtuaalisia tilejä tai ryhmähallittuja palvelutilejä suorittamaan etuoikeutettuja toimintoja tavallisten käyttäjien puolesta. (Just Enough Administration 2022.)

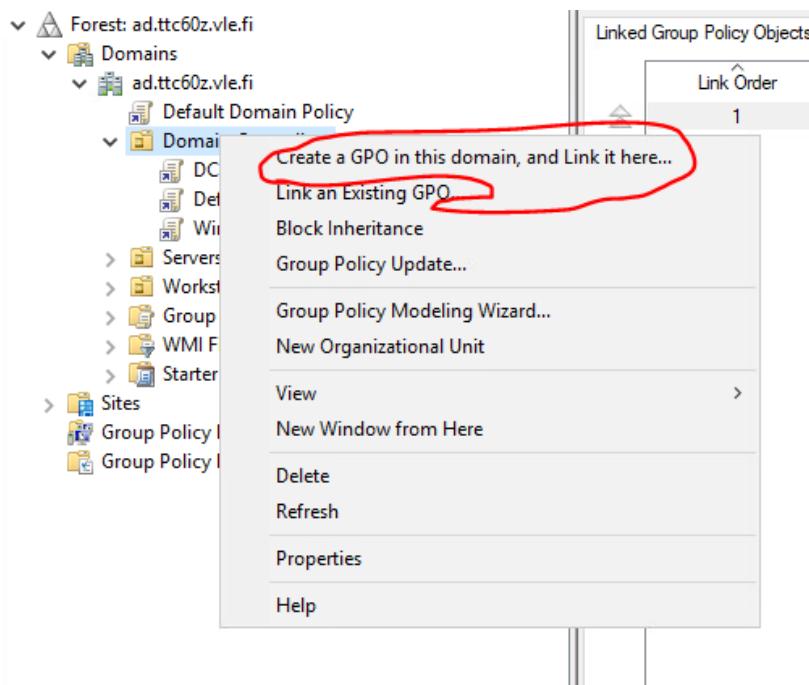
### 3 DC01 - KOVENNUKSET

#### 3.1 Windows päivityksen kovennukset

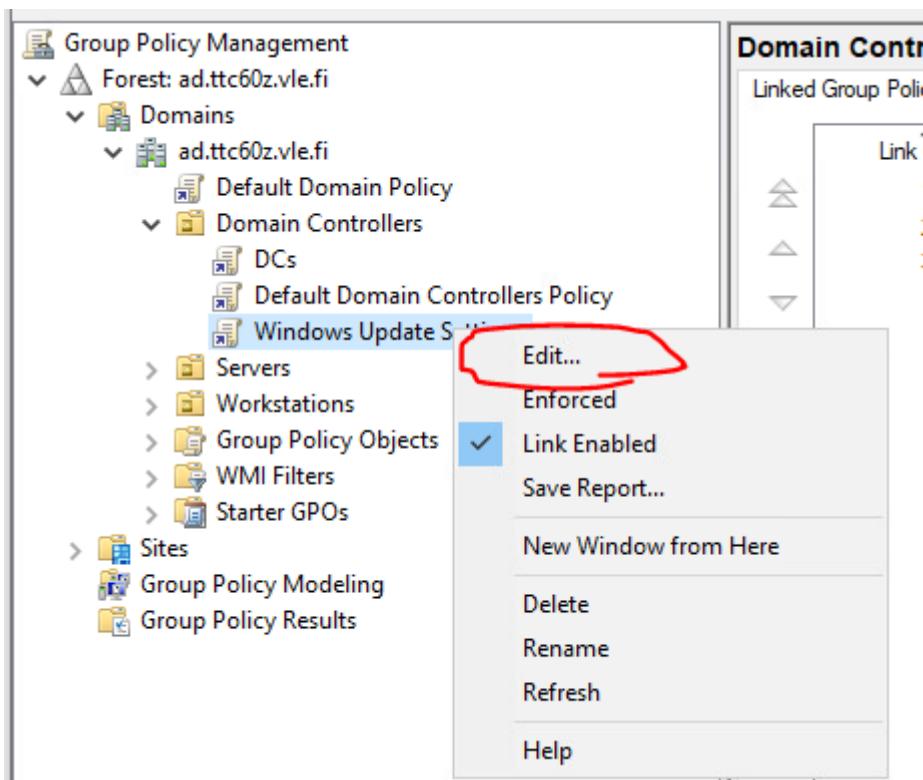
Kovennusohjeeksi valikoitui Microsoftin SecCon-Framework ja tarkemmin Level 1 Enterprise Basic Security Configuration (SecCon-Framework 2019).

Ehkä yksi vihatuimmista mutta samalla tärkeimmistä kovennuksista on Windows päivityksien automatisointi. Yleisin syy miksi järjestelmiin on päästy tunkeutumaan, on ettei päivitykset ole ajan tasalla. Tämä on myös yksi todennäköisimmistä kovennuksista mitä pääsee tekemään tulevaisuudessa työelämässä, sen takia päivityksen automatisointi valikoitui ensimmäiseksi kovennukseksi.

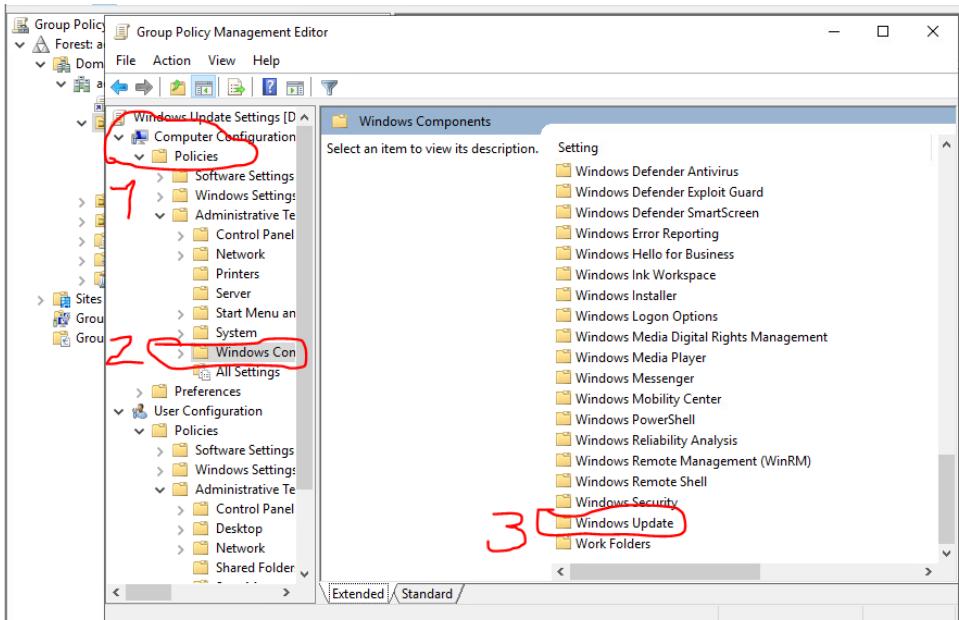
Esitetty kuvissa 4-6.



Kuva 4 Create a GPO

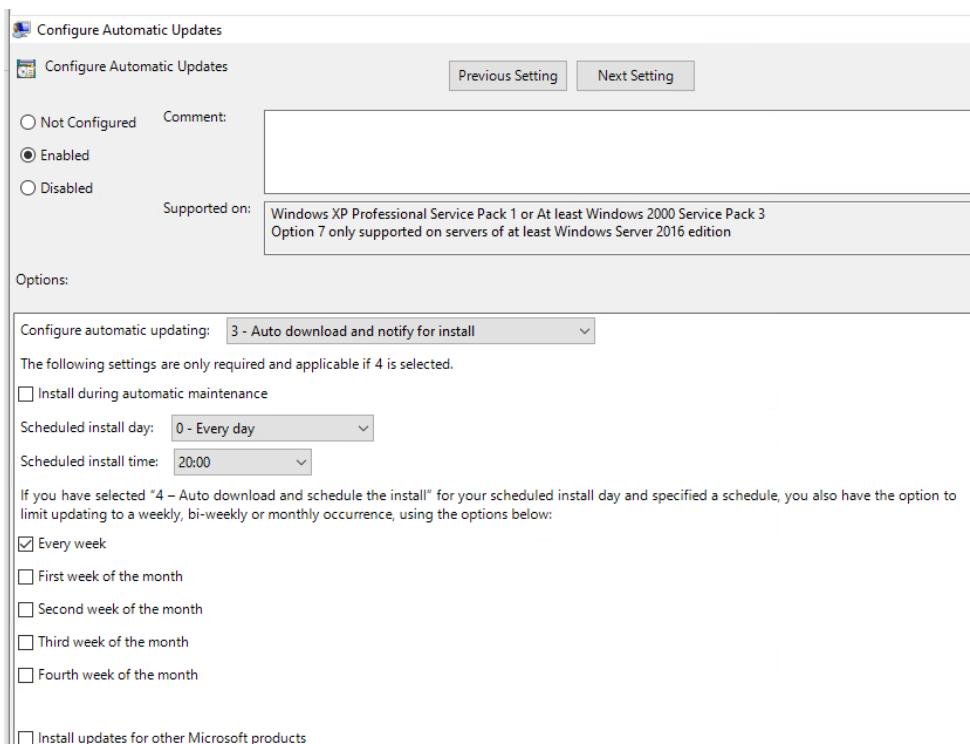


Kuva 5 Edit Windows Update Settings



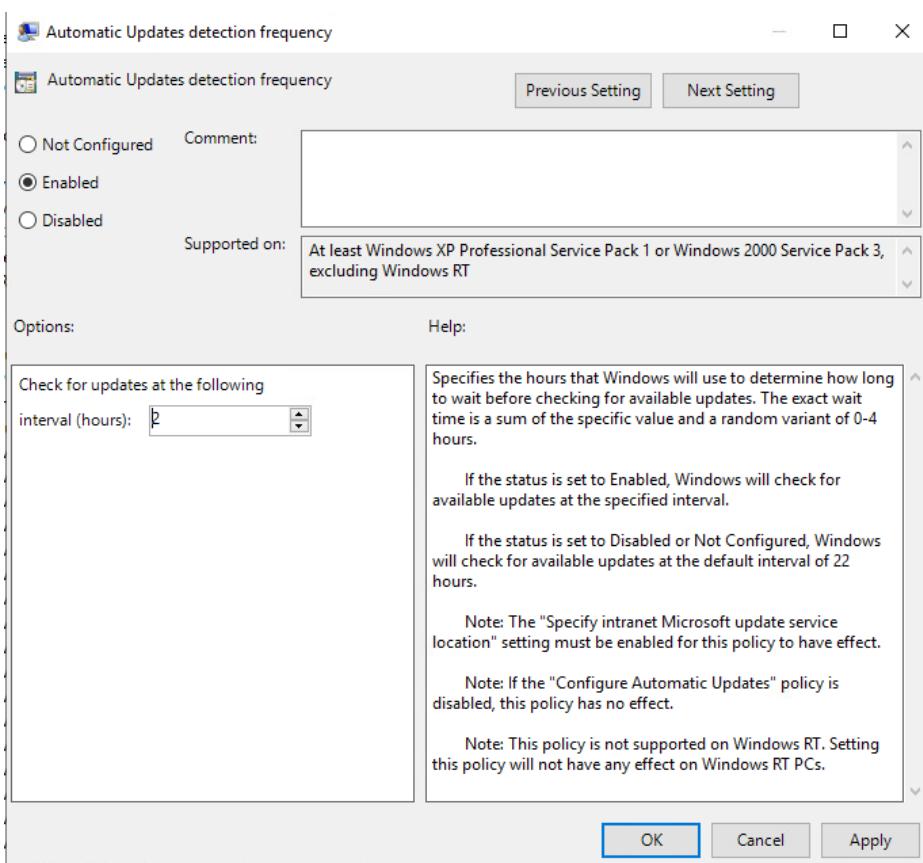
Kuva 6 Reitti kovennuksen tekemiseen

Valitaan miinkä kellon aikaan päivitykset asennettaan (20:00) ja joka viikko. Esitetty kuvassa 7.



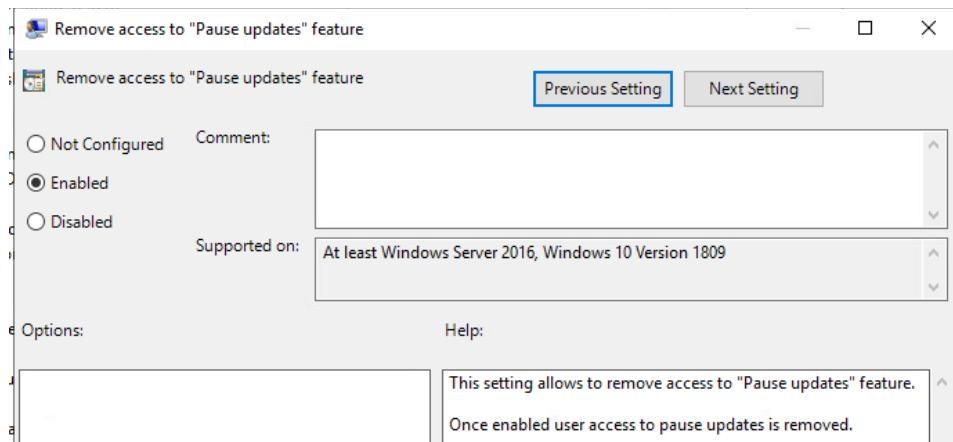
## Kuva 7 Päivityksien ajan automatisointi

Tarkistetaan, onko uusia päivityksiä saatavilla kahden tunnin välein. Esitetty kuvassa 8.



## Kuva 8 Uusien päivityksien tarkastus

Poistetaan peruskäyttäjiltä lupa myös peruua tai pysäyttää päivitys näin varmistetaan, että päivityksiä ei ainakaan käyttäjän toimesta jää tekemättä. Esitetty kuva 9.



Kuva 9 Päivityksien estämisen poisto normaali käyttäjiltä

Tarkistetaan, onko kaikki halutut kohdat enabloituna. Esitetty kuva 10.

<input type="checkbox"/> Configure Automatic Updates	Enabled	No
<input type="checkbox"/> Specify deadlines for automatic updates and restarts	Not configured	No
<input type="checkbox"/> Specify intranet Microsoft update service location	Not configured	No
<input type="checkbox"/> Automatic Updates detection frequency	Enabled	No
<input type="checkbox"/> Do not allow update deferral policies to cause scans against ...	Not configured	No
<input type="checkbox"/> Remove access to "Pause updates" feature	Enabled	No

Kuva 10 Enabloinnit

Yleensä kestää noin kaksi tuntia, että muutokset astuvat voimaan sen takia pakotettiin muutokset heti voimaan komennolla (gpupdate /force). Esitetty kuva 11.

```
C:\> Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>
```

Kuva 11 Muutosten pakotus

Tarkistetaan vielä, tuliko muutokset voimaan. Esitetty kuva 12.

## View configured update policies

Wondering why you're seeing 'Some settings are managed by your organization'?

This text is typically displayed on Windows Update after installation and delivery policies are configured.

Examples include:

- Your organization has set some policies to manage updates
- You have opted in for the Windows Insider Program

### Policies set on your device

Download the updates automatically and notify when they are ready to be installed

Source: Administrator

Type: Group Policy

Disable Pause updates by user

Source: Administrator

Type: Group Policy

Set Automatic Update options

Source: Administrator

Type: Group Policy

Specifies the hours before checking for updates

Source: Administrator

Type: Group Policy

## Kuva 12 Muutosten tarkistus

### 3.2 Salasanen kesto

Hyväntäntöön pidetään yleisesti salasanojen vaihtamista 90 päivän välein turvatoimenpiteenä, jolla vähennetään arkaluonteisten tietojen luvatonta pääsyn riskiä. Tämä johtuu siitä, että ajan myötä muut voivat tuntea tai arvata salasanat joko hakkerointirytysten, manipulointitaktiikkojen tai yksinkertaisesti huonojen salasanakäytäntöjen vuoksi. Säännöllinen salasanojen vaihtaminen vähentää luvattoman käytön riskiä ja pitää tiedot turvallisempaan. (How Often Should You Change Your Passwords.)

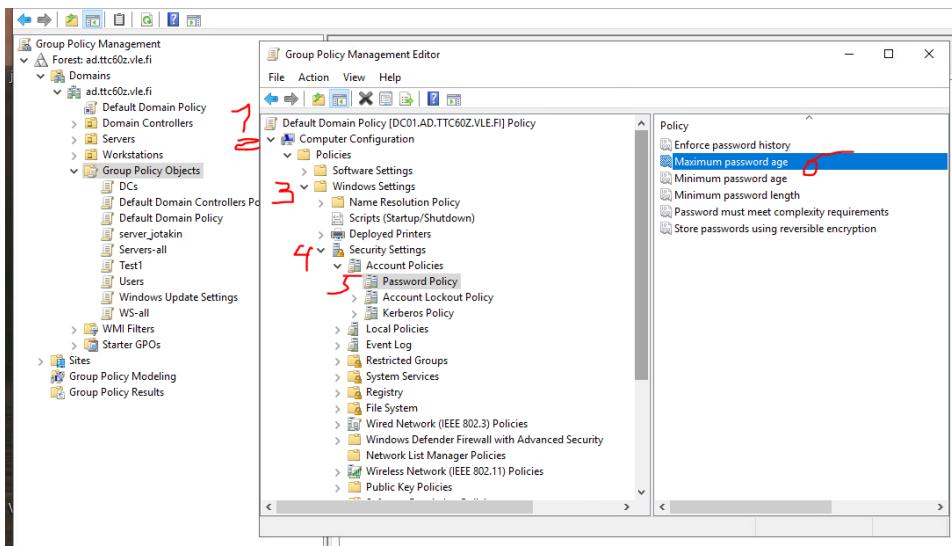
Seuraavassa on esimerkki salasanan vanhenemisiän vaihtamisesta. Esimerkkinä on laitettu 200 päivää salasanan vanhenemiseen, joka on huono käytäntö.

Siirry seuraavaan sijaintiin: 1 Oletus Domainin policy > 2 Tietokoneen asetukset > 3 Windows-asetukset > 4 Suojausasetukset > Tilikäytännöt > 5 Salasanakäytäntö. 6 Etsi "Salasanan enimmäisikä" -käytäntö ja avaa sen ominaisuudet kaksoisnapsauttamalla sitä.

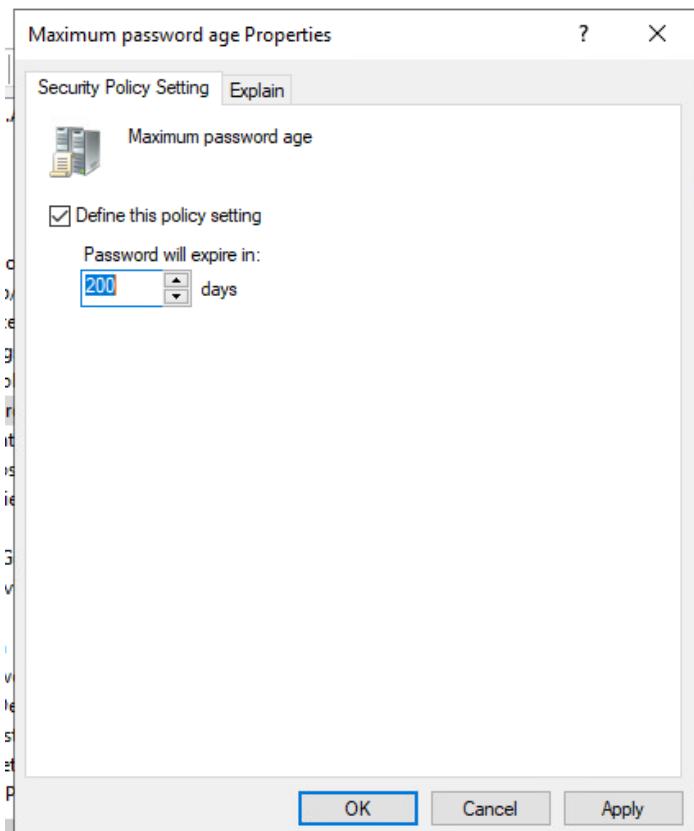
Muuta "Salasana vanhenee X päivän kuluttua" -kentässä päivien lukumäärä, jonka haluat salasanan pysyvän voimassa. Jos esimerkiksi haluat salasanan olevan voimassa 90 päivää, kirjoita "90".

Tallenna muutokset ja sulje ominaisuusikkuna napsauttamalla OK. Sulje ryhmäkäytäntöeditori.

Suorita seuraava komento komentokehotteessa: "gpupdate /force". Kun käytäntö on päivitetty, salasanan vanhenemisaika asetetaan ryhmäkäytännössä määritetyyn arvoon. Käyttäjät saavat ilmoitukseen Windowsissa, kun heidän salasanansa on vanhentumassa, ja heidän on vaihdettava se uuteen salasanaan jatkaakseen tilinsä käyttöä. Esitetty kuvissa 13 & 14.



Kuva 13 Maximum password age



Kuva 14 Salasanahan keston pituus

```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1217]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>

```

Kuva 15 Muutosten pakotus

Tarkistetaan muutokset komennolla: net user Administrator. Esitetty kuvassa 16.

```

Administrator: Command Prompt
C:\Users\Administrator>net user Administrator
s User name          Administrator
Full Name
Comment           Built-in account for administering the computer/domain
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never

Password last set   5.1.2023 9.50.37
Password expires    24.7.2023 9.50.37
Password changeable 5.1.2023 9.50.37
Password required    Yes
User may change password Yes

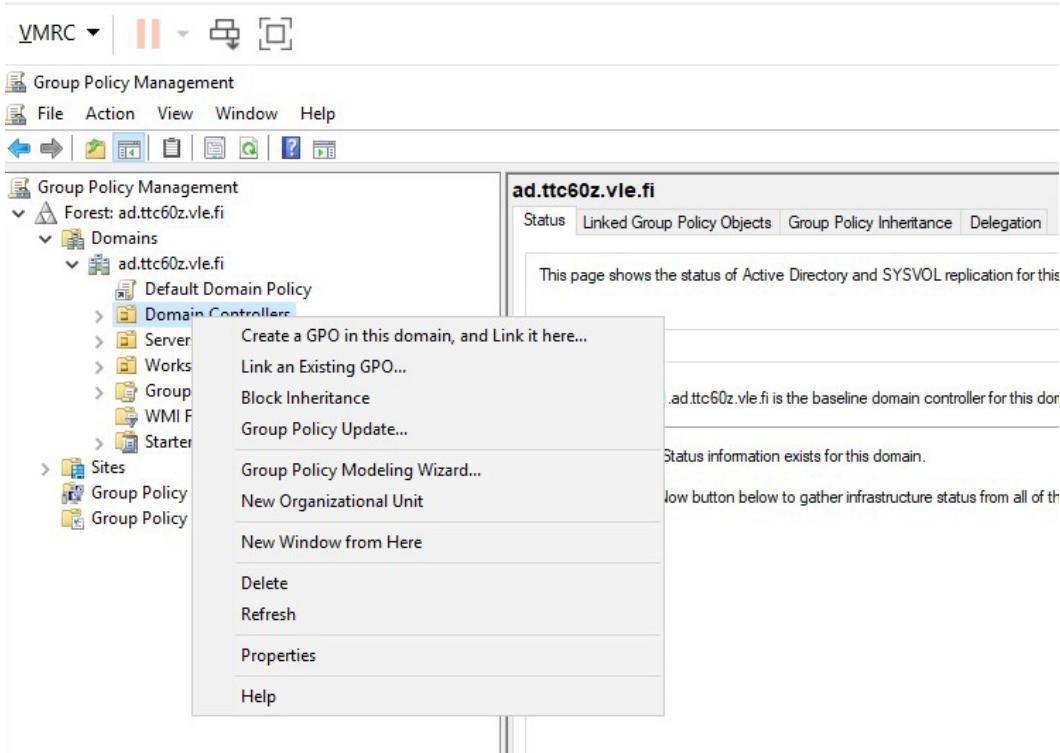
Workstations allowed All
Logon script
User profile
Home directory
Last logon          25.1.2023 15.44.01

```

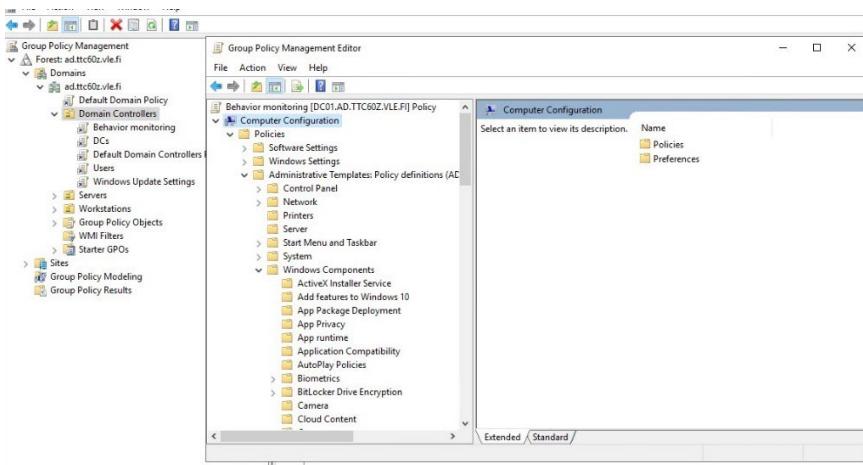
Kuva 16 Muutosten tarkistus

### 3.3 Estetään suojaamaton vieraskirjautuminen - Disable insecure guest logons

Estetään vieraana kirjautuminen, koska sen salliminen tekee haavoittuvaksi hyökkäyksille. Suojaamattomat vieraskirjautumiset voivat johtaa tietojen menetykseen, tietojen vioittumiseen ja altis-tumiseen haittaohjelmille. Lisäksi kaikki tietopalvelimelle suojaamattomalla vieraskirjautumisella kirjoitetut tiedot ovat mahdollisesti kaikkien verkon käyttäjien käytettävissä. (Guest access in SMB2 and SMB3 disabled by default in Windows 2023.) Esitetty kuvissa 15 & 16.

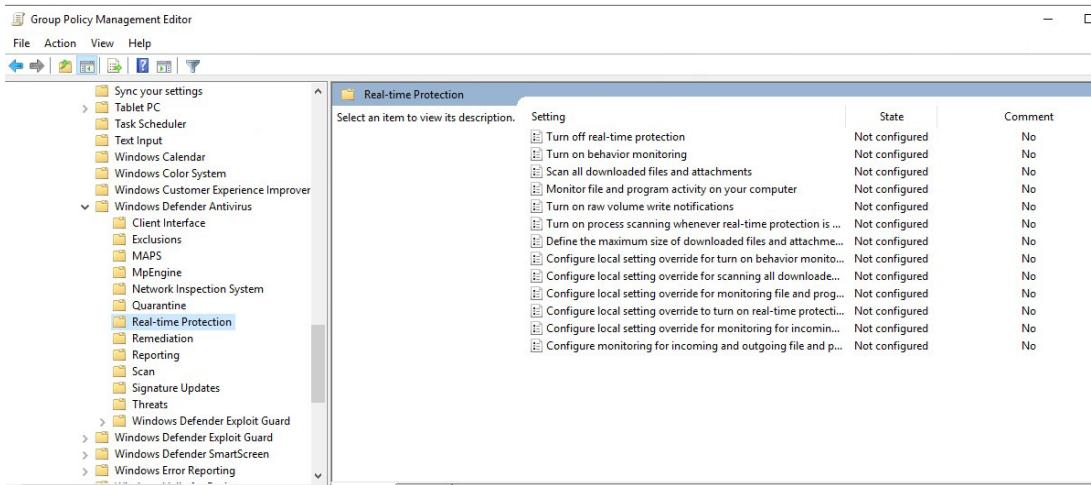


Kuva 15 Uuden GPO luominen

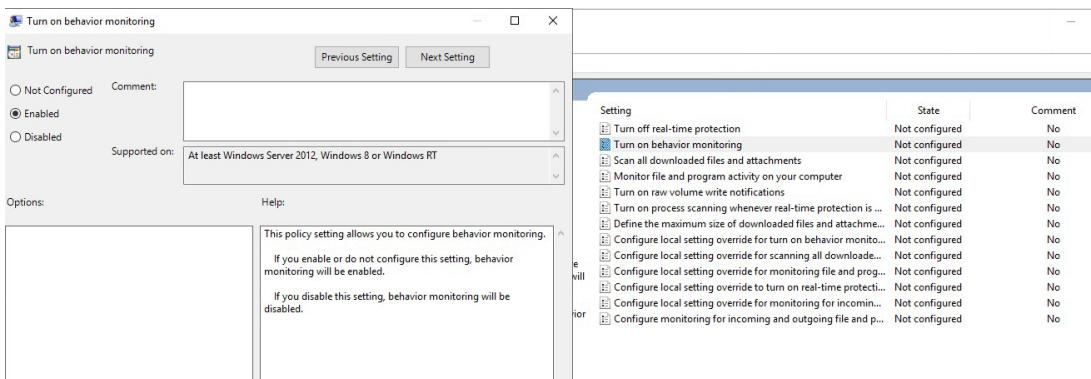


Kuva 16 Behavior Monitoring

Reitti määrittelyyn Computer Configuration – Policies – Administration Templates -Windows Components – Windows Defender Antivirus – Real-time Protection – Valittiin Turn On behavior monitoring – Enabled. Esitetty kuvissa 17 & 18.



Kuva 17 Real-time Protection

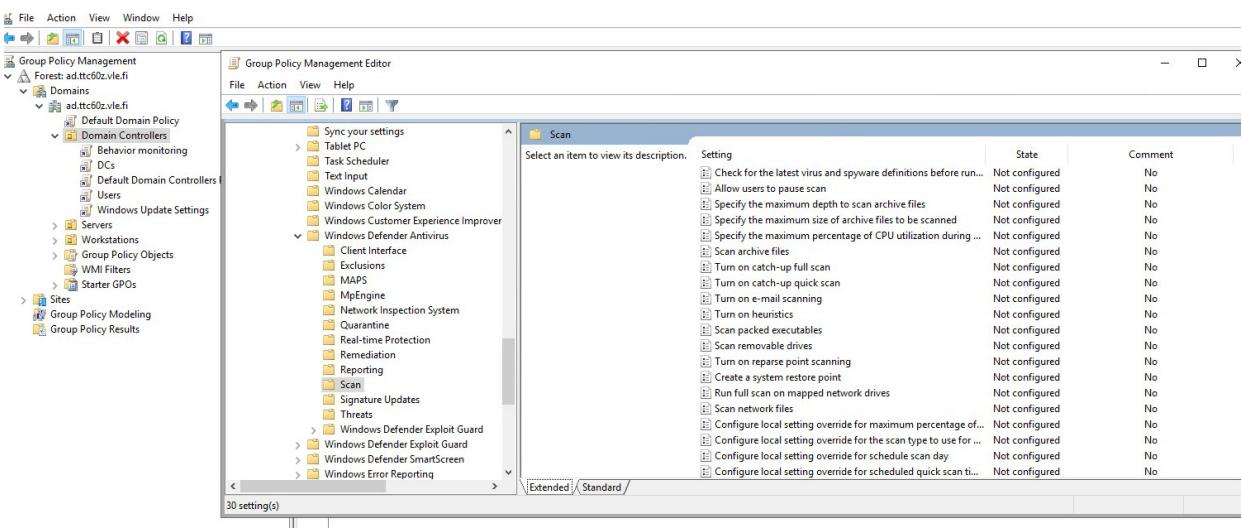


Kuva 18 Enabled - Behavior Monitoring

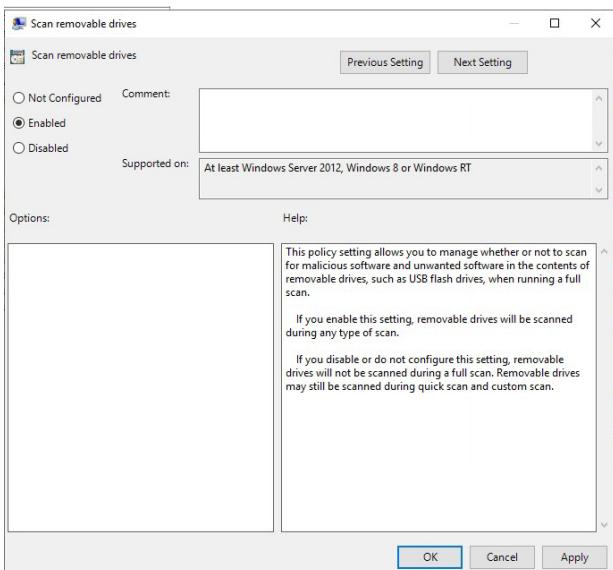
### 3.4 Skannaa irrotettavat asemat - Scan removable drives

Kun Windows Defender suorittaa ajoitetun tai manuaalisen koko järjestelmän tarkistuksen, se tarkistaa myös irrotettavien asemien, kuten esim. USB-muistitikkujen, sisällöstä viruksia tai muun tyypisiä haittaohjelmia ja ei-toivottuja ohjelmistoja (Configure Microsoft Defender Antivirus scanning options. 2022).

Reitti määrittelyyn Computer Configuration – Policies – Administration Templates -Windows Components – Windows Defender Antivirus – Scan – Valittu Scan removable drives – Enabled. Esitetty kuvissa 17 & 18.



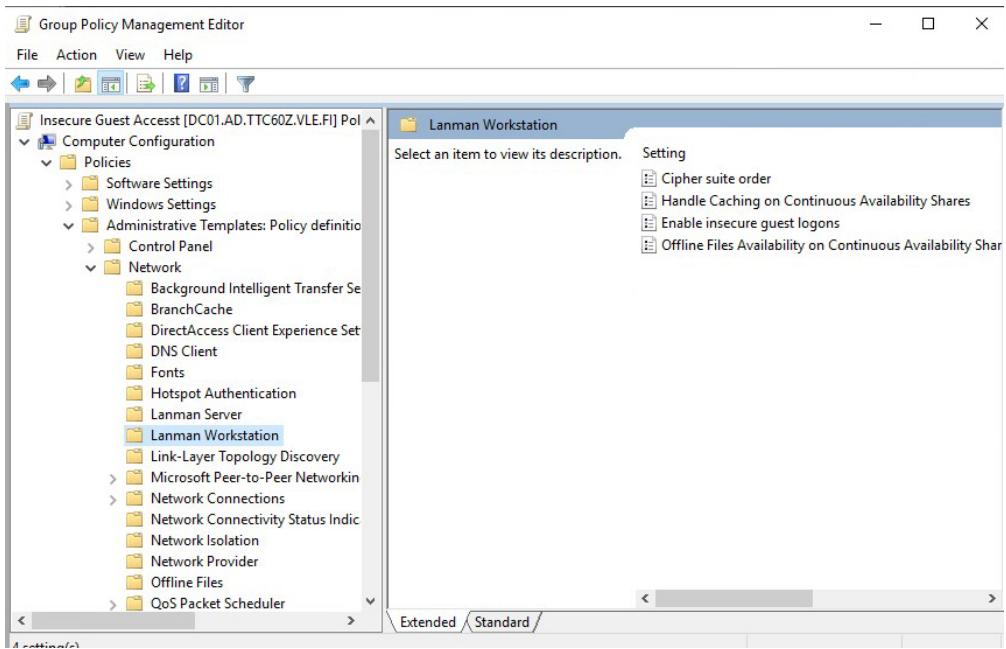
Kuva 17 Scan - Scan removable drives



Kuva 18 Enabled - Scan removable drivers

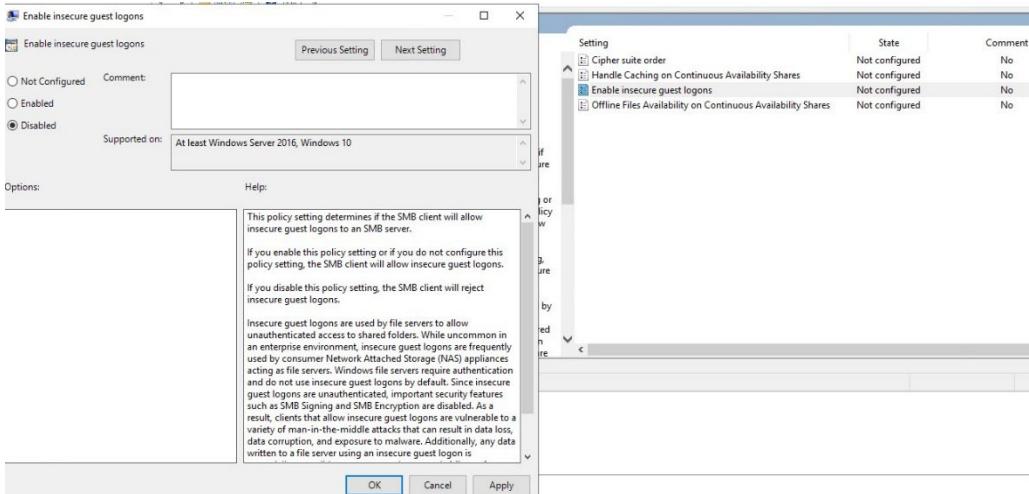
### 3.5 Käyttäytymisen seuranta - Behavior monitoring

Aina päällä oleva suojaus koostuu reaaliaikaisesta suojuksesta, käyttäytymisen seurannasta ja heuristiikasta haittaohjelmien tunnistamiseksi tunnettujen epäilyttävien ja haitallisten toimintojen perusteella. (Enable and configure Microsoft Defender Antivirus always-on protection in Group Policy 2022.)



Kuva 19 Insecure guest access – Lanman Workstation

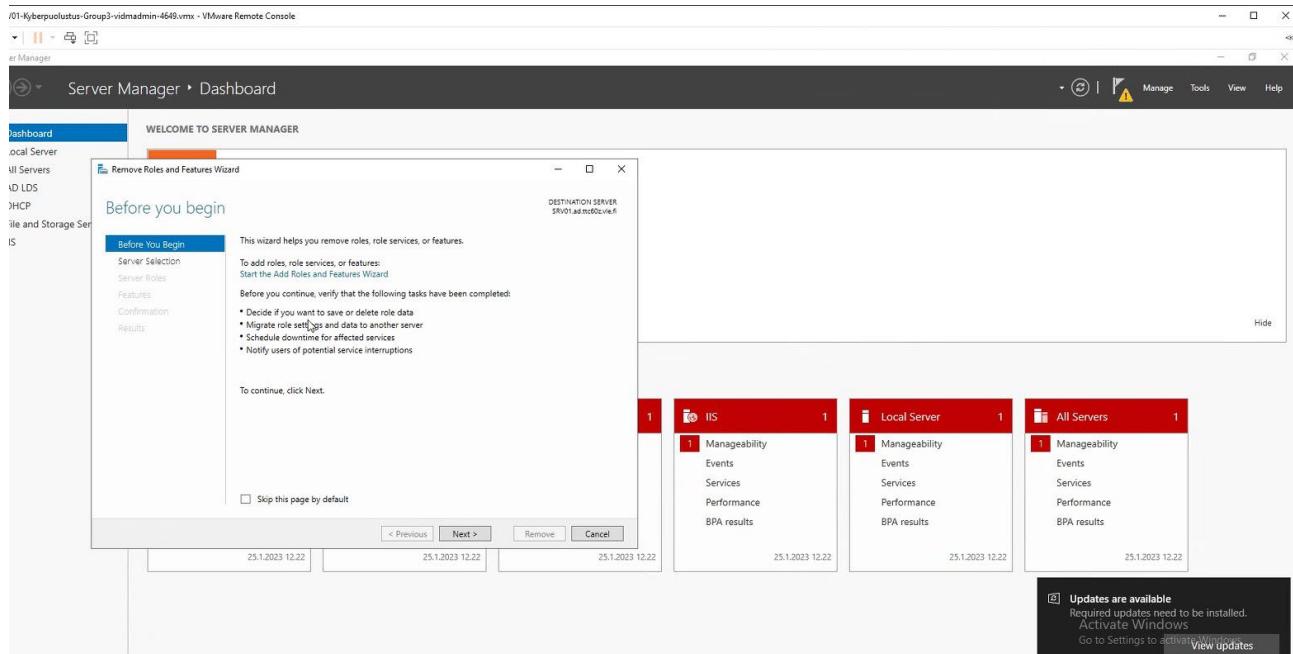
Reitti määrittelyyn Computer Configuration – Policies – Administration Templates - Network – Lanman Workstation – Valittuun Enable insecure guest logons – Disabled. Esitetty kuvissa 19 & 20.



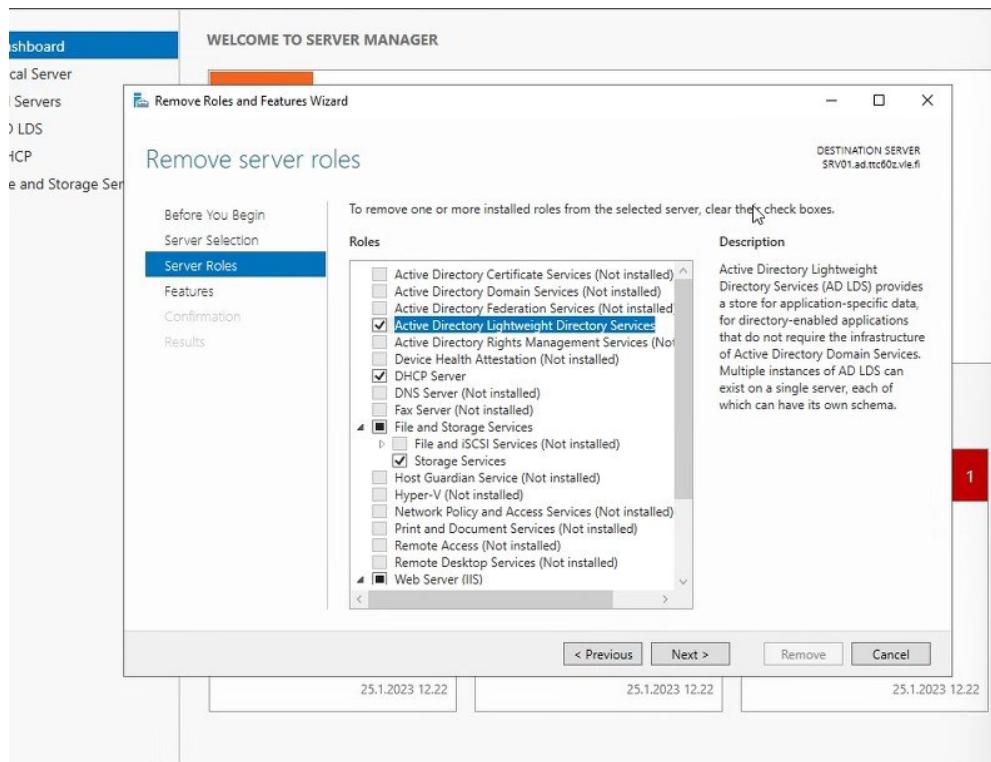
Kuva 20 Enable insecure guest logons – Disabled

## 4 FILE SERVERIN (SRV01) - KOHTALO

Ohjeistus organisaation johtoryhmältä on poistaa kaikki turhat roolit SRV01:ltä ja yritys tulee pitämään tämän jatkossa vain fileserverinä. Aloitettiin kirjautumalle SRV01:lle, esitetty kuvassa 21&22.

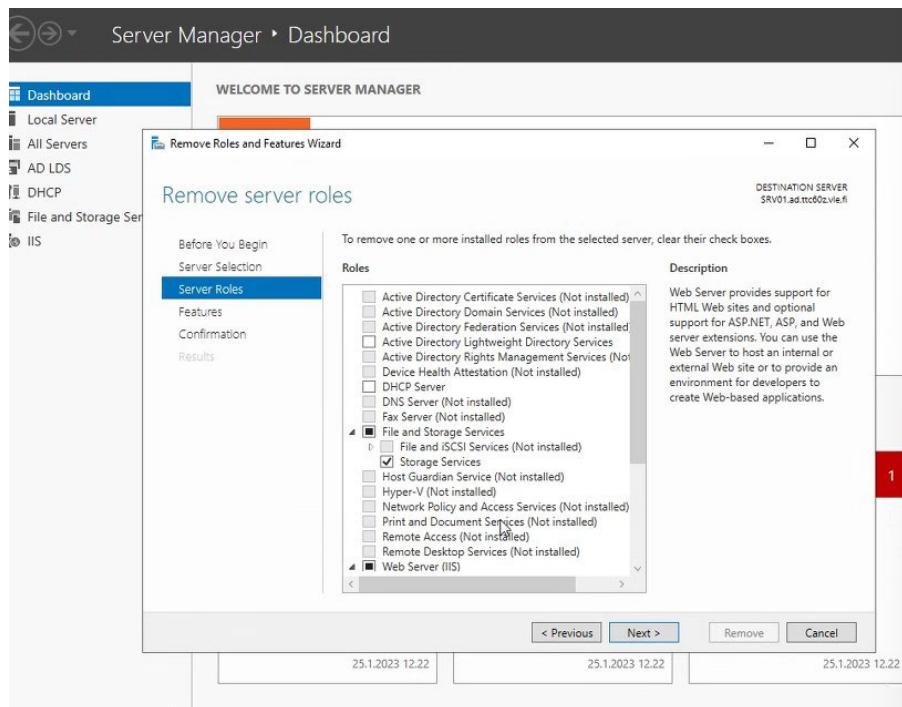


Kuva 21 Kirjautuminen SRV01

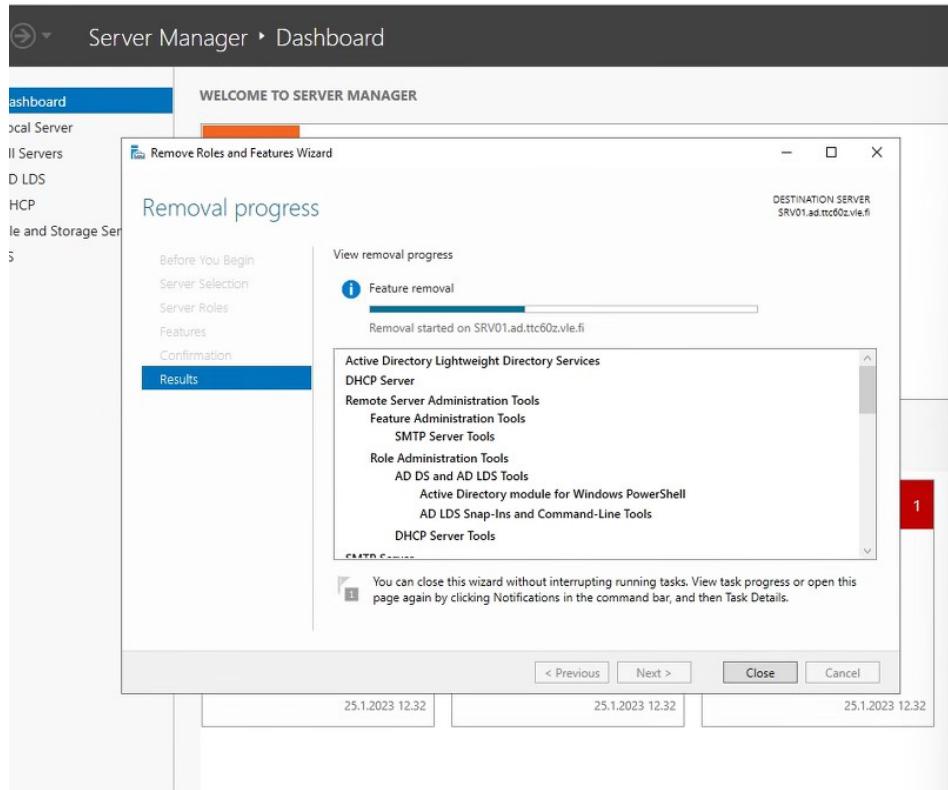


Kuva 22 Roles and Features – avaaminen

“Roles and Features” kautta poistettiin turhat ja jätettiin vain .net framework. Esitetty kuvissa 23 & 24.



Kuva 23 Poistetaan turhat



Kuva 24 Poisto käynnissä

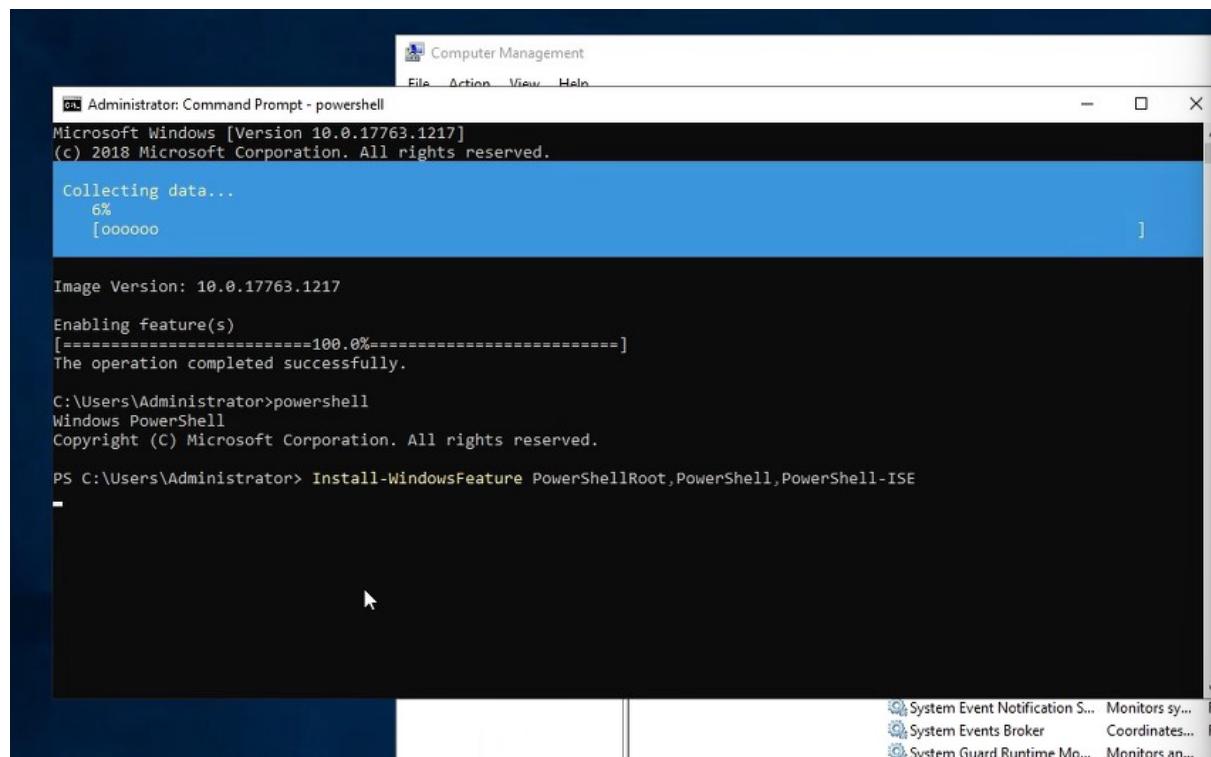
Turhien poiston jälkeen kaikki ominaisuudet eivät toimineet kunnolla tai niitä ei löytynyt, joten tehtiin lisäosan asennus uudestaan ongelman ratkaisemiseksi (.Net ominaisuus sekä Server Manager). Komennot (Command Prompt):

```
dism /online /enable-feature /featurename:NetFx4ServerFeatures /ALL
```

PowerShell

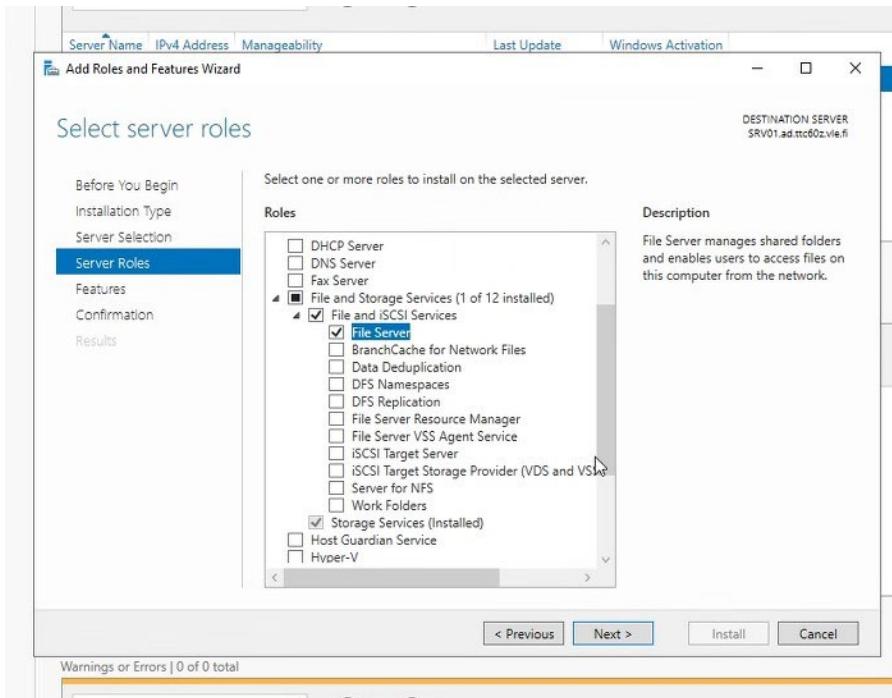
```
Install-WindowsFeature PowerShellRoot,PowerShell,PowerShell-ISE
```

(Sitten uudestaan käynnistys – restart ). Esitetty kuvassa 25.

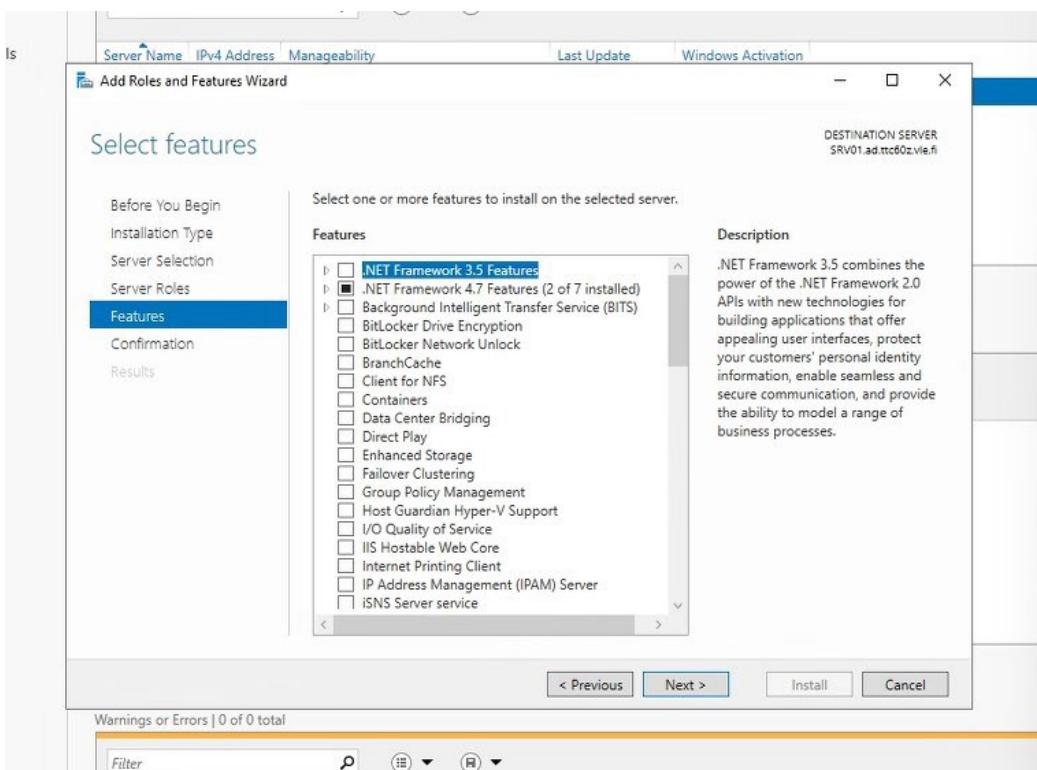


Kuva 25 PowerShell asennus

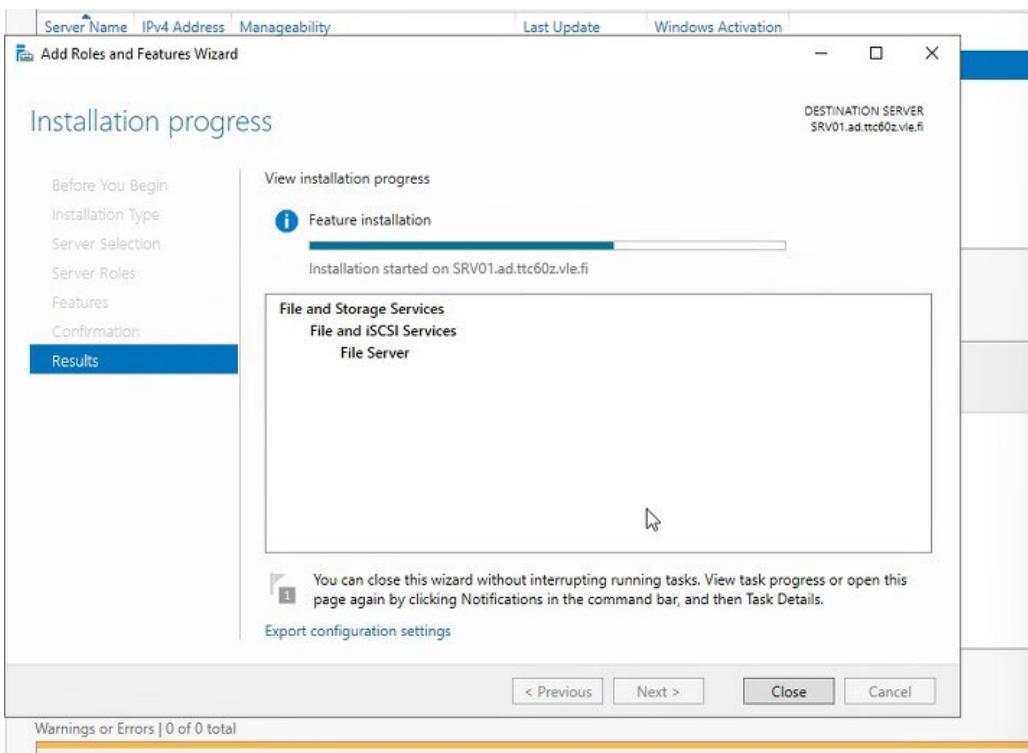
Kun asennus oli tehty uudestaan, tarkistettiin että kaikki tarvittavat asetukset/ohjelmat löytyvät hallintaan. Esitetty kuvissa 26 & 27.



Kuva 26 File Server - Asetuksien tarkistus uudestaan



Kuva 27 .Net asetuksien tarkastus



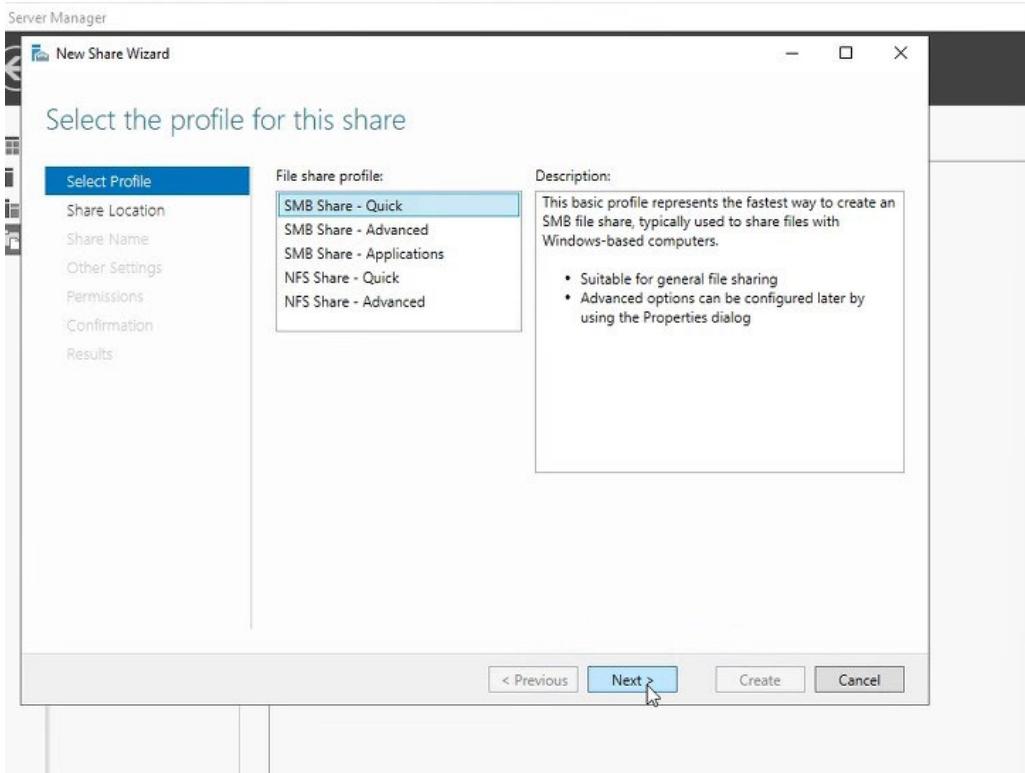
## Kuva 28 File Storage Services asennus

File and Storage Services tarvittavista ohjelmista/asetuksista puuttui File and Iscsi Services – File Server joka asennettiin. Esitetty kuvassa 28.

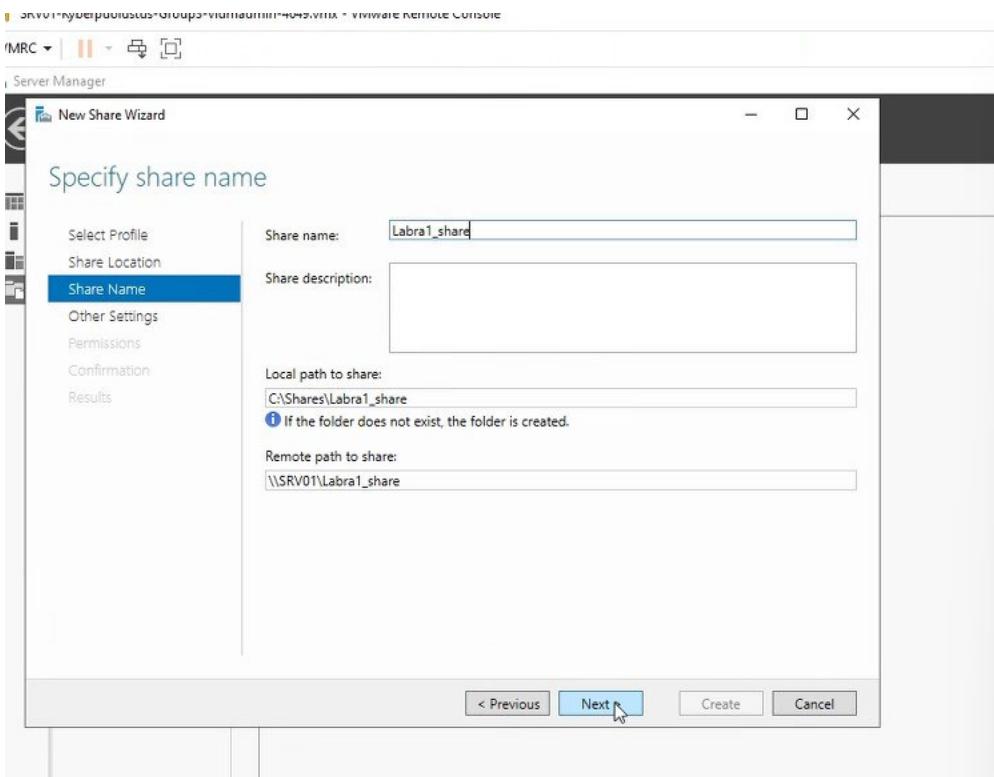
The screenshot shows the 'Server Manager' interface under 'File and Storage Services > Volumes > Disks'. The left sidebar has 'Servers', 'Volumes', 'Disks' (selected), 'Storage Pools', 'Shares', 'iSCSI', and 'Work Folders'. The 'DISKS' section shows 'All disks | 1 total' with one entry: 'SRV01 (1)' (Online, 90.0 GB, GPT, NVMe, VMware Virtual NVMe...). The 'VOLUMES' section shows 'Related Volumes | 3 total' with entries: 'C' (Fixed, 89.4 GB, 74.8 GB), '\\Volume\b6e...' (Fixed, 95.0 MB, 69.2 MB), and '\\Volume\af6...' (Fixed, 499 MB, 85.3 MB). The 'STORAGE POOL' section shows 'VMware Virtual NVMe Disk on SRV01' with the message 'No related storage pool exists.' Last refresh was on 25.1.2023 13:09:49.

## Kuva 29 Disks

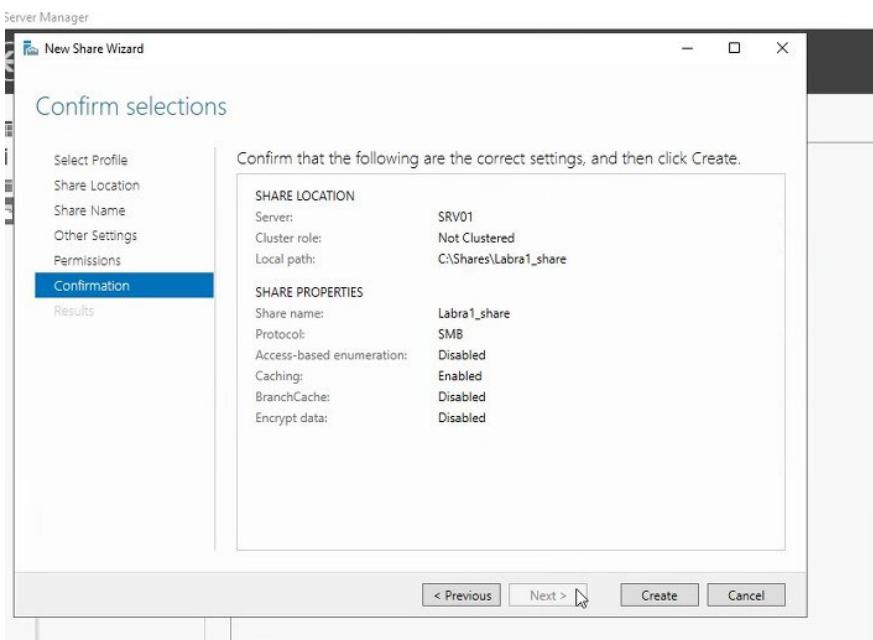
Tarkistettiin ohjeen mukaa tiedosto- ja tallennuspalveluista, että Volume välilehdessä kohdassa "Disks" on muodostunut rivi. Esitetty kuvassa 29. Sitten siirryttiin Shares-välilehdelle lisäämään uusi "share". Esitetty kuvissa 30-33.



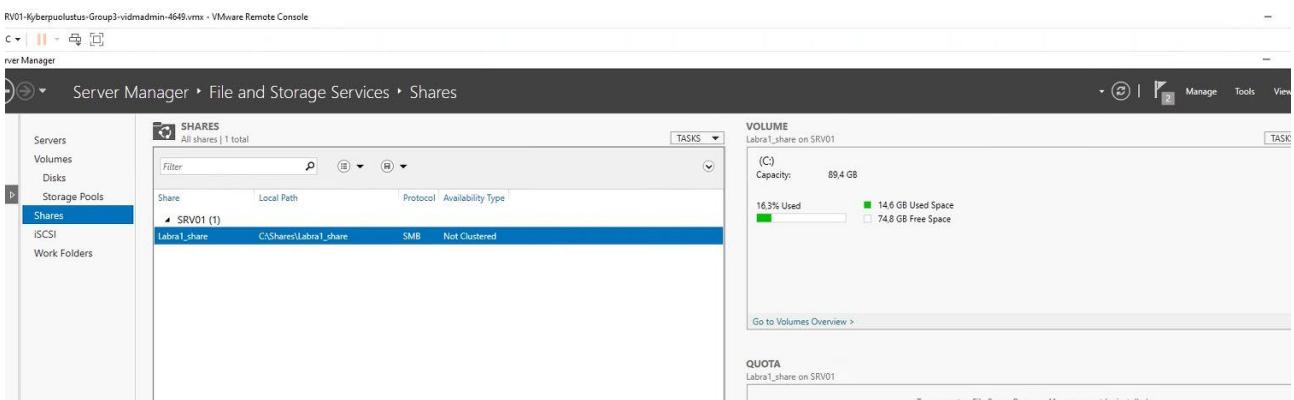
Kuva 30 SMB Share luontia



Kuva 31 Share nimi – Labra1\_share



Kuva 32 Valittujen tietojen vahvistus



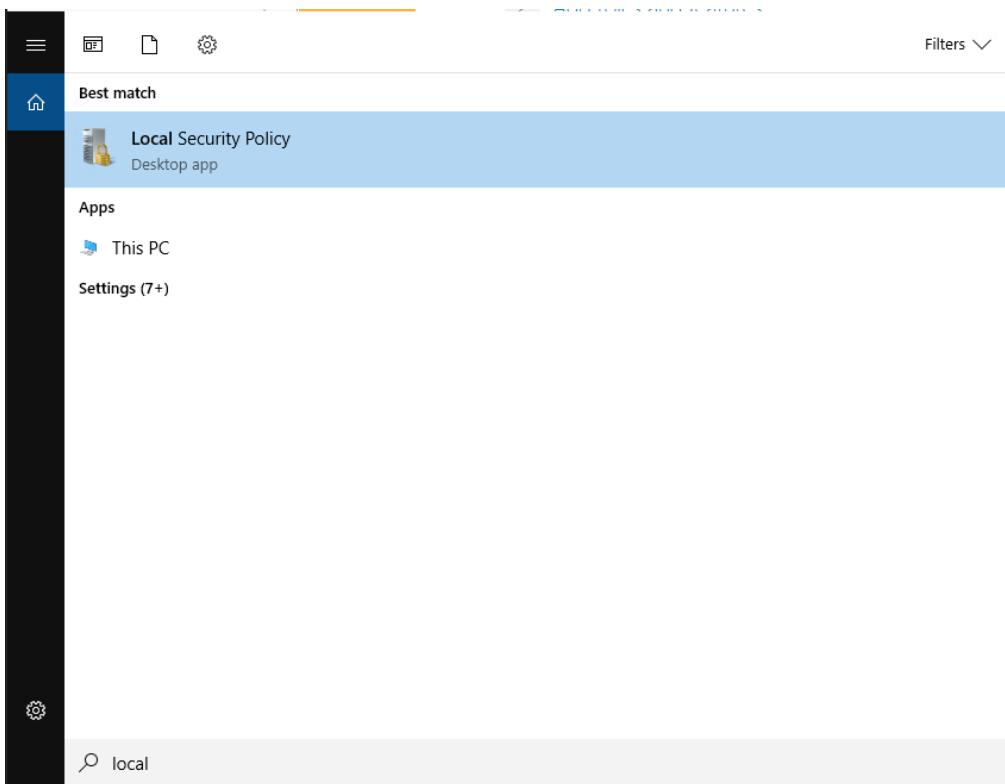
Kuva 33 Luotu Labra1\_share

## 5 FILE SERVER (SRV01) - KOVENNUKSET

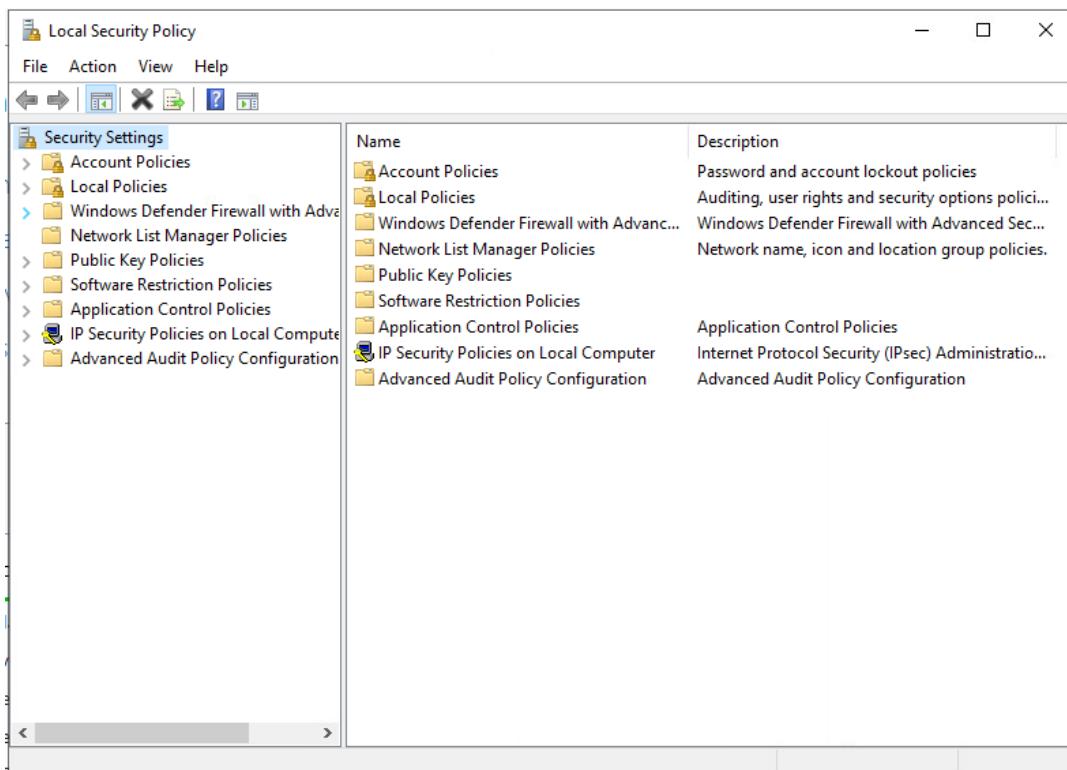
### 5.1 Sisäänsijautuminen

Otettaessa yhteys File Server – koneeseen kysytään käyttäjänimeä ja salasanaa. Oletusasetuksena ruudulla näkyy edellinen käyttäjänimi, jolla onnistuneesti kirjauduttiin. Jättämällä toimiva käyttäjä-nimi kaikkien nähtäväksi vaarantaa tietoturvallisuutta. (Bichel 2023)

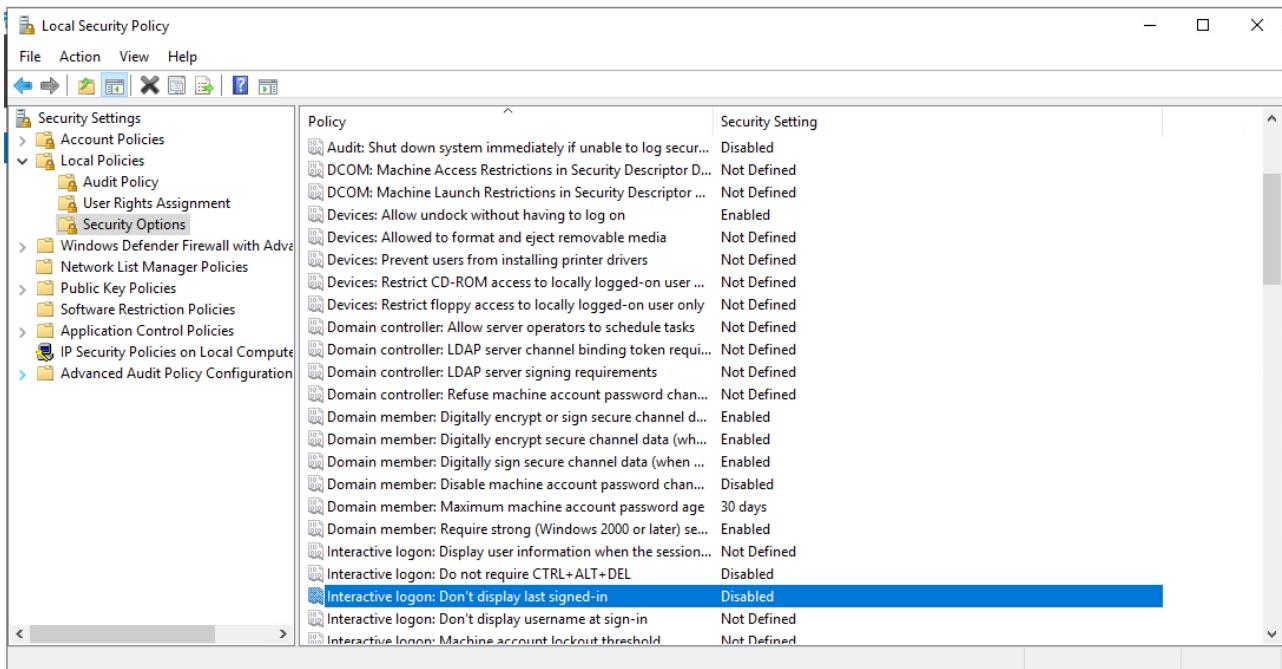
Muuttamalla "Interactive logon: Don't display last signed-in" – asetus käyttöön, ei edellisen käyttäjän käyttäjänimeä enää näytetä. Esitetyt kuvissa 34-37.



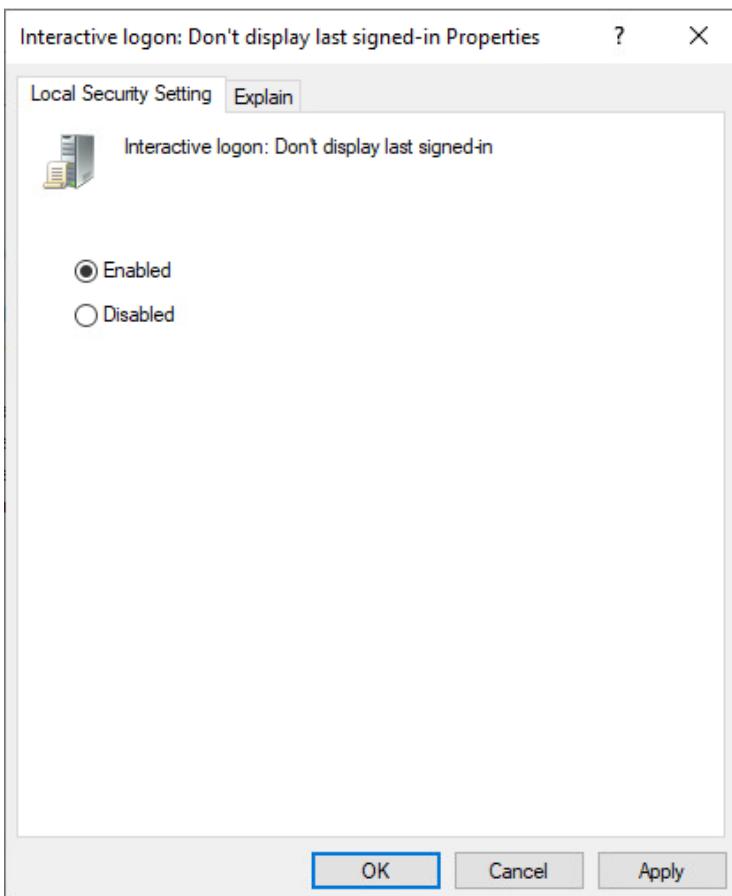
Kuva 34. Local Security Policy löytyy Windowsin Etsi-toiminnolla.



Kuva 35. Local Security Policy oletusikkuna.



Kuva 36. Local Policiesin alta Security Options ja tämän alta Interactive logon: Don't display last signed-in.

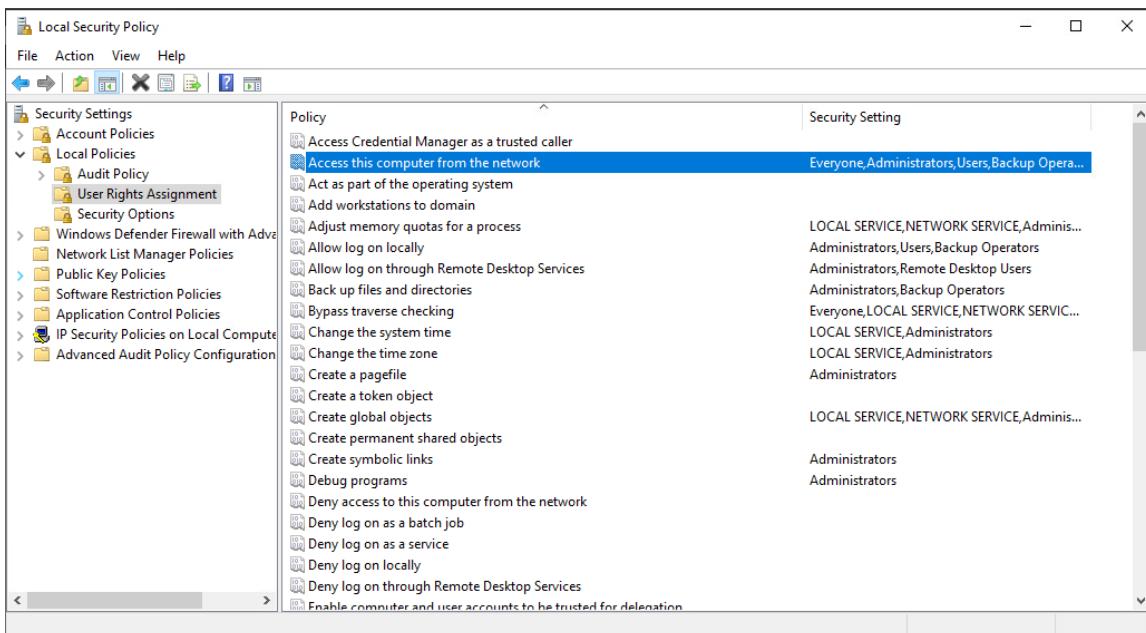


Kuva 37. Muutetaan asetus Enabled – tilaan

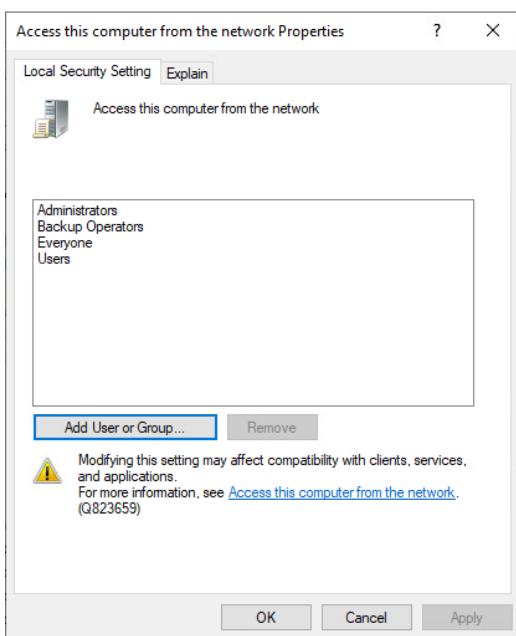
## 5.2 Yhteys verkon kautta

Tämä asetus, "Access this computer from the network", määrittelee millä käyttäjillä/ryhmillä on oikeus yhdistyä verkon kautta tähän tietokoneeseen. Suosituksena on, että lupa annetaan vain Järjestelmänvalvojalle sekä "Authenticated Users" – ryhmälle. (Pollack 2021)

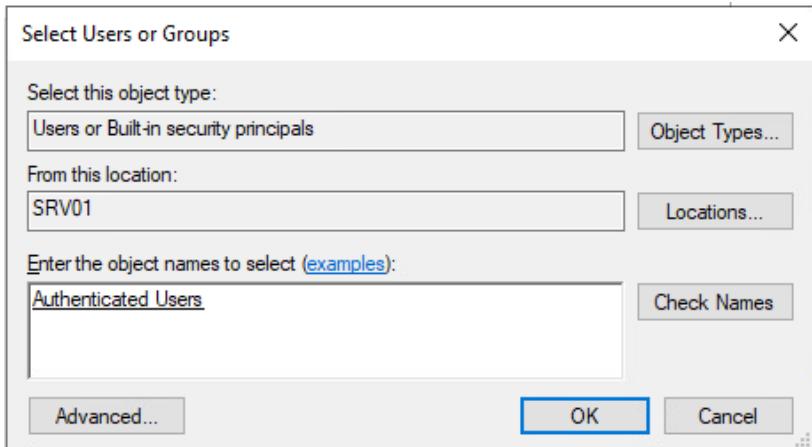
Jätimme luvan myös "Backup Operator"ille, koska tästä ei ollut mainintaa ohjeissa, joten oletimme sen olevan koulun puolelta asetettu. Esitetty kuvissa 38-41.



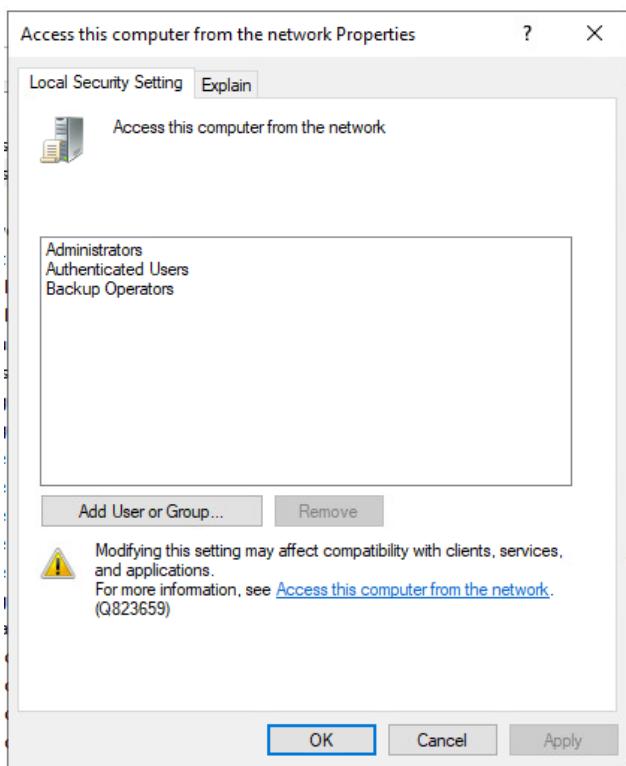
Kuva 38. "User Rights Assignment" ja tämän alta "Access this computer from the network"



Kuva 39. Käyttäjät joilla oletuksena oikeudet.



Kuva 40. Lisätään sallituksi käyttäjäksi "Authenticated Users".



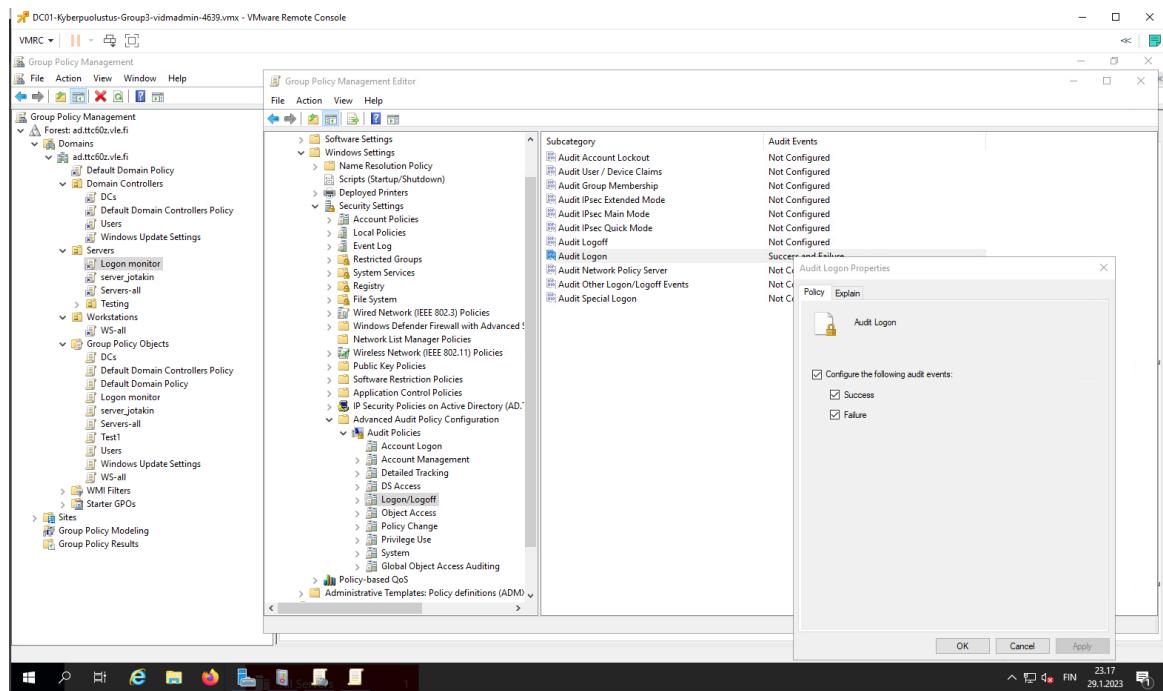
Kuva 41. Poistetaan sallituista käyttäjistä "Everyone" ja "Users".

### 5.3 Tilien kirjautumisten tarkkailu

File serverit pitävät yleensä sisällään paljon tietoa, minkä vuoksi niiden kovertaminen on tärkeää. Lähdimme etsimään ympäristössämme käytettävään File Serveriin (SRV01) yleispäteviä kovennuksia, joita esimerkiksi yritykset, jotka tällaisia servereitä omistavat voisivat käyttää. Apuna kovenosten löytämiseen käytimme Microsoftin SecCon-Frameworkia ja tarkemmin Level 1 Enterprise

Basic Security Configuration kohtaa. Löysimme Frameworkin Advanced Audit Policies kohdasta ominaisuuden, joka tarkkailee tilien sisäänsijautumista.

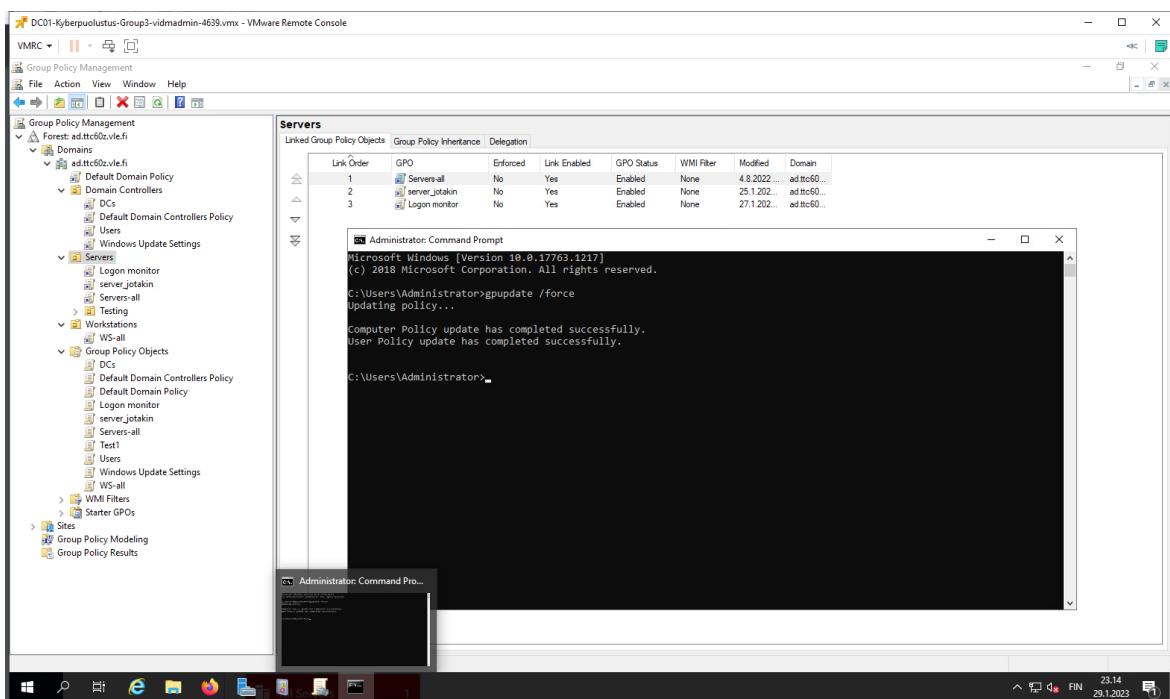
Kovennuksen avulla pystytään ennaltaehkäisemään kyberhyökkäyksiä tarkkailemalla epätavallisia kirjautumisaikoja, mutta myös helpottamaan kyberhyökkäyksen jälkeistä korjaustyötä tarkkailemalla hyökkäyksen tapahtuma-aikaa.



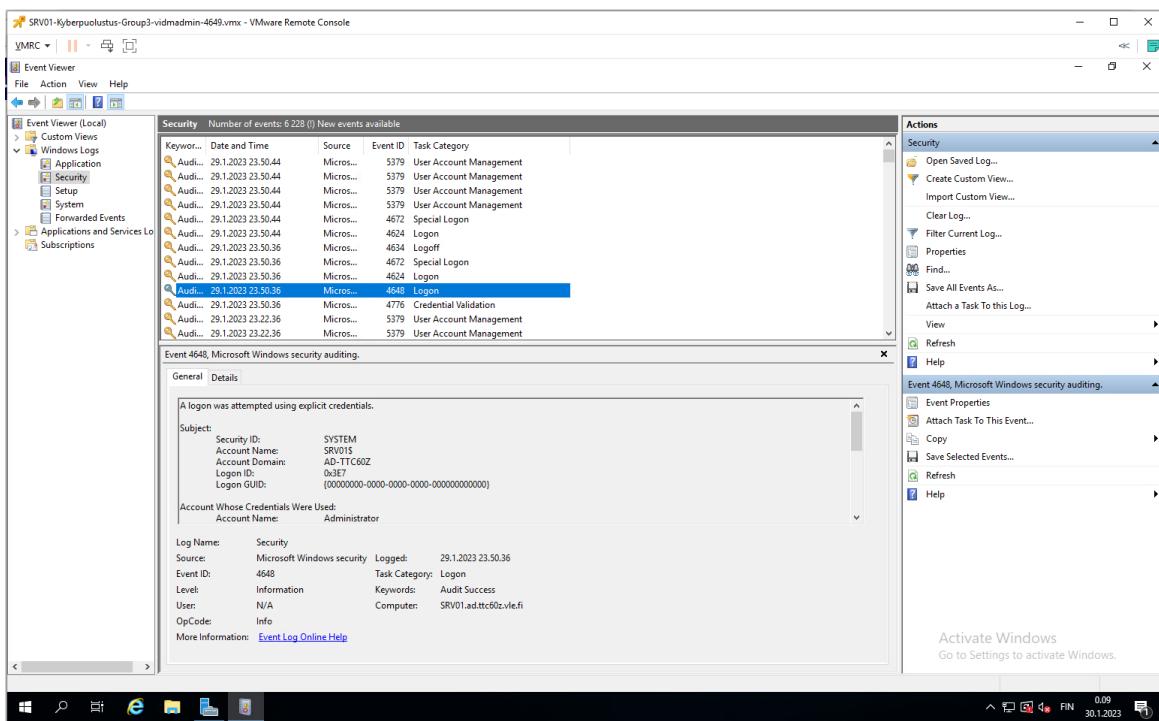
Kuva 42. Audit Logon Policyn käyttöönotto.

Luotiin uusi Group Policy Object ja linkitettiin se Servers domainin alle, että saadaan policy käyttöön Fileserverille. Audit logon policy löytyy kohdasta: Policies -> Windows settings -> Security settings -> Advanced Audit Policy Configuration -> Audit Policies -> Logon/Logoff -> Audit Logon. Audit Logon Policystä otettiin käyttöön molemmat; onnistunut ja epäonnistunut kirjautuminen.

Esitetty kuvassa 42.



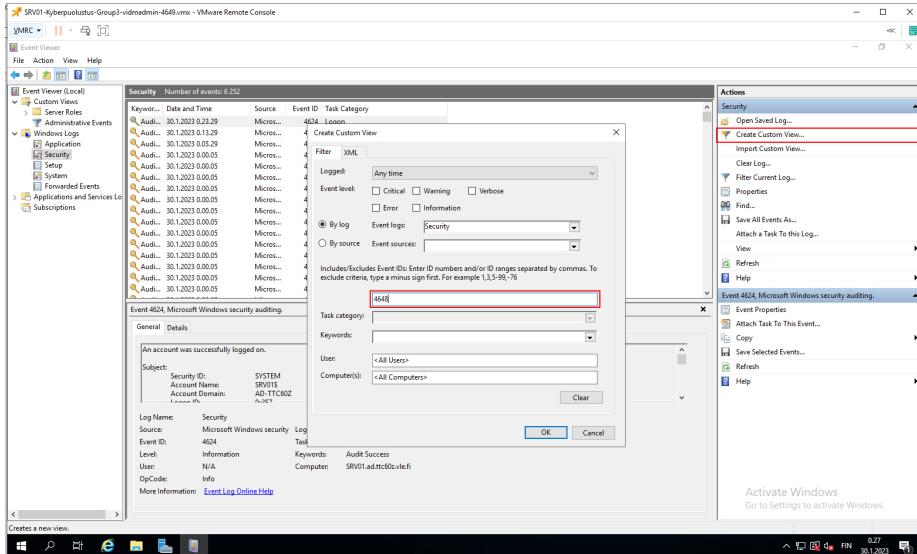
Kuva 43. Ajettiin gpupdate /force jotta policy tulee voimaan.



Kuva 44. Tili kirjautumisten tarkkailu

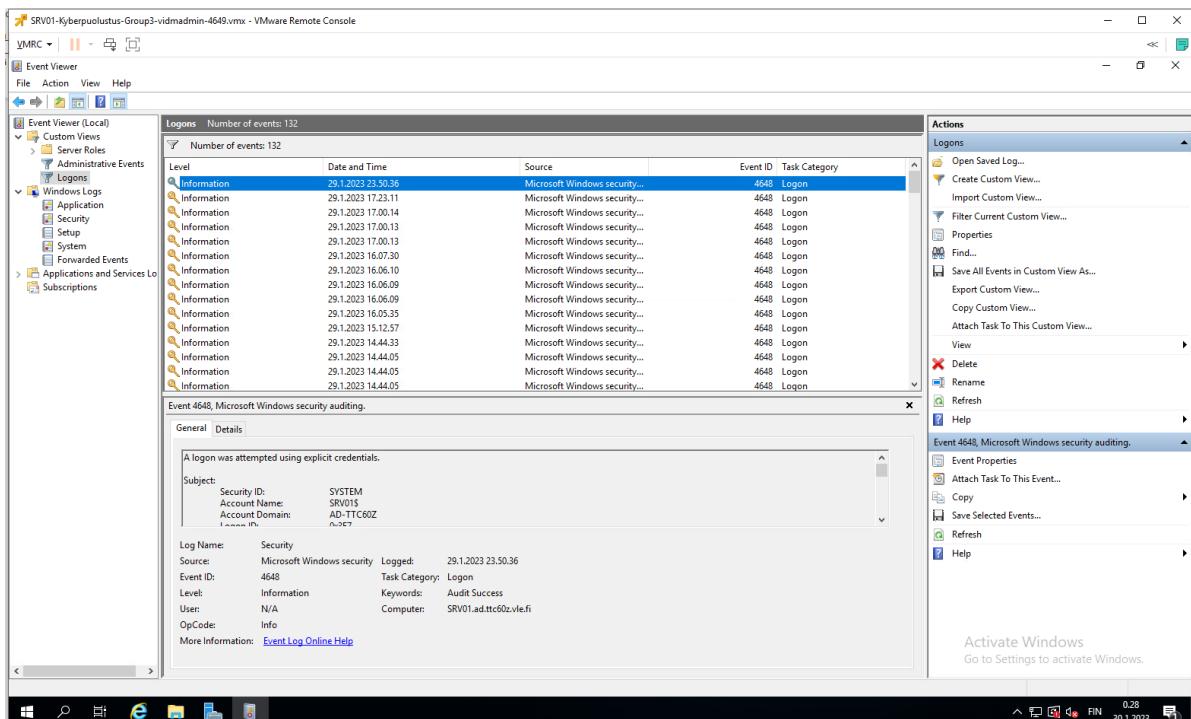
Audit Logon Policyn käyttöönnoton onnistumista ja tilien kirjautumisia File Serverille pystytään tarkkailemaan Event Viewer nimisestä Windows sovelluksesta koneella jolle Audit Policy on asetettu. Esitetty kuvassa 44.

Tilille kirjautumiset näkyvät Event Viewerissä Security välilehdellä ID:llä 4648 ”A Logon was attempted using explicit credentials”. Tapahtuma näyttää tilille kirjautumisesta erilaisia tietoja, esimerkiksi mihin aikaan kirjautuminen on tapahtunut sekä kirjautuneen tilin nimen. Esitetty kuvassa 45.



Kuva 45. Tapahtumien filtteröinti

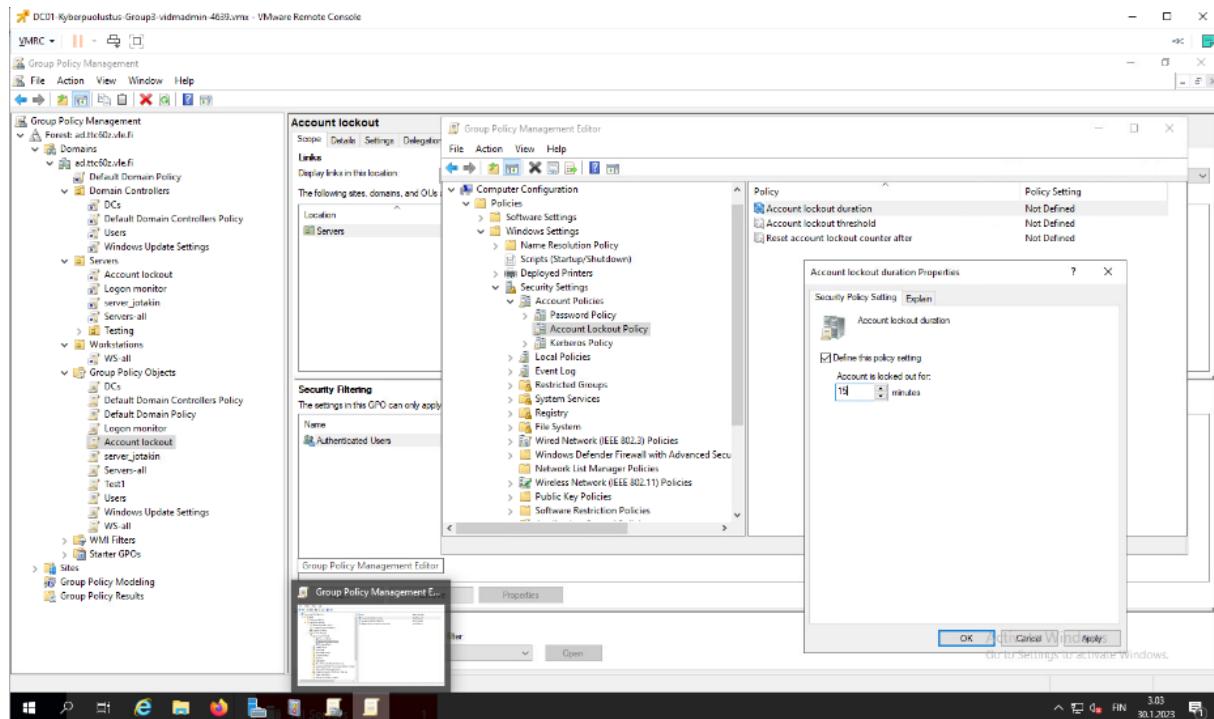
Koska Windows Event Viewer näyttää paljon erilaisia tapahtumia on järkevää tehdä filtteröintiä, jotta nähdään vain se mitä halutaan. Kuvassa 46 on esitetty esimerkki, miten tilien kirjautumiset pystytään suodattamaan.



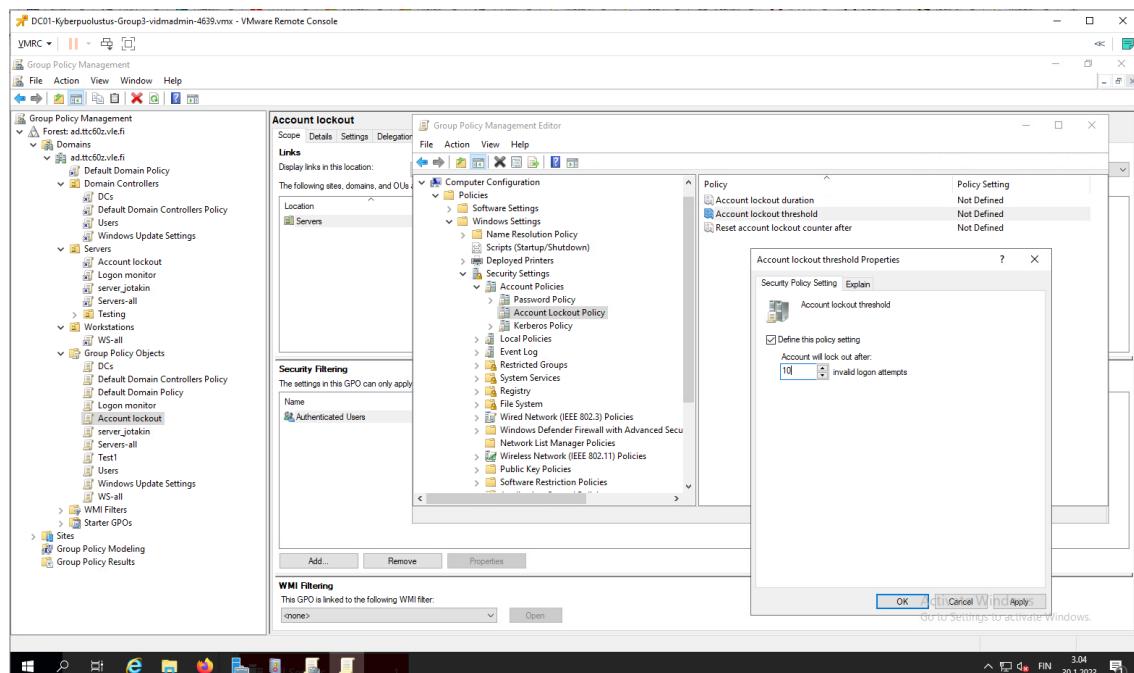
Kuva 46. Filtteröity näkymä

## 5.4 Tilin lukituskynnys

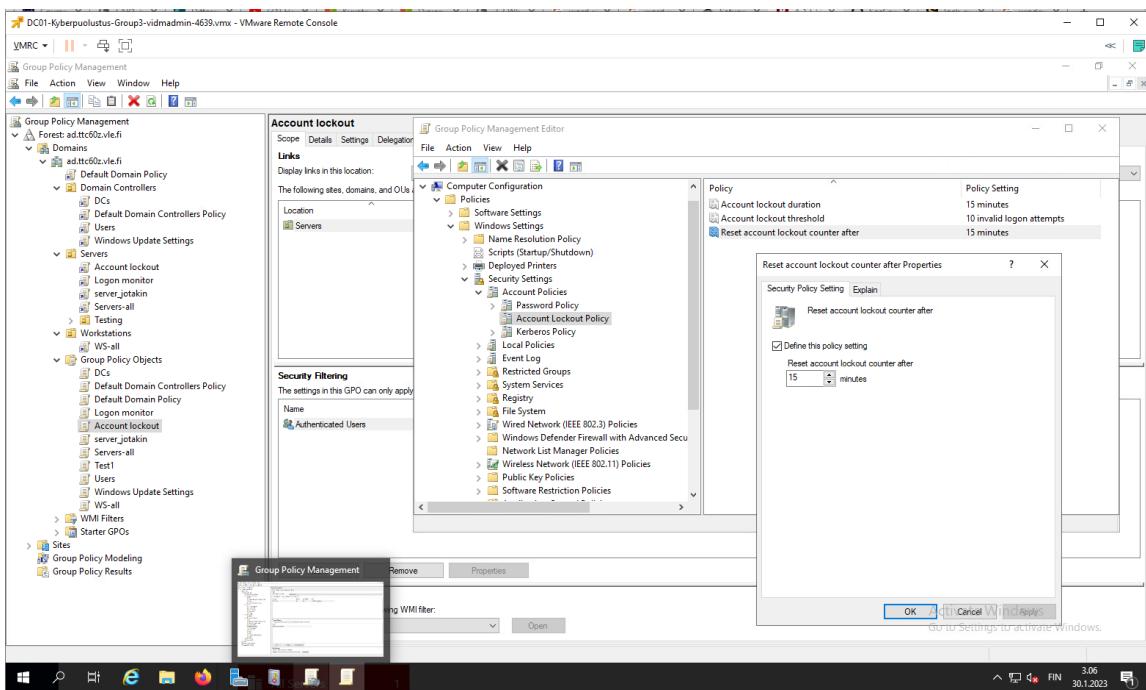
Tilien kirjautumisten tarkkailun lisäksi tileille on hyvä asettaa lukituskynnys. Lukituskynnys säännöllä pystytään määräämään, kuinka monta kertaa käyttäjä saa syöttää salasanan ennenkö tili lukiotaan. Lukituskynnys kovennus hankaloittaa esimerkiksi brute-force tapaisia hyökkäyksiä, joissa kiertetaan kokeilemalla syöttää monia eri salasanoja lyhyen ajan sisällä.



Kuva 47. Account lockout määritys

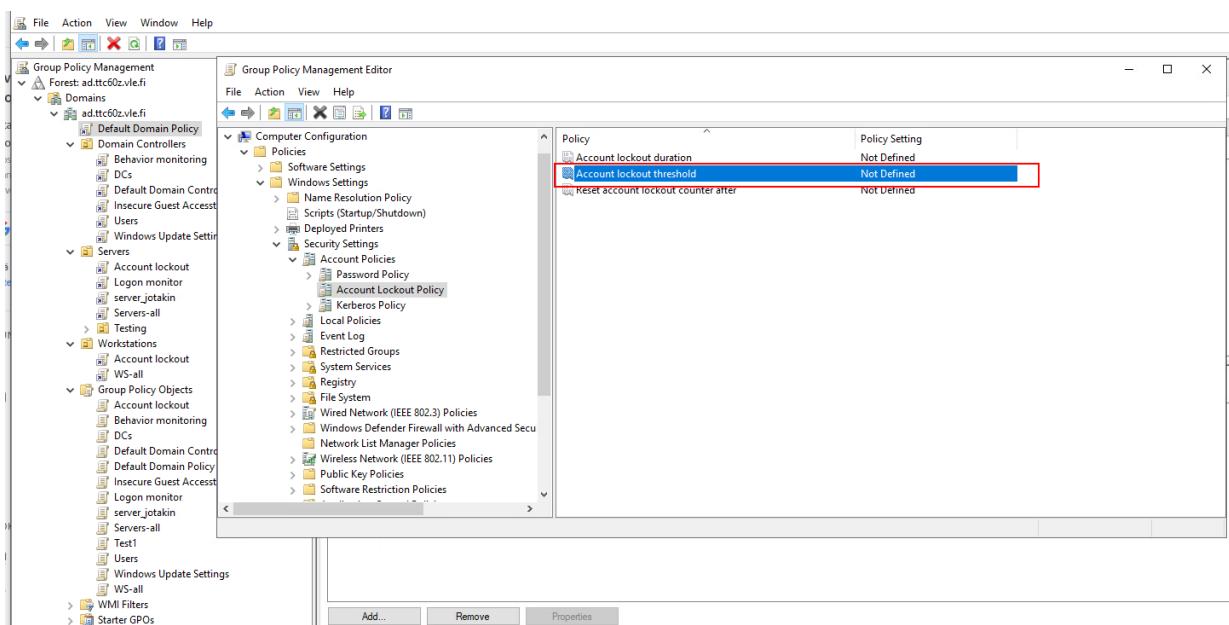


Kuva 48. Account lockout threshold määritys



Kuva 49. Reset account lockout counter after määritys

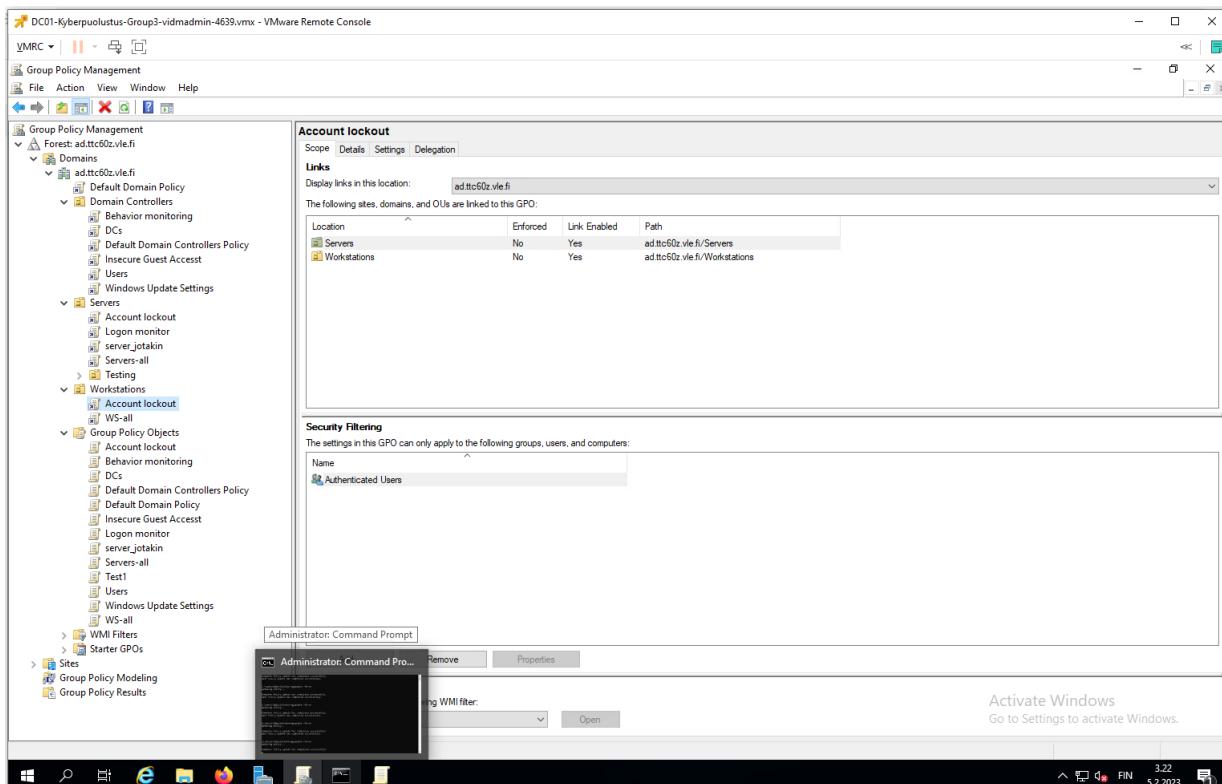
Tilin lukituskynnyksen säännön määrittämiseksi täytyi konfiguroida kolme asetusta, jotka löytyvät kuvista 47, 48 ja 49. Account Lockout policy eli tilin lukituskynnyksen asetukset löytyvät Group policy managerista: Policies -> Windows Settings -> Security Settings -> Account Policies -> Account Lockout Policy. Tilin lukitus asetettiin 10 väärään yritykseen. Tilin lukitus kannattaa pitää suhteellisen korkealla, ettei turhia lukituksia synny, esimerkiksi jo 10 väärää yritystä suojaa varmasti hyvin brute-force iskuilta. Lukituksen ja sen resetointi asetettiin 15 minuuttiin.



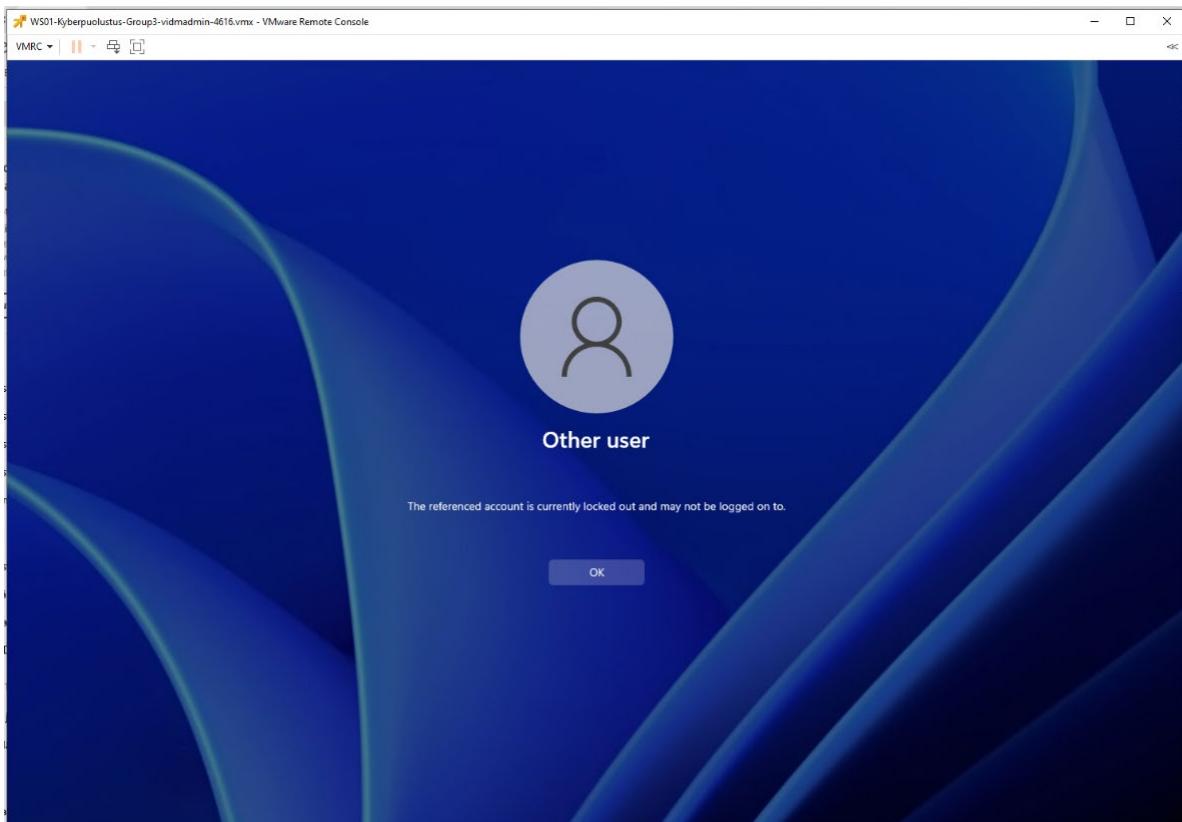
Kuva 50. Group Domain Policy Account lockout määritysten

Testatessa tilin lukituskynnyksen toimimista törmäsimeen ongelmaan, tili ei lukittautunut, vaikka salasanani syötti kuinka monta kertaa tahansa. Ongelma korjaantui osin, kun löysimme, että Account Lockout Policy oli määritelty jo Default Domain Policyssä. Account lockout threshold oli asetettu nollaan mikä tarkoittaa, ettei tili ikinä lukitu. Asetettiin siis Default Domain Policystä kaikki Account lockout määritykset pois. Esitetty kuvassa 50. (KB5020282—Account lockout available for built-in local administrators)

Account lockout ei kuitenkaan toiminut File serverillä SRV01 vieläkään. Lisätietoa netisä hakemalla löysimme Microsoftin sivuilta, ettei account lockout toimi Administrator käyttäjille. Sivuilla mainittiin kuitenkin, että kyseinen ominaisuus olisi tulossa. Kovennus ei siis osoittautunut lopulta hirveän hyödylliseksi ympäristöömme, sillä melkein kaikki ympäristöömme käyttäjät ovat Administrator käyttäjiä.



Kuva 51. Account lockout policy workstation domainiin



Kuva 52. User1 Account locked WS domainissa.

Halusimme vielä testata kuitenkin account lockout policyn toimintaa, joten linkitimme sen Workstations domainin alle. Esitetty kuvassa 51. Workstation domainissa saatiin kovennus toimimaan testatessa väärää tunnuksia tarpeeksi monta kertaa, kun kirjauduttiin User1, joka ei ollut domainin Administrator. Esitetty kuvassa 52.

## 6 POHDINTA

Harjoitustyön tavoitteena oli harjoitella ryhmätyönä VLE-ympäristöön Active Directoryn (AD) koventamista. Ryhmä sai valita itse kovennusohjeen ja mitä kovennuksia toteutti VLE ympäristössä oleville DC01:lle (IP 10.3.0.10) ja SRV01:lle (IP 10.3.0.12). Kovennusohjeeksi valikoitui Microsoftin SecCon-Framework ja tarkemmin Level 1 Enterprise Basic Security Configuration. Harjoituksen aikana SRV01 tyhjennettiin turhasta ja laitettiin se toimimaan vain fileserverinä. Harjoitustyössä käytettiin lisäksi läpi teoriaa koventamisesta, Active Directorysta, Microsoft Best Practices Analyzerista, PIM & PAMsta sekä JIT & JEAstaa.

Harjoitustyön aloittaminen oli ohjeistettu hyvin, mutta varmistimme vielä opettajalta millaiset kovennukset voimme valita, ettemme vaikuta negatiivisesti VLE ympäristön toimintaan. Tehtävänannon tarkentamisen jälkeen haasteeksi osoittautui löytää yksinkertaiset kovennukset harjoittelemaan. Ryhmän jäsenille aihealue oli uusi, joten pieni epävarmuus aiheutti epäröintiä ja pelkona oli koentaa ympäristöä liikaa. Tutkimme tarkasti kaikki kovennukset mitä teimme, jotta varmasti ymmärrämme sen vaikutuksen. Kovennuksia tehtiin yhteensä yhdeksän kappaletta, keskimääräisesti kaksi kappaletta per ryhmän jäsen.

Kovennuksien valitsemisen jälkeen harjoitustyö oli yksinkertainen ja ympäristö looginen käyttää. Ongelmatilanteita ei tullut kuin kerran, kun koitimme tehdä kovennusta, jota meillä ei ollutkaan oikeuksia toteuttaa. Ongelma ratkaistiin nopeasti valitsemalla toinen kovennus. Muutaman kovennuksen jälkeen ymmärrys miten koventamiset tehdään sekä niiden tärkeys antoivat motivaatiota myös ryhmän jäsenille oman henkilökohtaisen ympäristön koventamiseen.

Ajoimme harjoitustyön alussa ja lopussa Microsoft Best Practice Analyzerin ja tulokset olivat samat 8/42 varoitusta eli todennäköisesti tekemämme kovennukset olivat ensinnäkin määrällisesti liian vähäiset sekä laadullisesti ne vaikuttaneet tuloksissa mihinkään suuntaan.

Ajankäytön suhteen harjoitus oli nopea toteuttaa ympäristöön, mutta käytimme hieman liikaa aikaa itse kovennuksien valitsemiseen. Ensimmäisten kovennuksien tekemisen jälkeen, ryhmän itsevarmuus kasvoi selkeästi ja jatkossa koventamisten tekeminen ei aiheuta enää niin paljon epäröintiä.

## Lähteet

Allen, Robert 2022. How to Run Best Practices Analyzer using PowerSHell. Active Directory Pro. Julkaistu 24.4.2022. Viitattu 2.2.2023. <https://activedirectorypro.com/best-practices-analyzer-powershell/>

Configure Microsoft Defender Antivirus scanning options. 2022. Microsoftin verkkosivut. Julkaistu 29.9.2022. Viitattu 29.1.2023. <https://learn.microsoft.com/en-us/microsoft-365/security:defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide>

Enable and configure Microsoft Defender Antivirus always-on protection in Group Policy. 2022. Microsoftin verkkosivut. Julkaistu 20.10.2022. Viitattu 29.1.2023. <https://learn.microsoft.com/en-us/microsoft-365/security:defender-endpoint/configure-real-time-protection-microsoft-defender-antivirus?view=o365-worldwide>

Guest access in SMB2 and SMB3 disabled by default in Windows. 2023. Microsoftin verkkosivut. Julkaistu 28.1.2023. Viitattu 29.1.2023. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/guest-access-in-smb2-is-disabled-by-default>

How Often Should You Change Your Passwords?. McAfee verkkosivut n.d. Viitattu 4.2.2023. <https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/>

Interactive logon: Don't display last signed-in. 2023. Microsoftin verkkosivut. Julkaistu 9.1.2023. Viitattu 29.1.2023. <https://learn.microsoft.com/fi-fi/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name>

Just Enough Administration. 2022. Microsoftin verkkosivut. Julkaistu 17.11.2022. <https://learn.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.3>

KB5020282—Account lockout available for built-in local administrators. Microsoftin verkkosivut n.d. Viitattu 5.2023. <https://support.microsoft.com/en-us/topic/kb5020282-account-lockout-available-for-built-in-local-administrators-bce45c4d-f28d-43ad-b6fe-70156cb2dc00>

Keski-Simonen, T. 2016. PowerShell: Windows Server 2016 ja Active Directory hallinta. Opinnäytetyö, AMK. Haaga-Helia Ammattikorkeakoulu, tietojenkäsittelyn koulutusohjelma. Viitattu 3.2.2023. [https://www.thesaurus.fi/bitstream/handle/10024/150000/Keski-Simonen\\_Teemu.pdf?sequence=1&isAllowed=y](https://www.thesaurus.fi/bitstream/handle/10024/150000/Keski-Simonen_Teemu.pdf?sequence=1&isAllowed=y)

Katakri 2020: tietoturvallisuuden auditointityökalu viranomaisille. Kansallinen turvallisuusviranomainen. Helsinki. Viitattu 4.2.2023. [https://um.fi/documents/35732/0/Katakri+-+2020\\_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246](https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246)

Kuokkanen, A. 2020. Newcomer's introduction to Privileged Access Management. Opinnäytetyö, AMK. Jyväskylän Ammattikorkeakoulu, tekniikan ala, tieto- ja viestintäteknikan tutkinto-ohjelma. Viitattu 29.1.2023. [https://www.thesaurus.fi/bitstream/handle/10024/348503/Opinnaytetyo\\_Kuokkanen\\_Antti.pdf?sequence=2&isAllowed=y](https://www.thesaurus.fi/bitstream/handle/10024/348503/Opinnaytetyo_Kuokkanen_Antti.pdf?sequence=2&isAllowed=y)

SecCon-Framework 2019. Introducing the security configuration framework. Microsoft Github käyttäjätunnus. Viitattu 4.2.2023. <https://github.com/microsoft/SecCon-Framework/blob/master/windows-security-configuration-framework.md>

Simos, M. & Davies, J. 2022. Administration. Microsoftin verkkosivut. Julkaistu 2.2.2022. Viitattu 4.2.2023. <https://learn.microsoft.com/en-us/security/compass/critical-impact-accounts>

Pollack, Keren 2021. Access This Computer From the Network – Best Practices for DC and Member Servers. CalCom. <https://www.calcomsoftware.com/policy-expert-access-this-computer-from-the-network-best-practices-for-dc-and-member-servers/>

Run Best Practices Analyzer Scans and Manage Scan Results. 2023. Microsoftin verkkosivut. Julkaistu 25.1.2023. Viitattu 2.2.2023. <https://learn.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results>