



## WLabra 2

### Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Koventaminen TTC6050-3006

11.10.2024

Tieto- ja viestintätekniikka

## Sisältö

<b>1</b>	<b>Johdanto .....</b>	<b>4</b>
<b>2</b>	<b>Teoria.....</b>	<b>4</b>
2.1	Microsoft Security Compliance Toolkit .....	4
2.2	Group Policy Objects (GPO) .....	5
2.3	Fine-grained password policies (FGPP) .....	6
2.4	Muita termejä .....	6
<b>3</b>	<b>Kovennukset.....</b>	<b>7</b>
3.1	Security Compliance Toolkitin asennus .....	7
3.2	Etäkäytön estäminen.....	15
3.3	Työaseman asetusten muokkaamisen rajoittaminen.....	16
3.4	Fine grained password policies .....	20
<b>4</b>	<b>Pohdinta.....</b>	<b>24</b>
	<b>Lähteet .....</b>	<b>25</b>

## Kuviot

Kuvio 1.	Domain admin -käyttäjän luonti .....	8
Kuvio 2.	Käyttäjän lisääminen turvaryhmään .....	8
Kuvio 3.	Asennetut paketit.....	9
Kuvio 4.	PolicyAnalyzer .....	9
Kuvio 5.	Politiikkojen vertailu .....	10
Kuvio 6.	Konfliktit .....	10
Kuvio 7.	DC scripti .....	11
Kuvio 8.	Policy objects.....	12
Kuvio 9.	workstations.....	12
Kuvio 10.	Gpupdate.....	13
Kuvio 11.	Analyysi lopputilanteessa.....	13
Kuvio 12.	Asennetut politiikat.....	14
Kuvio 13.	Estetty asennus .....	15
Kuvio 14.	Etäkäytön estäminen .....	15

Kuvio 15. Estetty etäkäyttö.....	16
Kuvio 16. Limit_controlPanel GPO .....	17
Kuvio 17. Ohjauspaneelin rajoittaminen .....	17
Kuvio 18. Sallitut asetukset .....	18
Kuvio 19. Työntekijän ohjauspaneeli .....	18
Kuvio 20. Asetukset-valikon näkyvät sivut.....	19
Kuvio 21. Työntekijälle näkyvät asetukset .....	19
Kuvio 22. Local Log On .....	20
Kuvio 23. Muutettu asetus.....	20
Kuvio 24. Uusi turvallisuusryhmä salasanaikäytänteitä varten .....	21
Kuvio 25. Employees_Password ryhmän jäsenet .....	21
Kuvio 26. New password setting.....	22
Kuvio 27. Salasana-asetusten luonti .....	22
Kuvio 28. Ryhmään vaikuttavat .....	23
Kuvio 29. Powershell testi.....	23

# 1 Johdanto

Koventaminen-opintojakson toisessa labratyössä tarkoituksena on koventaa virtuaaliympäristömme Windows 11 virtuaaliympäristömme Microsoftin tuotteita. Tähän kuului varsinkin GPO kovennot (DC01:llä), sekä omia valikoituja kovennotuksia mitkä ryhmä näki tarpeellisiksi. Käytimme Security Compliance Toolkittiä luodaksemme pohjan kovennotuksille. Sen jälkeen valitsimme netistä löydettyjä yleisiä ohjeita Windowsin koventamiseen. Merkittäviä muutoksia teimme RDP, Kontrolli-paneelin, asetusten sekä käyttäjien käyttörajoituksiin.

## 2 Teoria

Koventamisen toteuttaminen voi olla monimutkaista ja aikaa vievää varsinkin, jos kyseessä on isompi organisaatio ja laajempi, monimutkaisempi ympäristö. Jotkut turvallisuusominaisuudet voivat aiheuttaa ylimääräistä kuormitusta järjestelmälle ja vaikuttaa sen suorituskykyyn. Lisäksi muutokset järjestelmän konfiguraatioissa voivat häiritä normaalia toimintaa. Koventamisen toteuttamisessa on myös tärkeää noudattaa alan standardeja kuten Computer Information Security (CIS) Benchmarks -ohjeita. Ympäristön koventamista varten on myös laaja valikoima työkaluja, skriptoja sekä automaatioita, jotka helpottavat tarvittavien muutosten toteuttamista ja analysointia. (Shruti456rawal. 2024).

### 2.1 Microsoft Security Compliance Toolkit

Security Compliance Toolkit (SCT) on Microsoftin kehittämä työkalu, jonka tarkoitus on administraattorin ryhmäpolitiikkaobjektien (GPO) ja tietoturva-asetusten hallitsemisen helpottaminen. Työkalulla pystytään vertaamaan käytössä olevien ryhmäpolitiikkaobjektien ja Microsoftin GPO-suositusten eroavaisuuksia, ja konfiguroimaan käytänteen noudattamaan Microsoftin suosituksia. (Microsoft Security Compliance Toolkit - How to use. 2024)

**Policy analyzer** on Microsoft SCT:n apuohjelma, jolla voidaan analysoida ja verrata GPO sääntöjä. Sen tehtävänä on esittää päällekkäiset asetukset ja ristiriidat ryhmäpolitiikoiden välillä. Työkalu voi

verrata esimerkiksi GPO:n asetuksia siihen, mitä on käytössä paikallisella tasolla. Näin työkalun avulla voidaan havaita poikkeamat ja muutokset vaikkapa paikallisella koneella verrattuna koko domainin asetuksiin. Policy Analyzer siis helpottaa erojen tunnistamista ja mahdollisten poikkeamien havaitsemista. (Microsoft Security Compliance Toolkit - How to use. 2024)

## 2.2 Group Policy Objects (GPO)

Group Policy Objects (GPO) ovat keskeinen osa Microsoftin Active Directory -infrastruktuuria. GPO:t mahdollistavat hallittujen asetusten määrittämisen käyttäjille ja tietokoneille. Oikein suunniteltuna ja toteutettuina niillä voidaan parantaa järjestelmän tietoturvallisuutta sekä parantaa IT-infrastruktuurin toimintaa merkittävästi. (Group Policy Objects. 2018)

Muutamia esimerkkejä parhaista käytännöistä (**Best Practices**) Group Policy Objects.

**Organisointiyksiköiden (OU) jakaminen käyttäjiin ja tietokoneisiin.** Jakamalla käyttäjät ja tietokoneet erillisiin OU:hin helpottaa erilaisten käytäntöjen soveltamista. Esimerkiksi tietokonepolitiikat voidaan kohdistaa ympäristön joka tietokoneeseen ja käyttäjäpolitiikat jokaiseen käyttäjään, tai vaikka vain tiettyyn ryhmään, esimerkiksi HR tai SALES.

**Selkeä nimeämiskäytäntö GPO.** Käytä GPO:n nimeämisessä selkeitä, kohdetta kuvaavia nimiä, jotta asetetun GPO:n merkitys helppo ymmärtää nimestä. Esimerkiksi käyttäjäpolitiikoille voi käyttää "U\_" ja tietokonepolitiikoille "C\_" alkuja, kuten "U\_user\_policy" ja "C\_computer\_policy". Näin nimi itsessään kertoo, mihin kohteeseen kyseinen GPO vaikuttaa.

**GPO priorisointi.** GPO:ta sovelletaan järjestyksessä **LSDOU** (Local, Site, Domain, OU). Asetukset paikallisella (Local) omaavat matalimman, kun taas OU-tason asetukset korkeimman prioriteetin. Priorisointi määrää, mitkä asetukset lopulta ovat voimassa.

**Rajoita pääsyä ohjauspaneeliin.** Rajoittamalla pääsyä ohjauspaneeliin voidaan estää vaikka normaali käyttäjiä tekemästä muutoksia järjestelmäasetuksiin, muutosten tekemisen kuullessa ylläpitäjille. Tämä estää virheiden syntyä perus käyttäjien toimesta ja näin parantaa turvallisuutta.

**Estä siirrettävien medioiden käyttö.** USB-tikut ja muut siirrettävät mediat voivat olla mahdollinen tietoturvariski, sillä ne voivat levittää haittaohjelmia. GPO:n soveltamisen avulla on mahdollisuus estää nämäkin. Tulee miettiä, käytetäänkö siirrettävää mediaa paljon ja miten niiden estäminen vaikuttaa käytettävyyteen. (Group Policy Best Practices. 2024)

## 2.3 Fine-grained password policies (FGPP)

Fine-grained password policies ovat active directory (AD) ominaisuus, jonka avulla voidaan määrittää erilaisia salasanojen ja tilin lukkiutumis- sääntöjä käyttäjille, sekä käyttäjäryhmille organisaatiossa. Tämä mahdollistaa salasanojen turvallisuuden hallinnan joustavammalla ja tarkemmalla tavalla. (Configure fine grained password policies for Active Directory Domain Services. 2024)

## 2.4 Muita termejä

**Windows toimialue (Domain)** kattaa koko ympäristön laitteet ja niiden keskitetyn hallinnan. **Domain** mahdollistaa käyttäjien kirjautumisen mille tahansa laitteelle toimialueella, eli kirjautuminen on toimialuekohtaista, eikä laitekohtaista. Toimialuetta voidaan hallita ryhmien ja sääntöjen avulla, jotka saadaan asetettua koko alueeseen kerralla, helpottaen ylläpitoa. (Hyytiäinen. 2024)

**Paikallinen pääkäyttäjä (Local Admin)** on tietyn päätelaitteen admin, joka on valtuutettu tehdä muutoksia vain tiettyyn laitteeseen toimialueella. **Toimialueen pääkäyttäjä (Domain Admin)** on koko toimialueen **Admin**, joka voi tehdä asetuksiin muutoksia koko toimialueessa. (Hyytiäinen. 2024)

**Korkeiden käyttöoikeuksien hallinta** tai **Privileged Access Management (PAM)** on tietoturvaratkaisu, jolla voidaan suojata ympäristön tietoturvaa hallitsemalla korkeampien käyttöoikeuksien

omaavia käyttäjiä ja auditoimalla niiden toimintaa. Hallitsemalla tavallisten käyttäjien pääsyä järjestelmien kriittisiin asetuksiin, saadaan suojattua järjestelmää esim. hakkereiden sivuttaisliikkeen (Lateral Movement) varalta, tai vaikka henkilökunnan tiettyjen ryhmien tarpeettoman pääsyn palomuuriasetuksiin tai ohjauspaneelin hallintaan. Korkean tason käyttöoikeudet käyttäjätileillä ovat tietoturvariski, mikäli kyberhyökkääjät pääsevät tilien tunnuksiin käsiksi. Tilien laajoilla käyttöoikeuksilla voidaan varastaa salaista tietoa organisaatiosta ja muunnella kriittisiä asetuksia toimialueen laitteilla. Tämän vuoksi näiden tilien suojauksen tulee olla huomattavasti vahvempi esimerkiksi monivaiheisen tunnistautumisen avulla (MFA), kuin toimialueen tavallisilla käyttäjillä. (Hyytiäinen. 2024)

**RDP** (Remote Desktop Protocol) on protokolla, joka mahdollistaa etäyhteyden luomisen toiseen tietokoneeseen verkon yli. RDP on salattu TCP (transmission control protocol) protokollaa käytetään. (Understanding the Remote Desktop Protocol (RDP).2023)

**Gpupdate /force** on komento, jonka avulla pakotetaan ryhmäkäytäntöjen päivittäminen välittömästi tietokoneeseen. (gpupdate.2023)

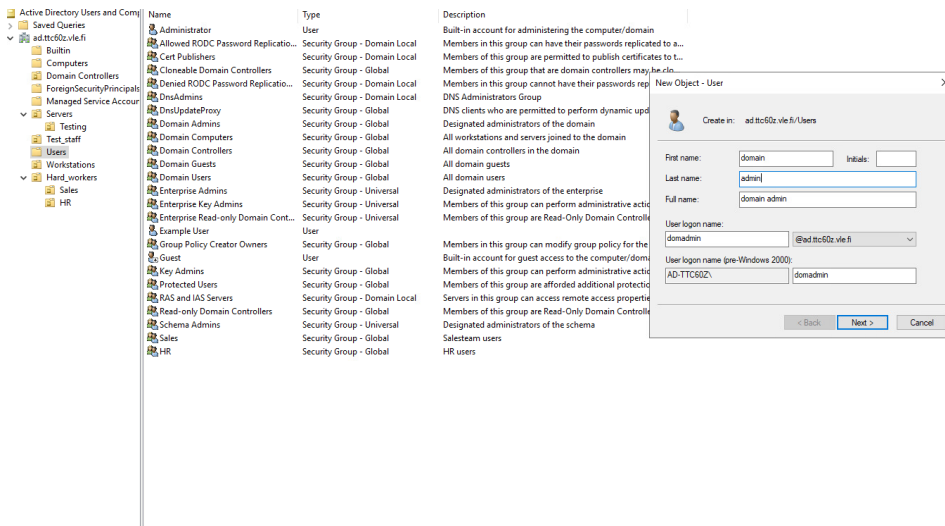
**Gpresult /r** on komento, joka näyttää tietokoneessa sovellettavat GPO:t. (gpresult.2023)

### 3 Kovennukset

Tässä harjoituksessa tarkoituksenamme oli koventaa Windows 11 -työasemaa. Ohjeistuksessa sanottiin, että tässä vaiheessa olisi hyvä käyttää Security Compliance Toolkitiä ja sen lisäksi tehdä muutamia muita kovennuksia. Aloitimme harjoituksen Security Compliance Toolkitin asennuksella.

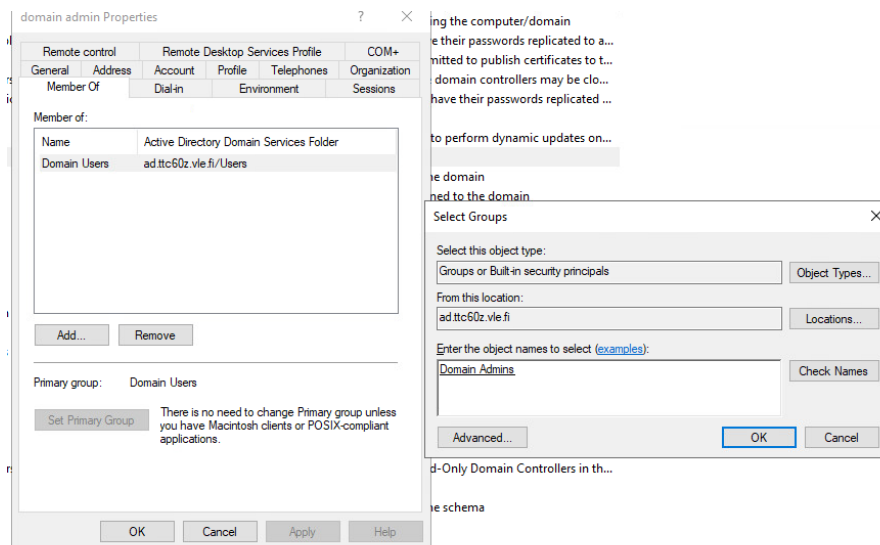
#### 3.1 Security Compliance Toolkitin asennus

Aloitimme Security Compliance Toolkitin asennuksen luomalla uuden domain admin -käyttäjän, jolla voimme asentaa ja ajaa tiedostoja. (Kuvio 1.)



Kuvio 1. Domain admin -käyttäjän luonti

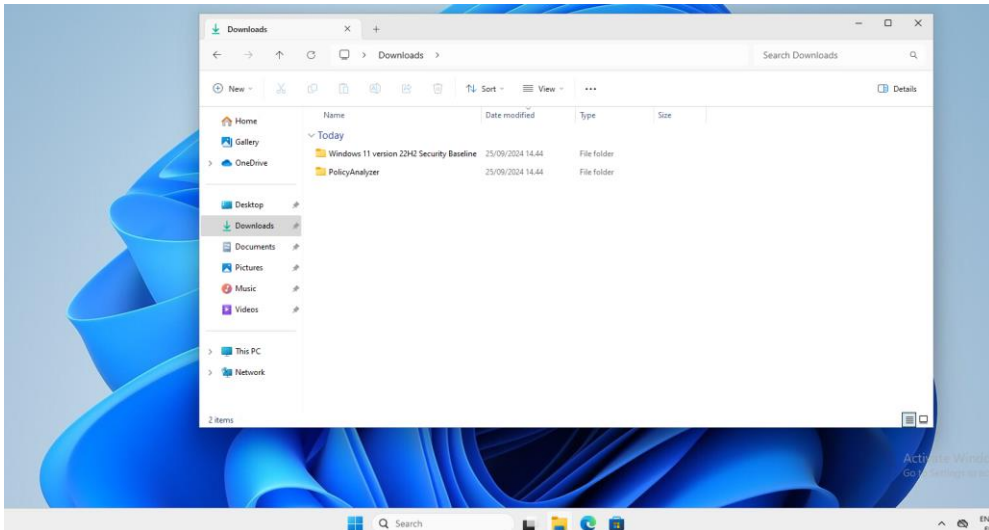
Lisäsimme käyttäjän turvaryhmään domain admins. (Kuvio 2).



Kuvio 2. Käyttäjän lisääminen turvaryhmään

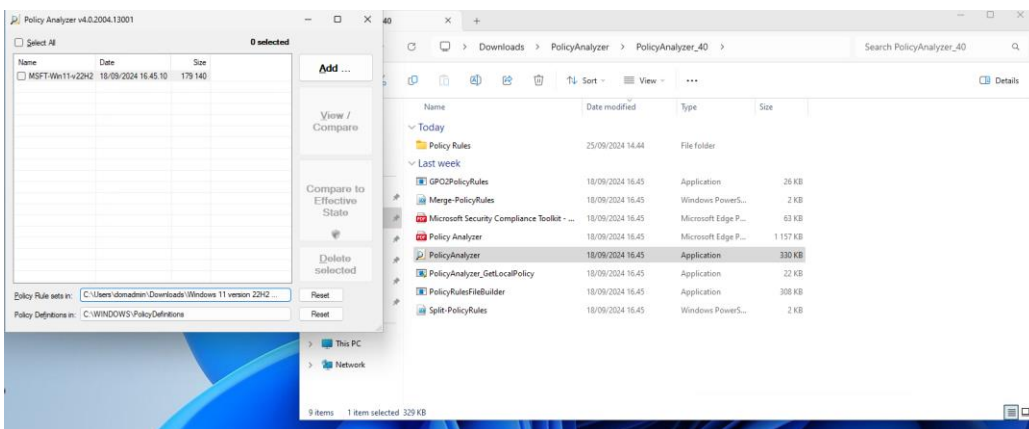
Latasimme Security Compliance Toolkitin WS01 -työasemalle ja asensimme kuvion 3 mukaiset paketit.





Kuvio 3. Asennetut paketit

Seuraavaksi ajoimme PolicyAnalyzerin, joka suoritti analyysin käytössä olevista turvallisuus politiikoista. (Kuvio 4.)



Kuvio 4. PolicyAnalyzer

Ohjelma listasi vertailun käytössä olevista ja työkalun mukaan hyvistä politiikoista. (Kuvio 5.)

Policy Viewer - 380 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 Failure	Success and Failure
Audit Policy	Account Management	Security Group Management	Success	Success and Failure
Audit Policy	Account Management	User Account Management	Success and Failure	Success and Failure
Audit Policy	Detailed Tracking	PNP Activity	Success	Success
Audit Policy	Detailed Tracking	Process Creation	Success	Success
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success and Failure
Audit Policy	Logon/Logoff	Group Membership	Success	Success and Failure
Audit Policy	Logon/Logoff	Logon	Success and Failure	Success and Failure
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Failure	Success and Failure
Audit Policy	Logon/Logoff	Special Logon	Success	Success and Failure
Audit Policy	Object Access	Detailed File Share	Failure	Success and Failure
Audit Policy	Object Access	File Share	Success and Failure	Success and Failure
Audit Policy	Object Access	Other Object Access Events	Success and Failure	Success and Failure
Audit Policy	Object Access	Removable Storage	Success and Failure	Success and Failure
Audit Policy	Policy Change	Audit Policy Change	Success	Success and Failure
Audit Policy	Policy Change	Authentication Policy Change	Success	Success and Failure
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Failure	Success and Failure
Audit Policy	Policy Change	Other Policy Change Events	Failure	Success and Failure
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Failure	Success and Failure
Audit Policy	System	Other System Events	Success and Failure	Success and Failure

**Policy Path:**  
Advanced Audit Policy Configuration  
System Audit Policies\Object Access  
Removable Storage

**Removable storage**

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested.

If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts.

If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage.

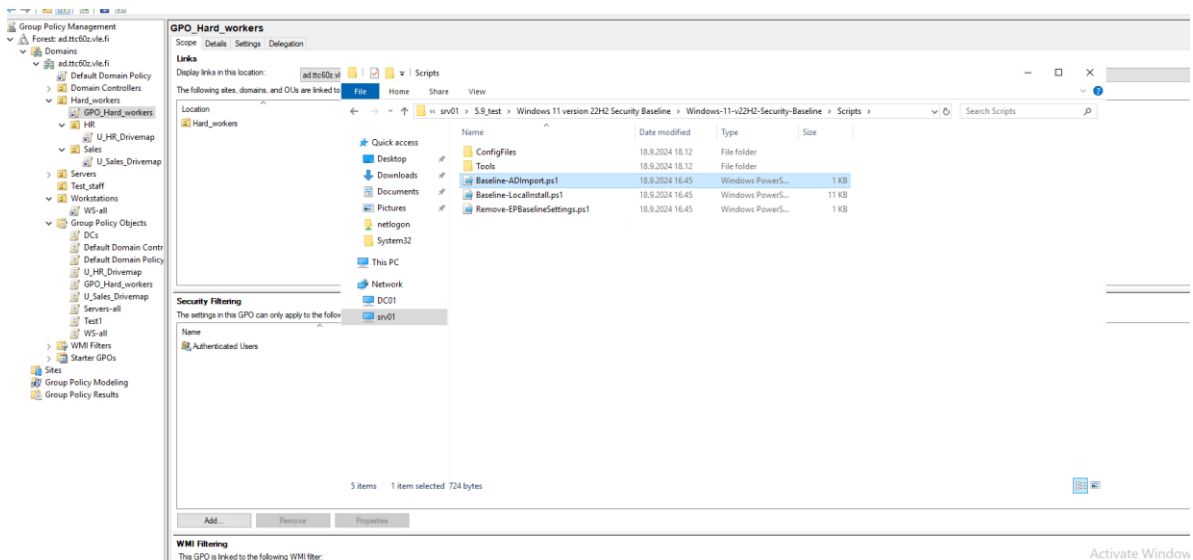
**Baseline(s):**  
**Option:** Success and Failure  
**GPO:** MSFT Windows 11 22H2 - Computer

**Effective state:**

Kuvio 5. Politiikkujen vertailu

Otimme kuvion 7 mukaisen kuvan konflikteista. (Kuvio 7).

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Management	Security Group Management	Success	Success and Failure
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success and Failure
Audit Policy	Logon/Logoff	Group Membership	Success	Success and Failure
Audit Policy	Logon/Logoff	Special Logon	Success	Success and Failure
Audit Policy	Object Access	Detailed File Share	Failure	Success and Failure
Audit Policy	Policy Change	Audit Policy Change	Success	Success and Failure
Audit Policy	Policy Change	Authentication Policy Change	Success	Success and Failure
Audit Policy	Policy Change	Other Policy Change Events	Failure	Success and Failure
Audit Policy	System	Security State Change	Success	Success and Failure
Audit Policy	System	Security System Extension	Success	Success and Failure
HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon	SeRemoteInit	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	RestrictedAnonymous	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\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-1-5-32-551
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-1-5-32	*S-1-5-32-544; *S-1-5-32-545; *S-1-5-32-546; *S-1-5-32-547; *S-1-5-32-548; *S-1-5-32-549; *S-1-5-32-550; *S-1-5-32-551; *S-1-5-32-552; *S-1-5-32-553; *S-1-5-32-554; *S-1-5-32-555; *S-1-5-32-556; *S-1-5-32-557; *S-1-5-32-558; *S-1-5-32-559; *S-1-5-32-560; *S-1-5-32-561; *S-1-5-32-562; *S-1-5-32-563; *S-1-5-32-564; *S-1-5-32-565; *S-1-5-32-566; *S-1-5-32-567; *S-1-5-32-568; *S-1-5-32-569; *S-1-5-32-570; *S-1-5-32-571; *S-1-5-32-572; *S-1-5-32-573; *S-1-5-32-574; *S-1-5-32-575; *S-1-5-32-576; *S-1-5-32-577; *S-1-5-32-578; *S-1-5-32-579; *S-1-5-32-580; *S-1-5-32-581; *S-1-5-32-582; *S-1-5-32-583; *S-1-5-32-584; *S-1-5-32-585; *S-1-5-32-586; *S-1-5-32-587; *S-1-5-32-588; *S-1-5-32-589; *S-1-5-32-590; *S-1-5-32-591; *S-1-5-32-592; *S-1-5-32-593; *S-1-5-32-594; *S-1-5-32-595; *S-1-5-32-596; *S-1-5-32-597; *S-1-5-32-598; *S-1-5-32-599; *S-1-5-32-600; *S-1-5-32-601; *S-1-5-32-602; *S-1-5-32-603; *S-1-5-32-604; *S-1-5-32-605; *S-1-5-32-606; *S-1-5-32-607; *S-1-5-32-608; *S-1-5-32-609; *S-1-5-32-610; *S-1-5-32-611; *S-1-5-32-612; *S-1-5-32-613; *S-1-5-32-614; *S-1-5-32-615; *S-1-5-32-616; *S-1-5-32-617; *S-1-5-32-618; *S-1-5-32-619; *S-1-5-32-620; *S-1-5-32-621; *S-1-5-32-622; *S-1-5-32-623; *S-1-5-32-624; *S-1-5-32-625; *S-1-5-32-626; *S-1-5-32-627; *S-1-5-32-628; *S-1-5-32-629; *S-1-5-32-630; *S-1-5-32-631; *S-1-5-32-632; *S-1-5-32-633; *S-1-5-32-634; *S-1-5-32-635; *S-1-5-32-636; *S-1-5-32-637; *S-1-5-32-638; *S-1-5-32-639; *S-1-5-32-640; *S-1-5-32-641; *S-1-5-32-642; *S-1-5-32-643; *S-1-5-32-644; *S-1-5-32-645; *S-1-5-32-646; *S-1-5-32-647; *S-1-5-32-648; *S-1-5-32-649; *S-1-5-32-650; *S-1-5-32-651; *S-1-5-32-652; *S-1-5-32-653; *S-1-5-32-654; *S-1-5-32-655; *S-1-5-32-656; *S-1-5-32-657; *S-1-5-32-658; *S-1-5-32-659; *S-1-5-32-660; *S-1-5-32-661; *S-1-5-32-662; *S-1-5-32-663; *S-1-5-32-664; *S-1-5-32-665; *S-1-5-32-666; *S-1-5-32-667; *S-1-5-32-668; *S-1-5-32-669; *S-1-5-32-670; *S-1-5-32-671; *S-1-5-32-672; *S-1-5-32-673; *S-1-5-32-674; *S-1-5-32-675; *S-1-5-32-676; *S-1-5-32-677; *S-1-5-32-678; *S-1-5-32-679; *S-1-5-32-680; *S-1-5-32-681; *S-1-5-32-682; *S-1-5-32-683; *S-1-5-32-684; *S-1-5-32-685; *S-1-5-32-686; *S-1-5-32-687; *S-1-5-32-688; *S-1-5-32-689; *S-1-5-32-690; *S-1-5-32-691; *S-1-5-32-692; *S-1-5-32-693; *S-1-5-32-694; *S-1-5-32-695; *S-1-5-32-696; *S-1-5-32-697; *S-1-5-32-698; *S-1-5-32-699; *S-1-5-32-700; *S-1-5-32-701; *S-1-5-32-702; *S-1-5-32-703; *S-1-5-32-704; *S-1-5-32-705; *S-1-5-32-706; *S-1-5-32-707; *S-1-5-32-708; *S-1-5-32-709; *S-1-5-32-710; *S-1-5-32-711; *S-1-5-32-712; *S-1-5-32-713; *S-1-5-32-714; *S-1-5-32-715; *S-1-5-32-716; *S-1-5-32-717; *S-1-5-32-718; *S-1-5-32-719; *S-1-5-32-720; *S-1-5-32-721; *S-1-5-32-722; *S-1-5-32-723; *S-1-5-32-724; *S-1-5-32-725; *S-1-5-32-726; *S-1-5-32-727; *S-1-5-32-728; *S-1-5-32-729; *S-1-5-32-730; *S-1-5-32-731; *S-1-5-32-732; *S-1-5-32-733; *S-1-5-32-734; *S-1-5-32-735; *S-1-5-32-736; *S-1-5-32-737; *S-1-5-32-738; *S-1-5-32-739; *S-1-5-32-740; *S-1-5-32-741; *S-1-5-32-742; *S-1-5-32-743; *S-1-5-32-744; *S-1-5-32-745; *S-1-5-32-746; *S-1-5-32-747; *S-1-5-32-748; *S-1-5-32-749; *S-1-5-32-750; *S-1-5-32-751; *S-1-5-32-752; *S-1-5-32-753; *S-1-5-32-754; *S-1-5-32-755; *S-1-5-32-756; *S-1-5-32-757; *S-1-5-32-758; *S-1-5-32-759; *S-1-5-32-760; *S-1-5-32-761; *S-1-5-32-762; *S-1-5-32-763; *S-1-5-32-764; *S-1-5-32-765; *S-1-5-32-766; *S-1-5-32-767; *S-1-5-32-768; *S-1-5-32-769; *S-1-5-32-770; *S-1-5-32-771; *S-1-5-32-772; *S-1-5-32-773; *S-1-5-32-774; *S-1-5-32-775; *S-1-5-32-776; *S-1-5-32-777; *S-1-5-32-778; *S-1-5-32-779; *S-1-5-32-780; *S-1-5-32-781; *S-1-5-32-782; *S-1-5-32-783; *S-1-5-32-784; *S-1-5-32-785; *S-1-5-32-786; *S-1-5-32-787; *S-1-5-32-788; *S-1-5-32-789; *S-1-5-32-790; *S-1-5-32-791; *S-1-5-32-792; *S-1-5-32-793; *S-1-5-32-794; *S-1-5-32-795; *S-1-5-32-796; *S-1-5-32-797; *S-1-5-32-798; *S-1-5-32-799; *S-1-5-32-800; *S-1-5-32-801; *S-1-5-32-802; *S-1-5-32-803; *S-1-5-32-804; *S-1-5-32-805; *S-1-5-32-806; *S-1-5-32-807; *S-1-5-32-808; *S-1-5-32-809; *S-1-5-32-810; *S-1-5-32-811; *S-1-5-32-812; *S-1-5-32-813; *S-1-5-32-814; *S-1-5-32-815; *S-1-5-32-816; *S-1-5-32-817; *S-1-5-32-818; *S-1-5-32-819; *S-1-5-32-820; *S-1-5-32-821; *S-1-5-32-822; *S-1-5-32-823; *S-1-5-32-824; *S-1-5-32-825; *S-1-5-32-826; *S-1-5-32-827; *S-1-5-32-828; *S-1-5-32-829; *S-1-5-32-830; *S-1-5-32-831; *S-1-5-32-832; *S-1-5-32-833; *S-1-5-32-834; *S-1-5-32-835; *S-1-5-32-836; *S-1-5-32-837; *S-1-5-32-838; *S-1-5-32-839; *S-1-5-32-840; *S-1-5-32-841; *S-1-5-32-842; *S-1-5-32-843; *S-1-5-32-844; *S-1-5-32-845; *S-1-5-32-846; *S-1-5-32-847; *S-1-5-32-848; *S-1-5-32-849; *S-1-5-32-850; *S-1-5-32-851; *S-1-5-32-852; *S-1-5-32-853; *S-1-5-32-854; *S-1-5-32-855; *S-1-5-32-856; *S-1-5-32-857; *S-1-5-32-858; *S-1-5-32-859; *S-1-5-32-860; *S-1-5-32-861; *S-1-5-32-862; *S-1-5-32-863; *S-1-5-32-864; *S-1-5-32-865; *S-1-5-32-866; *S-1-5-32-867; *S-1-5-32-868; *S-1-5-32-869; *S-1-5-32-870; *S-1-5-32-871; *S-1-5-32-872; *S-1-5-32-873; *S-1-5-32-874; *S-1-5-32-875; *S-1-5-32-876; *S-1-5-32-877; *S-1-5-32-878; *S-1-5-32-879; *S-1-5-32-880; *S-1-5-32-881; *S-1-5-32-882; *S-1-5-32-883; *S-1-5-32-884; *S-1-5-32-885; *S-1-5-32-886; *S-1-5-32-887; *S-1-5-32-888; *S-1-5-32-889; *S-1-5-32-890; *S-1-5-32-891; *S-1-5-32-892; *S-1-5-32-893; *S-1-5-32-894; *S-1-5-32-895; *S-1-5-32-896; *S-1-5-32-897; *S-1-5-32-898; *S-1-5-32-899; *S-1-5-32-900; *S-1-5-32-901; *S-1-5-32-902; *S-1-5-32-903; *S-1-5-32-904; *S-1-5-32-905; *S-1-5-32-906; *S-1-5-32-907; *S-1-5-32-908; *S-1-5-32-909; *S-1-5-32-910; *S-1-5-32-911; *S-1-5-32-912; *S-1-5-32-913; *S-1-5-32-914; *S-1-5-32-915; *S-1-5-32-916; *S-1-5-32-917; *S-1-5-32-918; *S-1-5-32-919; *S-1-5-32-920; *S-1-5-32-921; *S-1-5-32-922; *S-1-5-32-923; *S-1-5-32-924; *S-1-5-32-925; *S-1-5-32-926; *S-1-5-32-927; *S-1-5-32-928; *S-1-5-32-929; *S-1-5-32-930; *S-1-5-32-931; *S-1-5-32-932; *S-1-5-32-933; *S-1-5-32-934; *S-1-5-32-935; *S-1-5-32-936; *S-1-5-32-937; *S-1-5-32-938; *S-1-5-32-939; *S-1-5-32-940; *S-1-5-32-941; *S-1-5-32-942; *S-1-5-32-943; *S-1-5-32-944; *S-1-5-32-945; *S-1-5-32-946; *S-1-5-32-947; *S-1-5-32-948; *S-1-5-32-949; *S-1-5-32-950; *S-1-5-32-951; *S-1-5-32-952; *S-1-5-32-953; *S-1-5-32-954; *S-1-5-32-955; *S-1-5-32-956; *S-1-5-32-957; *S-1-5-32-958; *S-1-5-32-959; *S-1-5-32-960; *S-1-5-32-961; *S-1-5-32-962; *S-1-5-32-963; *S-1-5-32-964; *S-1-5-32-965; *S-1-5-32-966; *S-1-5-32-967; *S-1-5-32-968; *S-1-5-32-969; *S-1-5-32-970; *S-1-5-32-971; *S-1-5-32-972; *S-1-5-32-973; *S-1-5-32-974; *S-1-5-32-975; *S-1-5-32-976; *S-1-5-32-977; *S-1-5-32-978; *S-1-5-32-979; *S-1-5-32-980; *S-1-5-32-981; *S-1-5-32-982; *S-1-5-32-983; *S-1-5-32-984; *S-1-5-32-985; *S-1-5-32-986; *S-1-5-32-987; *S-1-5-32-988; *S-1-5-32-989; *S-1-5-32-990; *S-1-5-32-991; *S-1-5-32-992; *S-1-5-32-993; *S-1-5-32-994; *S-1-5-32-995; *S-1-5-32-996; *S-1-5-32-997; *S-1-5-32-998; *S-1-5-32-999; *S-1-5-32-1000; *S-1-5-32-1001; *S-1-5-32-1002; *S-1-5-32-1003; *S-1-5-32-1004; *S-1-5-32-1005; *S-1-5-32-1006; *S-1-5-32-1007; *S-1-5-32-1008; *S-1-5-32-1009; *S-1-5-32-1010; *S-1-5-32-1011; *S-1-5-32-1012; *S-1-5-32-1013; *S-1-5-32-1014; *S-1-5-32-1015; *S-1-5-32-1016; *S-1-5-32-1017; *S-1-5-32-1018; *S-1-5-32-1019; *S-1-5-32-1020; *S-1-5-32-1021; *S-1-5-32-1022; *S-1-5-32-1023; *S-1-5-32-1024; *S-1-5-32-1025; *S-1-5-32-1026; *S-1-5-32-1027; *S-1-5-32-1028; *S-1-5-32-1029; *S-1-5-32-1030; *S-1-5-32-1031; *S-1-5-32-1032; *S-1-5-32-1033; *S-1-5-32-1034; *S-1-5-32-1035; *S-1-5-32-1036; *S-1-5-32-1037; *S-1-5-32-1038; *S-1-5-32-1039; *S-1-5-32-1040; *S-1-5-32-1041; *S-1-5-32-1042; *S-1-5-32-1043; *S-1-5-32-1044; *S-1-5-32-1045; *S-1-5-32-1046; *S-1-5-32-1047; *S-1-5-32-1048; *S-1-5-32-1049; *S-1-5-32-1050; *S-1-5-32-1051; *S-1-5-32-1052; *S-1-5-32-1053; *S-1-5-32-1054; *S-1-5-32-1055; *S-1-5-32-1056; *S-1-5-32-1057; *S-1-5-32-1058; *S-1-5-32-1059; *S-1-5-32-1060; *S-1-5-32-1061; *S-1-5-32-1062; *S-1-5-32-1063; *S-1-5-32-1064; *S-1-5-32-1065; *S-1-5-32-1066; *S-1-5-32-1067; *S-1-5-32-1068; *S-1-5-32-1069; *S-1-5-32-1070; *S-1-5-32-1071; *S-1-5-32-1072; *S-1-5-32-1073; *S-1-5-32-1074; *S-1-5-32-1075; *S-1-5-32-1076; *S-1-5-32-1077; *S-1-5-32-1078; *S-1-5-32-1079; *S-1-5-32-1080; *S-1-5-32-1081; *S-1-5-32-1082; *S-1-5-32-1083; *S-1-5-32-1084; *S-1-5-32-1085; *S-1-5-32-1086; *S-1-5-32-1087; *S-1-5-32-1088; *S-1-5-32-1089; *S-1-5-32-1090; *S-1-5-32-1091; *S-1-5-32-1092; *S-1-5-32-1093; *S-1-5-32-1094; *S-1-5-32-1095; *S-1-5-32-1096; *S-1-5-32-1097; *S-1-5-32-1098; *S-1-5-32-1099; *S-1-5-32-1100; *S-1-5-32-1101; *S-1-5-32-1102; *S-1-5-32-1103; *S-1-5-32-1104; *S-1-5-32-1105; *S-1-5-32-1106; *S-1-5-32-1107; *S-1-5-32-1108; *S-1-5-32-1109; *S-1-5-32-1110; *S-1-5-32-1111; *S-1-5-32-1112; *S-1-5-32-1113; *S-1-5-32-1114; *S-1-5-32-1115; *S-1-5-32-1116; *S-1-5-32-1117; *S-1-5-32-1118; *S-1-5-32-1119; *S-1-5-32-1120; *S-1-5-32-1121; *S-1-5-32-1122; *S-1-5-32-1123; *S-1-5-32-1124; *S-1-5-32-1125; *S-1-5-32-1126; *S-1-5-32-1127; *S-1-5-32-1128; *S-1-5-32-1129; *S-1-5-32-1130; *S-1-5-32-1131; *S-1-5-32-1132; *S-1-5-32-1133; *S-1-5-32-1134; *S-1-5-32-1135; *S-1-5-32-1136; *S-1-5-32-1137; *S-1-5-32-1138; *S-1-5-32-1139; *S-1-5-32-1140; *S-1-5-32-1141; *S-1-5-32-1142; *S-1-5-32-1143; *S-1-5-32-1144; *S-1-5-32-1145; *S-1-5-32-1146; *S-1-5-32-1147; *S-1-5-32-1148; *S-1-5-32-1149; *S-1-5-32-1150; *S-1-5-32-1151; *S-1-5-32-1152; *S-1-5-32-1153; *S-1-5-32-1154; *S-1-5-32-1155; *S-1-5-32-1156; *S-1-5-32-1157; *S-1-5-32-1158; *S-1-5-32-1159; *S-1-5-32-1160; *S-1-5-32-1161; *S-1-5-32-1162; *S-1-5-32-1163; *S-1-5-32-1164; *S-1-5-32-1165; *S-1-5-32-1166; *S-1-5-32-1167; *S-1-5-32-1168; *S-1-5-32-1169; *S-1-5-32-1170; *S-1-5-32-1171; *S-1-5-32-1172; *S-1-5-32-1173; *S-1-5-32-1174; *S-1-5-32-1175; *S-1-5-32-1176; *S-1-5-32-1177; *S-1-5-32-1178; *S-1-5-32-1179; *S-1-5-32-1180; *S-1-5-32-1181; *S-1-5-32-1182; *S-1-5-32-1183; *S-1-5-32-1184; *S-1-5-32-1185; *S-1-5-32-1186; *S-1-5-32-1187; *S-1-5-32-1188; *S-1-5-32-1189; *S-1-5-32-1190; *S-1-5-32-1191; *S-1-5-32-1192; *S-1-5-32-1193; *S-1-5-32-1194; *S-1-5-32-1195; *S-1-5-32-1196; *S-1-5-32-1197; *S-1-5-32-1198; *S-1-5-32-1199; *S-1-5-32-1200; *S-1-5-32-1201; *S-1-5-32-1202; *S-1-5-32-1203; *S-1-5-32-1204; *S-1-5-32-1205; *S-1-5-32-1206; *S-1-5-32-1207; *S-1-5-32-1208; *S-1-5-32-1209; *S-1-5-32-1210; *S-1-5-32-1211; *S-1-5-32-1212; *S-1-5-32-1213; *S-1-5-32-1214; *S-1-5-32-1215; *S-1-5-32-1216; *S-1-5-32-1217; *S-1-5-32-1218; *S-1-5-32-1219; *S-1-5-32-1220; *S-1-5-32-1221; *S-1-5-32-1222; *S-1-5-32-1223; *S-1-5-32-1224; *S-1-5-32-1225; *S-1-5-32-1226; *S-1-5-32-1227; *S-1-5-32-1228; *S-1-5-32-1229; *S-1-5-32-1230; *S-1-5-32-1231; *S-1-5-32-1232; *S-1-5

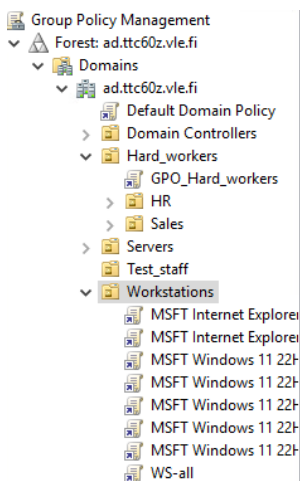


Kuvio 7. DC scriptit

Nyt kun policy objectit oli tuotu Active Directoryyn (kuvio 8), siirsimme ne workstations Organizational Unitin alle (kuvio 9). Credential Guard poistettiin, koska ohjeistuksen mukaan se aiheuttaa WS01:llä blue screenin VLE-ympäristössämme.

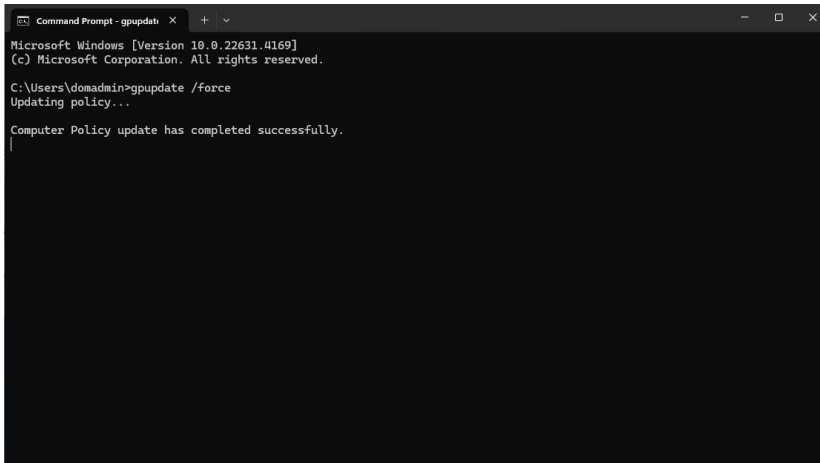
Name	GPO Status	WMI Filter	Modified	Owner
DCs	Enabled	None	4.8.2022 13.17.10	Domain Admi...
Default Domain Controllers Policy	Enabled	None	3.8.2022 14.55.52	Domain Admi...
Default Domain Policy	Enabled	None	23.9.2024 10.55...	Domain Admi...
GPO_Hard_workers	Enabled	None	20.9.2024 13.49	Domain Admi...
MSFT Internet Explorer 11 - Computer	User configuration s...	None	25.9.2024 15.12...	Domain Admi...
MSFT Internet Explorer 11 - User	Computer configurati...	None	25.9.2024 15.12...	Domain Admi...
MSFT Windows 11 22H2 - BitLocker	User configuration s...	None	25.9.2024 15.12...	Domain Admi...
MSFT Windows 11 22H2 - Computer	User configuration s...	None	25.9.2024 15.12...	Domain Admi...
MSFT Windows 11 22H2 - Defender Antivirus	User configuration s...	None	25.9.2024 15.12...	Domain Admi...
MSFT Windows 11 22H2 - Domain Security	User configuration s...	None	25.9.2024 15.12...	Domain Admi...
MSFT Windows 11 22H2 - User	Computer configurati...	None	25.9.2024 15.12...	Domain Admi...
Servers-all	Enabled	None	4.8.2022 13.16.32	Domain Admi...
Test1	Enabled	None	18.9.2024 18.09...	Domain Admi...
U_HR_Drivemap	Enabled	None	25.9.2024 10.29...	Domain Admi...
U_Sales_Drivemap	Enabled	None	25.9.2024 10.29...	Domain Admi...
WS-all	Enabled	None	4.8.2022 13.16.40	Domain Admi...

Kuvio 8. Policy objects



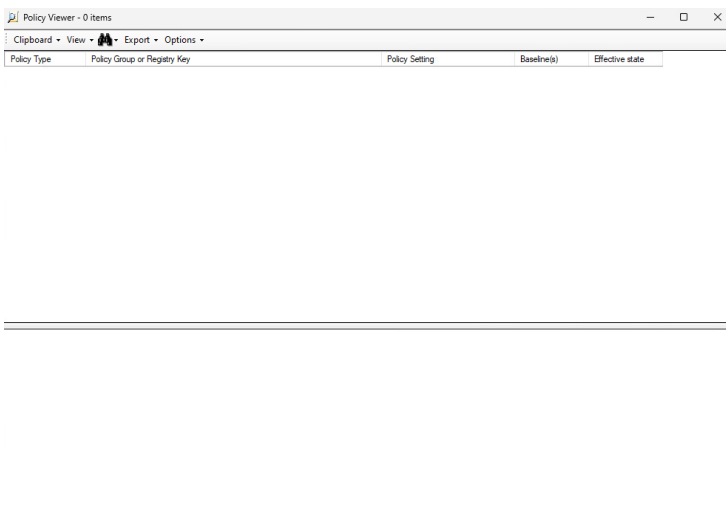
Kuvio 9. workstations

Ajoimme WS01-työasemalla komentokehotteella komennon gpupdate /force, jotta politiikat päivitettiin käyttöön. (Kuvio 10).



Kuvio 10. Gpupdate

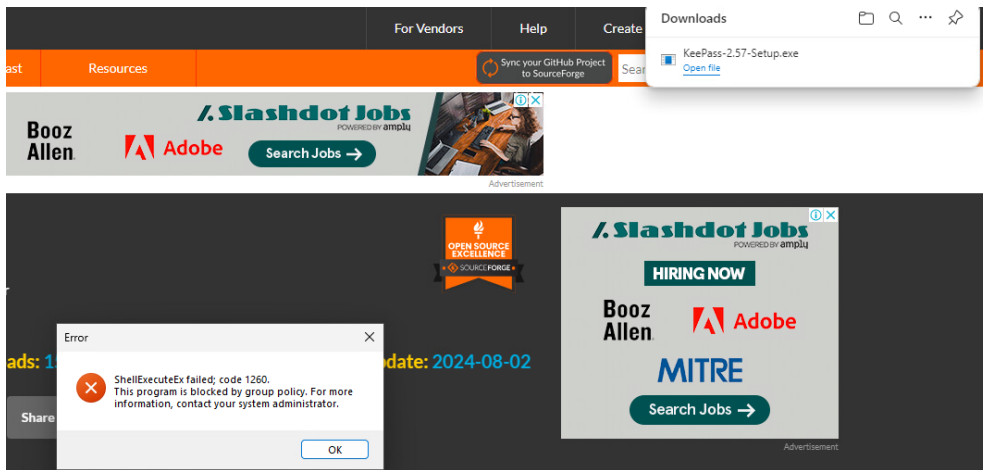
Ajoimme uuden analyysin konflikteista ja niitä ei enää ollut. Poliitikat olivat siis onnistuneesti asennettu. (Kuvio 11).



Kuvio 11. Analyysi lopputilanteessa

Ajoimme vielä analyysin asennetuista politiikoista. Lista on erittäin pitkä, joten vain pieni osa mahtui kuvaan, mutta kuten kuviosta 12 ilmenee, listassa on 311 kohtaa.

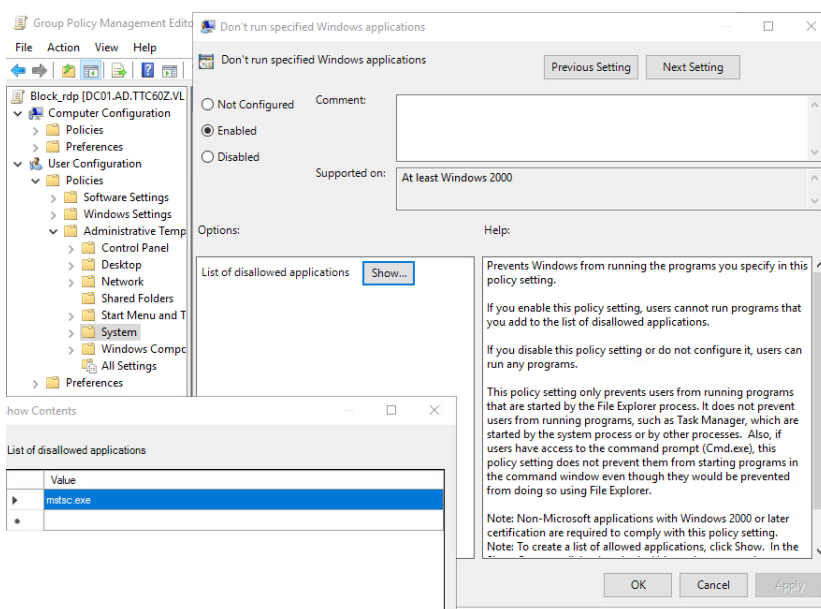




Kuvio 13. Estetty asennus

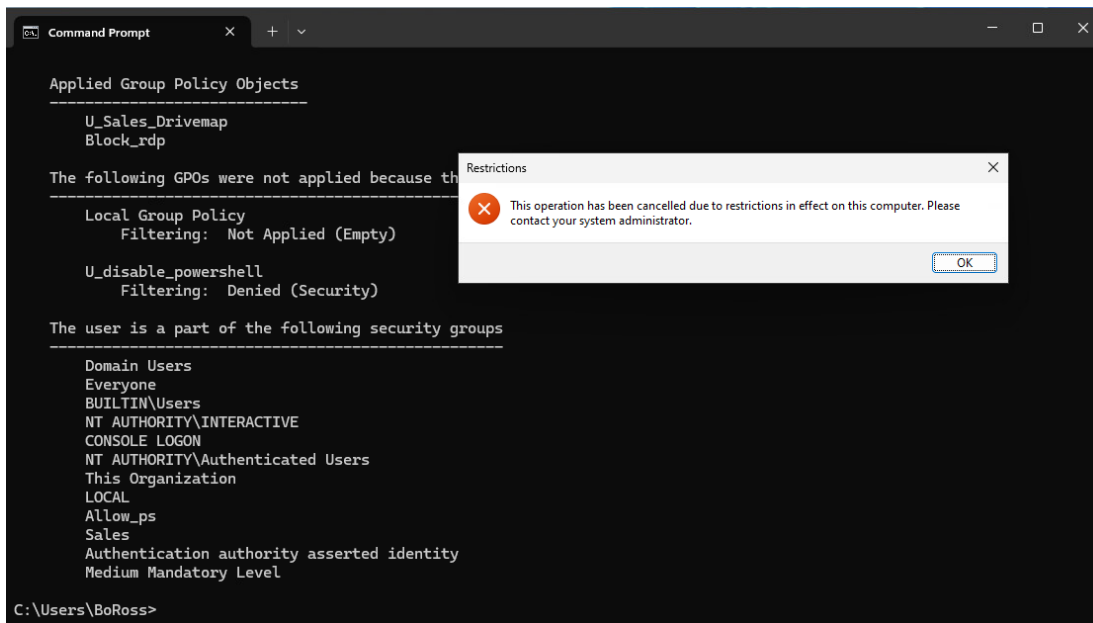
### 3.2 Etäkäytön estäminen

Halusimme estää etäkäytön niiltä käyttäjiltä, joilla ei ole siihen tarvetta. Etäkäyttö on yleinen turvallisuusriski, jota hyökkääjät käyttävät tunkeutuessaan järjestelmiin. Loimme siis uuden säännön, joka estää tämän työntekijöiltä. (Kuvio 14).



Kuvio 14. Etäkäytön estäminen

Yritimme käynnistää etäkäytön, kun olimme kirjautuneet WS01:lle työntekijän tunnuksilla. Tämä antoi virheilmoituksen, että etäkäytön käyttäminen on estetty. Tarkistimme myös komentokehoteella komennolla gpresult /r mitkä politiikat kohdetuvat käyttäjään ja sieltä löytyi luomamme etäkäytön estävä politiikka. (Kuvio 15).



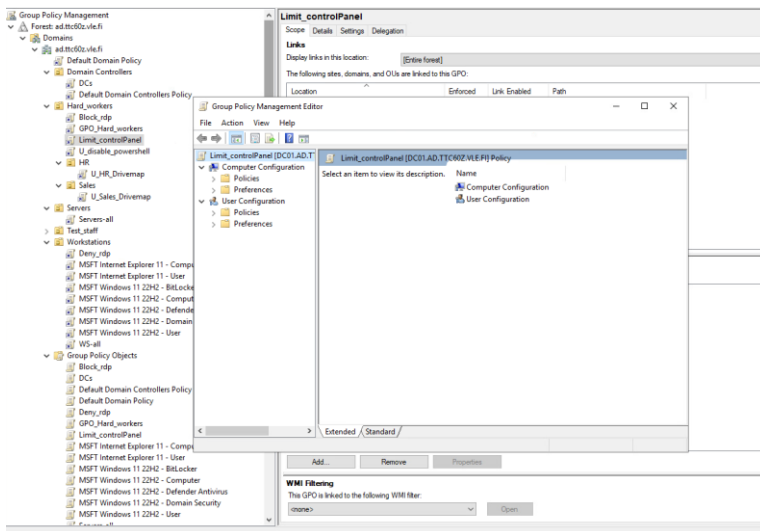
Kuvio 15. Estetty etäkäyttö

### 3.3 Työaseman asetusten muokkaamisen rajoittaminen

Kaikilla käyttäjillä ei ole tarvetta päästä käsiksi työaseman kaikkiin asetuksiin, joten päätimme rajoittaa näiden asetusten näkyvyyttä.

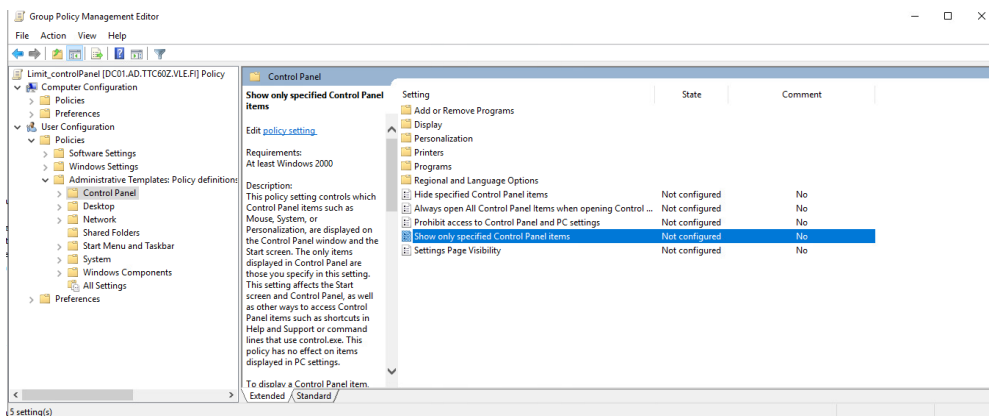
Loimme uuden GPO:n nimeltä Limit\_controlPanel ja avasimme group policy editorin. (Kuvio 16).





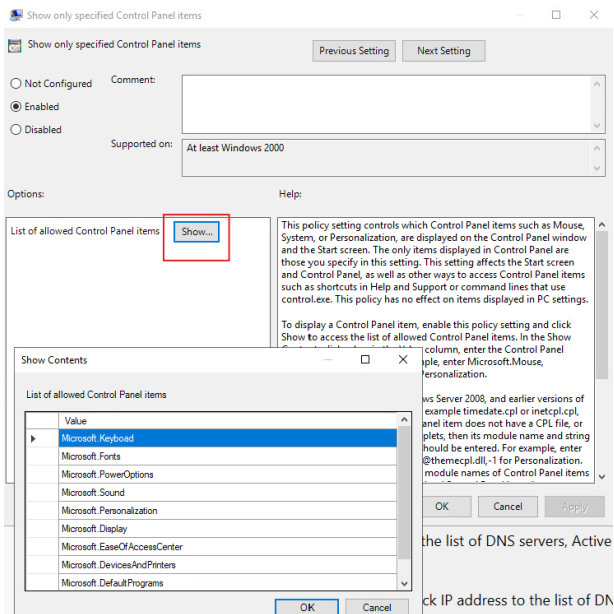
Kuvio 16. Limit\_controlPanel GPO

Muokkasimme asetusta Show only specified Control Panel items, jonka avulla saimme määritettyä käyttäjälle näkyvät paneelin asetukset. (Kuvio 17.)



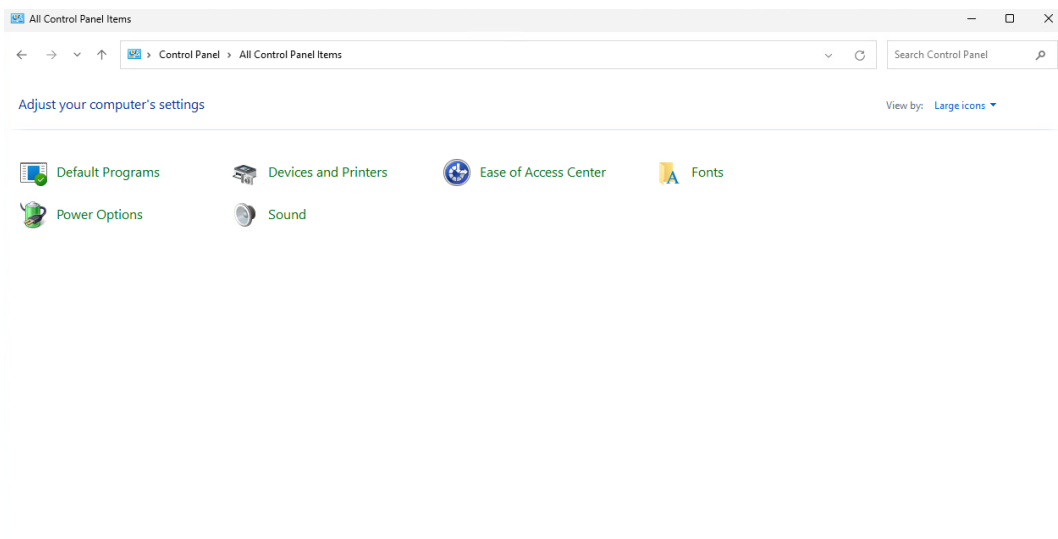
Kuvio 17. Ohjauspaneelin rajoittaminen

Vaihdoimme asetuksen enabled tilaan. Lisäsimme käyttäjille näkyviin ohjauspaneelin asetuksiin kohteita avaamalla options-ikkunan show-painikkeesta. Valitsimme kohteita tarpeen mukaan kuvion 18 mukaisesti.



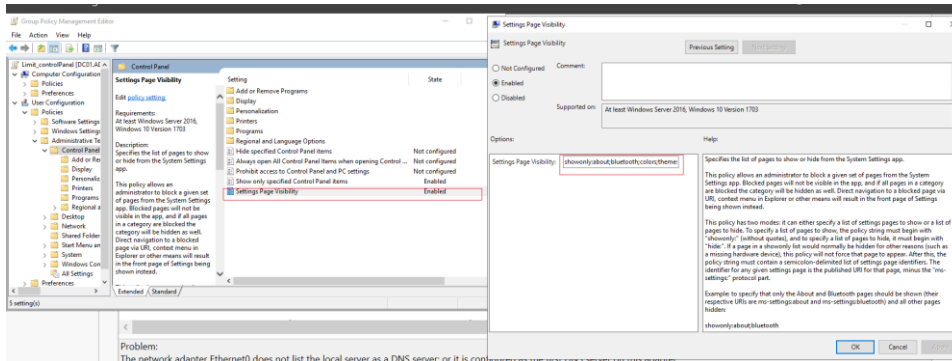
Kuvio 18. Sallitut asetukset

Siirryimme WS01:lle työntekijän tunnuksilla ja asetukset olivat astuneet voimaan. Käyttäjä pystyy siis muokkaamaan vain muutamia asetuksia ohjauspaneelin kautta. (Kuvio 19)



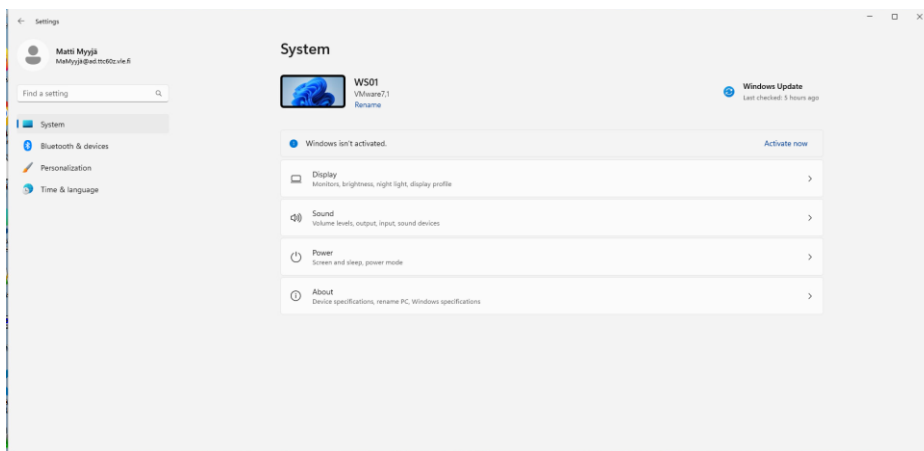
Kuvio 19. Työntekijän ohjauspaneeli

Rajasimme myös työntekijöiden mahdollisuutta muokata työaseman asetuksia Asetukset-valikon kautta. Laitoimme Settings page visibility asetuksen käyttöön ja listasimme sinne sivut, jotka halusimme näkyvän käyttäjien Asetukset-valikossa. (Kuvio 20)



Kuvio 20. Asetukset-valikon näkyvät sivut

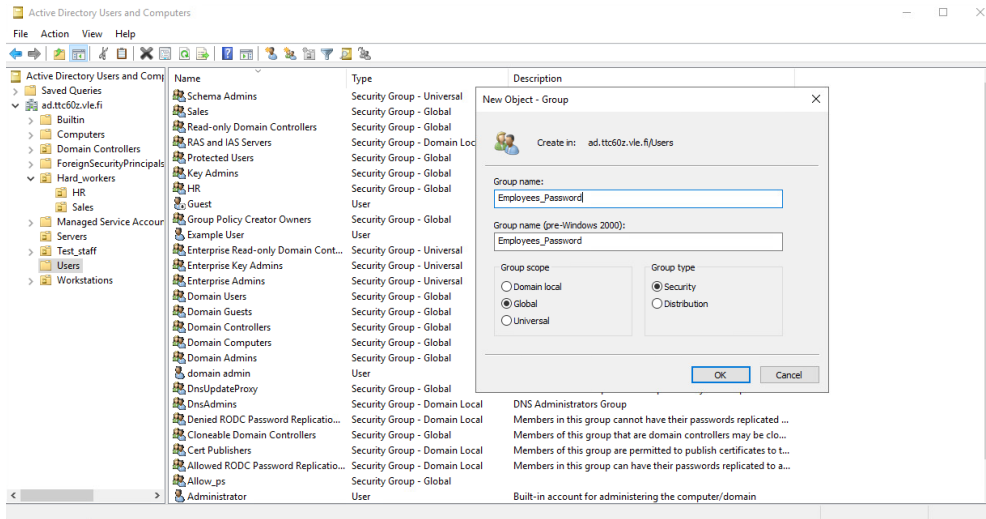
Asetusten voimaantumisen jälkeen työntekijöiden Asetukset-valikko näytti kuvion 21 mukaiselta.



Kuvio 21. Työntekijälle näkyvät asetukset

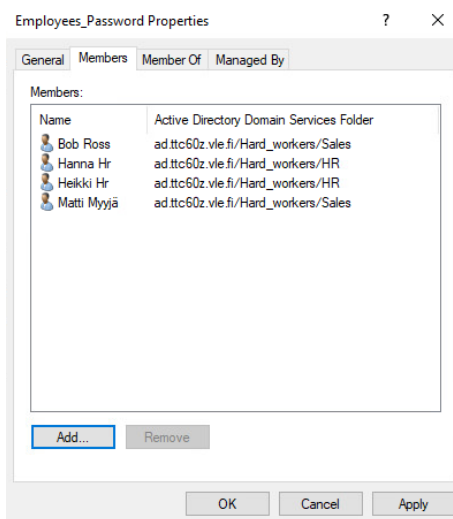
Huomasimme että file serverille SRV01 pystyi kirjautumaan millä vain tunnuksilla, ja päätimme rajata toistaiseksi kirjautumisen vain administraattoreille Allow log on locally asetuksella. (Kuvio 22).





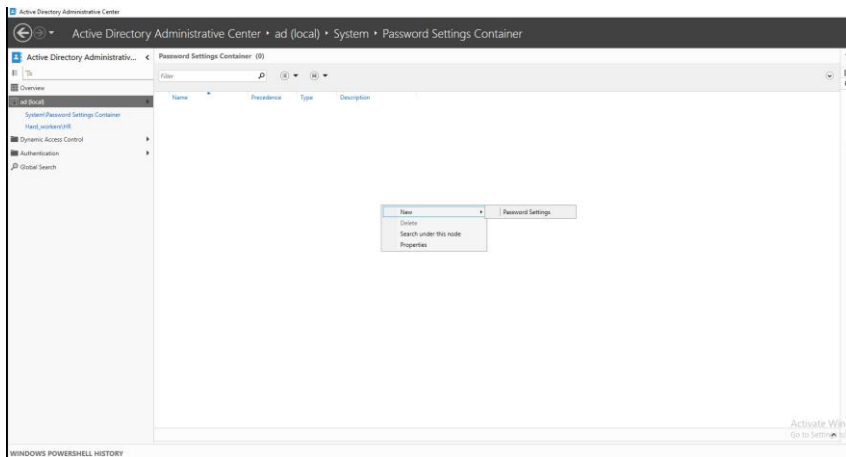
Kuvio 24. Uusi turvallisuusryhmä salasanaikäytänteitä varten

Lisäsimme luodun ryhmän työntekijöidemme käyttäjille. Siirsimme aiemmin tekemämme AD ryhmän myös Hard\_workers OU:n alle. (Kuvio 25).



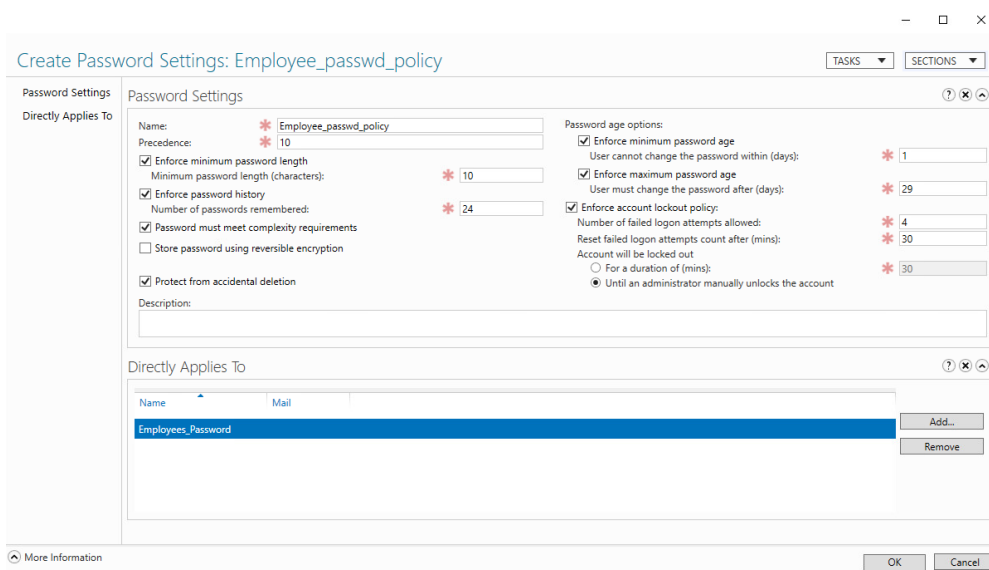
Kuvio 25. Employees\_Password ryhmän jäsenet

Avasimme DC01:lla Admin Directory Administrative centerin ja sijaintiin system\Password settings container ja loimme uuden salasana-asetuksen. (Kuvio 26).



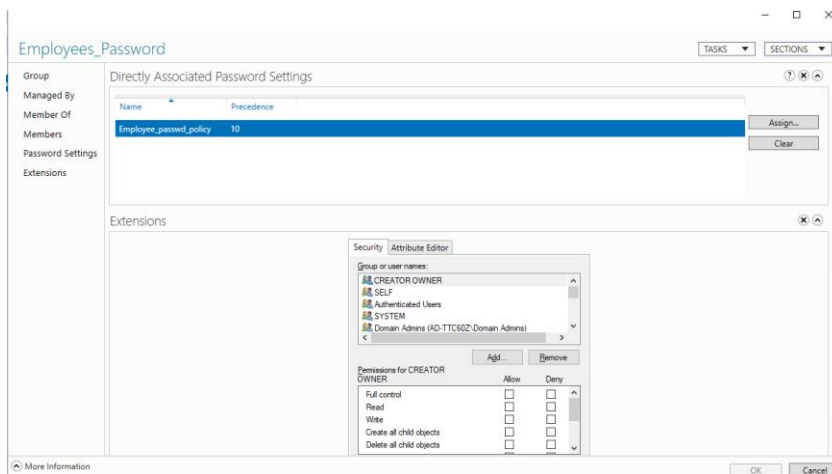
Kuvio 26. New password setting

Syötimme salasana-asetusten rajoitukset sekä ryhmän, jota se koskee. Halusimme, että työntekijöiden salasanat ovat vähintään 10 merkkiä pitkiä, salasana tulee vaihtaa 29 vuorokauden välein ja vanhoja salasanoja ei voi käyttää. (Kuvio 27).



Kuvio 27. Salasana-asetusten luonti

Kun siirryimme katsomaan employees\_password ryhmään vaikuttavia salasana-asetuksia password settings osiossa, näimme siellä tekemämme salasanapolitiikan. (Kuvio 28).



Kuvio 28. Ryhmään vaikuttavat

Ajoimme vielä powershell-komennon ja totesimme, että salasana politiikka tuli käyttöön työntekijöille. (Kuvio 29).

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ADUserResultantPasswordPolicy -Identity "BoRoss"

AppliesTo           : {CN=Employees_Password,OU=Hard_workers,DC=ad,DC=ttc60z,DC=vle,DC=fi}
ComplexityEnabled   : True
DistinguishedName   : CN=Employee_passwd_policy,CN=Password Settings Container,CN=System,DC=ad,DC=ttc60z,DC=vle,DC=fi
LockoutDuration     : 00:00:00
LockoutObservationWindow : 00:30:00
LockoutThreshold     : 4
MaxPasswordAge      : 29.00:00:00
MinPasswordAge      : 1.00:00:00
MinPasswordLength   : 10
Name                : Employee_passwd_policy
ObjectClass         : msDS-PasswordSettings
ObjectGUID          : 7c492259-21e3-4cb1-9321-62944813e9bd
PasswordHistoryCount : 24
Precedence          : 10
ReversibleEncryptionEnabled : False

PS C:\Users\Administrator>
```

Kuvio 29. Powershell testi

## 4 Pohdinta

Koventamisen toisessa labratyössä pääsimme syventymään koventamiseen ja käyttämään Microsoftin security compliance toolkittiä GPO kovennusten toteuttamiseksi. Saimme myös paremman kuvan GPO:iden käyttäytymisestä ja asetusten muokkaamisesta.

Yksi keskeisistä huomioista labratyössä oli ryhmäkäytäntöjen (GPO) monipuolisuus ja tehokkuus organisaation tietoturvan hallinnassa. GPO:n avulla voimme keskitetysti hallita ja määrittää turvallisuusasetuksia useille työasemille ja käyttäjäryhmille, mikä vähentää inhimillisten virheiden mahdollisuutta ja parantaa tietoturvan hallittavuutta. Tämä korostui esimerkiksi siinä, kuinka saimme estettyä RDP käytön tietyiltä käyttäjäryhmiltä ja rajoitettua Control Panel- ja settings valikkoja, mikä vähentää väärinkäytön riskiä ja yksinkertaistaa käyttäjäkokemusta.

Lisäksi salasanaikäytännöt (Fine-Grained Password Policies) olivat uusi oppimisen osa-alue. Niiden avulla pystyimme räätälöimään eri käyttäjäryhmille soveltuvat salasanavaatimukset, mikä tuo joustavuutta organisaation tietoturvakäytäntöihin. Tämä mahdollistaa sen, että korkeamman riskin ryhmillä, kuten ylläpitäjillä, voi olla tiukemmat salasanavaatimukset verrattuna tavallisiin käyttäjiin.

Labran toteuttaminen sujui suurimmaksi osaksi ilman isompia ongelmia, ja nekin ongelmat mitä tuli vastaan saatiin ratkottua yhteistuumin ja niistäkin opittiin paljon. Esimerkiksi SCT:n käyttäminen ja FGPP tulivat uusina asioina. Syvennyimme myös hieman ryhmäkäytäntöjen hallitsemiseen OU tasolla.



## Lähteet

Configure fine grained password policies for Active Directory Domain Services. Microsoft Learn artikkeli. 2024. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/adac/fine-grained-password-policies?tabs=adac>

gpresult. Microsoft Learn artikkeli. 2023. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult>

Group Policy Best Practices. Netwrix ohje. 2024. Viitattu 3.10.2024. [https://www.netwrix.com/group\\_policy\\_best\\_practices.html](https://www.netwrix.com/group_policy_best_practices.html)

Group Policy Objects. Microsoft Learn artikkeli. 2018. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/previous-versions/windows/desktop/policy/group-policy-objects>

gpupdate. Microsoft Learn artikkeli. 2023. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate>

Microsoft Security Compliance Toolkit - How to use. Microsoft Learn artikkeli. 2024. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/security-compliance-toolkit-10>

Pasi Hyytiäinen. TTC6050-Koventaminen AD, PIM&PAM, JIT & JEA. JAMK opetus PDF. 2024. Viitattu 3.10.2024. [https://moodle.jamk.fi/pluginfile.php/1461084/mod\\_label/intro/AD%20pimpam%20JIT.pdf](https://moodle.jamk.fi/pluginfile.php/1461084/mod_label/intro/AD%20pimpam%20JIT.pdf)

Shruti456rawal. What is System Hardening? Geeksforgeeks-verkkosivuston artikkeli. 1.3.2024. Viitattu 3.10.2024. [https://www.geeksforgeeks.org/what-is-system-hardening/?ref=header\\_outind](https://www.geeksforgeeks.org/what-is-system-hardening/?ref=header_outind)

Understanding the Remote Desktop Protocol (RDP). Microsoft Learn artikkeli. 2023. Viitattu 3.10.2024. <https://learn.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol>