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

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Koventaminen-opintojakson toisessa labratyössä tarkoituksena on koventaa virtuaaliympäristömme Windows 11 virtuaaliympäristömme Microsoftin tuotteita. Tähän kuului varsinkin GPO kovennukset (DC01:llä), sekä omia valikoituja kovennuksia mitkä ryhmä näki tarpeellisiksi. Käytimme Security Compliance Toolkittiä luodaksemme pohjan kovennuksille. 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 kuuluessa 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 tekemään 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 käyttäen. (Understanding the Remote Desktop Protocol (RDP).2023)

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

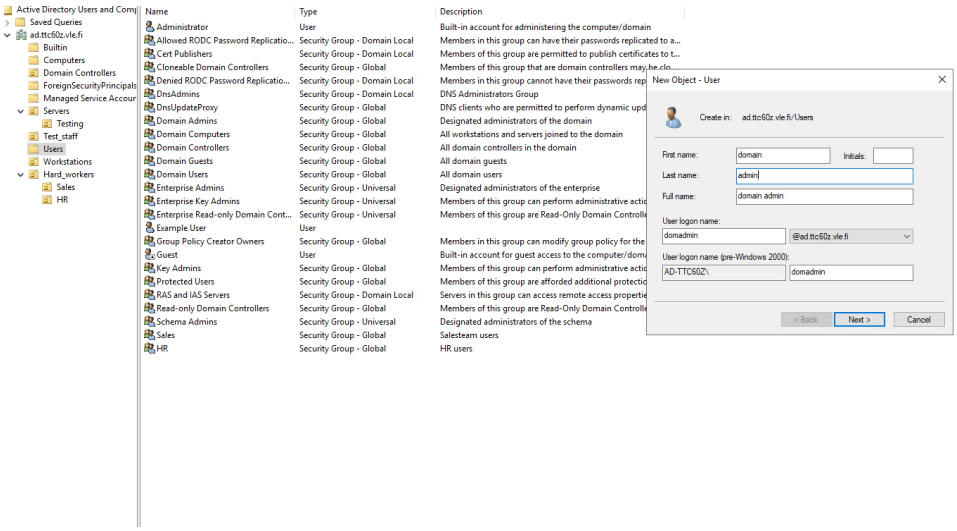
Gpresult /r on komento, joka näyttää tietokoneessa sovellettavat GPO:t. (gpresult.2023)

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.

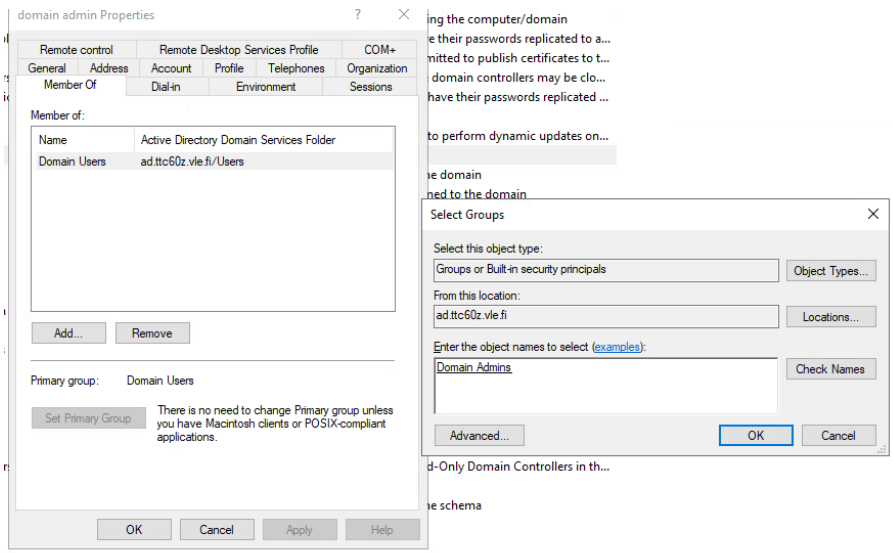
3.1 Security Compliance Toolkitin asennus

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



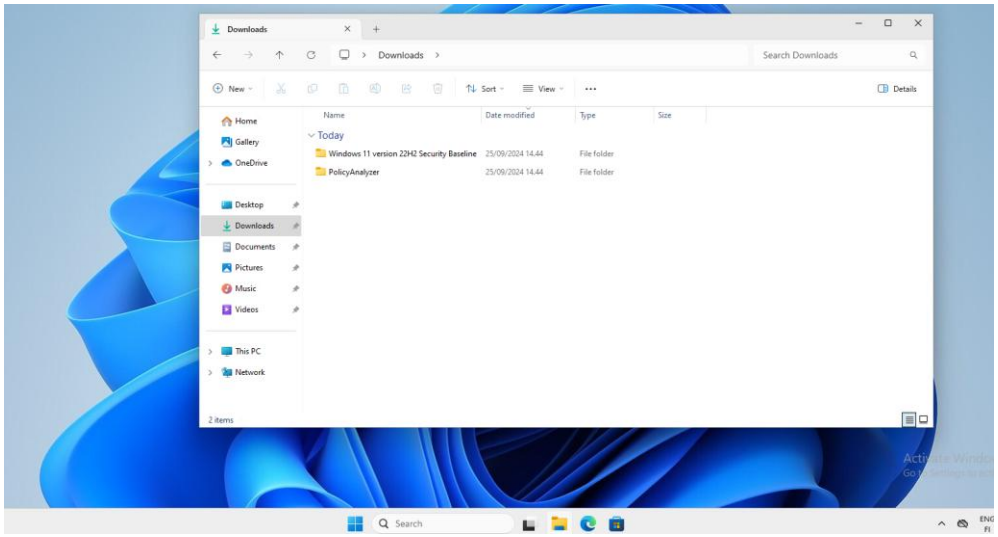
Kuvio 1. Domain admin -käyttäjän luonti

Lisäsimme käyttäjän turvaryhmään domain admins. (Kuvio 2).



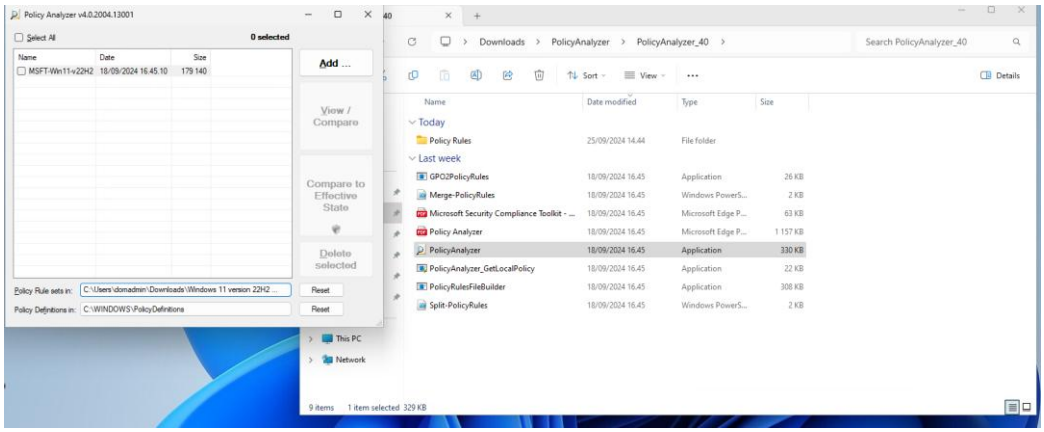
Kuvio 2. Käyttäjän lisääminen turvaryhmään

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



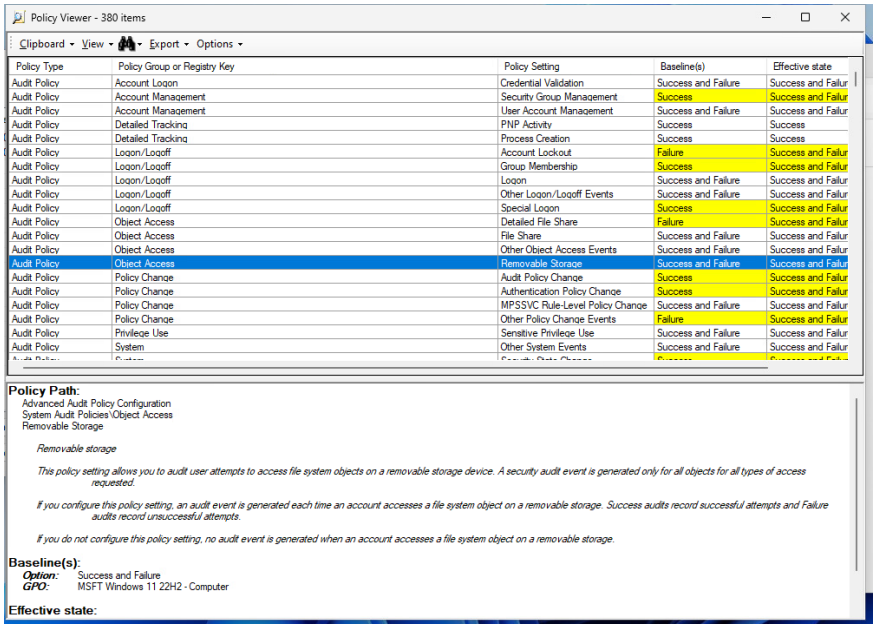
Kuvio 3. Asennetut paketit

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



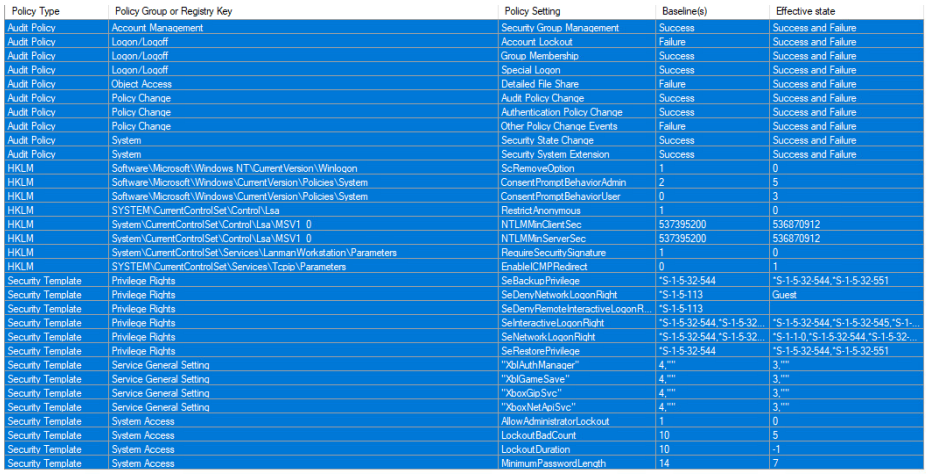
Kuvio 4. PolicyAnalyzer

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



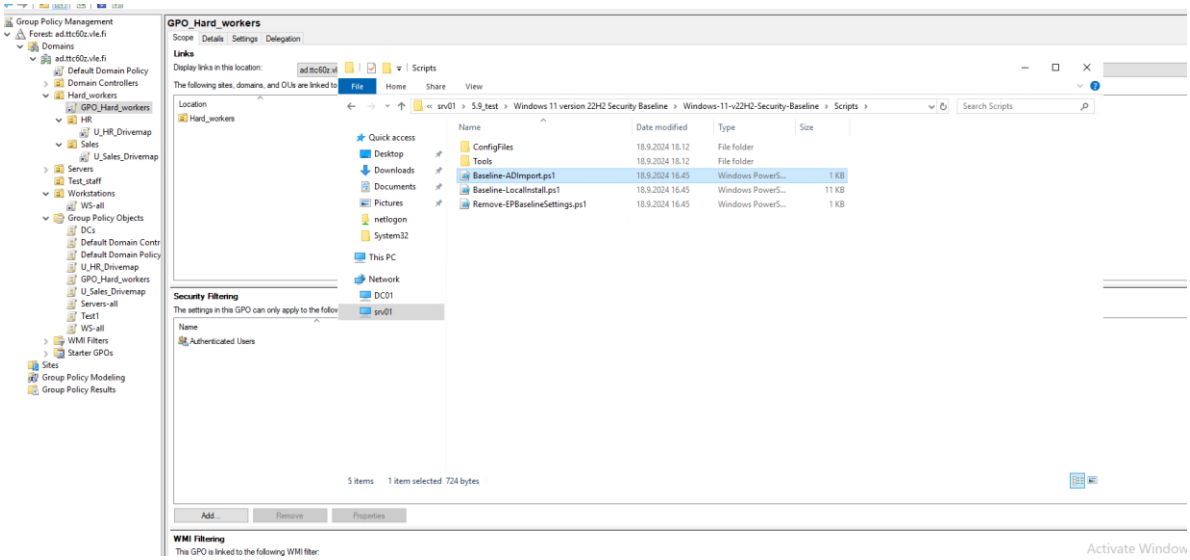
Kuvio 5. Politiikkojen vertailu

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



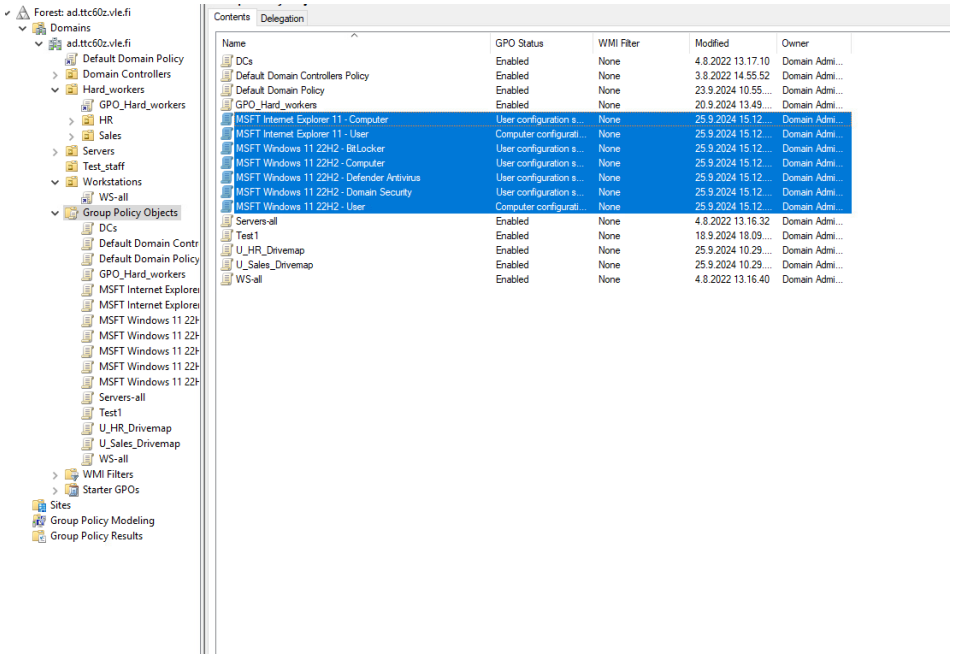
Kuvio 6. Konfliktit

Siirsimme WS01:llä toolkitin jaetulle verkkoasemalle, johon pääsimme käsiksi DC01:llä. Siirryimme DC01:lle ja ajoimme tiedoston Baseline-ADImport.ps1 powershellillä. (Kuvio 7).

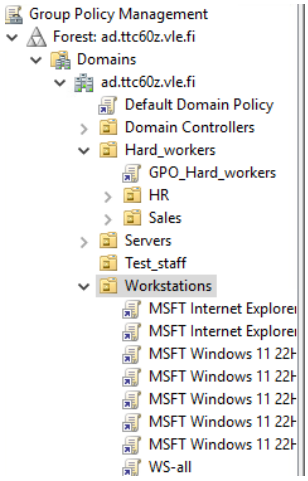


Kuvio 7. DC scripti

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.

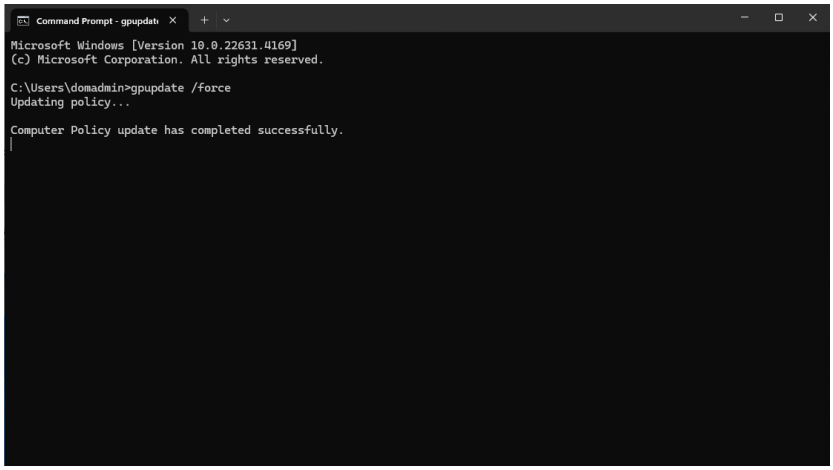


Kuvio 8. Policy objects



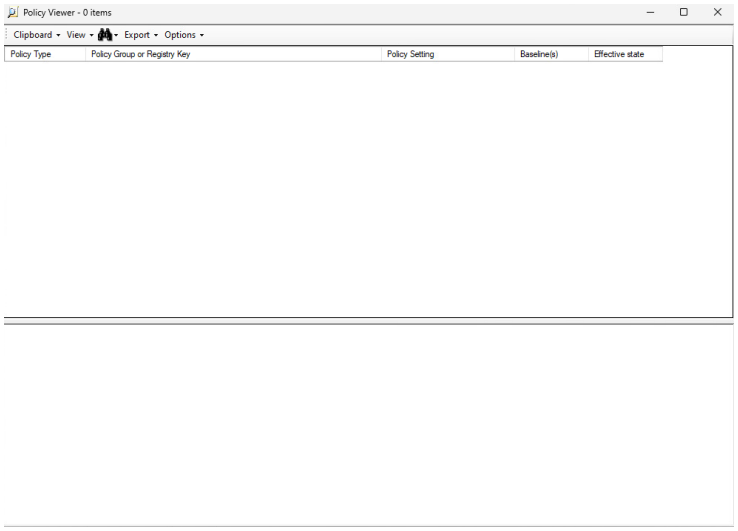
Kuvio 9. workstations

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



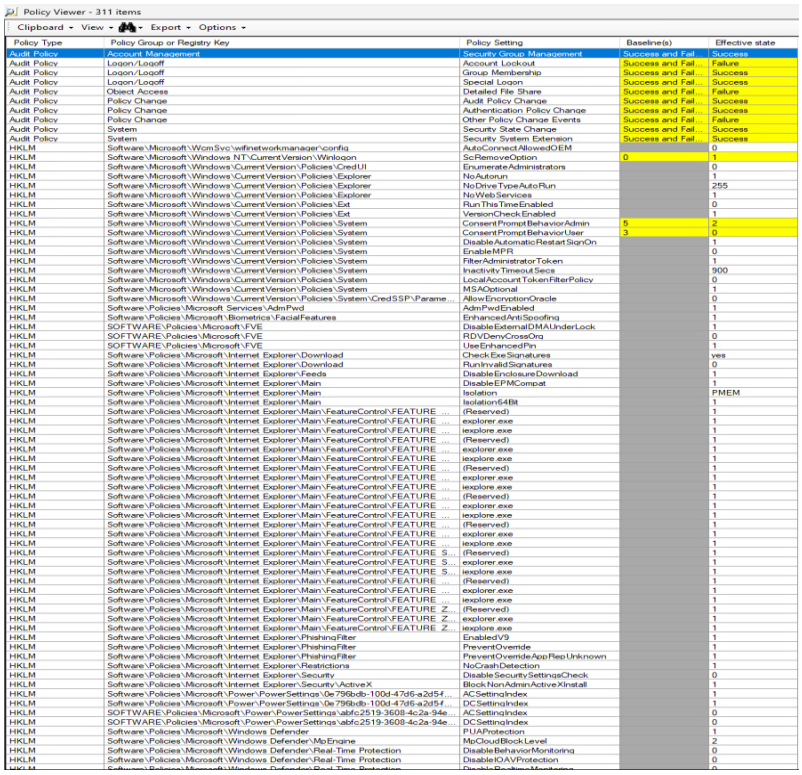
Kuvio 10. Gpupdate

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



Kuvio 11. Analyysi lopputilanteessa

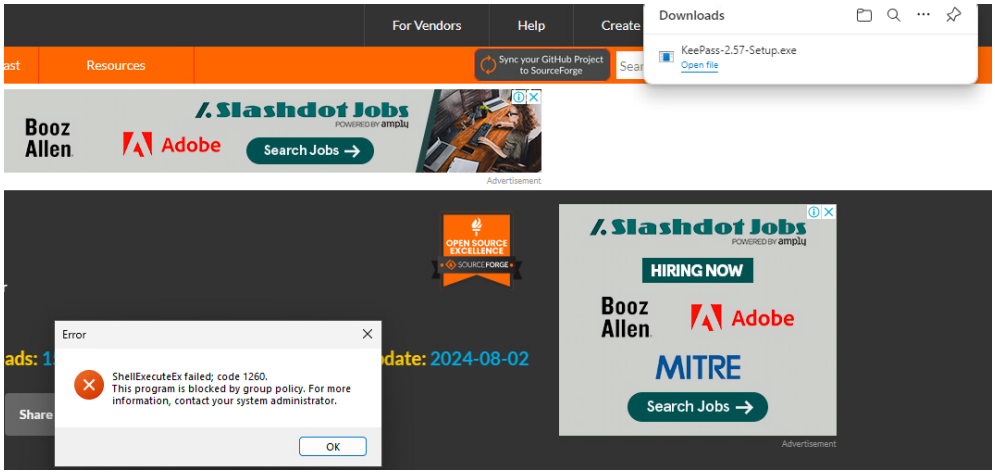
Ajoimme vielä analyysin asennetuista politiikoista. Lista on erittäin pitkä, joten vain pieni osa mahtui kuvaan, mutta kuten kuviosta 12 ilmenee, listassa on 311 kohtaa.



Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Management	Security Group Management	Success and Fail...	Success
Audit Policy	Logon/Logoff	Account Lockout	Success and Fail...	Failure
Audit Policy	Logon/Logoff	Group Membership	Success and Fail...	Success
Audit Policy	Logon/Logoff	Special Logon	Success and Fail...	Success
Audit Policy	Object Access	Detailed File Share	Success and Fail...	Failure
Audit Policy	Policy Change	Audit Policy Change	Success and Fail...	Success
Audit Policy	Policy Change	Authentication Policy Change	Success and Fail...	Success
Audit Policy	Policy Change	Other Policy Change Events	Success and Fail...	Failure
Audit Policy	System	Security State Change	Success and Fail...	Success
Audit Policy	System	Security System Extension	Success and Fail...	Success
HKLM	Software\Microsoft\WcmSvc\wifinetworkmanager\config	AutoConnectAllowedOEM		0
HKLM	Software\Microsoft\Windows NT\CurrentVersion\Winlogon	ScRemoveOption	0	1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\CredUI	EnumerateAdministrators		0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoAutorun		1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoDriveTypeAutoRun		255
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer	NoWebServices		1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Ext	RunThisTimeEnabled		0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\Ext	VersionCheckEnabled		1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorAdmin	5	2
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	ConsentPromptBehaviorUser	3	0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	DisableAutomaticRestartSignOn		1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	EnableMPR		0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	FilterAdministratorToken		1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	InactivityTimeoutSecs		900
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	LocalAccountTokenFilterPolicy		0
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System	MSAOptional		1
HKLM	Software\Microsoft\Windows\CurrentVersion\Policies\System\CredSSP\Parame...	AllowEncryptionOracle		0
HKLM	Software\Policies\Microsoft Services\AdmPwd	AdmPwdEnabled		1
HKLM	Software\Policies\Microsoft\Biometrics\FacialFeatures	EnhancedAntiSpoofing		1
HKLM	SOFTWARE\Policies\Microsoft\FVE	DisableExternalDMAUnderLock		1
HKLM	SOFTWARE\Policies\Microsoft\FVE	RDVDenyCrossOrg		0
HKLM	SOFTWARE\Policies\Microsoft\FVE	UseEnhancedPin		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Download	CheckExeSignatures		yes
HKLM	Software\Policies\Microsoft\Internet Explorer\Download	RunInvalidSignatures		0
HKLM	Software\Policies\Microsoft\Internet Explorer\Feeds	DisableEnclosureDownload		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main	DisableEPMCompat		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main	Isolation		PMEM
HKLM	Software\Policies\Microsoft\Internet Explorer\Main	Isolation64Bit		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE S...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE S...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE S...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE ...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE Z...	(Reserved)		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE Z...	explorer.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE Z...	iexplore.exe		1
HKLM	Software\Policies\Microsoft\Internet Explorer\PhishingFilter	EnabledV9		1
HKLM	Software\Policies\Microsoft\Internet Explorer\PhishingFilter	PreventOverride		1
HKLM	Software\Policies\Microsoft\Internet Explorer\PhishingFilter	PreventOverrideAppRepUnknown		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Restrictions	NoCrashDetection		1
HKLM	Software\Policies\Microsoft\Internet Explorer\Security	DisableSecuritySettingsCheck		0
HKLM	Software\Policies\Microsoft\Internet Explorer\Security\ActiveX	BlockNonAdminActiveXInstall		1
HKLM	Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f...	ACSettingIndex		1
HKLM	Software\Policies\Microsoft\Power\PowerSettings\0e796bdb-100d-47d6-a2d5-f...	DCSettingIndex		1
HKLM	SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94e...	ACSettingIndex		0
HKLM	SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519-3608-4c2a-94e...	DCSettingIndex		0
HKLM	Software\Policies\Microsoft\Windows Defender	PUAProtection		1
HKLM	Software\Policies\Microsoft\Windows Defender\MpEngine	MpCloudBlockLevel		2
HKLM	Software\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableBehaviorMonitoring		0
HKLM	Software\Policies\Microsoft\Windows Defender\Real-Time Protection	DisableIOAVProtection		0

Kuvio 12. Asennetut politiikat

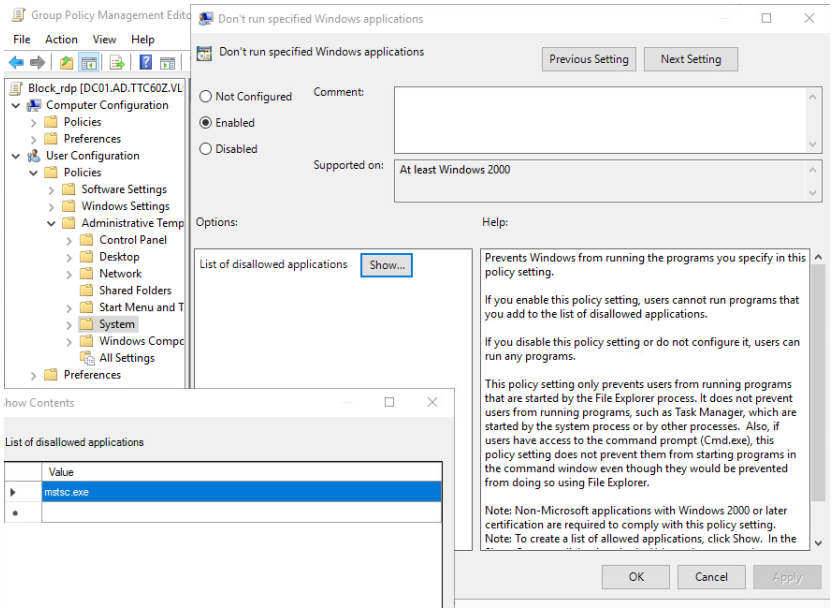
DC01:llä ajamamme skripti toi mukanaan useita koventamisen näkökulmasta hyödyllisiä asetuksia käyttöön, esimerkiksi yksi näistä on ohjelmistojen asentamisen estäminen käyttäjillä. (Kuvio 13).



Kuvio 13. Estetty asennus

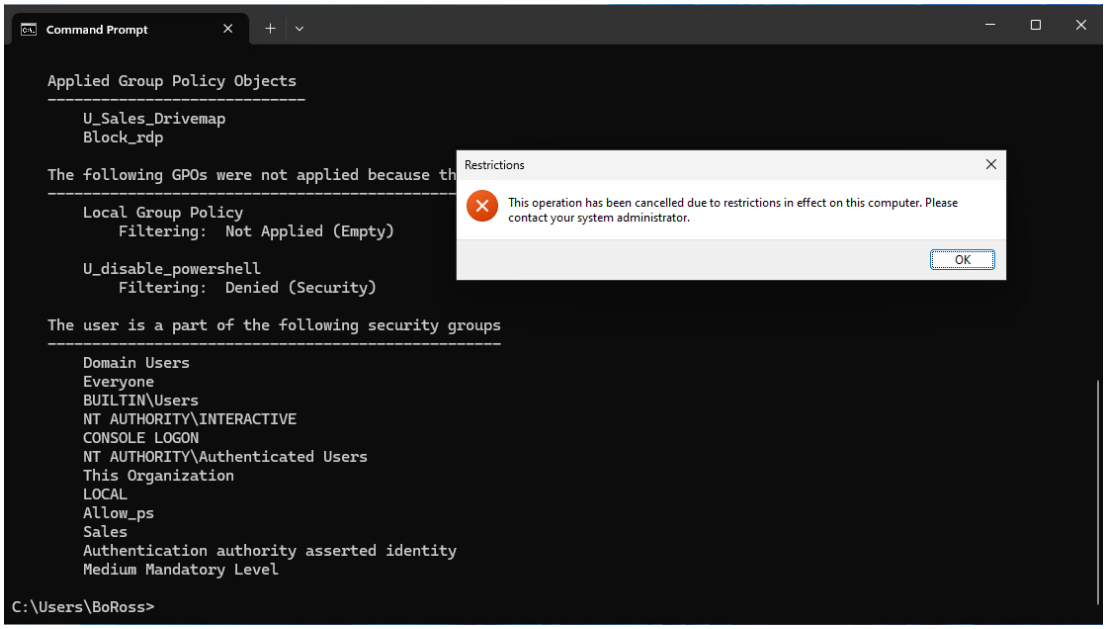
3.2 Etäkäytön estäminen

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 komentokehotteella komennolla gpresult /r mitkä politiikat kohdetuvat käyttäjään ja sieltä löytyi luomamme etäkäytön estävä politiikka. (Kuvio 15).

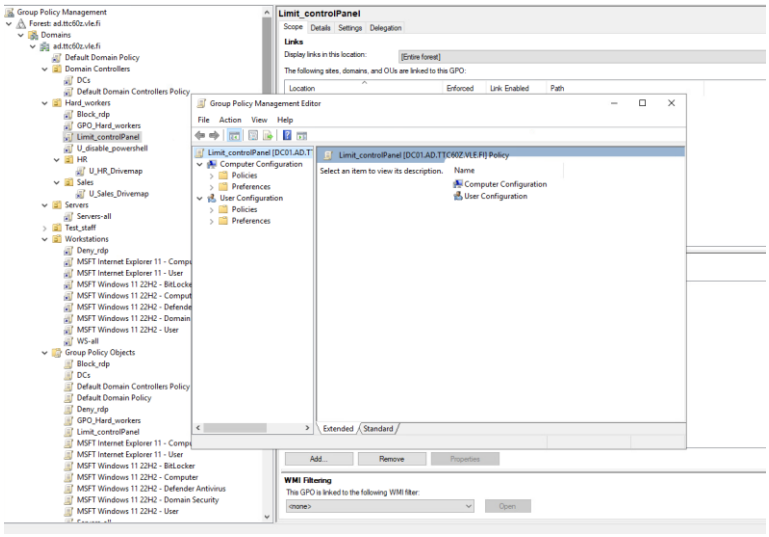


Kuvio 15. Estetty etäkäyttö

3.3 Työaseman asetusten muokkaamisen rajoittaminen

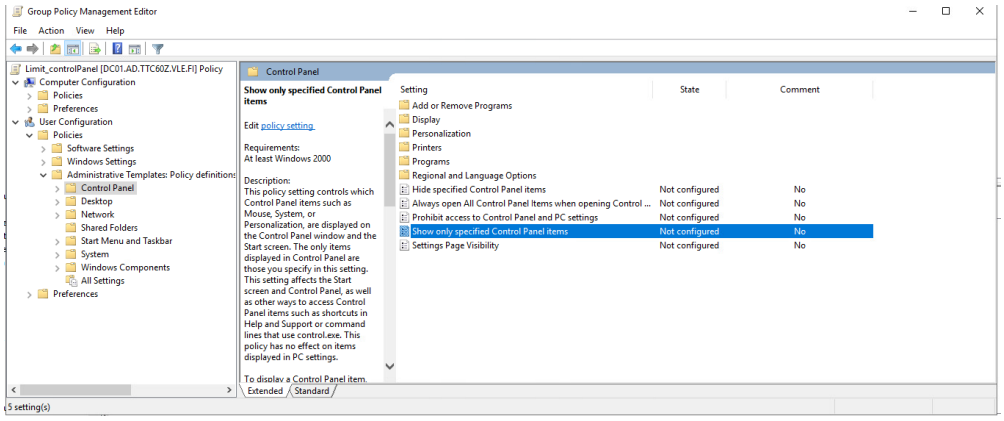
Kaikilla käyttäjillä ei ole tarvetta päästä käsiksi työaseman kaikkiin asetuksiin, joten päätimme rajoittaa näiden asetusten näkyvyyttä.

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



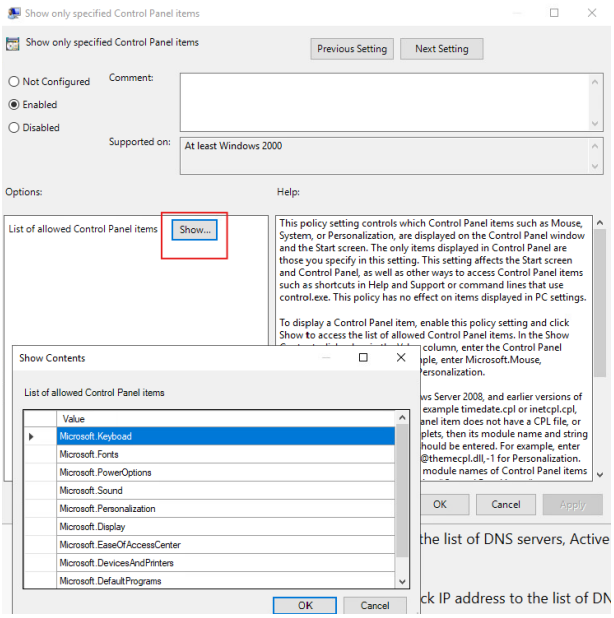
Kuvio 16. Limit_controlPanel GPO

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



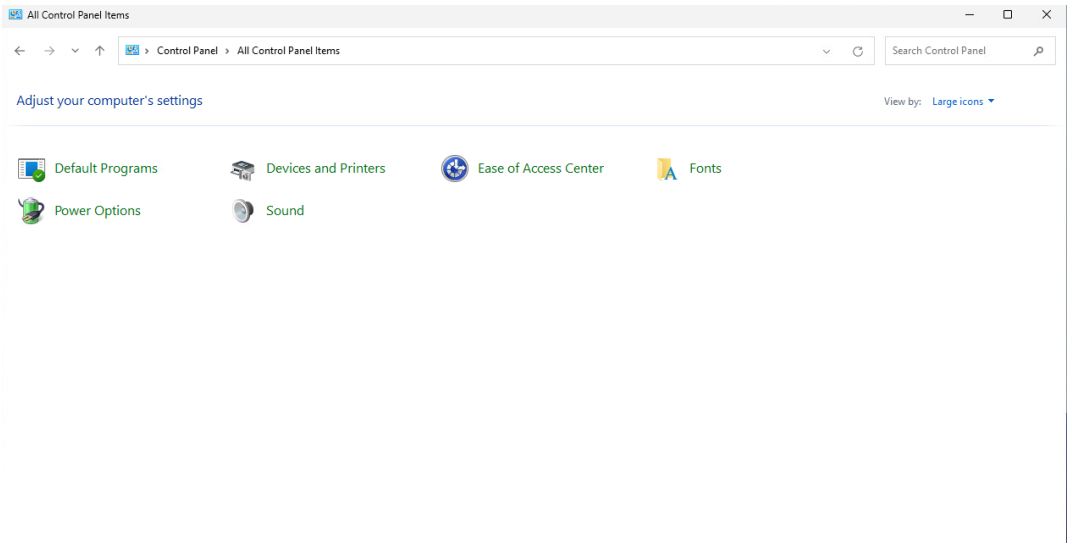
Kuvio 17. Ohjauspaneelin rajoittaminen

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



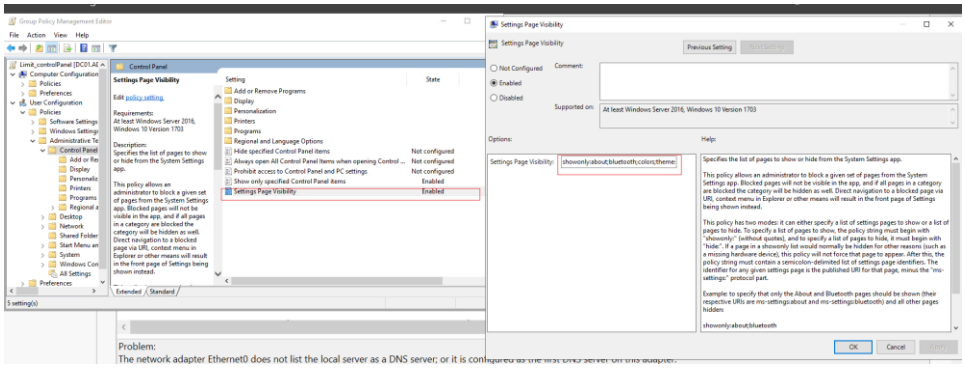
Kuvio 18. Sallitut asetukset

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



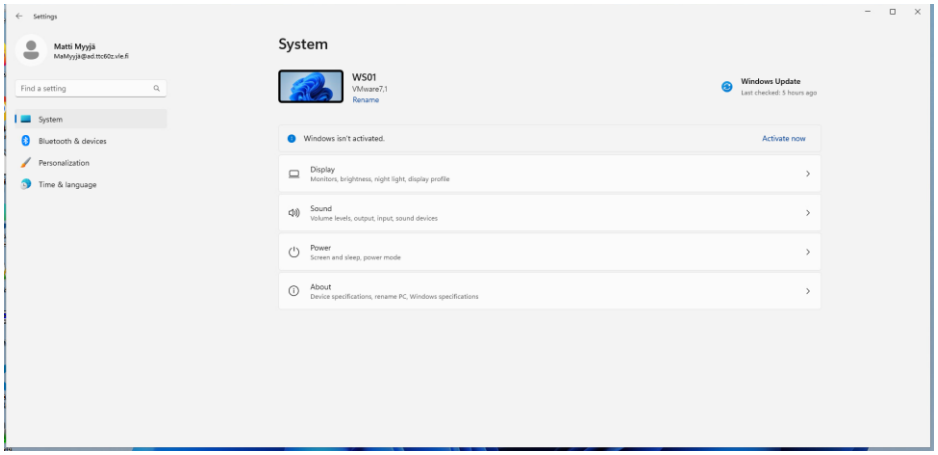
Kuvio 19. Työntekijän ohjauspaneeli

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)



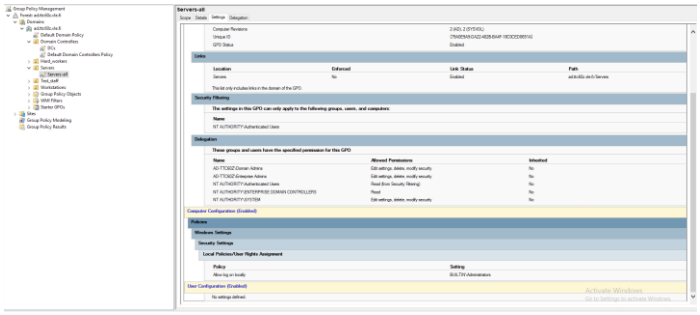
Kuvio 20. Asetukset-valikon näkyvät sivut

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



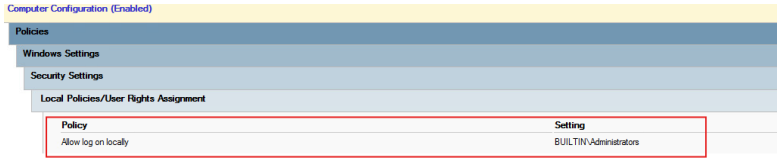
Kuvio 21. Työntekijälle näkyvät asetukset

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 22. Local Log On

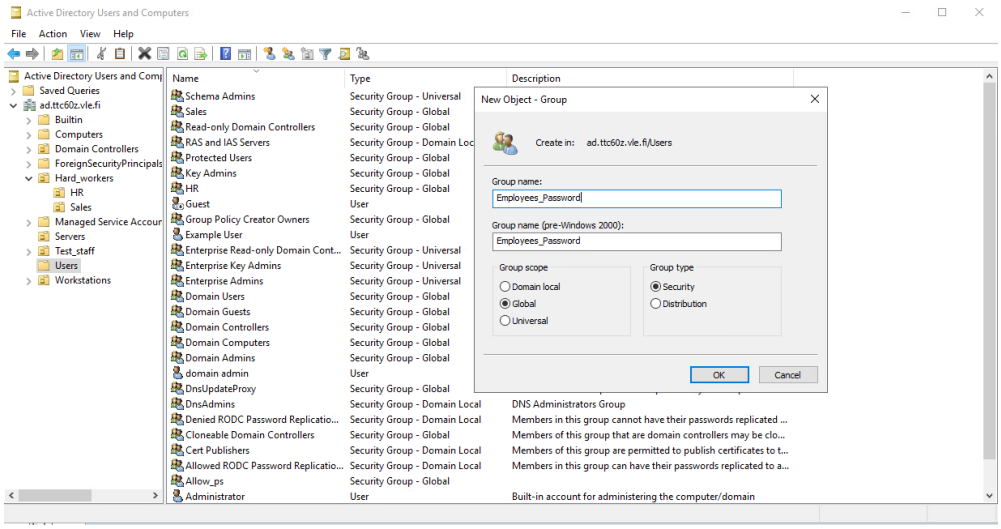
Käytännössä muutimme siis kuvion 23 mukaisen asetuksen.



Kuvio 23. Muutettu asetus

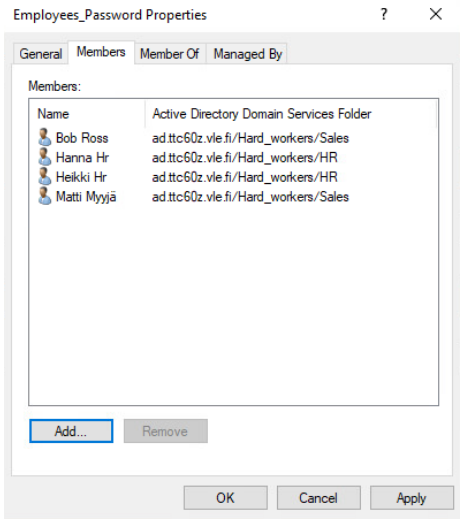
3.4 Fine grained password policies

Luodaksemme salasanakäytänteitä, jotka koskevat rajattua käyttäjäryhmää, käytimme fine grained password policy menetelmää. Teimme ensin turvallisuusryhmän, jonka lisäsimme kaikille työntekijöille, jotta salasana käytänteet koskevat vain heitä. Tämä asetus tulisi voimaan normaalisti kaikille, mutta emme halua muuttaa adminien salasanoja, koska se on ohjeistuksessa kielletty. (Kuvio 24). Turvallisuus ryhmä kannattaisi nimetä U_ alkuiseksi, selkeytettäväksi politiikan kohdistumista käyttäjiin.



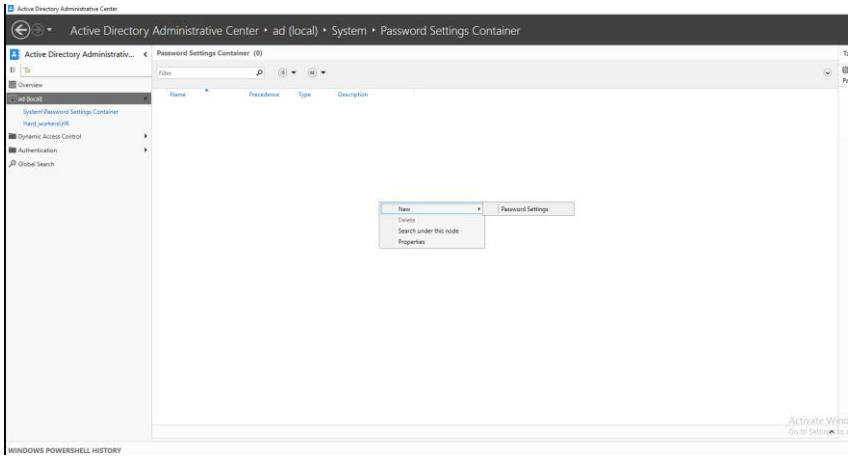
Kuvio 24. Uusi turvallisuusryhmä salasanakäytänteitä varten

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



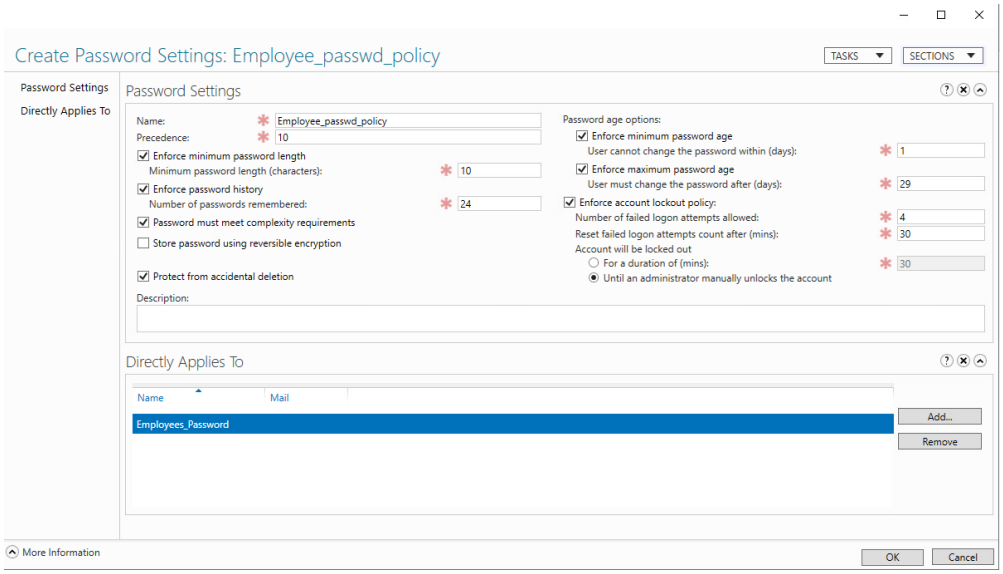
Kuvio 25. Employees_Password ryhmän jäsenet

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



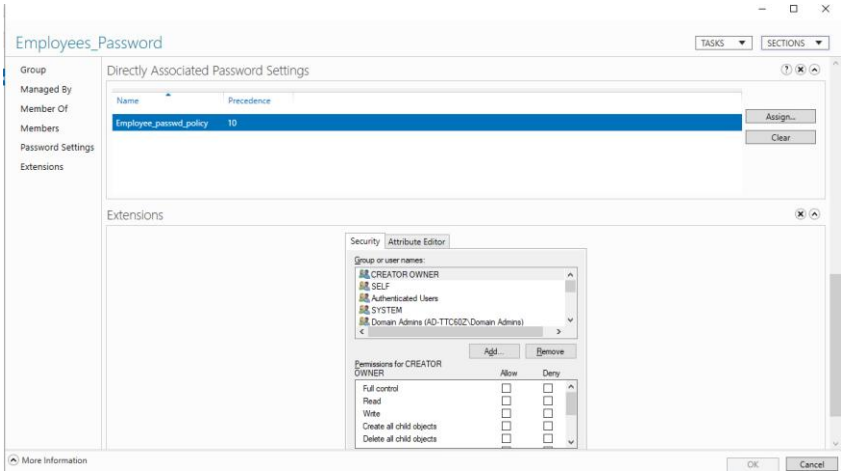
Kuvio 26. New password setting

Syötimme salasanapolitiikan 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).



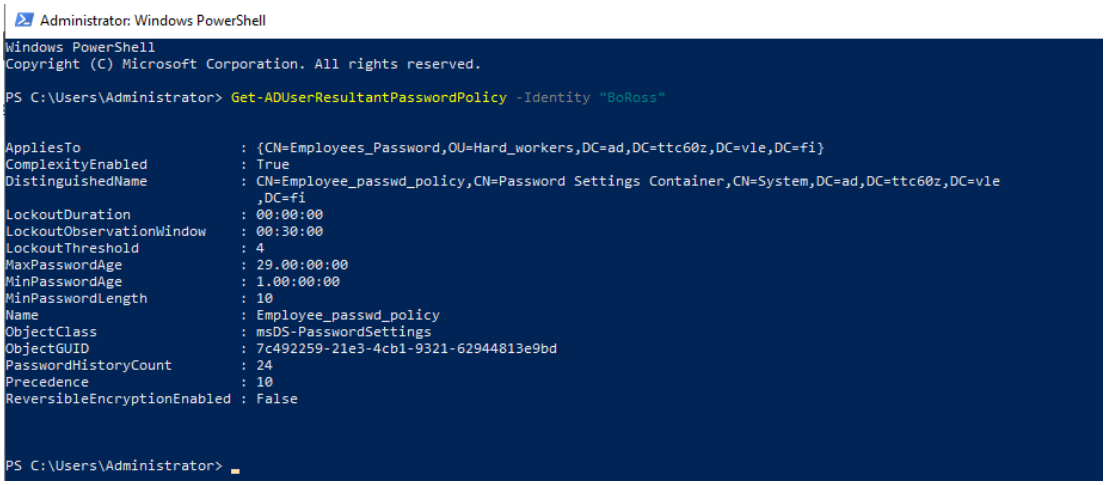
Kuvio 27. Salasana-asetusten luonti

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).



Kuvio 29. Powershell testi

4 Pohdinta

Koventamisen toisessa labratyössä pääsimme syventymään koventamiseen ja käyttämään Micosoftin 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. GPOn 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 salasanakäytännöt (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

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

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

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