jamk

Koventaminen – Labra 1

Ryhmä 3

Sami Koivisto

Eino Puttonen

Jussi-Pekka Rantala

Markku Sutinen

Harjoitustyö

Helmikuu 2024

Tieto- ja viestintätekniikan tutkinto-ohjelma (AMK)

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

1 Johdanto 4
2 Teoria 5
2.1 Koventaminen 5
2.2 Active Directory 5
2.3 Group Policy 6
3 Toteutus 7
3.1 Best Practise Analyzer -alkutilanne 7
3.2 Tiedostopalvelimen asennus 8
3.3 Tiedostonpalvelimen varmuuskopionti 14
3.4 Organization Unitin suojaaminen 20
3.5 Microsoft Defender Antivirus 21
3.6 Strong key 22
3.7 Account lockout threshold 23
3.8 Audit account logon events sekä Audit policy change 24
3.9 Best Practice Analyzer -loppuanalyysi 26
4 Pohdinta 28
Lähteet 30

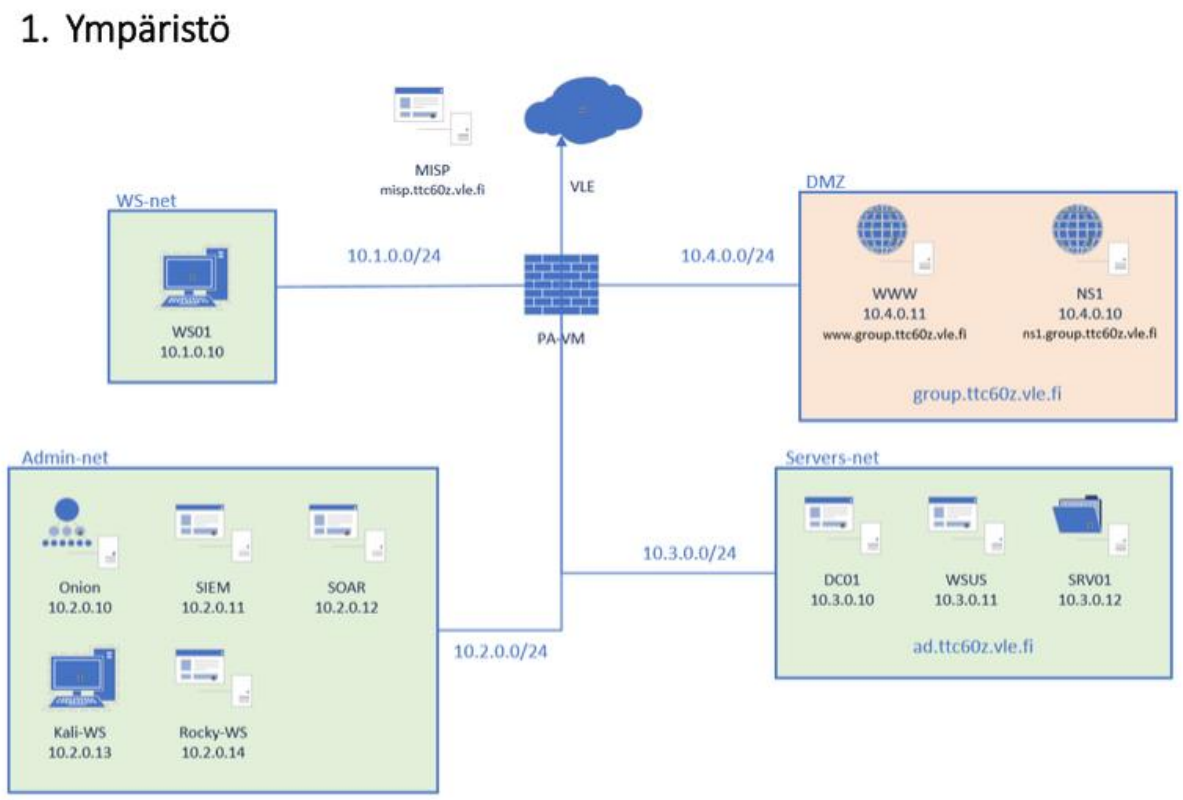
Kuviot

Kuvio 1. VLE -ympäristö 4
Kuvio 2. BPA -tulokset 1/2 7
Kuvio 3. BPA -tulokset 2/2 8
Kuvio 4. Poistetut roolit ja ominaKovisuudet 9
Kuvio 5. File Server -ominaisuuksien asennus 10
Kuvio 6. Lisäosan asennus File Serverille 11
Kuvio 7. SMB Share - Advancen valinta 12
Kuvio 8. Kansion ominaisuudet ja asennus 13
Kuvio 9. Ryhma 3 -kansion todentaminen 14
Kuvio 10. Varmuuskopiota ei löytynyt 15

Kuvio 11. Osion alustus kiintolevylle 16
Kuvio 12. Uusi varmuuskopionti osio 17
Kuvio 13. Windows Server Backup -roolin asennus 18
Kuvio 14. Schedule Task asetuksien asentaminen 19
Kuvio 15. Onnistunut varmuuskopionti 20
Kuvio 16. OU:n suojaaminen 21
Kuvio 17. Turn off Windows Defender Antivirus disabled tilassa 22
Kuvio 18. Vahva istuntoavain enabled tilassa 23
Kuvio 19. Account lockout threshold 24
Kuvio 20. Audit logon events policy 25
Kuvio 21. Audit policy change -policy 26
Kuvio 22. BPA -analyysi lopussa 27

1 Johdanto

Tässä labrassa syvennymme Active Directoryn (AD) ja Group policy objectin (GPO) käyttöön tietoturvallisuuden koventamisessa. Samalla tutustumme Best Practice Analyzer (BPA) -ohjelman käyttöön ja arvioimme sen antamia tuloksia. Harjoituksen aikana SRV01 Windows Server -palvelinta kovennetaan poistamalla tarpeettomat roolit, ja se konfiguroidaan toimimaan tiedostopalvelimena. Raportissa käsitellään teoriaa, kovennustoimenpiteitä, tiedostopalvelimen konfigurointia sekä ryhmän kolme pohdintaa harjoituksen kokonaisuudesta. Harjoitus suoritetaan VLE-ympäristössä, ja käytetty topologia on esitetty kuviossa 1 (ks. Kuvio 1).



Kuvio 1. VLE -ympäristö

2 Teoria

2.1 Koventaminen

Järjestelmän koventaminen on olennainen osa tietoturvallisuudessa. Järjestelmän koventaminen on sovellusten, järjestelmien ja infrastruktuurin parhaiden käytäntöjen soveltamista yhdessä muiden peruselementtien ohella. Noudattamalla keskeisten tietoturvallisuuden toimijoiden ohjeita kuten esimerkiksi CIS benchmark, Microsoft security baseline tai National Institute of Standards and Technology (NIST), organisaatiot voivat merkittävästi alentaa tietoturvauhkaa, poistaa järjestelmän haavoittuvuuksia tai pienentää hyökkäyspinta-alaa. On olemassa monenlaisia kovennuksia, joista osa on seuraavia: (John Gates 2023.)

- Sovelluksen koventaminen,
- Palvelimen koventaminen,
- Tietokannan koventaminen,
- Tietoliikenneverkon koventaminen,
- Käyttöjärjestelmän koventaminen.

2.2 Active Directory

Active Directory on Microsoftin kehittämä hakemistopalvelu. Se on suunniteltu toimimaan Windows Serverillä ja antamaan järjestelmänvalvojille mahdollisuuden hallita käyttöoikeuksia ja valvoa verkkoresurssien käyttöä. Active Directory tallentaa verkossa olevista objekteista tietoja ja tekee niistä helposti löydettäviä ja käytettäviä järjestelmänvalvojille ja käyttäjille. Active Directory käyttää jäsenneltyä tietovarastoa perustana loogiselle, hierarkkiselle hakemistotiedon järjestämiselle. (Active Directory Domain Services Overview 2022.)

Tietovarasto, joka tunnetaan myös hakemistona, sisältää tietoja Active Directoryn objekteista. Objektit sisältävät yleensä jaettuja resursseja kuten verkon käyttäjä ja tietokonetilejä, palvelimia ja tulostimia. (Active Directory Domain Services Overview 2022.)

Turvallisuus on integroitu Active Directoryyn sisäänkirjautumisen todennuksen ja pääsynhallinnan kautta hakemiston objekteihin. Yhdellä sisäänkirjautumisella, järjestelmänylläpitäjät voivat hallita organisaatiota ja hakemistotietoja kaikkialla heidän verkossaan ja valtuutetut verkon käyttäjät voivat käyttää resursseja missä tahansa verkossa. Käytäntöpohjainen hallinta helpottaa monimutkaisimmankin verkon hallintaa. (Active Directory Domain Services Overview 2022.)

2.3 Group Policy

Group Policy on ominaisuus, jolla voidaan hallita käyttäjätilejä ja tietokoneiden konfiguraatioita Windows Active Directory (AD)domaineissa. Policyt eli käytänteet voidaan ulottaa organisaation laajuisiksi tai koskemaan vain tiettyjä ryhmiä tai osastoja organisaatiossa. Group policyitä käytetään Group Policy Objectien (GPO) avulla. (John Gates 2023.)

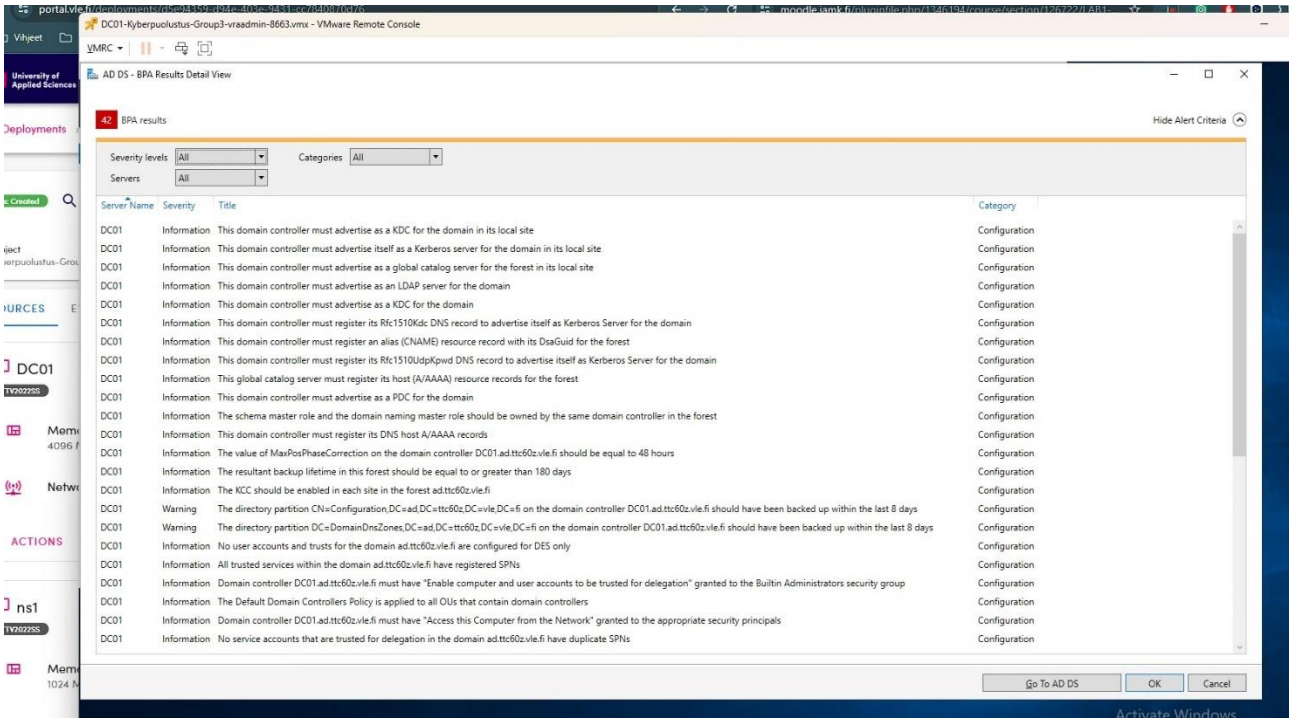
Hyvin organisoidussa AD ympäristössä, Organizational unittien (OU), on oltava hyvin järjesteltyjä, jotta niiden hallinnoiminen on sujuvaa (Group policy 2024). OU on alayksikkö Active Directoryssa, johon voit sijoittaa käyttäjiä, ryhmiä, tietokoneita ja muita organisaatioyksiköitä (About organizational units in Active Directory 2023). Järjestelemällä käyttäjät ja tietokoneet erillisiin OU:n, on tiettyjen ryhmien tunnistaminen ja hallinnoiminen helppoa verkossa helppoa. (John Gates 2023.)

Kun policy-asetuksia halutaan käyttää vain tietyllä tietokoneella tai vain yhdelle käyttäjälle, käytetään *Local Group Policy Objecteja*. Toisin kuin paikallisten asetusten kanssa *Non-local Policy Objectit* vaativat Windows koneiden olevan yhteydessä AD-objekteihin sivustojen domainen tai OU:den kautta. Lisäksi käytössä on ei paikallisia GPO- templateja - *Starter Group Policy Objects*. Näitä käytetään, kun AD:n luodaan uusia GPO:ta. Niiden avulla adminin on mahdollista esikonfiguroida ryhmäasetuksia, joita voidaan käyttää tulevien käytänteiden (GPO) baseline-asetuksina. (John Gates 2023.)

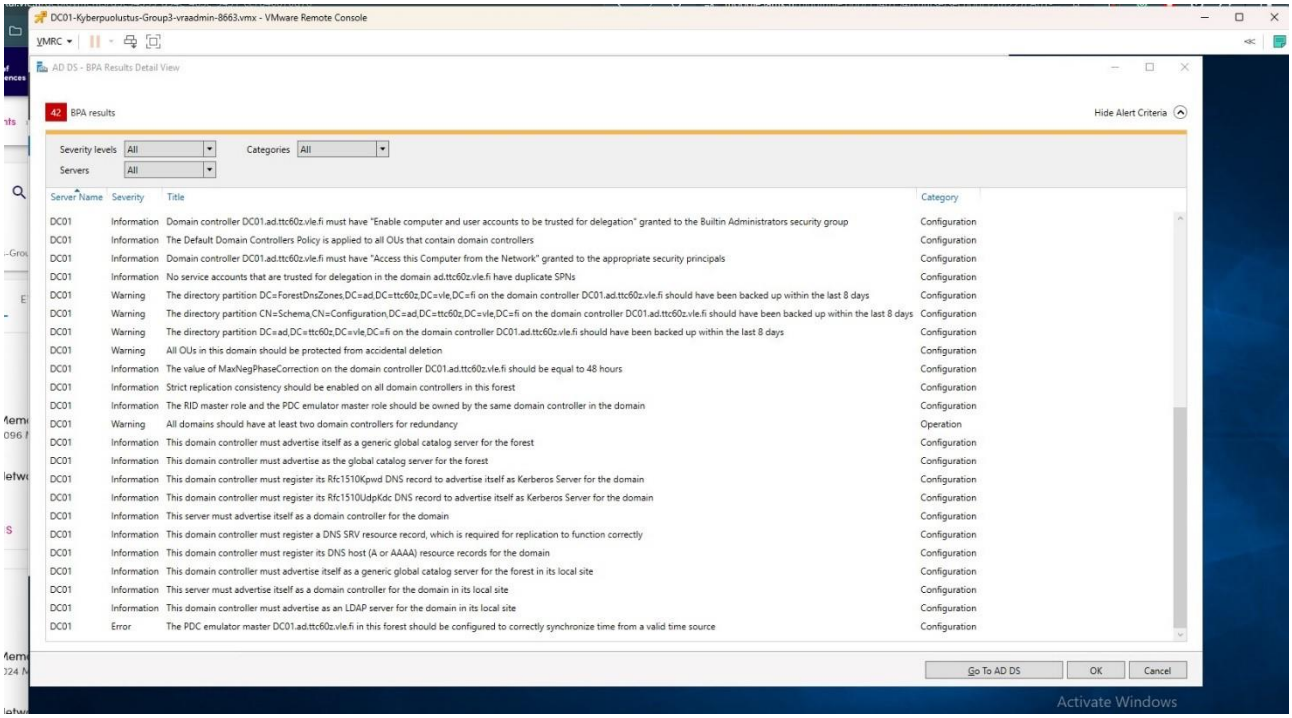
3 Toteutus

3.1 Best Practise Analyzer -alkutilanne

Toteutuksessa ensimmäisenä suoritimme Microsoft Best Practise Analyzerin DC01 –koneella, jonka tulokset olivat seuraavat (Ks. Kuvio 2 & Kuvio 3). Tästä saimme tämän labran alkutilanteen, josta lähdimme liikkeelle. Tämän jälkeen ensimmäisenä lähdimme tekemään srv01:n yksinkertaistamista ja tekemään siitä pelkkää fileserveriä. Sen jälkeen teimme muutamia kovennuksia, joista seuraavissa kappaleissa tarkemmin.



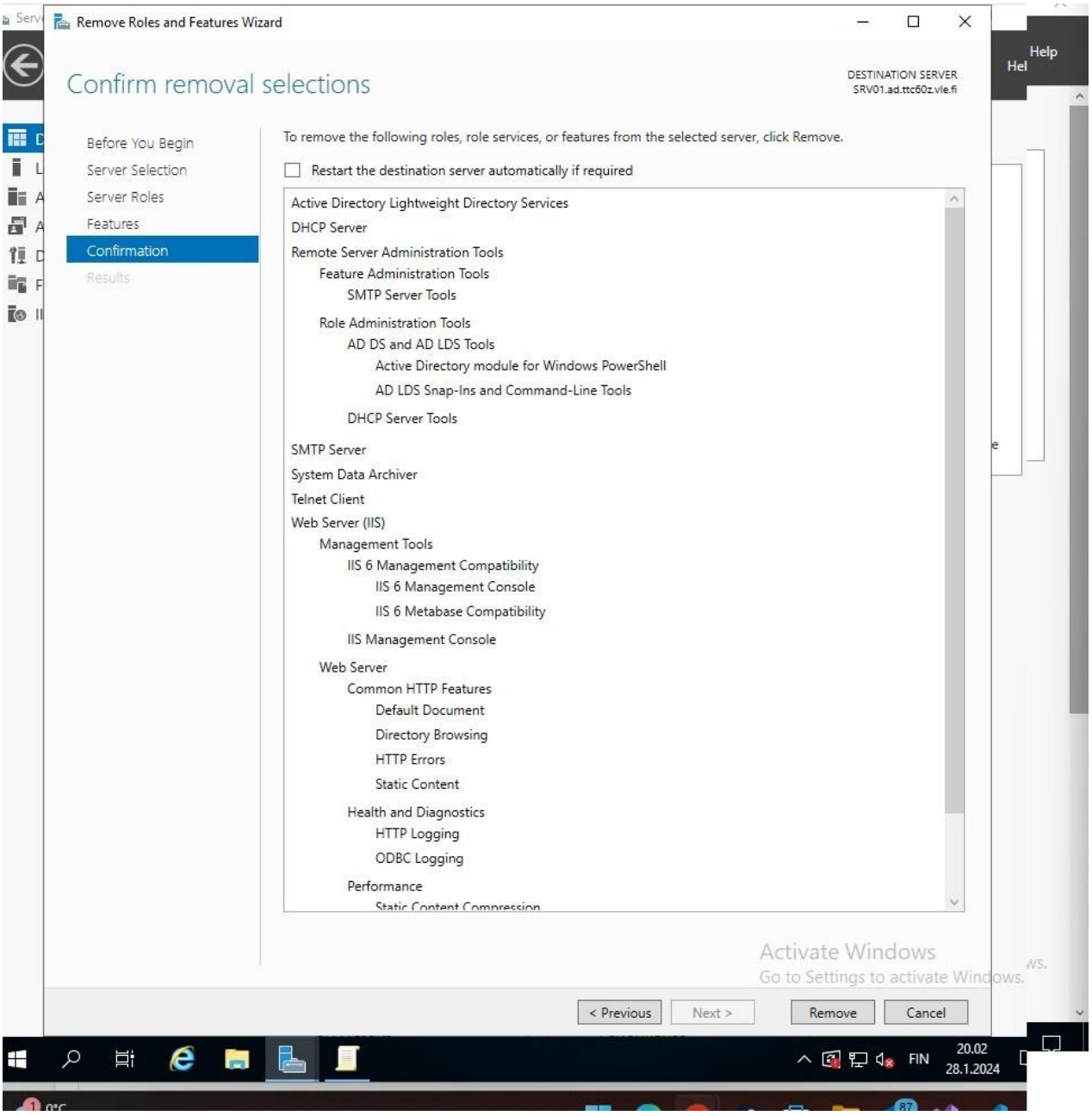
Kuvio 2. BPA -tulokset 1/2



Kuvio 3. BPA -tulokset 2/2

3.2 Tiedostopalvelimen asennus

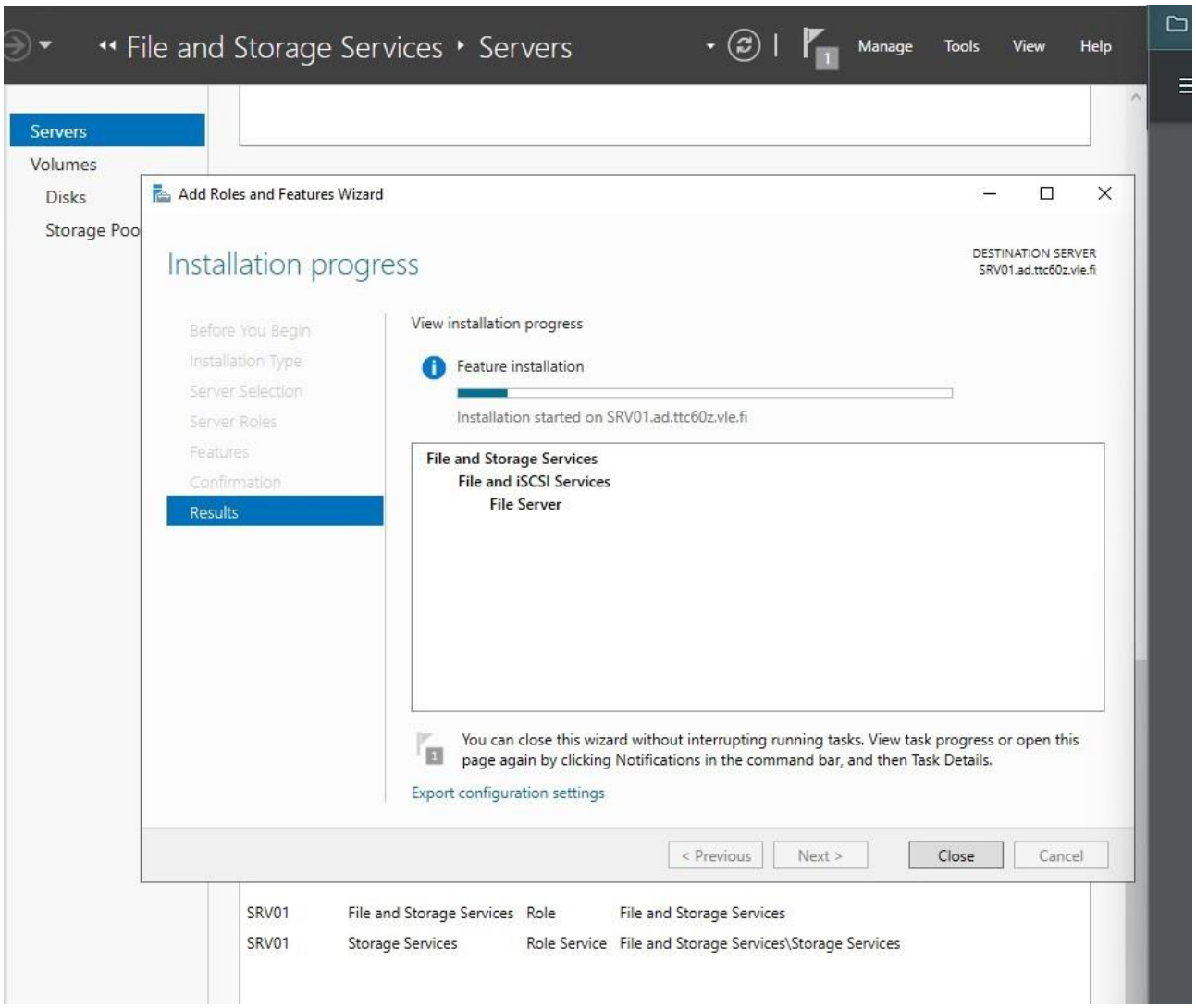
Tehtävänä oli tehdä srv01:stä toimimaan pelkästään fileserverinä erillisen ohjeen mukaisesti. Aloitimme poistamalla turhia rooleja ja ominaisuuksia srv01:stä, joita olivat meidän ryhmällemme seuraavat: DHCP server, Active directory lightweight directory services, WEB Server, Remote Server, Administration tools, SMTP Server, System Data Archiver, Telnet client, Windows Subsystem for Linux, XPS Viewer. (Ks. Kuvio 4). Kyseinen paikka löytyi Server Manager –ohjelmasta, Manage -> Remove Roles and Features Wizard –kohdasta.



Kuvio 4. Poistetut roolit ja ominaisuudet

Päädyimme kyseisiin poistoihin, koska srv01:n on tarkoitus olla vain fileserverinä, ja ei tarvetta mm. DCHP –palvelimelle, AD –tukeen, WEB-serverinä olemiseen. Tämän lisäksi ajatuksena oli, että tarpeen mukaan lisäämme sitten eri rooleja tai ominaisuuksia takaisin, mikäli huomaamme niiden olevan tarpeellisia fileserverin toimivuuden kannalta.

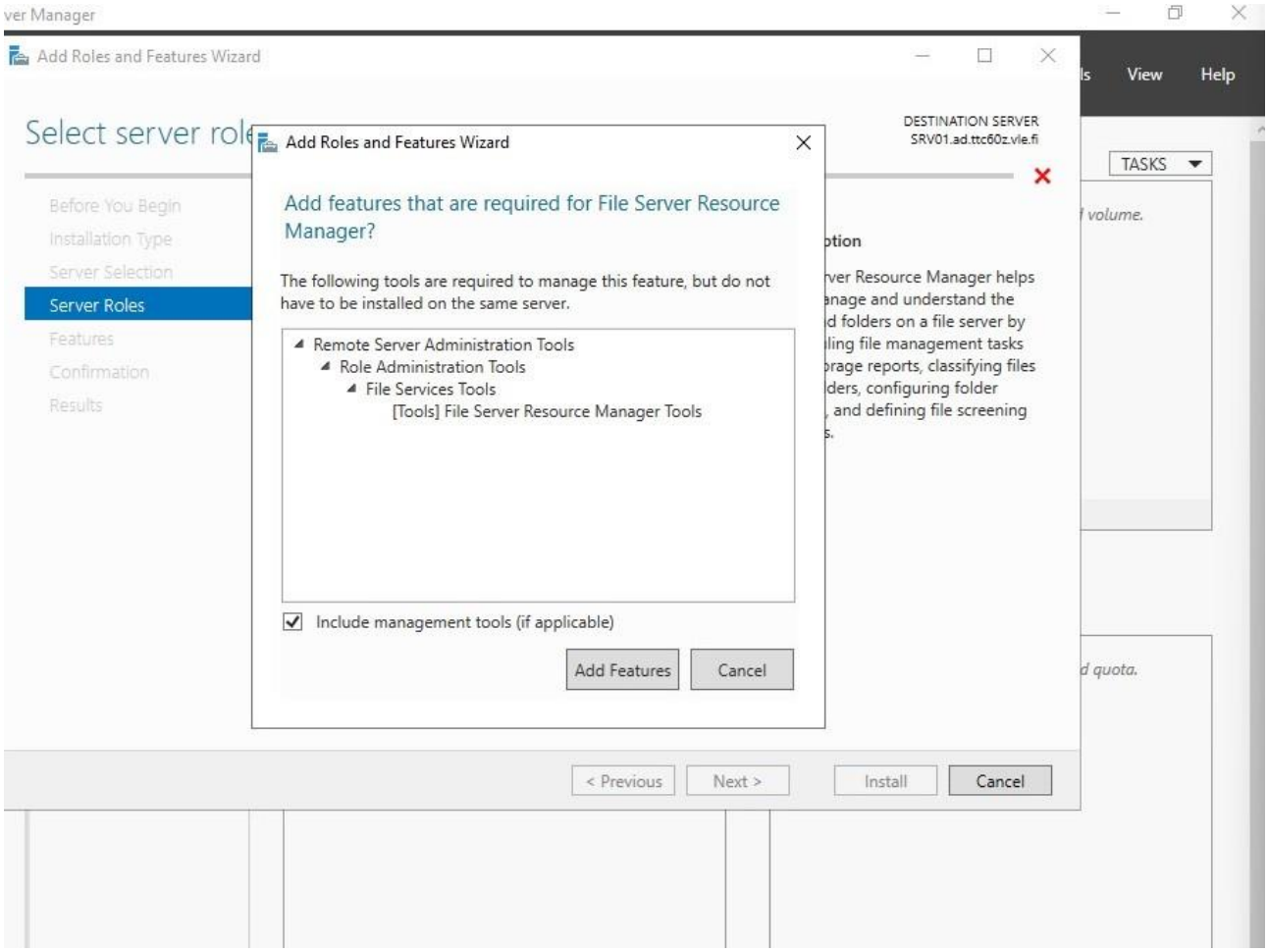
Tämän jälkeen ohjeistuksen mukaisesti tarkoituksena oli asentaa tarpeelliset roolit ja ominaisuudet File Server –kohdan alta (Ks. Kuvio 5). Tämä löytyi lähes samasta paikkaa, mistä poistimme rooleja ja ominaisuuksia. (Server Manager –ohjelma -> Manage -> Add Roles and Features Wizard)



Kuvio 5. File Server -ominaisuuksien asennus

File ja iSCSI Services -asennuksen jälkeen lähdimme tekemään ohjeistuksen mukaisesti jakokansiota. Tähän lähdettiin Server Manager -ohjelmasta katsomaan File and Storage Services -kohtaa, ja sieltä Shares -välilehtä josta pääsimme sitten tekemään uutta jakokansiota. Aluksi katsoimme että vaihtoehdot olivat hieman vähäiset, ja halusimme päästä valitsemaan profiileista SMB Share - Advance. Tämä vaati kuitenkin lisäosan asennuksen File Serverille, joka piti käydä lisäämässä taas

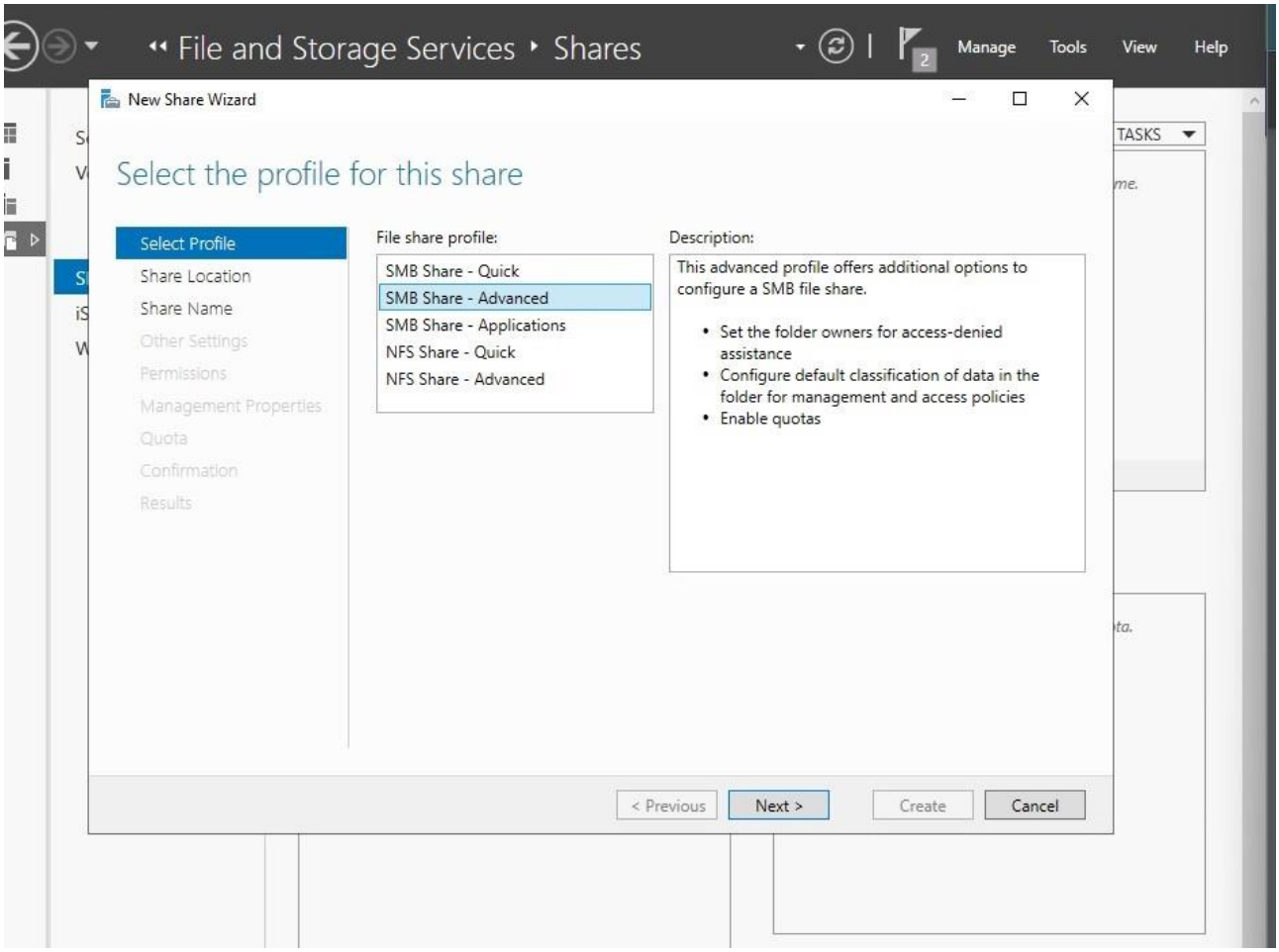
Add Role and Features Wizardilla. Kyseinen lisäosa oli File Services Tools → File Server Resource Manager Tools (Ks. Kuvio 6).



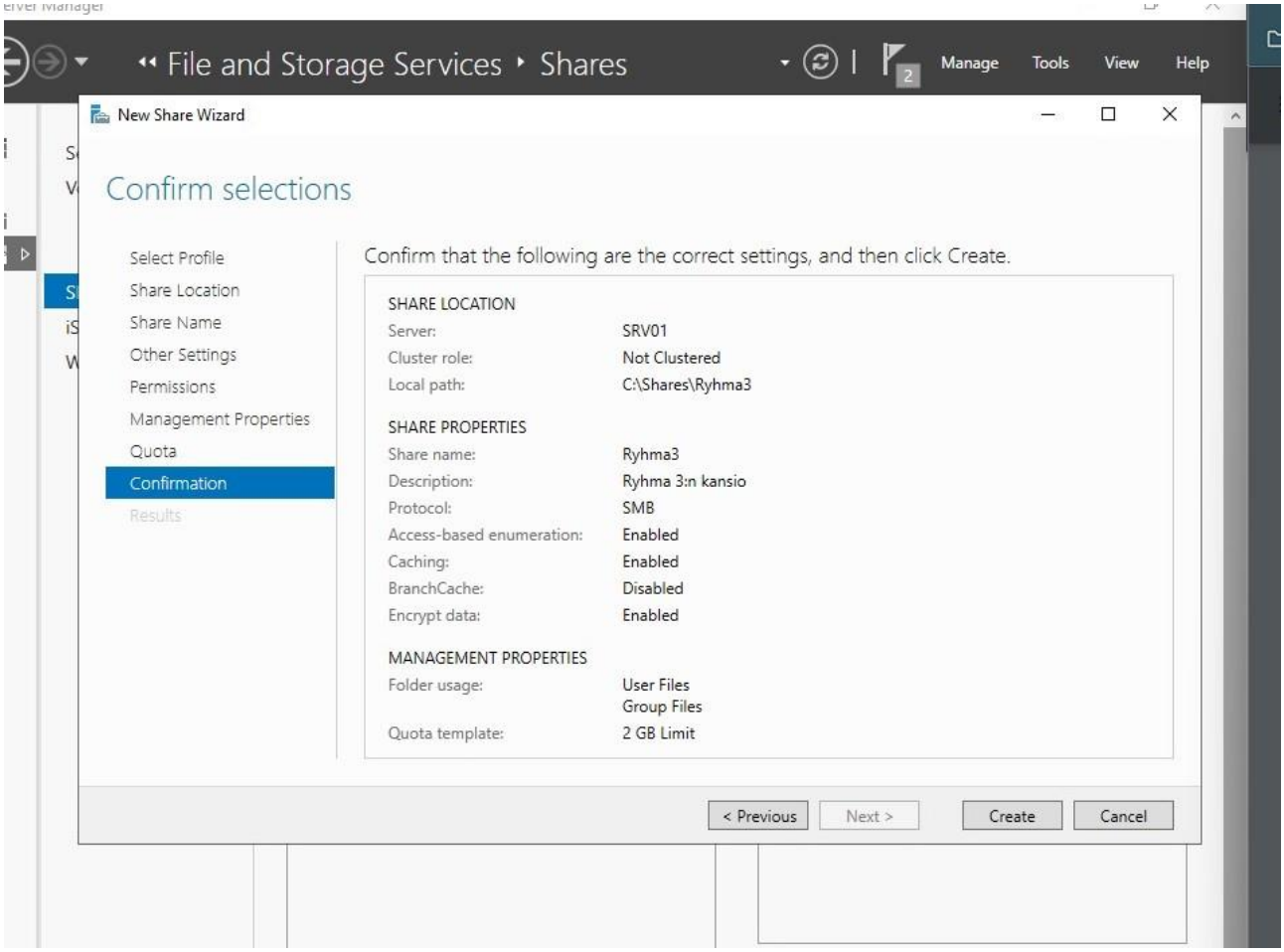
Kuvio 6. Lisäosan asennus File Serverille

Tämän lisäosan asennuksen jälkeen pääsimme valitsemaan SMB – Advancen (Ks. Kuvio 7). Tämä löytyi kuten edellisessä kappaleessa viittasin niin Server Manager -ohjelma → File and Storage Services → Shares → Hiiren oikealla boxissa → New Share -kohdasta. Advance haluttiin sen vuoksi, että halusimme nähdä minkälaisia vaihtoehtoja, on kyseisen kansion tekemisessä. Tämän jälkeen lähdimme asennusohjelman mukaisesti valitsemaan meidän mielestä hyvät asetukset kyseiselle kansiolle (Ks. Kuvio 8). Valitsimme kansion käyttötarkoitukseksi sekä käyttäjän että ryhmän tiedostojen hallinta. Tämän lisäksi rajoitimme kansion tässä harjoituksessa 2GB suuruuteen. Kansio to-

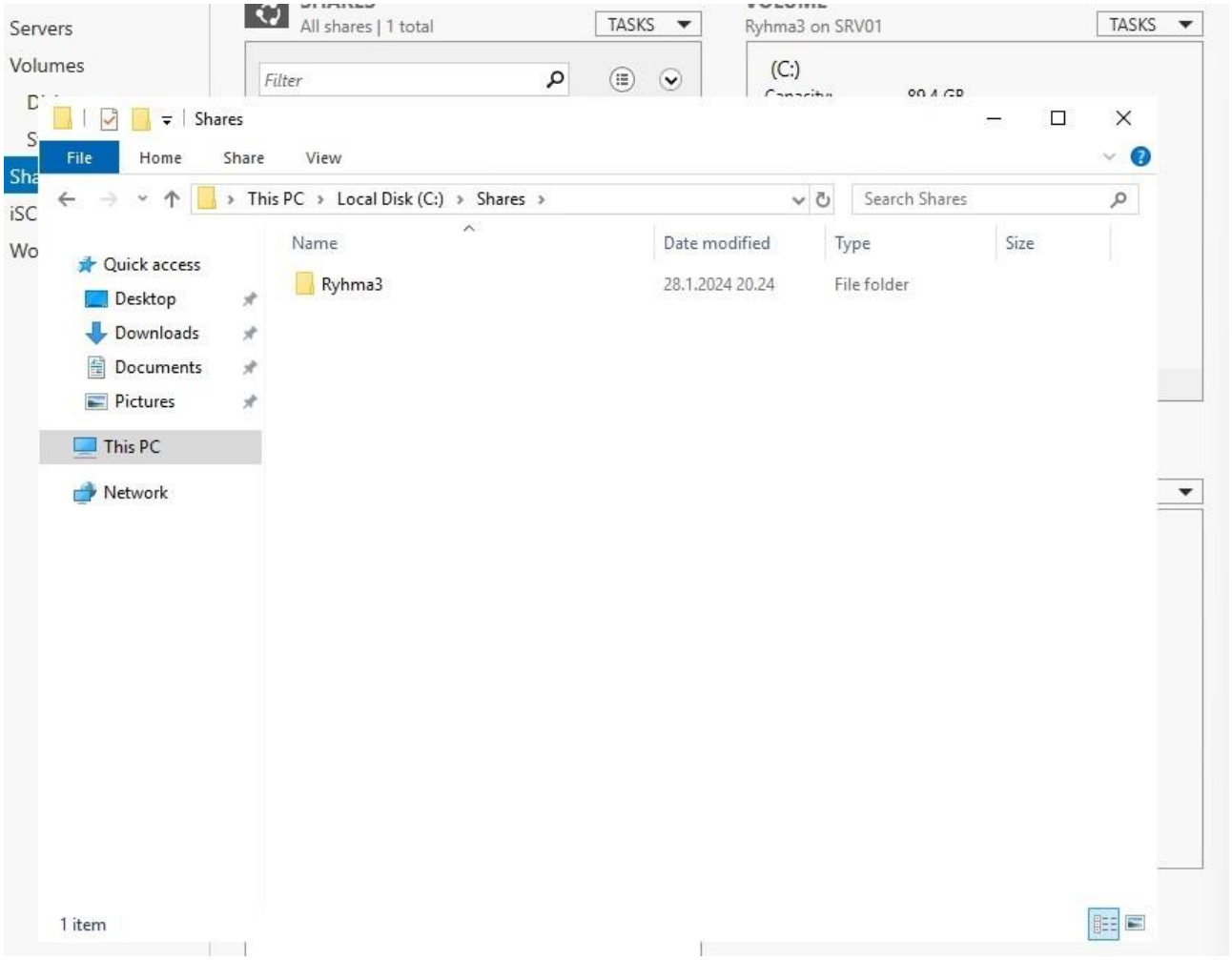
dennettiin vielä katsomalla, että oliko C -asemalle tullut kyseiseen paikkaan uusi kansio, joka kantoi nimeä Ryhma3 (Ks. Kuvio 9)



Kuvio 7. SMB Share - Advancen valinta



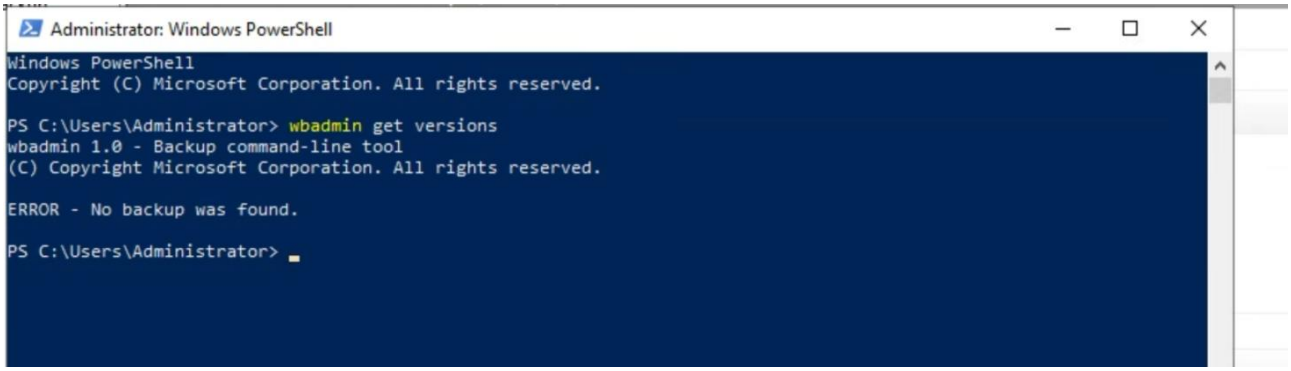
Kuvio 8. Kansion ominaisuudet ja asennus



Kuvio 9. Ryhma 3 -kansion todentaminen

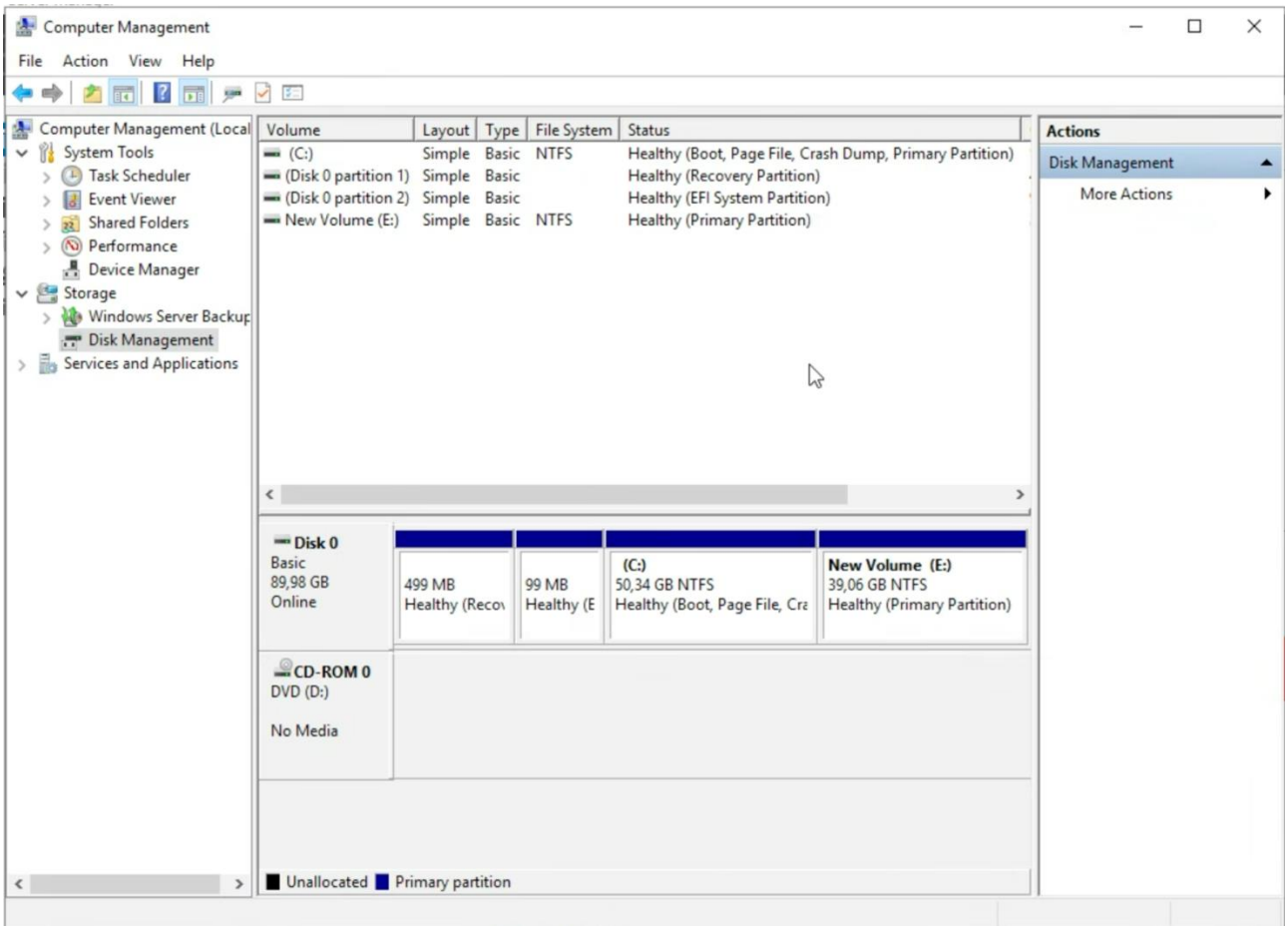
3.3 Tiedostonpalvelimen varmuuskopionti

Ajoimme BPA-analyysin läpi ja saimme tuloksena, että tiedostopalvelimella ei ole käytössä varmuuskopiointia tai sitä ei ole tehty vähään aikaan. Tarkistimme asian myös PowerShell komennon kautta (Ks. Kuvio 10).

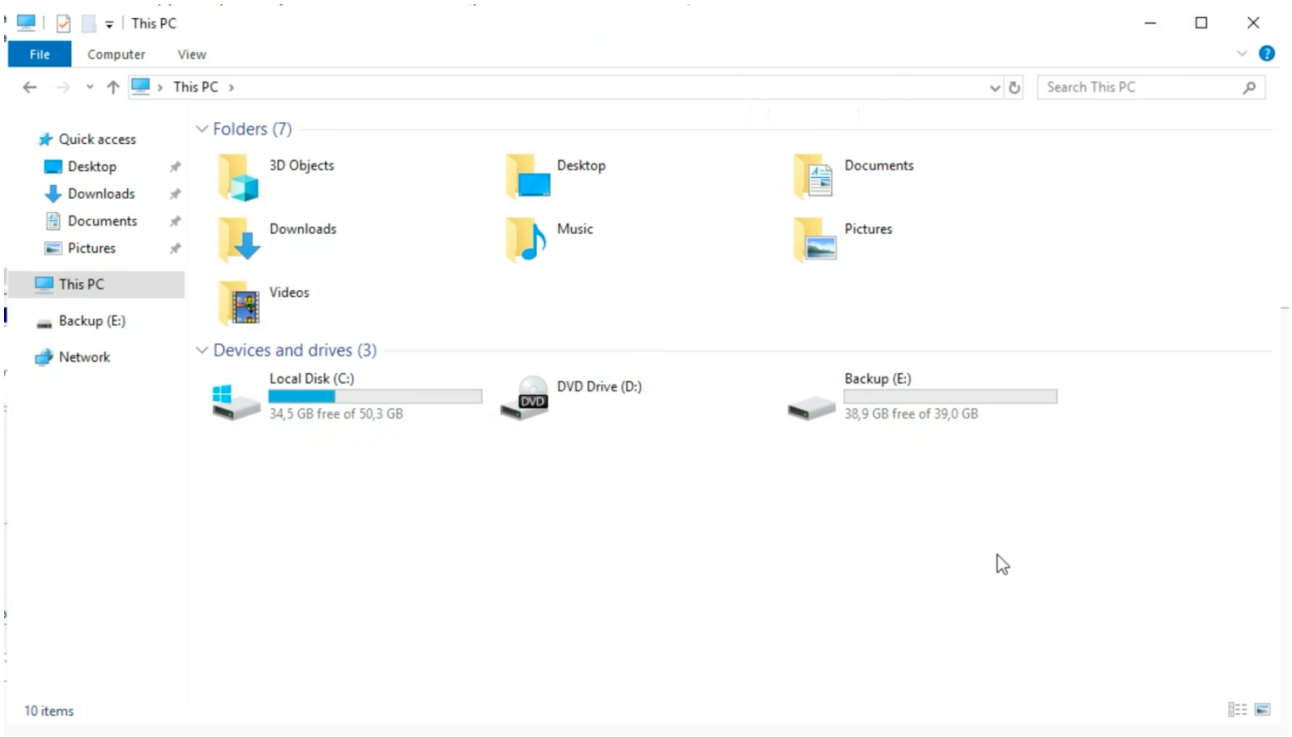


Kuvio 10. Varmuuskopiota ei löytynyt

Asensimme varmuuskopioinnin päälle seuraavan asennuksen mukaisesti. Ensimmäiseksi teimme uuden osion tietokoneen kiintolevylle (Ks. Kuvio 11). Onnistunut alustus tuotti uuden osion, jonka nimesimme Backup -tiedostoksi (Ks. Kuvio 12).



Kuvio 11. Osion alustus kiintolevylle



Kuvio 12. Uusi varmuuskopionti osio

Seuraavaksi piti asentaa SRV01 -palvelimelle uusi rooli. Roolin nimi oli Windows Server Backup. Asennus meni ohjatun wizardin kautta (Ks. Kuvio 13). Asennuksen aikana valitsimme seuraavat asetukset:

Select backup configuration: custom

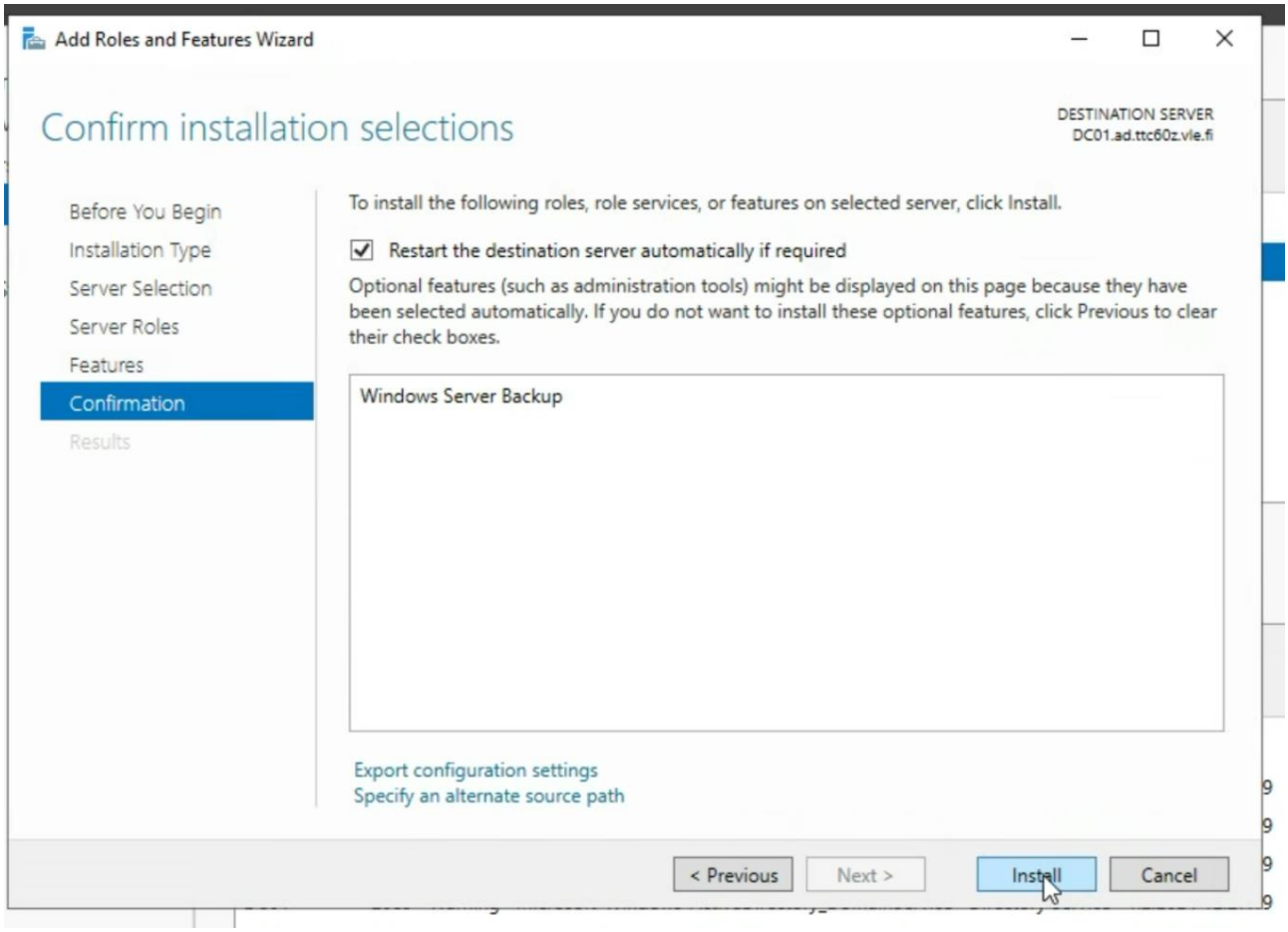
Advandec settings: VSS full backup

Select items for backup: System state

Specify backup time: once a day 04:00

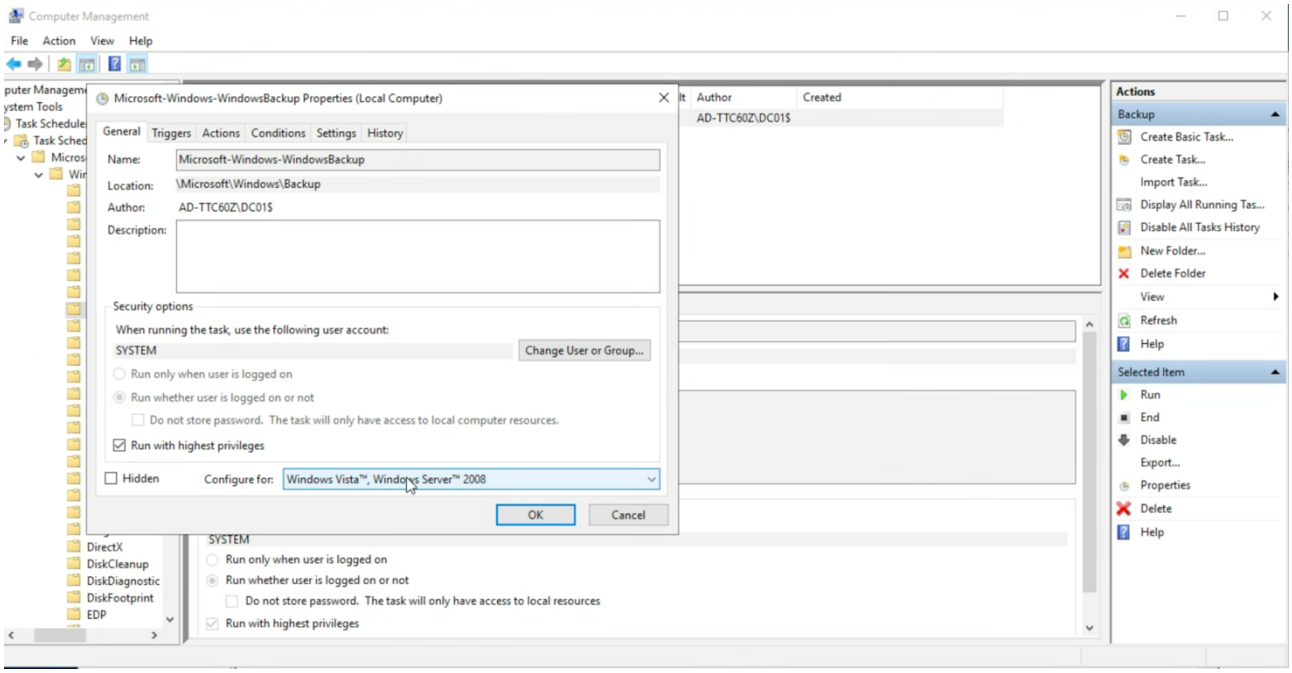
Specify destination type: back up to a volume

Select destination volume: backup (E:) capacity 39 GB



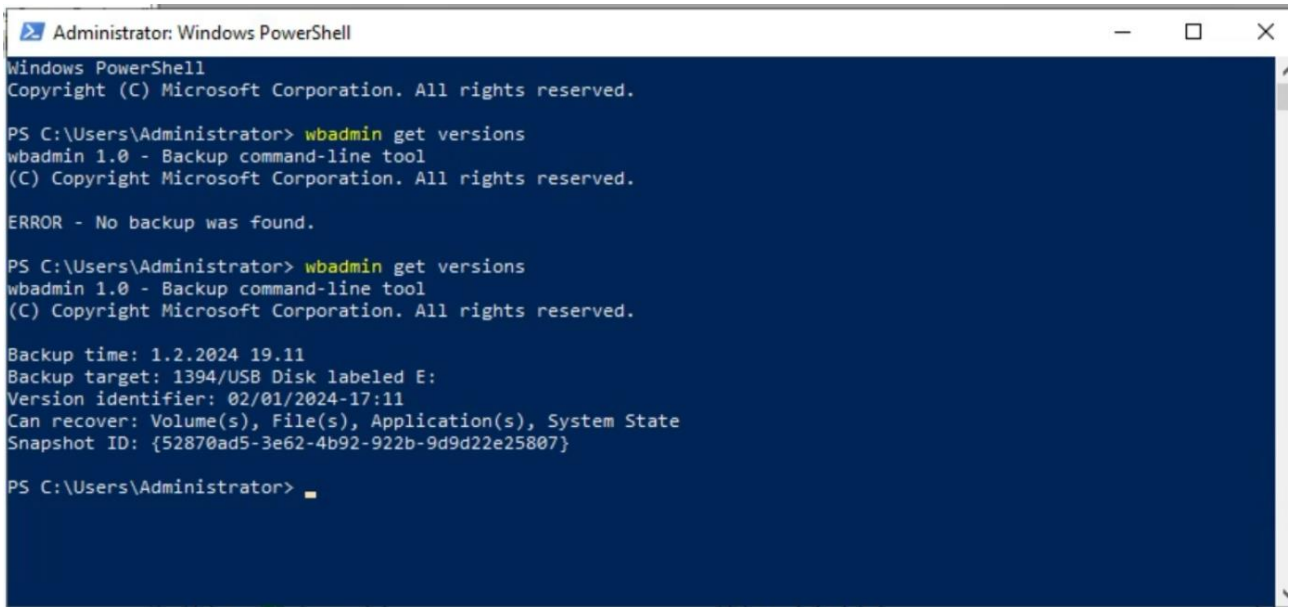
Kuvio 13. Windows Server Backup -roolin asennus

Seuraavaksi asensimme aikataulutetun tehtävän computer management ohjelman kautta (Ks. Kuvio 14).



Kuvio 14. Schedule Task asetuksien asentaminen

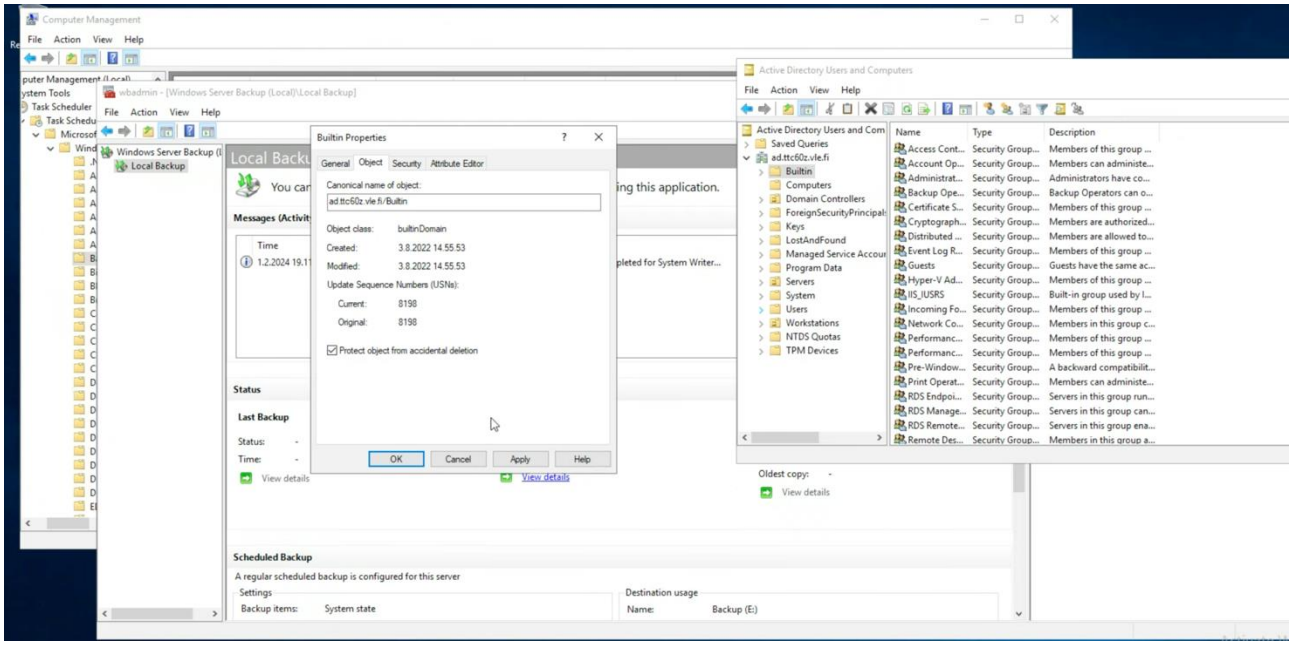
Tämän jälkeen pääsimme käynnistämään ensimmäisen varmuuskopioinnin ajon, joka meni onnistuneesti läpi (Ks. Kuvio 15).



Kuvio 15. Onnistunut varmuuskopionti

3.4 Organization Unitin suojaaminen

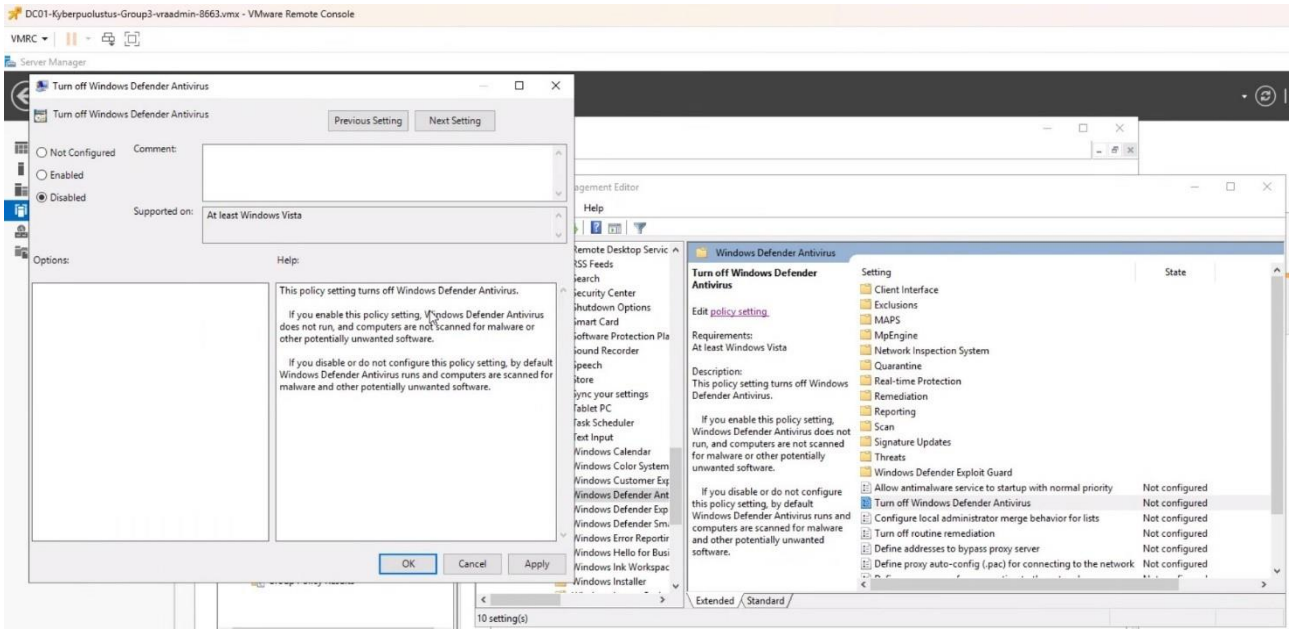
BPA-analyysissä tuli myös ilmi, että OU:t voidaan poistaa vahingossa. Tähän löytyi kovennustapa millä voidaan suojata, ettei OU:ta voidaan poistaa vahingossa. Avaa Active Directory Users and Computers. Hiiren oikealla klikkaa OU:ta, jonka haluat suojata. Navigoi välilehdelle Ohject ja laita täppä kohtaan protect object from accidental deletion ja ok (Ks. Kuvio 16). Tämän toimenpiteen jälkeen ajettiin uusi BPA-analyysi ja todettiin, että varoitus oli poistunut.



Kuvio 16. OU:n suojaaminen

3.5 Microsoft Defender Antivirus

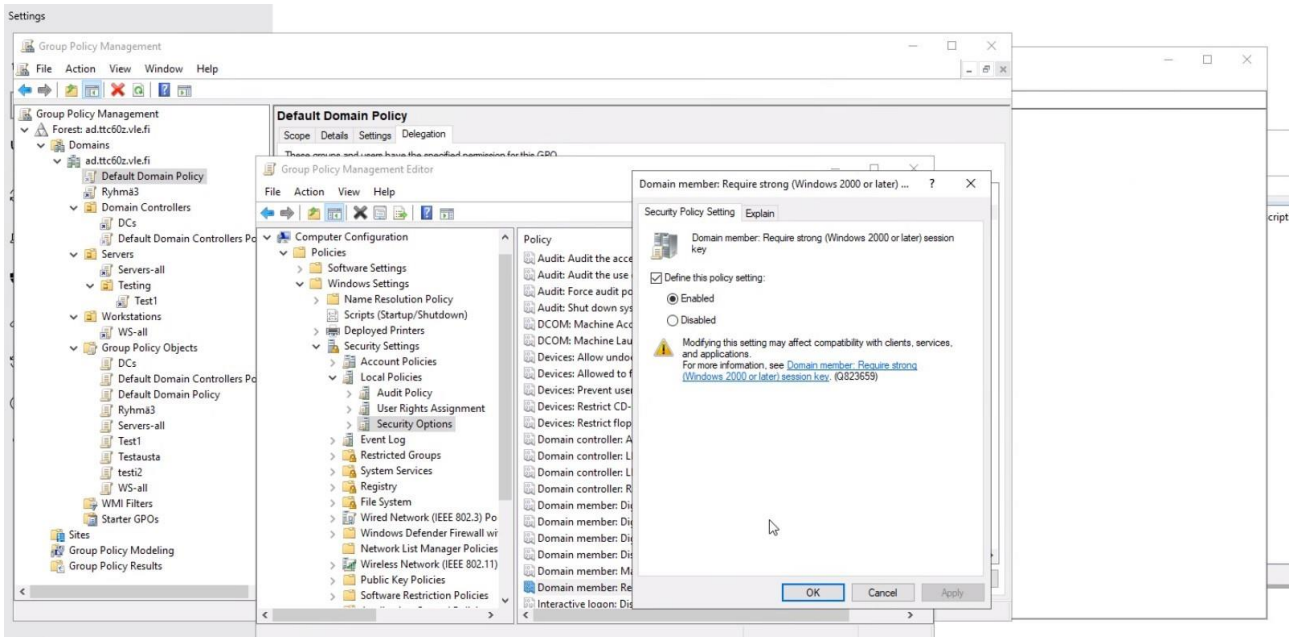
Microsoft tarjoaa Microsoft Defender Antiviruksen, joka on tehokas ratkaisu virustentorjuntaan. Tietokoneissa olisi hyvä olla ajan tasalla oleva virustentorjunta, joten päätimme tehdä tähän kovennuksen, joka pitää Microsoft Defender Antiviruksen päällä skannaamassa tietokoneita haittaohjelmien ja muiden ei-toivottujen ohjelmistojen varalta. Suuntasimme Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirust\Turn off Microsoft Defender AntiVirus ja valitsimme asetuksen disabled (ks. Kuvio 17). Disabled asetus pitää Microsoft Defender Antiviruksen skannaamassa tietokoneita haittaohjelmilta. Jos kohtaan olisi valinnut enabled, Microsoft Defender Antivirus ei skannaisi tietokoneita haittaohjelmilta.



Kuvio 17. Turn off Windows Defender Antivirus disabled tilassa

3.6 Strong key

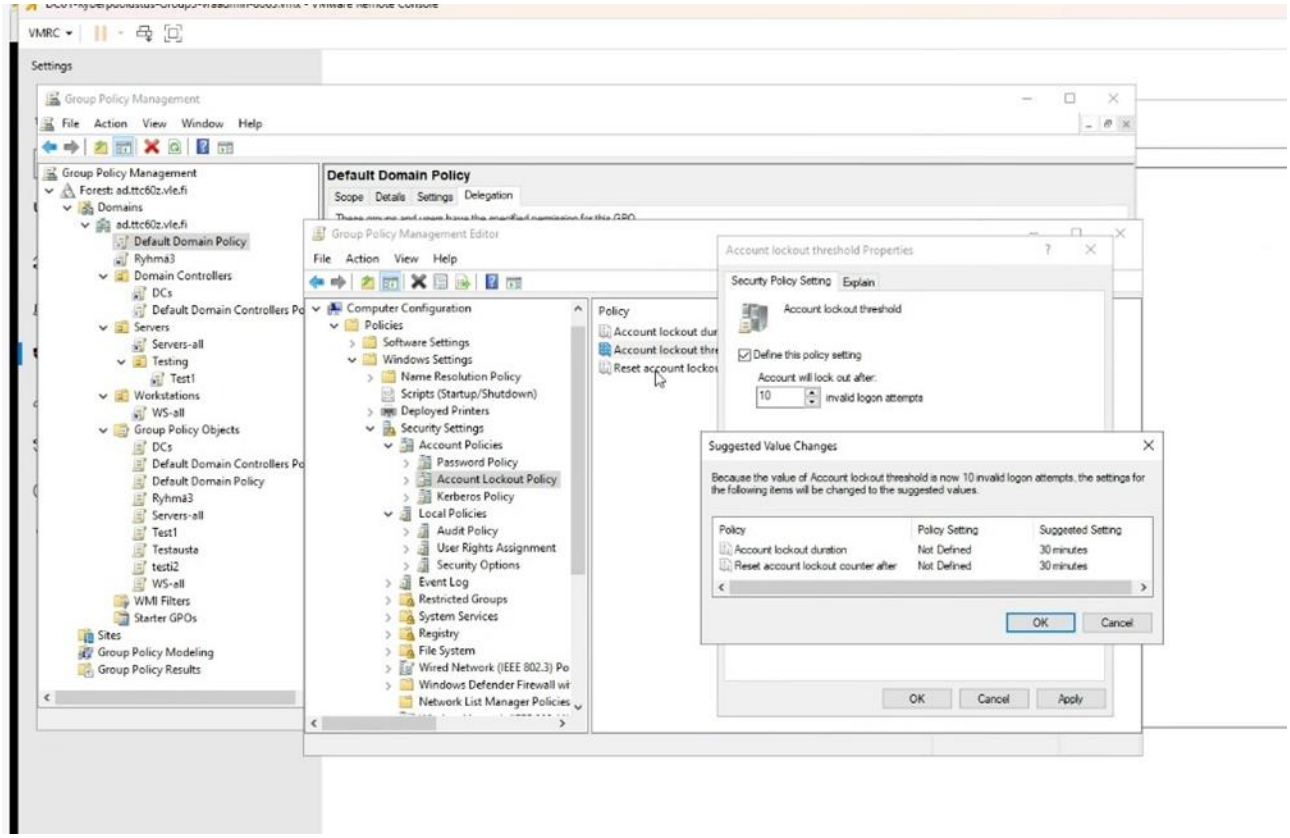
Teimme kovennuksen, joka vaatii vahvan, vähintään Windows 2000 istuntoavaimen. Tämä tarkoittaa, että Domain Controllereita käytetään Microsoft Windows 2000 tai uudemmalla käyttöjärjestelmällä. Istuntoavaimet ovat Windows 2000 käyttöjärjestelmästä ja eteenpäin paljon vahvempia kuin edellisissä versioissa. Vahvat istuntoavaimet auttavat suojaamaan hyökkäyksiltä, jotka yrittävät kaapata verkkosession ja salakuuntelemaan. Suuntasimme Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key ja laitoimme tämän enabled tilaan (ks. Kuvio 18). Kun tämä käytäntö on enabled tilassa, suojattu kanava voidaan muodostaa vain Domain Controllereiden kanssa, jotka pystyvät salaamaan suojatun kanavan datan vahvalla 128-bittisellä istuntoavaimella.



Kuvio 18. Vahva istuntoavain enabled tilassa

3.7 Account lockout threshold

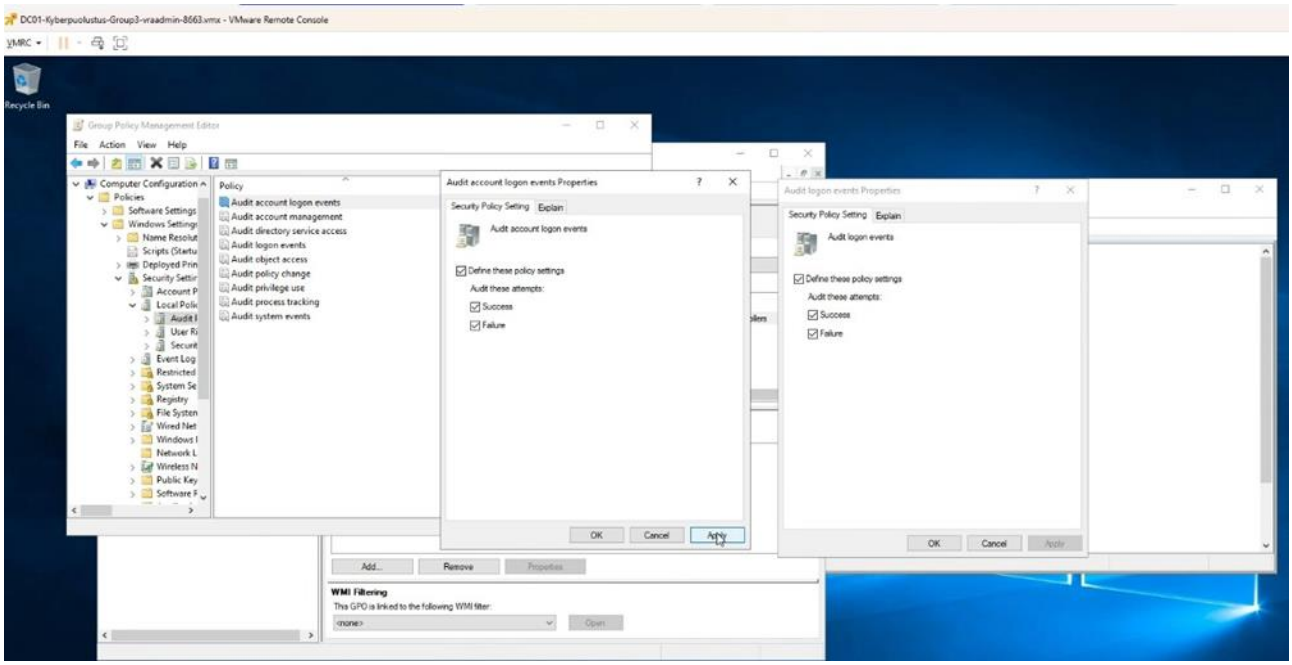
Account lockout treshold policy, määrittää montako kertaa käyttäjä voi yrittää kirjautua väärällä salasanalla. Tällä voidaan estää ei toivottujen käyttäjien loputtomat yritykset salasanan murtamiseksi. Policyn kanssa yhdessä toimii Account lockout duration, jolla voidaan määrittää, milloin kyseinen tili on jälleen käytettävissä. Asetimme Account lockout thresholdin 10 yritykseen, arvioimme sen riittävän tässä tehtävässä todentamaan, että säännön luominen onnistuu. Ja yritysmäärä pysyy riittävän isona, jotta yksittäiset typot eivät lukitse ympäristöä. Account lockout durationiin emme puuttuneet. Ympäristössämme lockout-aika voisi olla lyhytkin, jotta emme ainakaan itseämme sulje ympäristön ulkopuolelle. Account lockout thresholdin asetukset on nähtävissä kuviossa (Ks. Kuvio 19). (Account lockout threshold 2023)



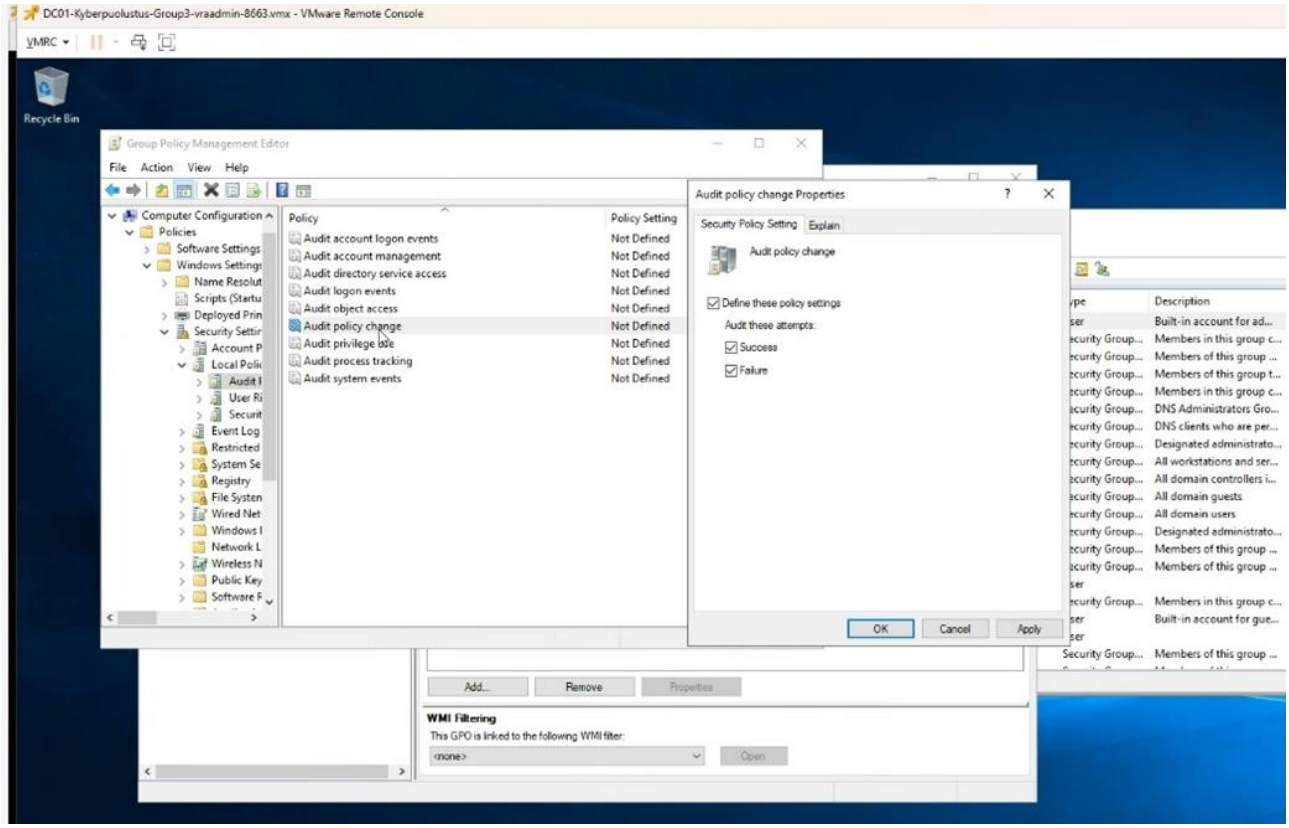
Kuvio 19. Account lockout threshold

3.8 Audit account logon events sekä Audit policy change

Windowsin Audit Policyt määrittävät ne tietyt tapahtumat jotka adminit haluavat tallentaa logeihin. Esimerkiksi logiin voidaan tallentaa kaikki etäyhteydellä otetut yhteydet, mutta yrityksen ympäristössä otetuista yhteyksistä logia ei tarvitse pitää (Windows Auditing 2024). Päätimme lisätä ympäristöömme Audit account logon events (Ks. Kuvio 20) ja Audit policy change (Ks. Kuvio 21) -policyt. Näiden avulla meidän on jatkossa mahdollista valvoa, millä tunnuksilla ympäristön Windowskoneille on kirjauduttu tai milloin ja onko policyiden muutos ympäristössä onnistunut vai ei.



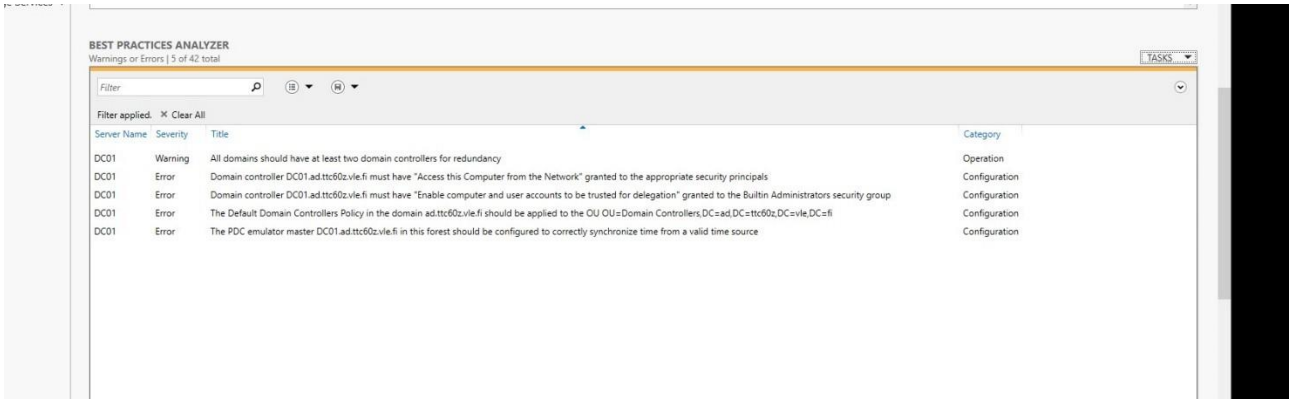
Kuvio 20. Audit logon events policy



Kuvio 21. Audit policy change -policy

3.9 Best Practice Analyzer -loppuanalyysi

Lopuksi ajoimme vielä Best Practice Analyzerin uusiksi, josta saimme hieman erilaiset tulokset kuin ensimmäisellä kerralla (Ks. Kuvio 22). Analyzerissä yhteisvirheiden määrä oli pysynyt hyvin samana, mutta Warning sekä Error -kohtien määrä oli pudonnut. Olimme onnistuneesti saaneet varmuuskopio -huomautuksen pois, kuten myös OU:n suojaamisen vahinkopoistoilta. Näiden tilalle oli tullut uusia huomautuksia, joita emme lähteneet vielä analysoimaan tarkemmin.



Kuvio 22. BPA -analyysi lopussa

4 Pohdinta

AD ei ollut ryhmälle kovin tuttu tehtävään lähdettäessä ja sen takia koventamisestakin tuli hieman hyppy syvään päätyyn. Alkuun jouduimme porukalla miettimään, mihin mikäkin policy-muutos tulisi tehdä ja mihin se oletettavasti vaikuttaa. Meille ei myöskään ollut täysin selvää mitä meidän kannattaa lähteä ympäristöstä koventamaan. Joitain vastauksia saimme BPA:n tuloksista ja muutamaan varoitukseen olikin selkeä puuttua. Päädyimme siihen, että ympäristöä koventaessa sen olisi hyvä olla kunnolla tuttu ennen kuin mitään lähdetään sörkkimään. Selkeä kokonaiskuva ja tavoite siitä mihin pyritään, helpottaisivat kovennusten valitsemista. Kun halutut kovennukset on valittu, ohjeet juuri tietyn käytänteen (policyn) koventamiseen kyllä löytyvät melko helposti.

Ryhmälle tuotti myös pientä päänvaivaa Windows AntiVirus – Disabled -kohta, koska ensinnäkin kyseinen policy tuntui alkuun oudosti ilmaistulta, ja tämän lisäksi ryhmämme ajatteli, että kun kyseinen asetus on laitettu niin käyttäjä ei voisi kytkeä AntiVirusta pois päältä. Tätä testailimmekin hyvän tovin, ja huomasimme että joko olimme kyseisen käytännön ajatelleet väärin tai sitten emme olleet osanneet tehdä sitä oikein. Selvityksen jälkeen kuitenkin huomaismme että kyseinen sääntö ei ota pois mahdollisuutta käyttäjältä itse ottaa AntiVirusta pois päältä, jota aluksi ajattelimme. Tässä myös samalla huomattiin, että säännöissä pitää olla tarkka ja katsoa niiden info -kohdat läpi, että tiedetään tarkemmin mitä esimerkiksi Enable tai Disable -kohta tekee kyseiselle säännölle. Näiden lisäksi, kun AD ja GPO ovat ryhmälle hieman tuntemattomia niin vaatii paljon, että niihin pääsee kunnolla ns. sisään ja oppii niiden kunnollisen ja oikeaoppisen käytön.

Ryhmässä pohdittiin myös, että olisiko ollut helpompi lähteä näitä asioita tekemään, jos ei olisi ollut valmista organisaatiota vaan olisi päässyt lähtemään aivan alusta eli suunnittelusta. Tiedostimme toki, että harvemmin tällaista tilannetta tulee vastaan vaan usein on tilanne se, että otat valmiin organisaation haltuun ja sitten pitää päästä tilanteen tasalle ja mahdollisesti selkeyttää sekä AD- että GPO -puolta.

Haastetta myös osakseen tuottaa tällaisessa ympäristössä se, että kun ei ole ns. henkilökuntaa määrätty vielä yrityksessä, joille voisi tehdä käyttjän ja liittää johonkin ryhmään, jolle sitten tekisi tietyn säännön. Tätä kuitenkin pystyy testailemaan ja sehän näiden labrojen tarkoitus onkin, mutta ajoittain huomataan ryhmässä että asioita rupeaa miettimään joko liian monimutkaisesti tai sitten aivan liian laajasti heti alkuun.

Lähteet

About organizational units in Active Directory. University Information Technology Services. 16.11.2023. Viitattu 3.2.2024. https://kb.iu.edu/d/atvu

Account lockout threshold. 2023. Microsoft. Viitattu 3.2.2024. https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold

Active Directory Domain Services Overview. 2022. Viitattu 4.2.2024. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

Gates, J. 2023. Group policy guide for baseline hardening. CalCom 27.9.2023. Viitattu 3.2.2024. https://www.calcomsoftware.com/group-policy-guide-for-baseline-hardening/

Gates, J. 2023. What is the relationship between hardening and NIST standards? CalCom 2023. Viitattu 3.2.2024. https://www.calcomsoftware.com/how-hardening-is-reflected-in-the-different-nist-standards/

Group policy. 2024. ManageEngine 2024. Viitattu 3.2.2024. https://www.manageengine.com/products/active-directory-audit/kb/what-is/group-policy-in-active-directory.html