jamk

Labra 1

Ryhmä 13

Leevi Kauranen, AC7750
Samir Benjenna, AD1437
Eelis Suhonen, AA3910
Juho Eräjärvi, AD1276
Mikke Kuula, AC7806

Koventaminen TTC6050-3006
30.9.2024
Tieto- ja viestintätekniikka

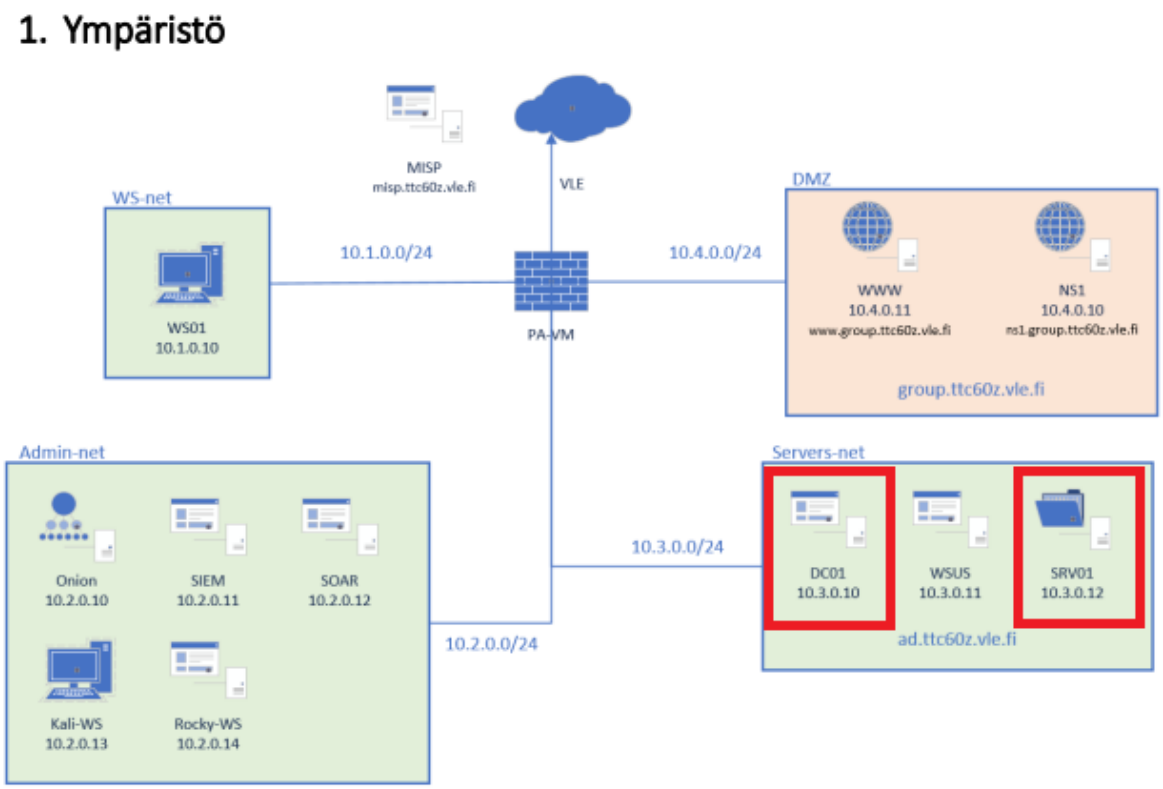
jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

1 Johdanto

Koventaminen-opintojakson ensimmäisessä labratyössä tarkoituksena on koventaa virtuaaliympäristömme tiedostopalvelin (SRV01) ja Active Directory (DC01) (kuvio 1). Active Directoryn koventamisen yhteydessä kovennetaan myös ryhmäkäytäntöjä (Group Policies). Tiedostopalvelimen koventamiseen meille annettiin erillinen ohje, mutta Active Directoryn koventamiseen valitsimme itsellemme mieleisen ohjeen. Ryhmämme valitsi kurssimateriaalista löytyvän Center for Internet Security (CIS) Benchmarks -ohjeen ja tämän lisäksi tutkimme myös muita ohjeita, kuten Microsoftin omia parhaiden käytäntöjen ohjesääntöjä. Edellä mainittu ohje on erittäin laaja, joten emme toteuttaneet kaikkea siellä mainittua, vaan valitsimme mielestämme tärkeitä kovennuksia, joita toteutimme.



Kuvio 1. Laboratorioympäristö

2 Teoria

Koventaminen tarkoittaa tietoturvan parantamista tietojärjestelmissä, verkkolaitteissa, palvelimissa ja ohjelmistoissa. Koventamista voidaan tehdä esim. poistamalla tarpeettomia ja vanhentuneita sovelluksia, ohjelmistoja ja rooleja tavoitteena pienentää hyökkäyspinta-alaa ja siten vähentää mahdollisten hyökkääjien mahdollisuuksia, joita he voivat käyttää päästäkseen järjestelmään sisään tai vahingoittaakseen järjestelmää. (Schrader, D. 2023)

Koventamiseen kuuluu myös käyttäjäoikeuksien hallitseminen. Käyttäjäoikeuksia voidaan hallita esim. Vähimmän etuoikeuden periaateella (Principle of Least Priviledge). Tämä tarkoittaa sitä, että käyttäjille, sovelluksille ja prosesseille annetaan vain ne oikeudet, jotka ovat välttämättömiä niiden tehtävien suorittamiseksi. Tällä pyritään vähentämään luvattoman pääsyn ja virheellisten toimintojen riskiä ja sitä, että ne johtaisivat tietoturvauhkiin tai -loukkauksiin. Esimerkiksi varastotyöntekijällä ei ole tarvetta päästä käsiksi yrityksen verkkosivujen hallintaan tai myyjän ei välttämättä tarvitse päästä tekemään muutoksia tietokoneen palomuurin asetuksiin. (Systems Hardening. 2023)

2.1 File server

Tiedostopalvelin (File Server) on palvelin tietoverkossa, joka tarjoaa käyttäjille ja muille järjestelmän osille keskitetyn paikan tiedostojen tallentamiseen, hallintaan ja jakamiseen. Tiedostopalvelin voi sisältää asiakirjoja, ohjelmistoja, kuvia, varmuuskopioita ja muita tietotyyppejä ja se mahdollistaa pääsyn näihin tiedostoihin useista laitteista ja sijainneista. (Wright, G. 2021; Yu, E. 2023.)

Tiedostopalvelimen keskeisiä tehtäviä ovat tiedostojen turvallinen tallentaminen, varmuuskopiointi, jakaminen ja oikeuksien hallinta. Oikeuksien hallinnan avulla voidaan määrittää, ketkä voivat lukea, muokata tai poistaa tiettyjä tiedostoja. Tämä on keskeinen osaa tietoturvaa ja koventamista. (Wright, G. 2021; Yu, E. 2023.)

Käyttämämme tiedostopalvelin pyörii Windows Server 2019:ssa ja se käyttää SMB (Server Message Block) protokollaa, joka takaa nopean ja turvallisen tiedostojen jakamisen. SMB:sta on kolme

versiota, SMB1, SMB2 ja SMB3, joista SMB1 ei ole enää vuonna 2024 tietoturvallinen eikä sitä pitäisi käyttää. (Wright, G. 2021; Yu, E. 2023.)

2.2 Active Directory

Active Directory (AD) on tietokanta ja palvelukokonaisuus, joka sisältää tietoa käyttäjistä, tietokoneista ja verkon resursseista. AD yhdistää käyttäjät tarvittaviin verkkoresursseihin, jotta haluttu työ saadaan tehtyä. AD toimii Windowsin serverissä ja yksinkertaisesti sen avulla järjestelmänvalvojat voivat hallita käyttöoikeuksia ja verkkoresurssien käyttöä.

Tietokanta sisältää kriittisiä tietoja ympäristöstäsi, kuten mitä käyttäjiä ja koneita ympäristöön kuuluu sekä sääntöjä kuka saa tehdä ja mitä. Palvelu valvoo ympäristöä ja varmistaa autentikoinnilla sen, että jokainen henkilö on se, kuka väittää olevansa ja valtuutuksella sen, että henkilöllä on pääsy vain niihin tietoihin, mihin hänellä on lupa. Active Directory parantaa organisaation turvallisuutta ja antaa ylläpitäjien sekä käyttäjien toimia helposti ja turvallisesti. Järjestelmänvalvojat voivat hallita käyttäjiä ja käyttöoikeuksia koko organisaatiossa sekä hallita tietokone- ja käyttäjäkokoonpanoja AD-ryhmäkäytännön avulla. (What is Active Directory and how does it work?. 2024)

Tärkein Active Directory -palvelu on Active Directory Domain Service (AD DS), joka on osa Windows Server -käyttöjärjestelmää. Kun AD DS on asennettu palvelimelle, siitä tulee domain controller (DC). Tämä palvelin tallentaa koko AD-tietokannan. Organisaatiolla on yleensä useita DC:itä. AD DS perustuu useisiin protokolliin ja standardeihin, kuten LDAP, Kerberos ja DNS. (What is Active Directory? Structure, Benefits & How it works. 2024.)

2.3 Muita termejä

Account Lockout Policies (tilin lukituskäytännöt), määrittävät, miten kirjautumisen epäonnistuneet yritykset käsitellään AD:ssa, esimerkiksi tili lukitaan kolmen yrityksen jälkeen ja lukitus kestää tietyn ajan. Konfiguroinnissa tulee ottaa huomioon mahdollisen tietoturvauhan riski (Brute-force

attack) ja samalla toiminnon käytettävyys itse käyttäjille. (CIS. 2019. Luku 1.2 Account Lockout Policy)

Strong Password Policies -konfiguroinnilla Windows AD:ssa voidaan suojata käyttäjätilejä ja muita resursseja hakkereiden tunkeutumisyrityksiltä, kuten bruteforce-hyökkäyksiltä ja helppojen salasanojen arvailulta. CIS STIG Benchmark dokumentissa on vaatimuksia salasanojen pituudelle, monimutkaisuudelle ja vaihtoväleille. Esimerkiksi salasanan tulee olla vähintään 14 merkkiä pitkä, sisältää numeroita ja erikoismerkkejä, salasanahistorian vähimmäisarvo on 24 edellistä (ei voi asettaa aiemmin käyttämäänsä salasanaa), salasanan enimmäisikä 60 päivää ja vähimmäisikä (kun voi vaihtaa seuraavan kerran) on vähintään 1 päivä. (CIS. 2019. Luku 1.1 Password Policy)

LAN Manager Hash (LM Hash) on vanha hajautusalgoritmi, jota on aiemmin käytetty salasanojen tallentamiseen Windowsilla. LM-hajautus muuntaa salasanat pelkästään isoiksi kirjaimiksi, jakaa ne 7 merkin osiksi, menetelmä on myös helposti murrettavissa tunnettujen hyökkäysten avulla (erityisesti heikkojen salasanojen kohdalla). Näin hyökkääjät voivat purkaa salauksen ja päästä käsiksi käyttäjien salasanoihin. LM Hash estettiin AD:n asetuksissa, jotta salasanojen hash tiedot eivät tallennu salasanan vaihdossa. (CIS. 2019. s.327)

SMB (Server Message Block) Signing on turvallisuusominaisuus, joka lisää digitaalisen allekirjoituksen SMB pakettiliikenteeseen tietoturvauhkien varalle. Tällä voidaan varmistaa, ettei lähetettyä tietoa ole urkittu (man-in-the-middle attack, replay attack) tai muutettu tiedonsiirron aikana hakkereiden toimesta. (Microsoft network server: Digitally sign communications (always). 2023)

LDAP (Lightweight Directory Access Protocol) on protokolla, joka mahdollistaa hakemisto- ja tietokantapalvelujen käytön verkossa. LDAP protokollaa voidaan käyttää tietojen hakemiseen, päivittämiseen ja poistamiseen hakemistosta, kuten Active Directorysta. Sen avulla voidaan hakea AD:sta tietoa ja muokata sitä. Se siis toimii AD:n käyttöliittymänä. LDAP Access Control: määritetään rajoituksia LDAP:n käyttäjille ja myös millä tavalla sitä voidaan käyttää. Esim. vain valtuutetut henkilöt

ja sovellukset pääsevät käyttämään Active Directorya. (How Does LDAP Work: Everything IT Administrators Should Know. 2024)

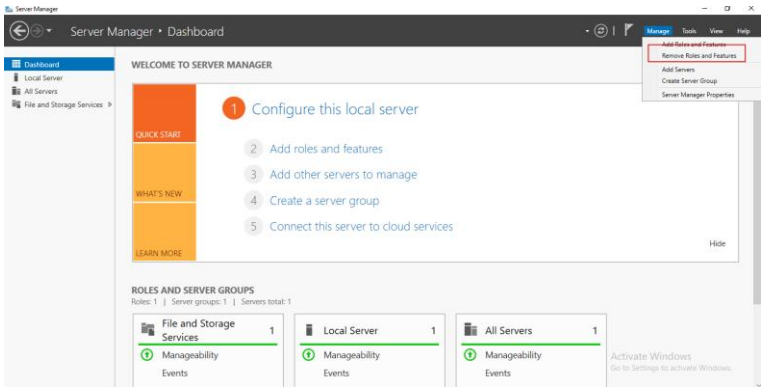
Kerberos on Active Directoryssa käytetty protokolla käyttäjien verkkoautentikointiin. Se on turvallinen tapa todentaa käyttäjät ilman salasanan syöttämistä, lippujärjestelmän (tickets) avulla. Järjestelmässä käyttäjä saa AES-salatun lipun, jolla hän todentaa itsensä järjestelmään. Kerberos salauksessa Key Distribution Center (KDC) myöntää käyttäjille lippuja, joiden avulla kerran autentikoitu käyttäjä voi käyttää verkon palveluita kirjautumatta uudestaan järjestelmiin. Hyviä käytänteitä Kerberos järjestelmään on esim. lippujen voimassaoloaika tulee olla rajoitettu 10 tuntiin väärinkäytön mahdollisuuden vuoksi, käytettävä vahvaa AES-salausta varmistamaan turvallinen käyttö, kirjataan lokiin Kerberos-autentikoinnit hakkereiden havaitsemiseksi. (Kerberos Authentication Overview. 2021)(CIS. 2019. Luku 1.3 Kerberos Policy)

3 Työn kulku

3.1 Tiedostopalvelimen koventaminen

Ensimmäisenä kovennus kohteena oli ympäristömme Servers-Netistä löytyvä SRV01 palvelin, joka on tarkoitettu tiedostopalvelinkäyttöön. Aloitimme poistamalla kaiken tarpeettoman palvelimelta pienentääksemme hyökkäys pinta-alaa.

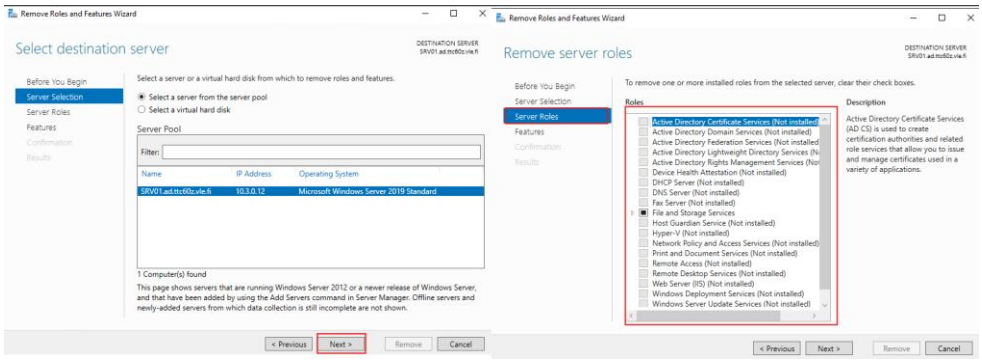
Pääsimme poistamaan tarpeettomia rooleja ja ominaisuuksia oikean yläkulman manage ja remove roles and features alta. (Kuvio 2.)



Kuvio 2. Roolien ja ominaisuuksien poisto

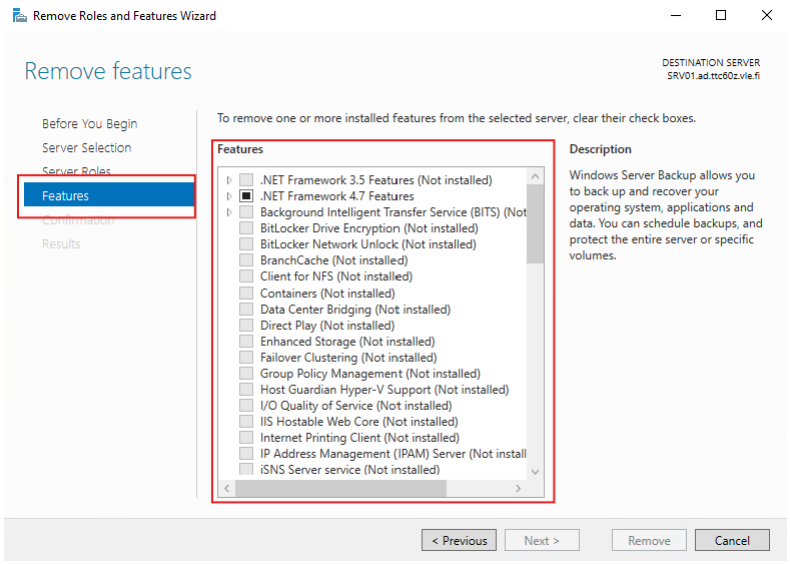
Painoimme server selection osiossa next-painiketta ja siirryimme server roles osioon.

Server roles osiossa poistimme kaikki muut paitsi tiedosto ja tallennus palvelut (File and Storage Services) ja painoimme next-painiketta. (Kuvio 3.)



Kuvio 3. Server Roles

Features välilehdellä voimme poistimme valinnan kaikista paitsi .NET framework 4.7 features, Windows Defender Antivirus ja Windwos PowerShell ja WoW64 Support. Näitä voi lisätä ja poistaa myöhemmin lisää tarpeen mukaan. (Kuvio 4.)

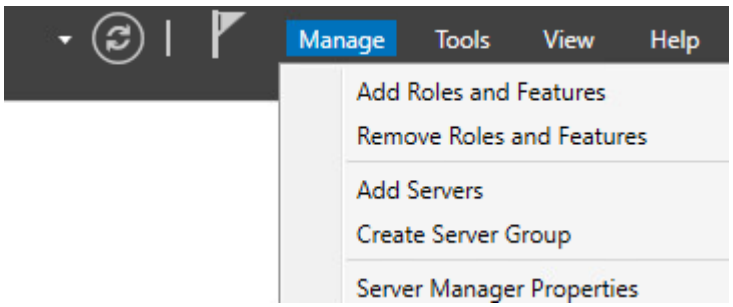


Kuvio 4. Server Features

T

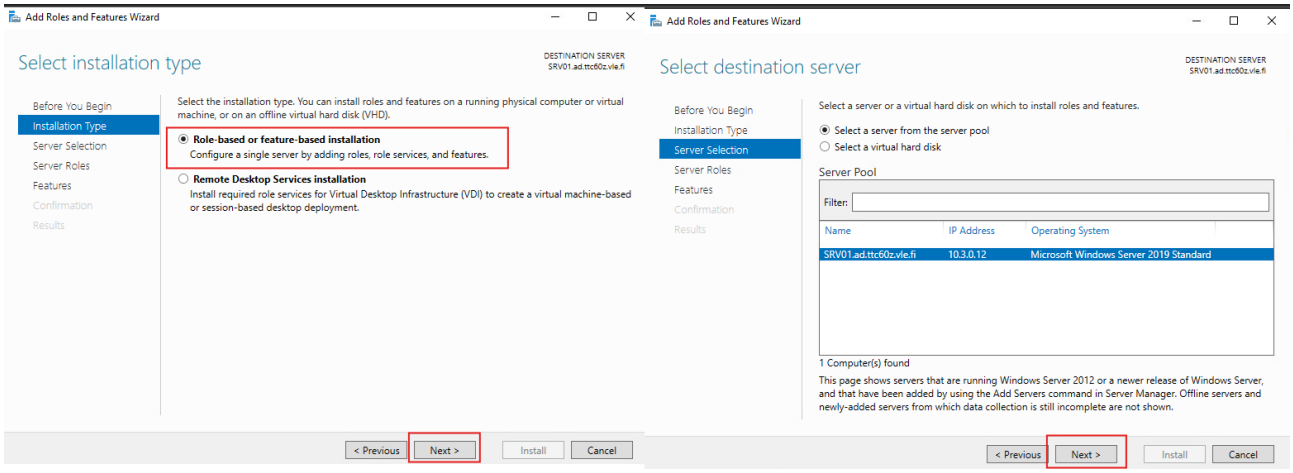
Tämän jälkeen siirryimme eteenpäin Next-painikkeella Confirmation-näyttöön, jossa valitsimme Restart the destination server automatically if required, jonka jälkeen siirryimme taas eteenpäin.

Seuraavaksi asensimme tarvittavat roolit ja ominaisuudet palvelimelle. Valitsimme oikean yläkulman Manage-otsikon alta Add Roles And Features (Kuvio 5).



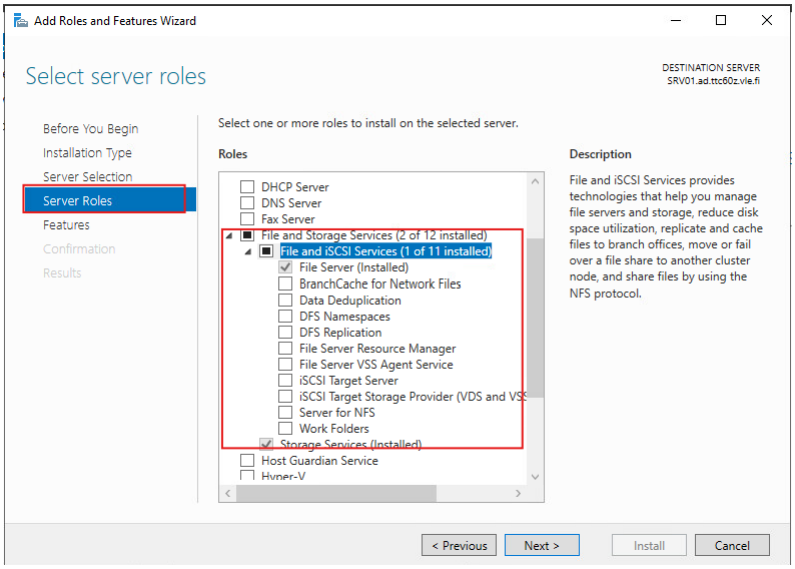
Kuvio 5. Roolien ja ominaisuuksien lisääminen

Latauksen tyyppi (installation Type) osiossa valitsimme ylemmän ja siirryimme seuraavaan kohtaan. Palvelimen valinnassa (server selection) valitsimme taas meidän palvelimemme, SRV01, joka on ainut vaihtoehto. (Kuvio 6.)



Kuvio 6. Installation Type ja Server Selection

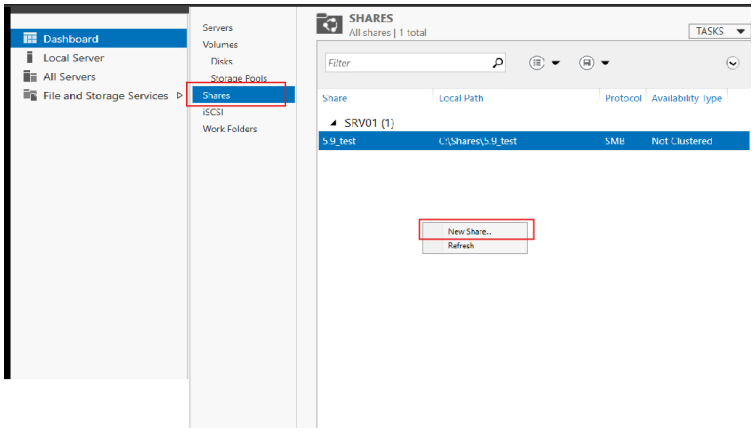
Seuraavaksi valitsimme asennetavat roolit. Valitsimme ohjeen mukaan File and Storage Services otsikon alta Storage Services, sekä File Server and iSCSI services otsikon alta File Server. Kuviossa 7 näkyy valitut roolit jo valmiiksi asennettuna. (Kuvio 7.)



Kuvio 7. Asennettavat roolit

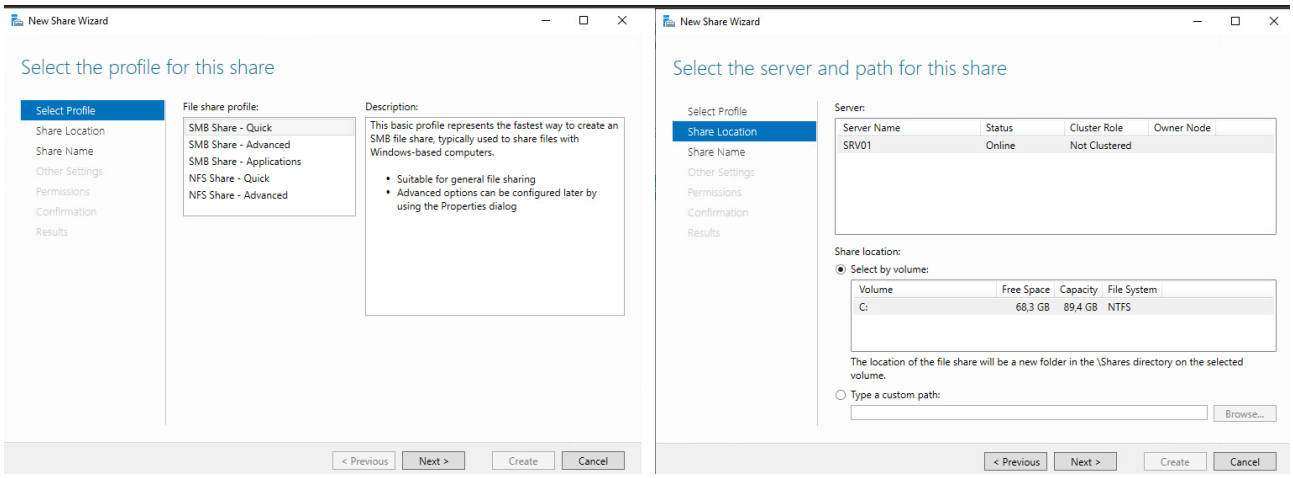
Features osiosta emme valinneet mitään, vaan jatkoimme suoraan Confirmation osioon, jossa valitsimme Restart the destination server automatically if required, kuten aiemminkin. Nyt kaikki tarvittavat ominaisuudet ja roolit olivat asennettu. Poistimme siis kaiken tarpeettoman ja jätimme jäljelle ainoastaan ominaisuudet ja roolit, joita tiedostopalvelimen käyttöön vaaditaan.

Loimme vielä ohjeen mukaan jaetun kansion kuvion 8 mukaan. (Kuvio 8.)



Kuvio 8. New Share

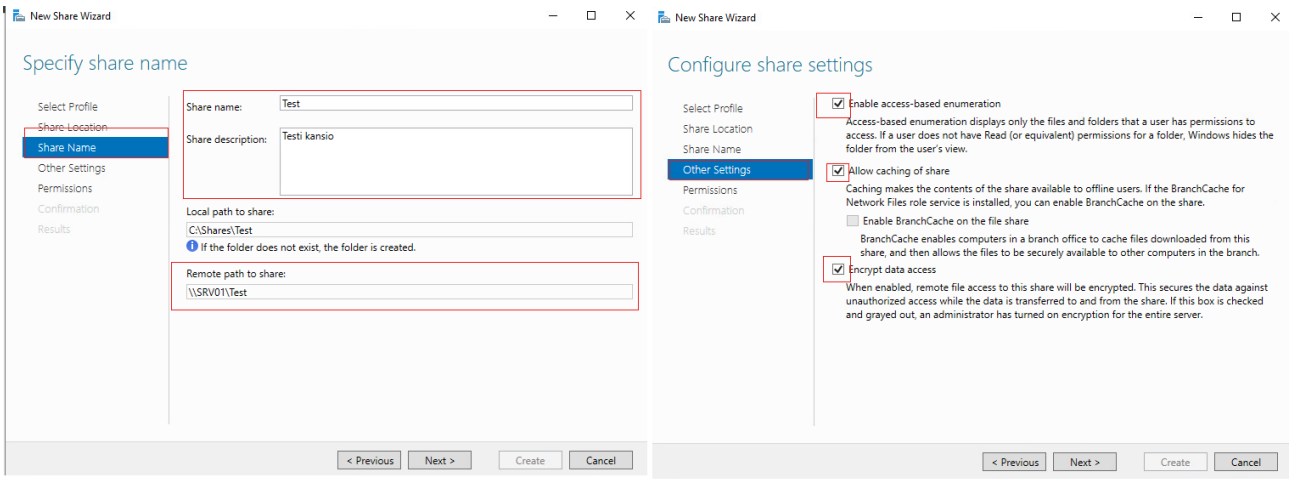
Valitsimme profiiliksi SMB Share – Quick. Emme muuttaneet Share Location välilehdellä mitään, mutta sieltä olisi voinut valita palvelimelta jonkin toisen tallennuspaikan C-levyn sijasta.. (Kuvio 9.)



Kuvio 9. Profiili ja sijainti

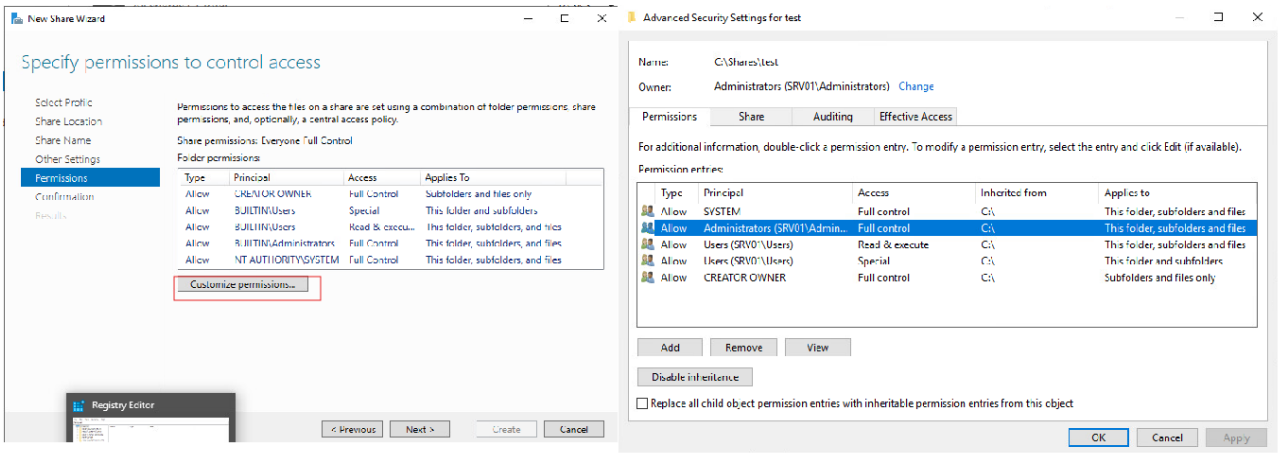
Share Name välilehdellä määritimme kansiolle nimen ja asetimme sille kuvauksen. Koska teimme ensimmäistä kansiota ja harjoittelimme sen tekemistä, nimesimme kansion nimellä Test. Täältä asetimme polun, jolla etäkäyttäjät pääsevät käsiksi kansioon. Asetimme poluksi \\SRV01\Test. (Kuvio 10).

Siirryimme Other settings välilehdelle, jossa valitsimme turvallisuuden kannalta tärkeitä asetuksia kuten Enable access-based enumeration ja Encrypt data access. Valitsimme nämä, koska ne auttavat salaamaan tietoja tahoilta, joille ne eivät kuulu. (Kuvio 10.)



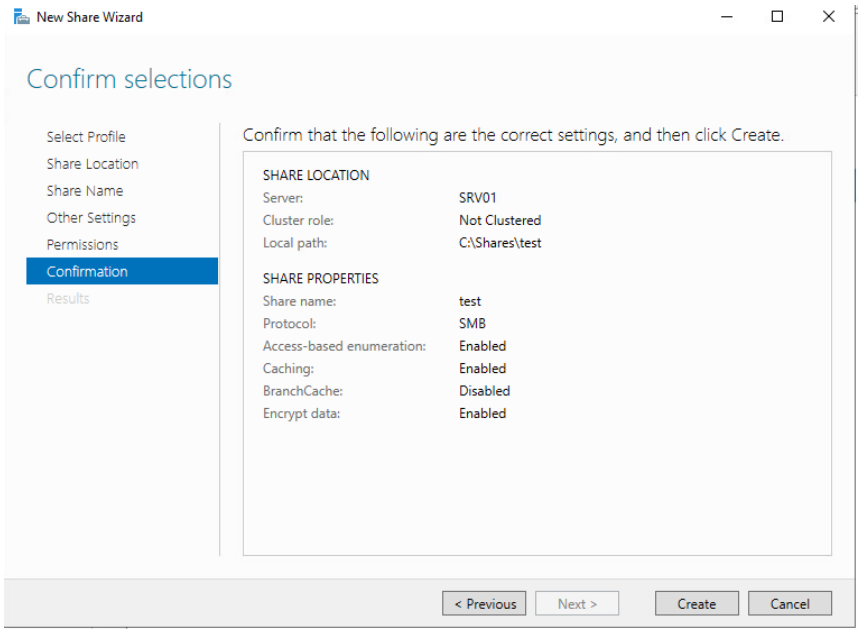
Kuvio 10. Nimi ja muut asetukset

Permissions välilehdellä määrittelimme käyttäjiä ja käyttäjäryhmiä, joilla on oikeus jaettuun kansioon. Näitä voi määrittää myöhemminkin luonnin jälkeen niin kuin teimmekin. (Kuvio 11.)



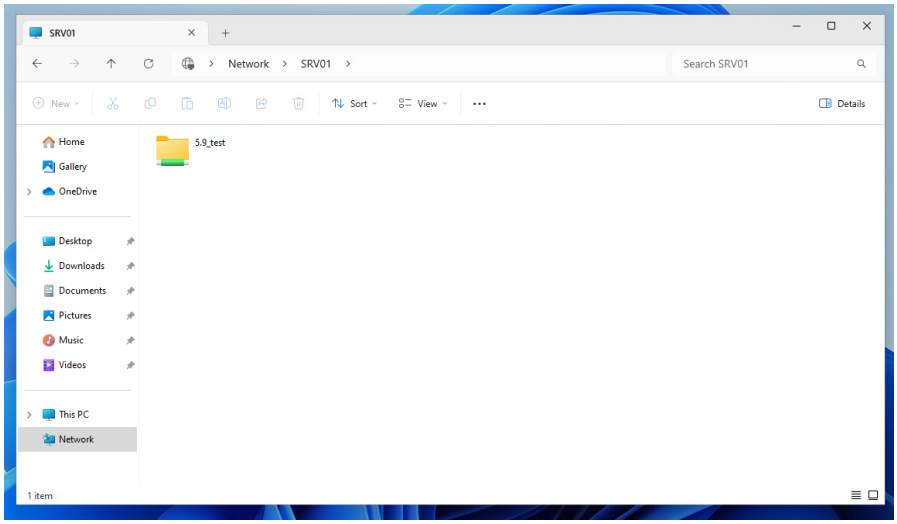
Kuvio 11. Oikeudet

Confirmation välilehdellä tarkistimme vielä, että asetukset ovat oikein ja painoimme Create-painiketta luodaksemme kansion. (Kuvio 12).



Kuvio 12. Tietojen varmistus

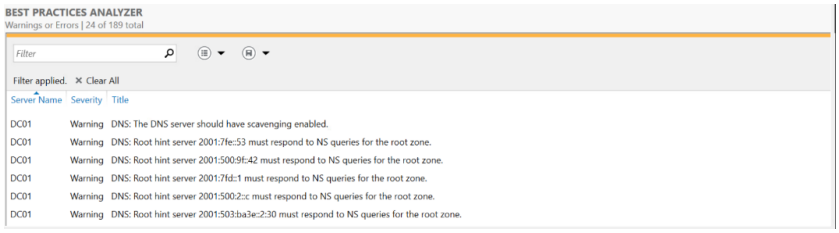
Esimerkin vuoksi lisäsimme testikäyttäjän käyttäjiin, joilla on oikeus nähdä kansio. Kuvion 13 mukaisesti, kansio löytyi aiemmin määritetystä polusta \\SRV01\, kun olimme kirjautuneet WS01-koneelle testikäyttäjällä.



Kuvio 13. Testikäyttäjä verkkolevyllä

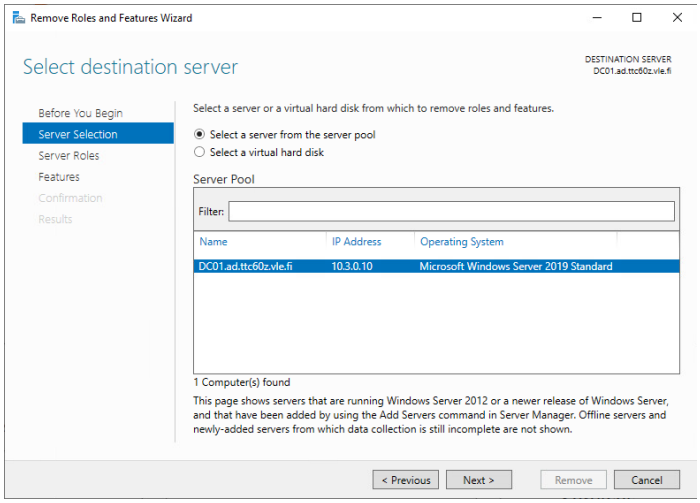
3.2 Active Directoryn Koventaminen

Seuraavaksi kovensimme Active Directoryn (AD) palvelimellamme DC01. Active Directoryn koventaminen on olennainen osa domain controllerin (DC), ja näin koko ympäristön suojaamista. AD:n olennaisiin kovennuksiin liittyy esimerkiksi 3 tasoinen administraattori malli, SIEM järjestelmät, monivaiheinen autentikointi (MFA). Emme tässä labra työssä toteuttaneet näitä vaan keskityimme enemmän yksittäisiin kovennuksiin, mutta on hyvä tiedostaa näiden tärkeys. Ennen kovennusten suorittamista otimme talteen kuvan Best practices analyzer (BPA) tuloksista jotta voimme verrata niitä lopputilanteessa. (Kuvio 14.)



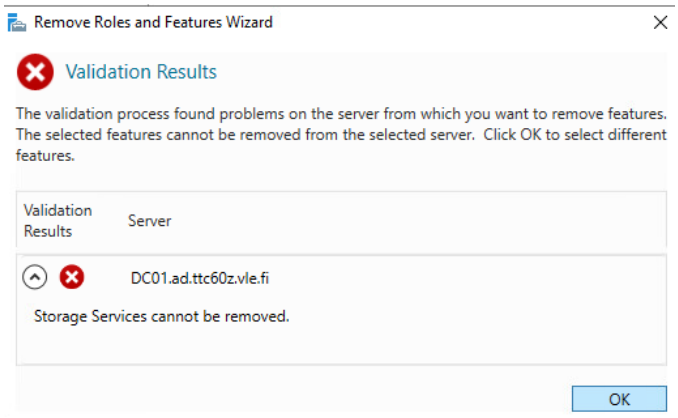
Kuvio 14. BPA alkutilanne

Aloitimme koventamisen poistamalla palvelimelta turhaksi näkemämme roolit ja ominaisuudet niin kuin teimme tiedostopalvelimen luonnin yhteydessä. Tämä löytyi samasta paikasta kuin alussa (Kuvio 1.). valitsimme palvelimen valinnassa (server selection) tämänhetkisen palvelimen. (Kuvio 15.)



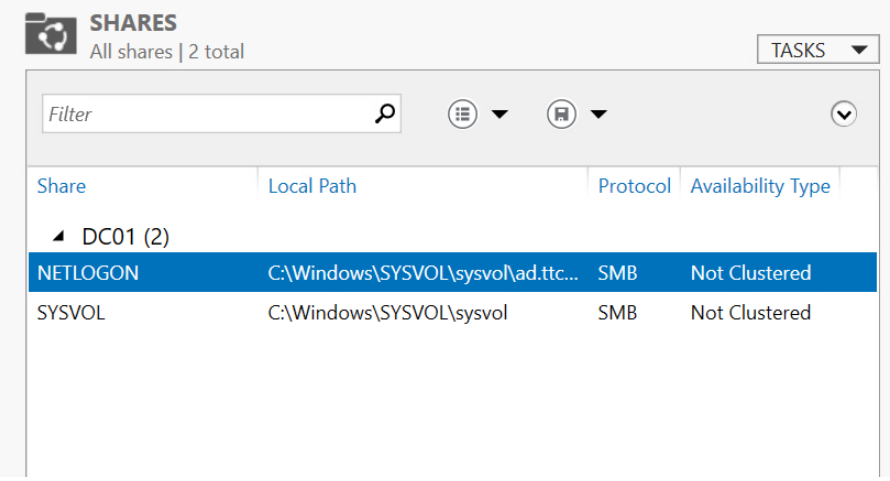
Kuvio 15. Palvelimen valinta

Server Roles osiossa yritimme poistaa file and storage services AD:lta mutta saimme virhe ilmoituksen. (Kuvio 16.)



Kuvio 16. error

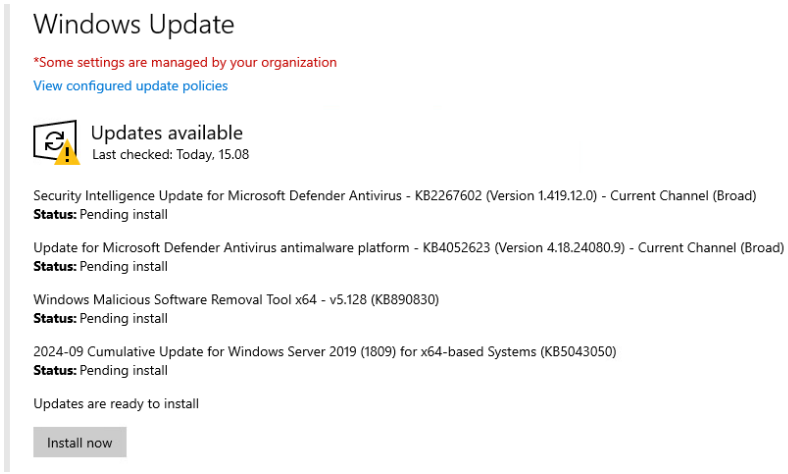
Tämä johtui siitä, että meillä oli jaossa kaksi kansiota. Emme siis poistaneet kyseistä roolia, koska kansioilla on tarkoituksensa. NETLOGON tarkoitus liittyy kirjautumisskripteihin ja autentikointiin ja SYSVOL liittyy ryhmäkäytäntöjen ja AD:n toimintaan liittyvien tiedostojen ja asetusten tallentamiseen. (Kuvio 17.)



Kuvio 17. Sharet

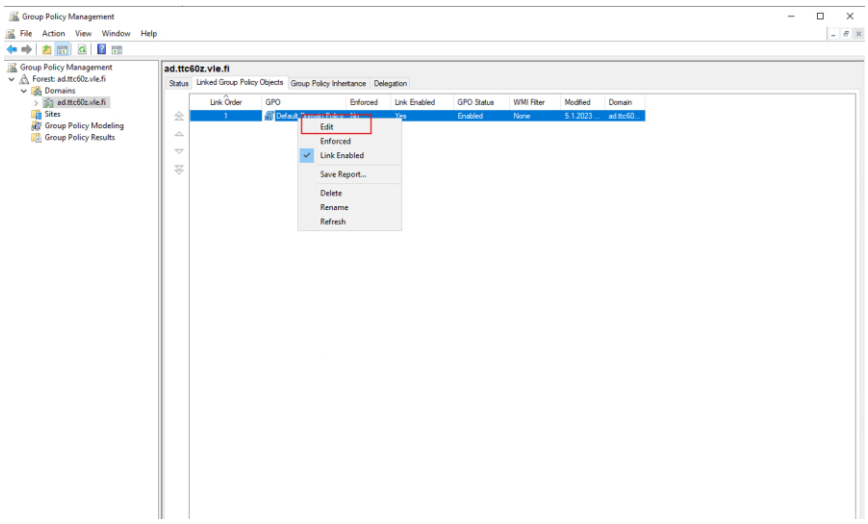
Emme siis toistaiseksi poista mitään rooleja tai ominaisuuksia.

Olennainen osa koventamista on järjestelmän ajan tasalla pitäminen. Uudet päivitykset lisäävät järjestelmän tietoturvaa ja poistavat tiedettyjä heikkouksia järjestelmästä. Myöhemmässä vaiheessa tämä tapahtuu WSUS-palvelimen (Windows Server Update Services) kautta, mutta tässä vaiheessa päivitimme palvelimet käsin Windows Updaten kautta. (Kuvio 18.)



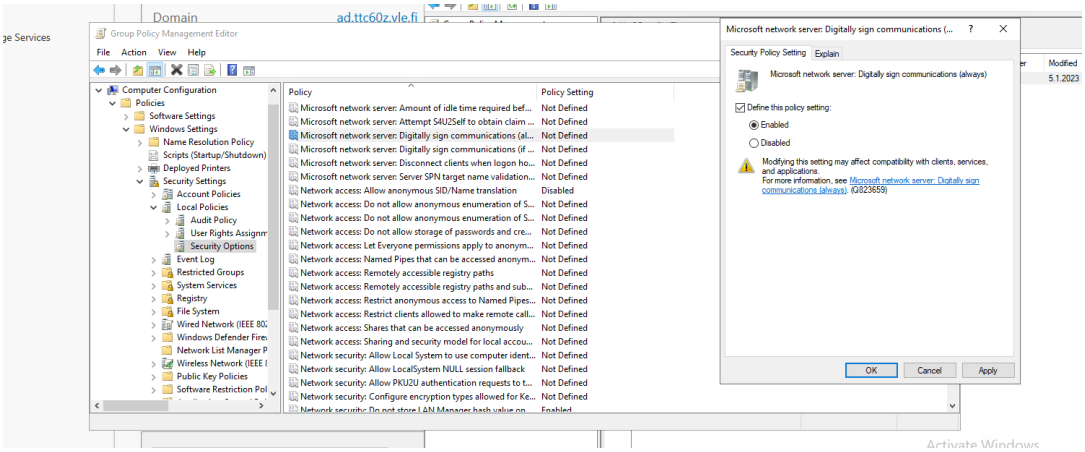
Kuvio 18. Windows Update

Siirryimme tarkastelemaan SMB- ja LAN manager hash -asetuksia. Hyökkääjät voivat hyödyntää näitä MitM (Man in the Middle) hyökkäyksissä, joten on hyvä tarkastaa ne.
Avasimme Group Policy management-ohjelman ja Domains-välilehdeltä valitsimme meidän palvelimemme. Oikealla hiiren painikkeella valitsimme edit. (Kuvio 19.)



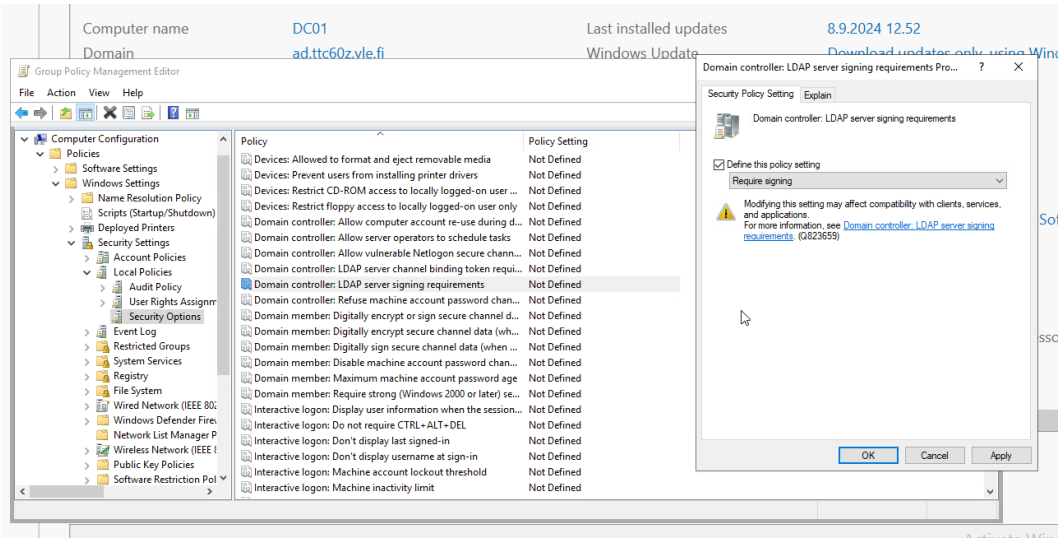
Kuvio 19. Group policy management

Seuraavaksi siirryimme näytön vasemmassa laidassa polkuun Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Microsoft network server: Digitally sign communication (always). Kaksoisklikkaamalla saimme auki ikkunan, josta laitoimme säännön käyttöön, eli valitsimme Enabled. (Kuvio 20.)



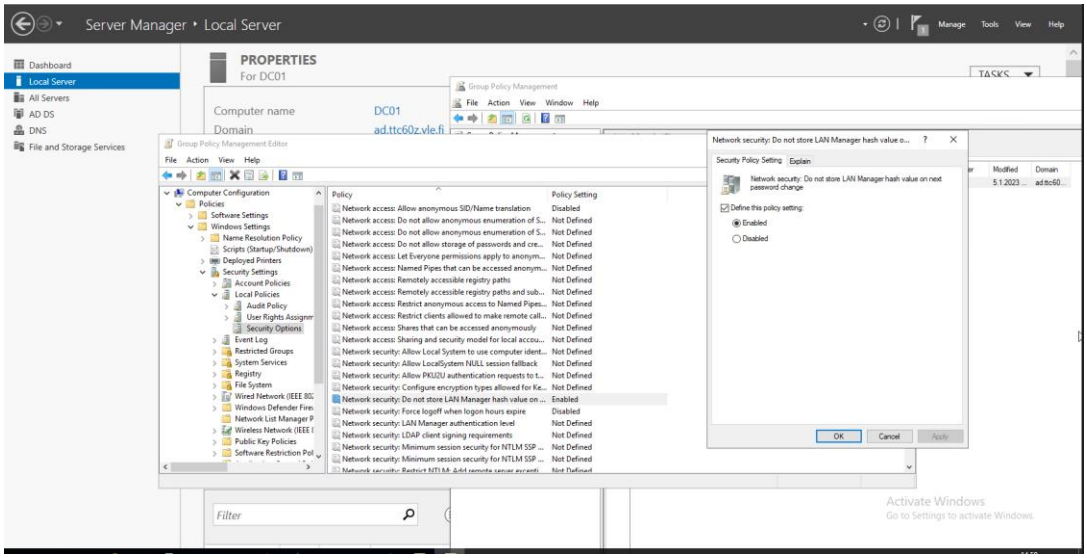
Kuvio 20. SMB allekirjoitus

Katsoimme samasta paikkasta LDAP server signing requirements. Vaihdoimme tähän asetukseksi Require signing. Näin hyväksytään vain allekirjoitetut LDAP pyynnöt. (Kuvio 21.)



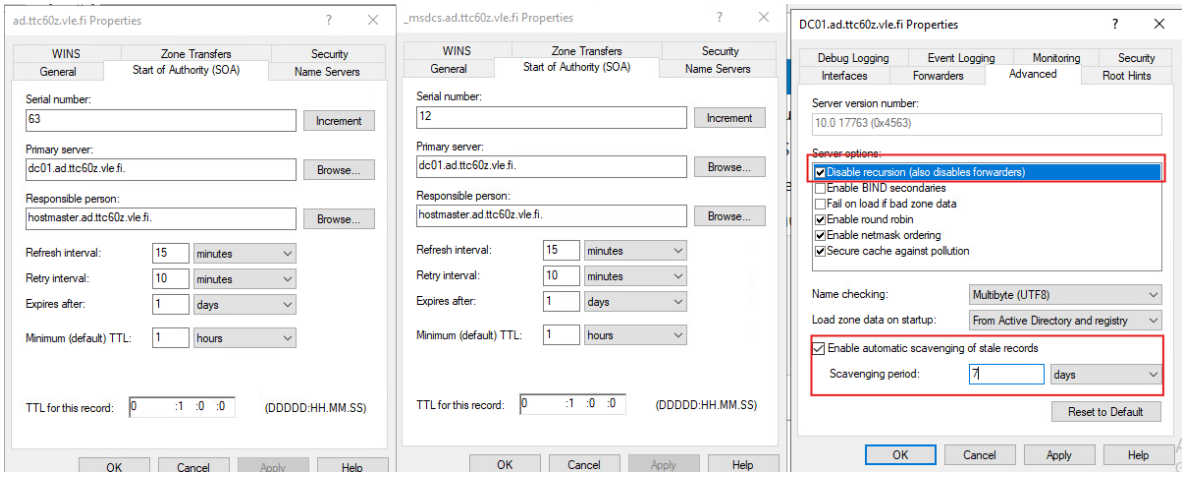
Kuvio 21. LDAP

LAN Manager Hash asetus sijaitsee myös samassa paikassa ja oli valmiiksi asetettu Enabled-tilaan, joten tätä ei tarvitse muuttaa. (Kuvio 22.)



Kuvio 22. LAN manager Hash

Seuraavaksi pyrimme koventamaan DNS:sää (Domain Name System) Disable recursion ruksi aiheutti ongelmia, tämän jälkeen WS01 ei saanut enää yhteyttä DNS palvelimelle eikä päässyt verkkoon. Tuo siis korjautui, kun otimme raksin taas pois. Enable automatic scavenging of stale records tarkoittaa, että käyttämättömät dns tietueet tyhjennetään. Tämä vähentää kuormitusta, joten kytkimme sen päälle. (Kuvio 23.)

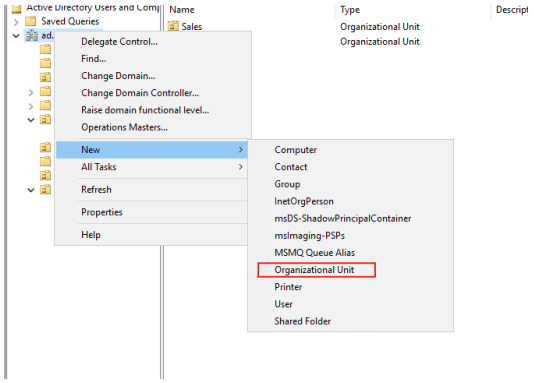

ad.ttc60z.vle.fi Properties
WINS
Zone Transfers
Security
General
Start of Authority (SOA)
Name Servers
Serial number:
63
Increment
Primary server:
dc01.ad.ttc60z.vle.fi.
Browse...
Responsible person:
hostmaster.ad.ttc60z.vle.fi.
Browse...
Refresh interval:
15
minutes
Retry interval:
10
minutes
Expires after:
1
days
Minimum (default) TTL:
1
hours
TTL for this record:
0 :1 :0 :0
(DDDDD:HH.MM.SS)
OK
Cancel
Apply
Help
_msdcs.ad.ttc60z.vle.fi Properties
WINS
Zone Transfers
Security
General
Start of Authority (SOA)
Name Servers
Serial number:
12
Increment
Primary server:
dc01.ad.ttc60z.vle.fi.
Browse...
Responsible person:
hostmaster.ad.ttc60z.vle.fi.
Browse...
Refresh interval:
15
minutes
Retry interval:
10
minutes
Expires after:
1
days
Minimum (default) TTL:
1
hours
TTL for this record:
0 :1 :0 :0
(DDDDD:HH.MM.SS)
OK
Cancel
Apply
Help
DC01.ad.ttc60z.vle.fi Properties
Debug Logging
Event Logging
Monitoring
Security
Interfaces
Forwarders
Advanced
Root Hints
Server version number:
10.0 17763 (0x4563)
Server options:
Disable recursion (also disables forwarders)
Enable BIND secondaries
Fail on load if bad zone data
Enable round robin
Enable netmask ordering
Secure cache against pollution
Name checking:
Multibyte (UTF8)
Load zone data on startup:
From Active Directory and registry
Enable automatic scavenging of stale records
Scavenging period:
7
days
Reset to Default
OK
Cancel
Apply
Help

Kuvio 23. DNS

3.3 GPO koventaminen

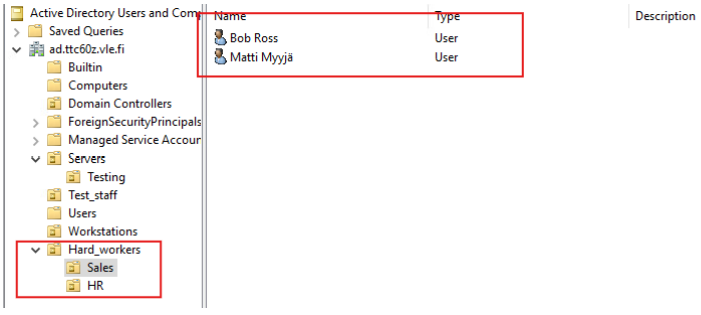
GPO eli Group Policy Objects on olennainen osa AD ympäristön työkaluja. Se vastaa nimensä mukaan ryhmäkohtaisista politiikoista, ja sen avulla voidaan asettaa tietyt käytänteet ja rajoituksen käyttäjille, laitteille ja ympäristöille.

Loimme muutaman Organizational Unitin (OU), groupin ja käyttäjän AD:lla, jotta pystyimme tekemään käyttäjäryhmiä koskevia säädöksiä ja kovennuksia. Ensin teimme uuden Organizational unitin ”Hard_workers” jonka alle teimme kaksi OU:ta lisää, Sales ja HR. (Kuvio 24.)



Kuvio 24. Organizational unit

Kun OU:t oli luotu, lisäsimme kaksi käyttäjää molempiin. (Kuvio 25.)

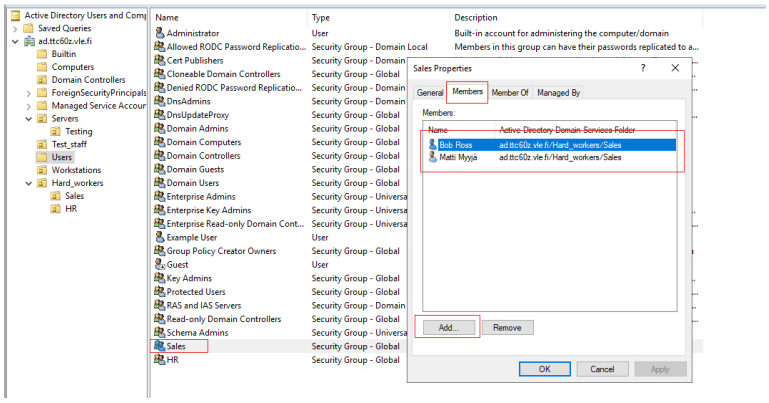


Kuvio 25. lopputulos

Seuraavaksi teimme kaksi ryhmää Users-kansion alle: Sales ja HR. Nämä ryhmät ovat tarkoitettu käyttäjien käyttöoikeuksien määrittämiseen, esimerkiksi kansion luku- ja muokkausoikeudet. (Kuvio 26.) Lisätään myös käyttäjät heille luotuihin ryhmiin.

Kuvio 26. groups

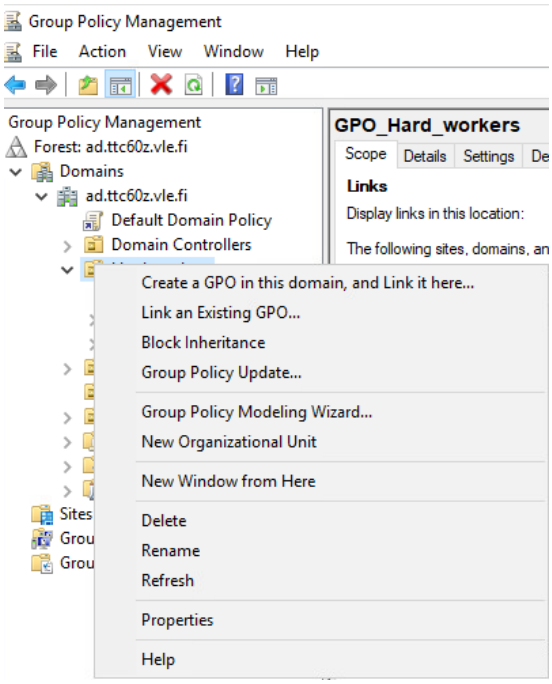
Lisäsimme käyttäjät heille kuuluviin ryhmiin ryhmän ominaisuudet-ikkunan jäsenet-välilehden kautta Add-painikkeesta. Teimme saman molemmille ryhmille. (Kuvio 27.)



Kuvio 27. Ryhmän jäsenet

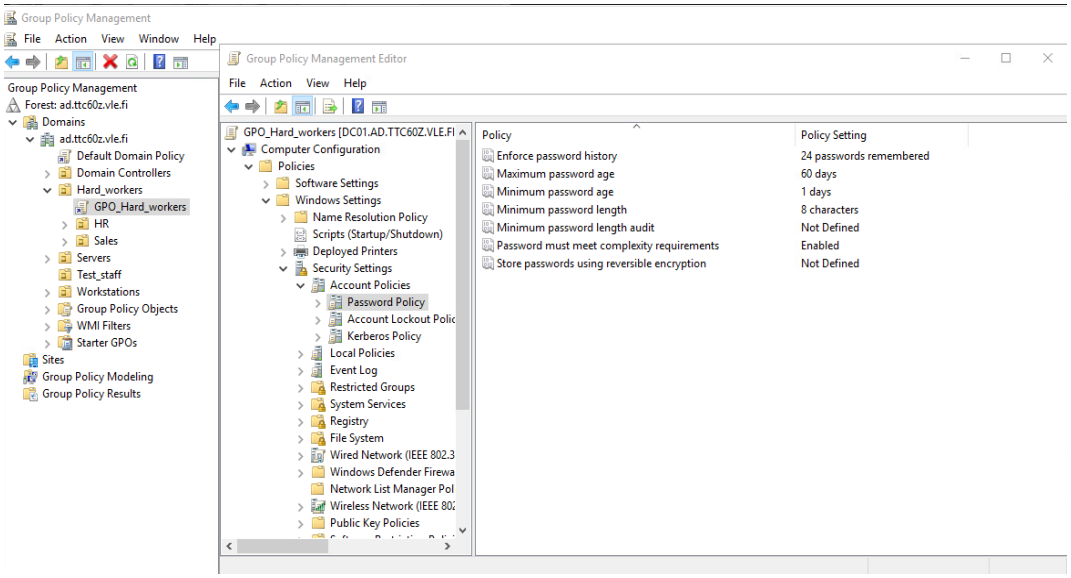
Pystymme nyt luomaan ryhmäpolitiikkoja, jotka koskevat joko molempia työ ryhmiä tai vain toista.

Seuraavaksi teimme Group Policy Objectin (GPO) OU:lle Hard_workers. Tämä tapahtui klikkaamalla hiiren oikealla painikkella OU:n nimeä ja valitsemalla Create a GPO in this domain and Link it here. Nimesimme sen GPO_Hard_workers. (Kuvio 28).



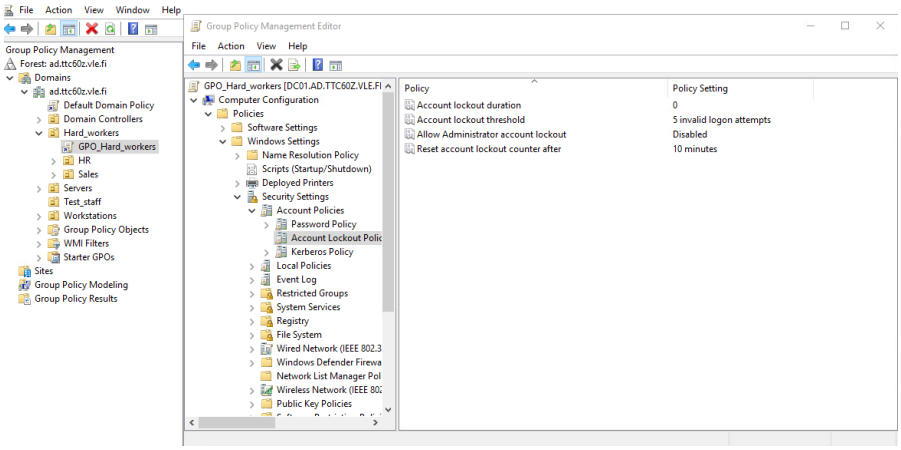
Kuvio 28. GPO:n luonti

Seuraavaksi asetimme ryhmälle salasanakäytäntöjä. Asetimme salasanakäytännöt tämän ryhmän alle, jotta Admin-käyttäjän salasana voidaan pitää samana, kuten kurssin ohjeistuksessa on toivottu. Teimme säännöt, joiden mukaan salasanan tulee olla kahdeksan merkkiä pitkä, se ei saa sisältää käyttäjänimeä, siinä on isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä. Salasana tulee myös vaihtaa kahden kuukauden välein, eikä mitään samaa salasanaa, joka on ollut yksi viimeisestä 24 salasanasta voi käyttää. (kuvio 29.)



Kuvio 29. Salasanakäytänteet

Asetimme käyttäjätileille myös muita rajoituksia. Käyttäjätili lukittuu viiden virheellisen kirjautumisyrityksen jälkeen ja lukitus voidaan purkaa ainoastaan järjestelmänvalvojan toimesta (Kuvio 30). Tällä halusimme ehkäistä Brute Force -hyökkäyksiä.

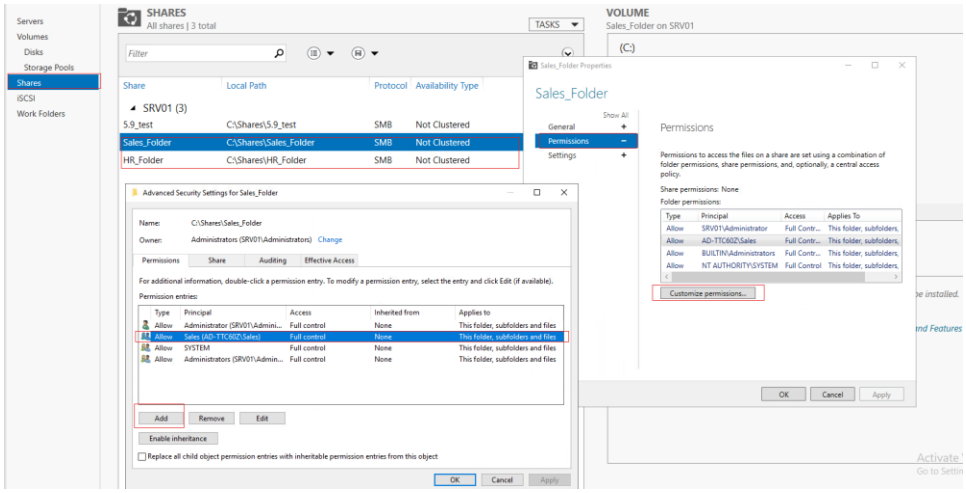


Kuvio 30. Käyttäjätilin lukituskäytänteet

3.3.1 Korjaus Salasanakäytänteisiin

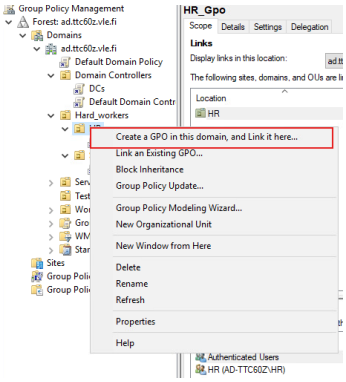
Nämä käytänteet eivät tulleet käytäntöön koska password policy ovat computer configurations osuuden alla joka koskee vain laitteita, ei käyttäjiä. Korjasimme tämän muokkaamalla Salasana vaatimukset Default Domain Policyyn. Asetimme tähän minimi salasana pituudeksi 6 merkkiä koska adminin salasanoja ei saa vaihtaa. Tähän olisi varmaan keino, jolla gpo ei koskisi administraattoreita, kuten fine grained password policy. Tämän palautukseen mennessä emme sitä kerenneet saada toimimaan.

Tahdoimme luoda myös käyttäjäryhmille työtehtävän mukaiset verkkoasemat tiedostopalvelimemme kautta niin kuin labran alussa. Tällä kertaa määritimme luodut kansiot vain tietyn ryhmän käyttöön. Määrittelimme SRV01 tiedostopalvelimella kaksi jaettua kansiota Sales_Folder ja HR_Folder, ja lisäsimme oikeudet välilehdelle aiemmin määrittelemämme käyttäjäryhmät. (Kuvio 31.)



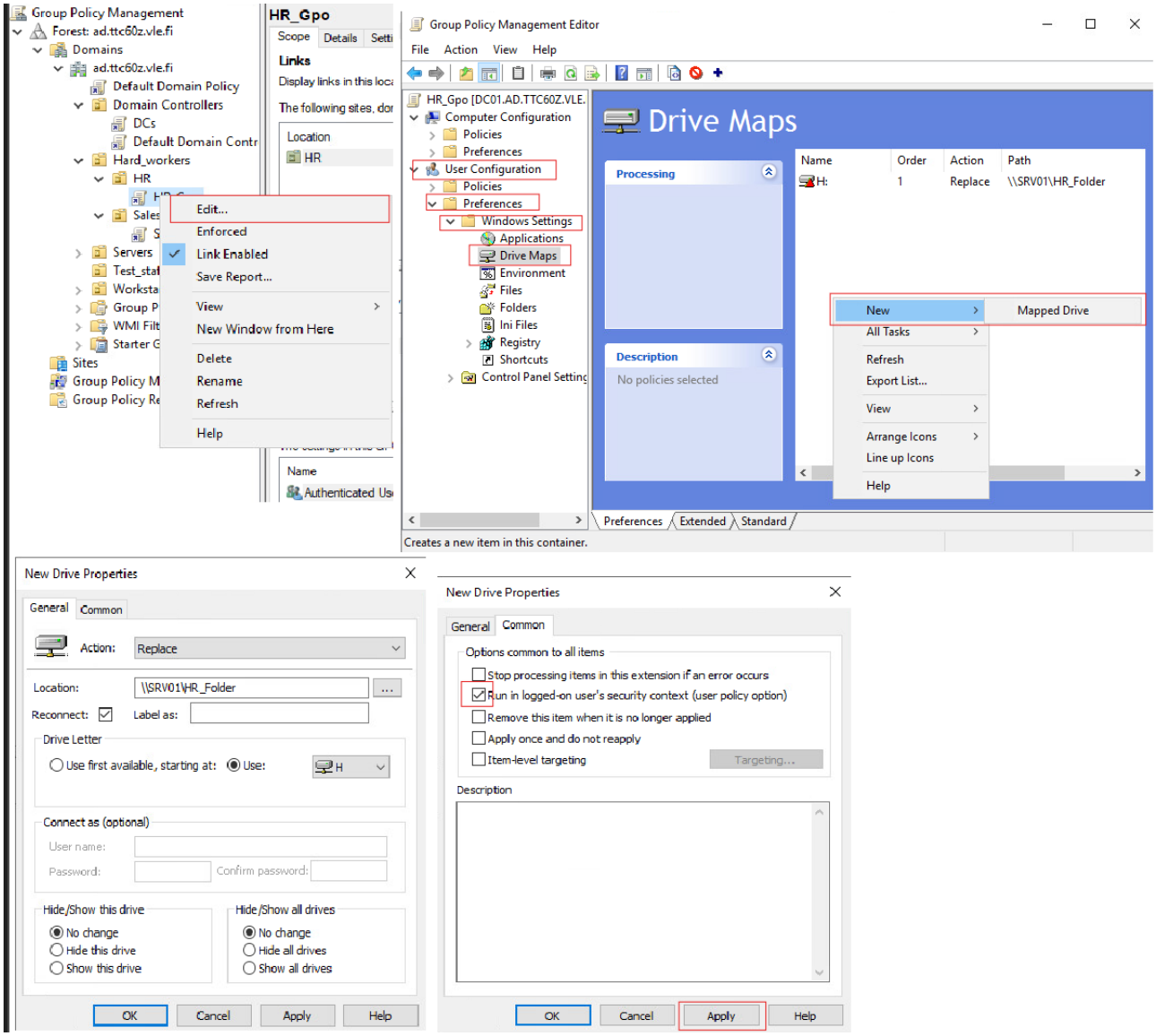
Kuvio 31. File Sharet

Seuraavaksi siirryimme takaisin DC01 domain controllerille ja määritämme aiemmin luoduille OU:ille omat GPO:t. Nämä GPO:t koskevat vain joko HR tai Sales OU:ta, jos tahdomme tehdä kaikkia työntekijöitä koskevia politiikkoja, muokkaamme salasanakäytäntöjen yhteydessä luotua GPO:ta tai muokkaamme koko palvelinta koskevaa GPO:ta, joka kuvassa nimellä Default Domain Policy. (Kuvio 32.)



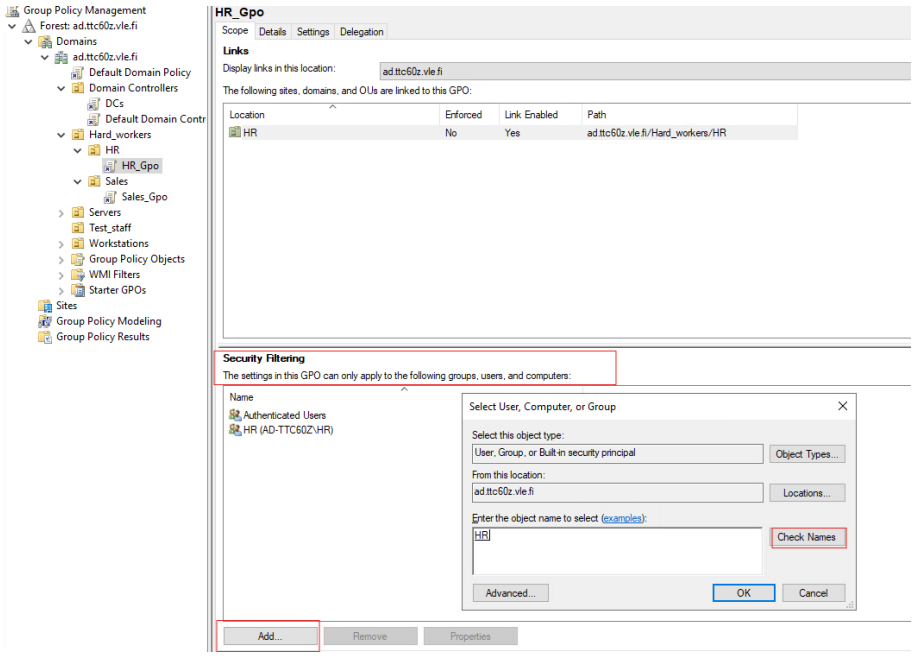
Kuvio 32. GPOn luonti

Seuraavaksi muokkasimme GPO:ta ja lisäsimme tämän politiikan alaisille käyttäjille luomamme jaetun kansion automaattisesti lisättäväksi verkkolevyksi (Kuvio 33.) mukaisesti.



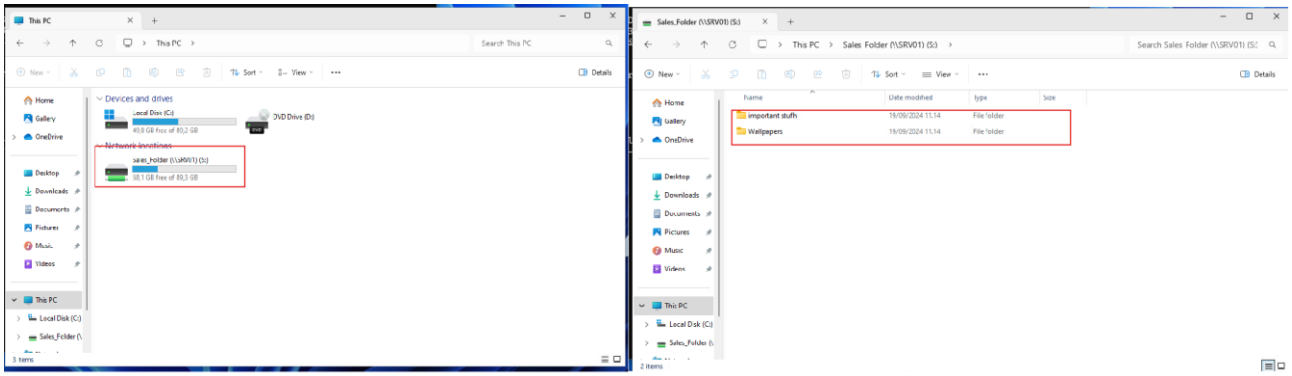
Kuvio 33. Drive map

Lisäsimme GPO:n Scope-osioon aiemmin luodun turvallisuusryhmän HR. Lisäsimme sen myös Delegation välilehdellä. (Kuvio 34.)



Kuvio 34. GPO_Scope

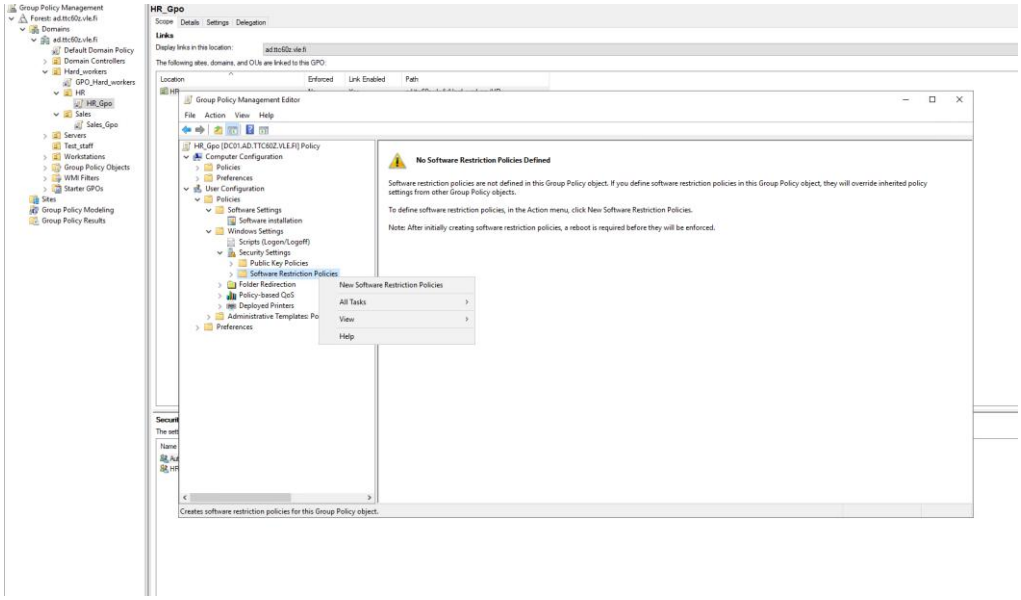
Kirjauduttuamme WS01-työasemalle luomallamme Matti Myyjä käyttäjätilillä, näimme asettamamme verkko aseman ja testasimme että pääsemme siihen käsiksi. Loimme kaksi kansiota testataksemme, että oikeudet on niin kuin pitää. (Kuvio 35.)



Kuvio 35. Verkkoasema

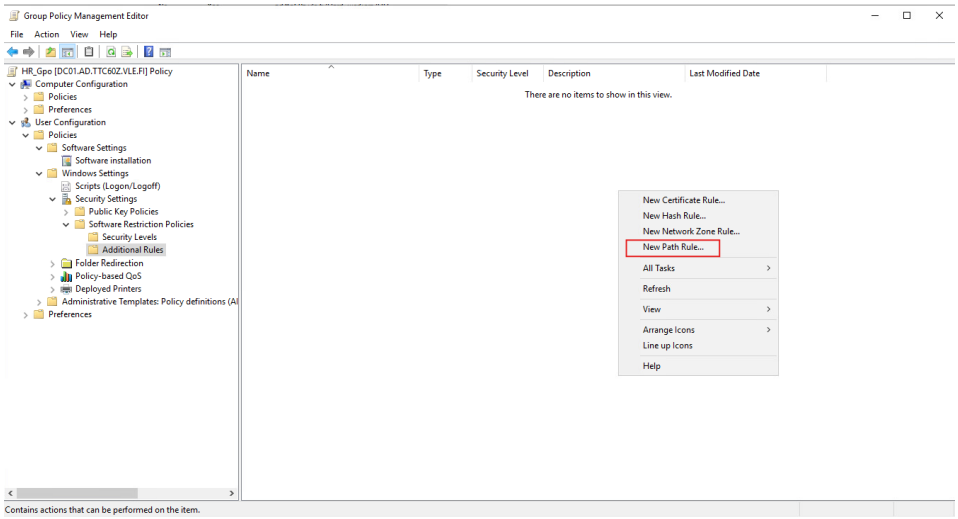
Kun olimme luoneet kaksi OU:ta ja niille omat ryhmäpolitiikat, pystyimme rajaamaan mitä käyttäjää mitkäkin säännöt koskevat. On oleellista, että käyttäjät eivät pysty käyttämään ominaisuuksia joille ei ole tarvetta. Seuraavaksi estimme Sales ja HR tiimien PowerShellin käytön.

Valitsimme aiemmin tekemämme HR_Gpo muokattavaksi ja suuntasimme Software Restriction Policies osuuteen, johon loimme uuden ”New Software Restriction Polices”. (Kuvio 36.)



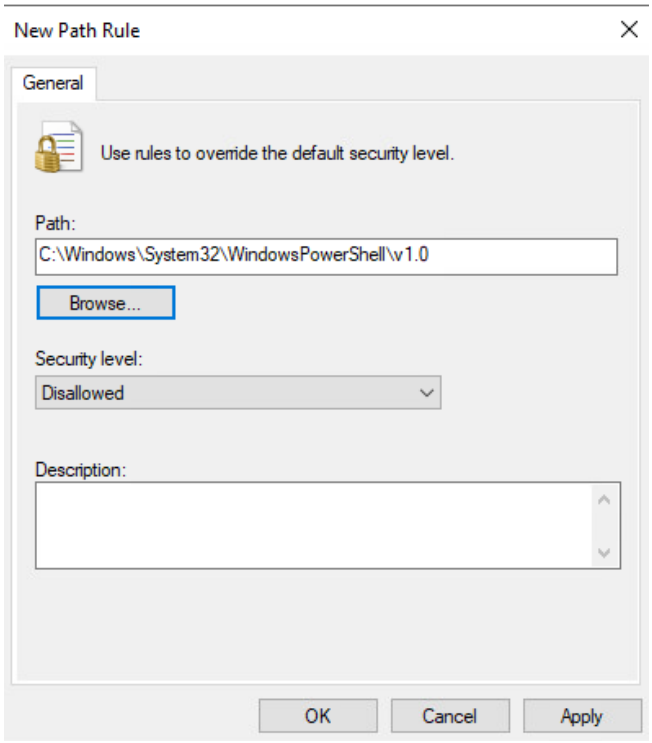
Kuvio 36. New Restriction policy

Rajoitetun sovelluksen voi valita eri tavoilla kuten Hash valuen tai sertifikaatin perusteella. Valitsimme kuitenkin nyt ”New Path Rule” ja määritimme polun josta sovellus löytyy. (Kuvio 37.)



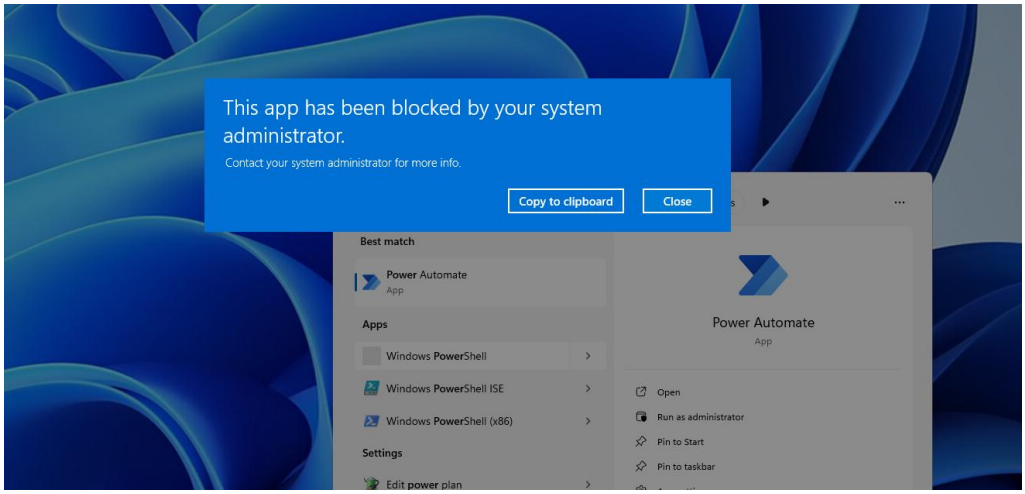
Kuvio 37. New Path Rule

Määritimme polun rajattuun sovellukseen ja painoimme Apply. Teimme tämän molemmille HR sekä Sales GPO:ille. (Kuvio 38.)



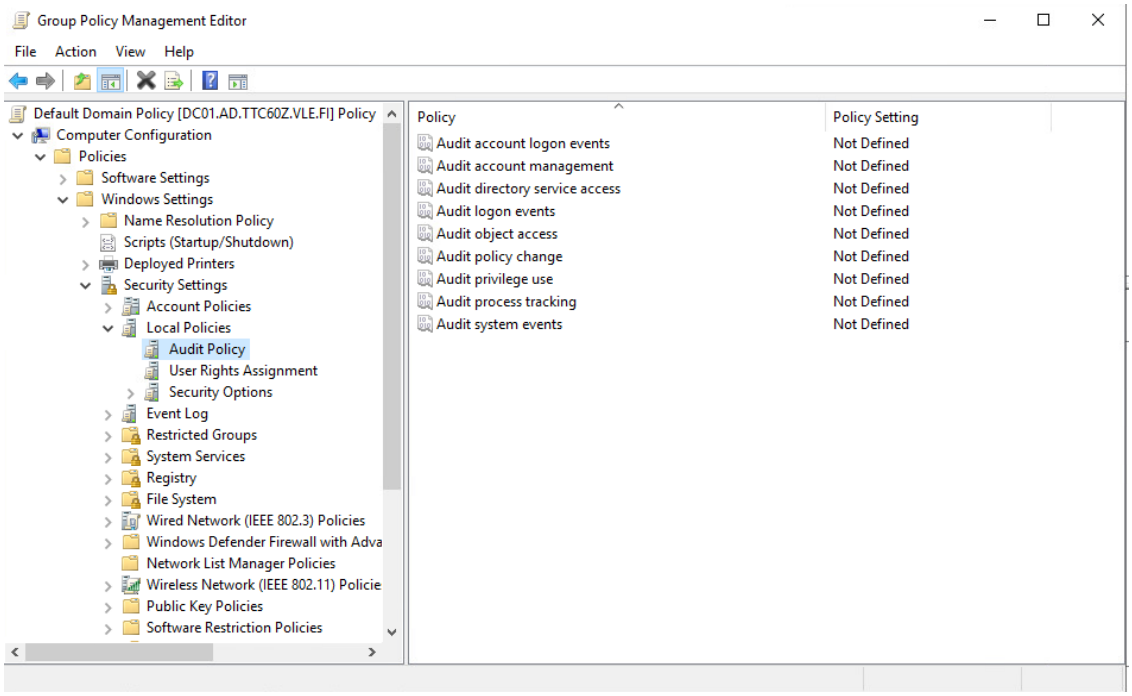
Kuvio 38. Path Rule

Kirjauduimme WS01-työasemalle HR-tiimiin kuuluvalla käyttäjällä ja yritimme käynnistää PowerShellin. Säännön mukaisesti emme sitä kuitenkaan pystyneet tekemään. (Kuvio 39.)



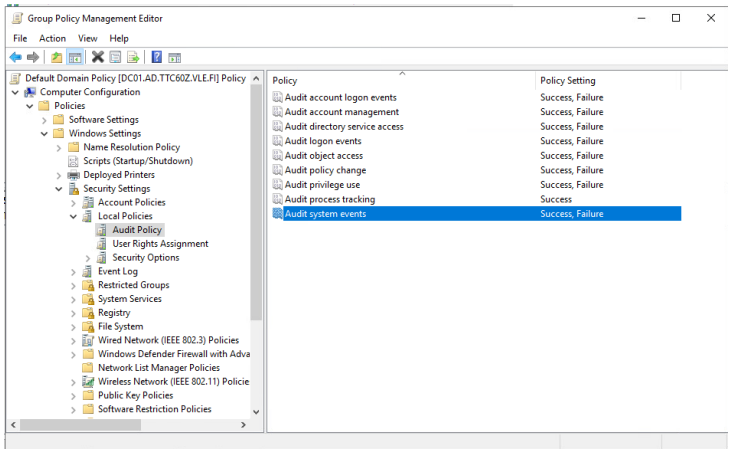
Kuvio 39. Blocked

Asetimme koko palvelinta koskevaan GPO:hon Audit Policyn, eli käytännön, jonka avulla järjestelmä seuraa ja kirjaa tiettyjä tapahtumia. (Kuvio 40.)



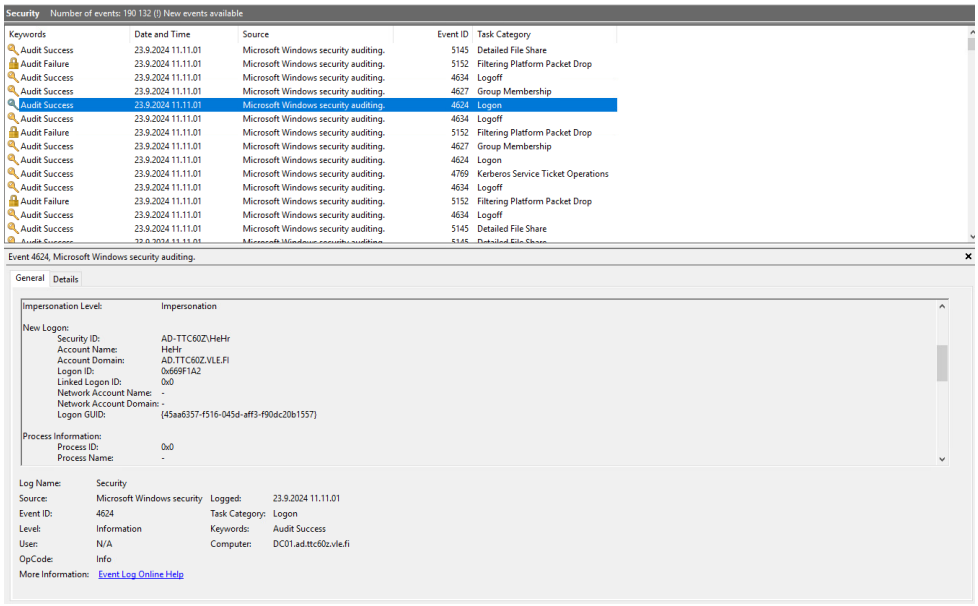
Kuvio 40. Auditointi käytänteet

Asetimme kuvion 41 mukaiset käytänteet, eli melkein kaikkiin valitsimme success/failure, koska haluamme saada tiedon epäonnistuneista sekä onnistuneista tapahtumista pystyäksemme analysoimaan mahdollisesti haitallisia tapahtumia. (Kuvio 41.)



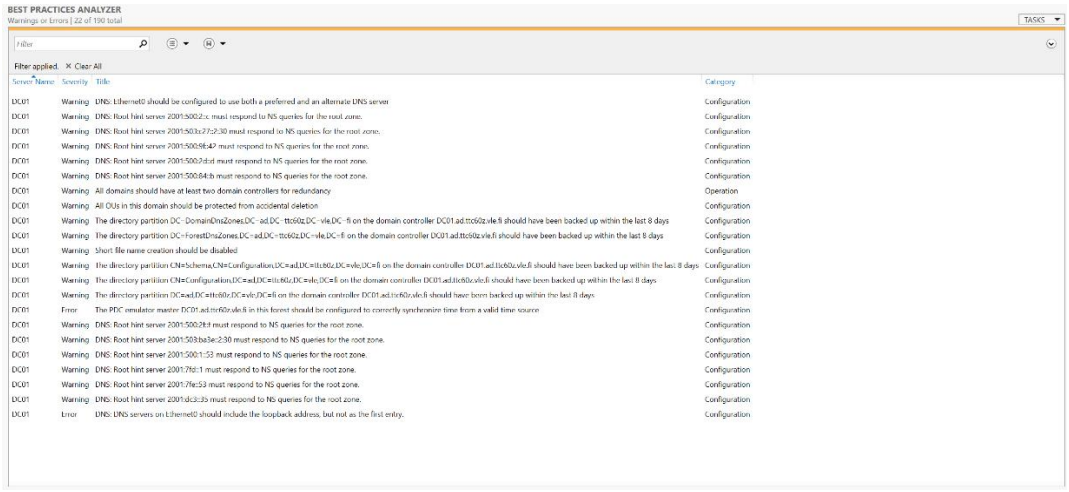
Kuvio 41. Auditointikäytänteiden asetukset

Nyt pystymme tarkastelemaan lokeja esimerkiksi käyttäjien kirjautumisista. (Kuvio 42.)



Kuvio 42. Event Viewer

Lopuksi otimme vielä kuvan Best Practices Analyzeristä vertaillaksemme muutoksia alkutilanteeseen. Varoitusten ja virheiden kokonaismäärä kasvoi hieman mutta itse ilmoitusten määrä väheni parilla (Kuvio 43.)



Kuvio 43. BPA_loppu

4 Pohdinta

Koventamisen ensimmäinen labratyö oli hyvä ensikosketus koventamiseen. Erilaisia kovennusohjeita löytyi valtavasti, ja osa niistä oli erittäin laajoja, joten alkuun tuntui todella vaikealta löytää ohjetta, jota lähteä seuraamaan. Kun vihdoin hyväksyimme, että yhdestä ohjeesta ei kannata kaikkea tekemään, vaan valitsimme muutamia kohtia, homma lähti rullaamaan. Kovennusten tekeminen tuntui aluksi hieman sekavalta, mutta kun uskaltautui klikkailemaan ja testailemaan niin erilaisten sääntöjen ja rajoitusten tekeminen lähti avautumaan.

Labrasta jäi loppujen lopuksi kuitenkin hyvä fiilis. Alkuvaikeuksien jälkeen saimme kuitenkin tehtyä joitakin meidän mielestämme tärkeitä kovennuksia. Esimerkiksi salasanakäytänteet ja sovellusten käytön rajoittaminen olivat suhteellisen helposti tehtävissä ja ne ovat hyödyllisiä. Kovennuksia olisi varmasti voinut tehdä vielä enemmänkin, ja jatkossa varmasti joitain teemmekin lisää mutta nyt kurssien aikataulujen puitteissa kaikkea ei voinut valmiiksi saada.

Lähteet

How Does LDAP Work: Everything IT Administrators Should Know. Blogi kirjoitus www.trio.so- sivustolla. 2024. Viitattu 18.9.2024. https://www.trio.so/blog/how-does-ldap-work/

Kerberos Authentication Overview. Microsoft Learn artikkeli. 2021. Viitattu 18.9.2024. https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview

Microsoft network server: Digitally sign communications (always). Microsoft Learn artikkeli. 2023. Viitattu 18.9.2024. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always

Schrader, D. What is System Hardening? Blogikirjoitus Netwrix-verkkosivustolla. 2023. Viim. muokkaus. 19.4.2024. Viitattu 18.9.2024. https://blog.netwrix.com/2023/02/22/system-hardening/

Systems Hardening. Beyondtrust.com -verkkosivusto. 2023. Viitattu 18.9.2024. https://www.beyondtrust.com/resources/glossary/systems-hardening

What is Active Directory and how does it work? Quest.com- verkkosivusto. Viitattu 18.9.2024. https://www.quest.com/solutions/active-directory/what-is-active-directory.aspx

What is Active Directory? Structure, benefits & How It Works. Lepide.com -verkkosivusto. 2024. Viitattu 18.9.2024. https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/

Wright, G. Definition File Server. Techtarget.com -verkkosivusto. 8/2021. Viitattu 18.9.2024. https://www.techtarget.com/searchnetworking/definition/file-server

Yu, E. What is a file server and why is it important? Blogikirjoitus synology -verkkosivustolla. 14.8.2023. Viitattu 18.9.2024 https://blog.synology.com/file-server