



Labra 1

Ryhmä 3

Antti Tammelin

Tero Räsänen

Elmeri Söderholm

Eliel Taskinen

Raportti

Syyskuu 2022

Tieto- ja viestintätekniikan tutkinto-ohjelma

Koventaminen TTC6050-3001

Sisältö

1	Johdanto	3
1.1	Tehtävänanto.....	3
1.2	Labran teoria ja termit	3
1.2.1	Koventaminen.....	3
1.2.2	VLE 4	
1.2.3	Windows Active Directory	4
1.2.4	Active Directory Domain Services.....	4
1.2.5	Windows Best Practises Analyzer	5
1.2.6	Domain Controller	5
1.2.7	DNS 5	
1.2.8	Varmuuskopiointi	5
2	Virtuaalisen Koneen Koventaminen	6
2.1	Lähtötilanne	6
2.2	Väärän toimeksiannon tekeminen.....	6
2.3	Best Practices Analyzer	6
2.4	AD DS:än koventaminen, ja toisen DC:n lisääminen.....	7
2.5	File and Storage Services koventaminen, Varmuuskopioinnin luominen	10
2.6	DNS koventaminen.....	15
2.6.1	Scavenging	16
2.6.2	Root Hint Warning	17
2.6.3	Loopback Address Error.....	19
3	Microsoft Security Compliance Toolkit.	21
3.1	Manuaalinen Group Policy konfiguraatio	22
3.2	Automaattinen Group Policyjen konfiguraatio	25
4	Pohdinta.....	29
	Lähteet	30
	Liitteet	32
	Liite 1. Labraympäristö.....	32

Kuviot

Kuvio 1. Esimerkki BPA:sta.....	6
Kuvio 2. BPA, AD DS.	7
Kuvio 3. Installing features to second controller.	8

Kuvio 4. Promoting to domain controller.	8
Kuvio 5. Credentials for the domain controller.	9
Kuvio 6. Checks passed.	9
Kuvio 7. Second Domain Controller.	10
Kuvio 8. Windows Server Backup.....	11
Kuvio 9. Backup Schedule.	11
Kuvio 10. Shared Network Folder.	12
Kuvio 11. Backup location.	13
Kuvio 12. Credentials for Backup.	14
Kuvio 13. Scheduled Backup.	14
Kuvio 14. Backup in SRV01.....	15
Kuvio 15. AD DS Analyzer empty	15
Kuvio 16. BPA DNS.	16
Kuvio 17. Scavenging enabled.....	16
Kuvio 18. Root hint warnings.	17
Kuvio 19. Resolving Root Hint Warnings.....	18
Kuvio 20. Resolved IP	18
Kuvio 21. Loopback Error	19
Kuvio 22. Loopback address added.....	20
Kuvio 23. WSUS IP:n lisääminen	20
Kuvio 24. Baseline vs Effective state.....	22
Kuvio 25. Policy Analyzer ja eriävät arvot mitä tulimme muuttamaan manuaalisesti.....	23
Kuvio 26. Group Policy Management, Default Domain Policy.	23
Kuvio 27. Salasana policy lähtötilanne.....	24
Kuvio 28. Manuaalisesti muutetut salasana policyt	24
Kuvio 29. gpupdate	25
Kuvio 30. Baseline vs Effective	25
Kuvio 31. BaselineLocalInstall skripti.	26
Kuvio 32. Skriptin vaatimukset.....	27
Kuvio 33. Ajettu skripti.....	27
Kuvio 34. Skriptin jälkeen Policy Analyzer.	28
Kuvio 35. gpupdate, ja virhe.	28
Kuvio 36. Policy Analyzer Eroavaisuudet päivittämisen jälkeen.....	29

1 Johdanto

Tämä labra on osa kurssia Koventaminen TTC6050-3001. Kurssilla opiskelijoiden on tarkoitus opetella koventamaan VLE (Virtual Learning Environment) ympäristössä olevia virtuaalisia koneita. Kurssissa toimitaan käytännön läheisesti, missä kaikki harjoitustyöt ovat labroja, ja niissä saa keilla työelämässä käytettyjä kovennustekniikoita.

1.1 Tehtävänanto

Ensimmäisen labran toimeksiantona oli Active Directory (AD) koventaminen. Ryhmä sai valita itse koventamisohjeet, mutta niillä piti saavuttaa Windows Server, Windows AD ja Group Policy kovennus. Windows AD kovennusten todentamiseen piti myös käyttää MS BPA:ta (Microsoft Best Practices Analyzer). Kovennuskohteena toimi VLE-ympäristön Servers-netin DC01 virtuaalinen kone, mutta muitakin Servers-netin virtuaalisia koneita käytettiin hyväksi labran aikana, esimerkiksi koventamiseen tarvittuun varmuuskopiointiin.

1.2 Labran teoria ja termit

Labran aikana käytämme termejä, jotka eivät ole niin tunnettuja kaikille. Yritämme selittää kaikki termit mitä käytämme tässä raportissa parhaamme mukaan tässä sektiossa. Selitämme myös, miten käytimme eri teknologioita siinä vaiheessa, kun niistä tulee aiheellisia.

1.2.1 Koventaminen

Koventaminen on tähän labraan, ja oikeastaan koko kurssille, keskeinen konsepti. Koventamisella halutaan tehdä verkosta turvallinen. Käytännössä koventaminen (hardening) tarkoittaa sitä, että kyberhyökkäyksien hyökkäyspinta-ala on mahdollisimman pieni. Koventamiseen on monia erilaisia keinoja. Yleisimpiä ovat turhien ohjelmien, tietokantojen yms. poistamien sekä tietysti ohjelmistojen pitäminen ajan tasalla eli päivittäminen. Lisäksi verkon eri käyttäjien rooleja verkossa kannattaa pitää sellaisina, että niillä onnistuu vain välttämättömimmät toimenpiteet. Sama koskee myös verkkoon kytkettyjä laitteita. Niille kannattaa varata vain yksi käyttötarkoitus, jos vain mahdollista. Myös palomuuuri ja virustorjunta ovat tärkeitä (What is Systems Hardening? N.d.).

1.2.2 VLE

VLE, eli Virtual Learning Environment, on JAMK:in sisäisessä verkossa eli labranetissä toimiva oppimisympäristö. Kyberpuolustus moduuliin liittyen, mihin koventamiskurssi sijoittuu, on tehty jokaiselle ryhmälle oma ympäristö, missä he voivat kokeilla jokaiseen kurssiin liittyviä tekniikoita ja teorioita. Jokaisessa labrassa ei käytetä kaikkia VLE:n osia, vaan vain relevantteja osia. Esimerkiksi jotkut labrat keskittyvät palomuurin konfigurointiin, ja jotkut keskittyvät tietyn virtuaalisen koneen koventamiseen (Labranet services for JAMK students. N.d.).

1.2.3 Windows Active Directory

Windows Active Directory on domainin käyttäjätietokanta sekä hakemistopalvelu. Domain tarkoittaa verkkoa, jota hallitaan keskitetysti. Active Directoryn avulla tämän verkon hallinta on helpompaa, koska voidaan yhdellä komennolla/muutoksella vaikuttaa koko verkon käyttäjiin ja laitteisiin. Admin-rooleja domainissa voi olla myöskin eri tasoja, esimerkiksi domain admin sekä local admin. Domain adminilla on oikeudet tehdä muutoksia koko verkkoon, kun taas local adminin oikeudet koskevat vain tiettyä tietokonetta (Active Directory Domain Services Overview. 2022).

Domainin käyttäjätilien hallinta on tärkeää siksi, koska hyökkääjät voivat yrittää esimerkiksi yksinkertaisia salasanoja tai vanhaa poistamatonta käyttäjätiliä kirjautuakseen domainiin. Siksi käyttäjätilit täytyisi pitää ajan tasalla sekä asettaa salasanoille tietty vaatimus, koska liian yksinkertainen salasana on helppo arvata (esim. admin123). Pääkäyttäjän oikeuksia ei saisi myöskään jaella ylimääräisille henkilöille (Active Directory Domain Services Overview. 2022).

1.2.4 Active Directory Domain Services

Domain Services on käyttäjärooli Active Directoryssa, jolla järjestelmänvalvojat (adminit) voivat hallita ja tallentaa verkon (domainin) tietoja. Domain Servicessa hallitaan verkossa olevia käyttäjätietoja, palveluja sekä laitteita. Active Directory Domain Services on Active Directoryn tärkeimpiä osia. Domain Servicen tietojen perusteella verkkoon kirjautujat todennetaan ja heille myönnetään pääsy verkkoon (Active Directory Domain Services Overview. 2022.).

1.2.5 Windows Best Practises Analyzer

Windows Best Practices Analyzer on ohjelma, jolla tarkistetaan, onko Active Directoryn koventaminen tehty standardien mukaisesti. Best Practices Analyzer sisältää ammattilaisten kokoamat konfiguraatiot ja se vertaa AD:n asetuksia niihin (Run Best Practices Analyzer Scans and Manage Scan Results. 2021).

1.2.6 Domain Controller

Domain Controller (DC) on serveri, mikä vastaa autentikointipyyntöihin, ja varmistaa että sisäisessä verkossa olevilla käyttäjillä on oikeat käyttöluvat niille koneille mitä ne käyttävät. Esimerkiksi kun käyttäjät kirjautuvat domainiin, Domain Controller tarkistaa kaikki käyttäjän kredentiaalit, ja päättää saako tämä käyttäjä pääsyn domainin sisälle (Buckbee M. 2020).

1.2.7 DNS

DNS, tai Domain Name System (suomeksi nimipalvelin) on internetin järjestelmä, joka muuttaa domain-osoitteet (esim. jamk.fi) IP-osoitteiksi. DNS:n vuoksi ei tarvitse muistaa nettisivujen monimutkaisia IP-osoitteita vaan voidaan käyttää domainia, joka on helpompi muistaa. Jokaisella internettiin kytketyllä laitteella on oma yksilöllinen IP-osoite. DNS antaa nämä osoitteet (What Is DNS? N.d.)

Kun henkilö kirjoittaa selaimen osoitepalkkiin osoitteen, DNS selvittää tämän kyseisen osoitteen IP-osoitteen sekä nimipalvelimen ja välittää tiedon henkilön selaimelle. Näin selain pystyy lataamaan sivun tietokoneelle (What Is DNS? N.d.).

1.2.8 Varmuuskopiointi

Varmuuskopioiminen on tärkeä ominaisuus serveriympäristössä. Se suojaa järjestelmän tietoja ja muutoksia ja jos esimerkiksi koneesta katoaa tärkeitä tiedostoja tai koneella tehdään jokin muutos, joka rikkoo asioita, voidaan varmuuskopiointilla hakea vanhempi varmuuskopiointi takaisin toiselta laitteelta tai esimerkiksi pilvipalvelusta, jolla pystyy palauttamaan aikaisempaan tilaan. Varmuuskopiointia tehdessä täytyy varmistaa, että levyllä on tarpeeksi tilaa (What is Backup? N.d.).

2 Virtuaalisen Koneen Koventaminen

2.1 Lähtötilanne

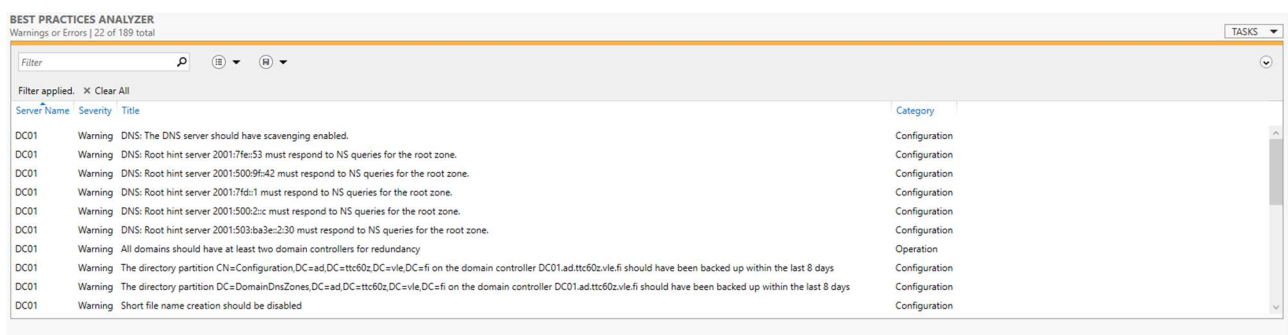
Aloitimme labran tutkimalla DC01 Server Manageria kokonaisuudessaan. Serverin pystyi jakamaan AD Domain Serviceen (DS), Domain Name Systemiin (DNS) sekä File and Storage Serviceen. Näillä kaikilla oli omat sektiot. Tämän lisäksi labrassa oli myös Group Policy puoli, jota piti vielä koventaa erillisen Analyzerin avulla.

2.2 Väärän toimeksiannon tekeminen

Tämän labran, ja oikeastaan kurssin alussa, olimme hyvin eksyksissä, ja emme tienneet oikein mistä aloittaa. Labran ohjeissa sanottiin, että meidän pitäisi aloittaa valitsemalla mieluinen kovenusohje, mutta me aloimme korjaamaan manuaalisesti warningeja ja errorereita mitä Best Practices Analyzer (BPA) tuotti.

2.3 Best Practices Analyzer

BPA:ssa oli alussa monia warningeja ja errorereita. Näitä oli esimerkiksi toisen domain controllerin ja varmuuskopioinnin puuttuminen. Vaikka koventaminen pohjautui meillä CIS Benchmarkkiin, niin kuten jo mainitsimme, suurimmaksi osaksi seurasimme tässä Analyzereita ja etsimme ohjeita Microsoftin virallisilta sivuilta ja erilaisista ohjevideoista ja foorumeista tässä osassa labraa. Esimerkki miltä BPA näytti, löytyy alta olevasta kuvasta, missä lukee kaikkien servereiden warningeja ja errorereita (ks. kuvio 1).

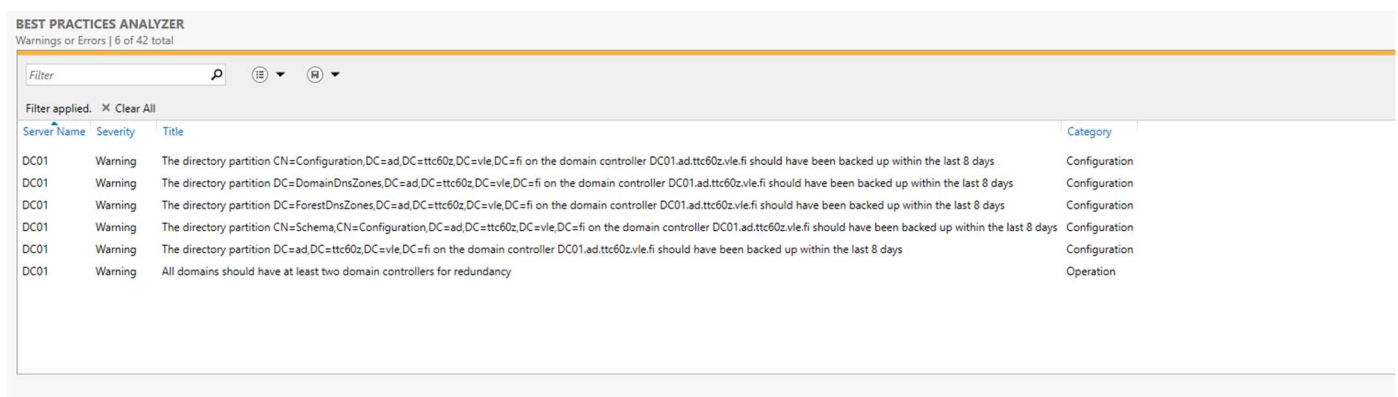


Kuvio 1. Esimerkki BPA:sta.

Korjasimme monenlaisia pieniä errorereita ja warningeja mitä BPA tuotti, mutta raportissa kerromme niistä mihin meillä meni eniten aikaa, ja mitkä korjaamalla korjasimme myös suurimman osan muista warningeista ja errorereista.

2.4 AD DS:än koventaminen, ja toisen DC:n lisääminen

Aloitimme tutkimaan ja koventamaan AD DS puolta ensimmäisenä. Analyzerista näkyi varoitus **`All domains should have at least two domain controllers for redundancy`**. Tämän takia aloimme työstämään toisen domain controllerin lisäämistä domainiin (ks. kuvio 2).



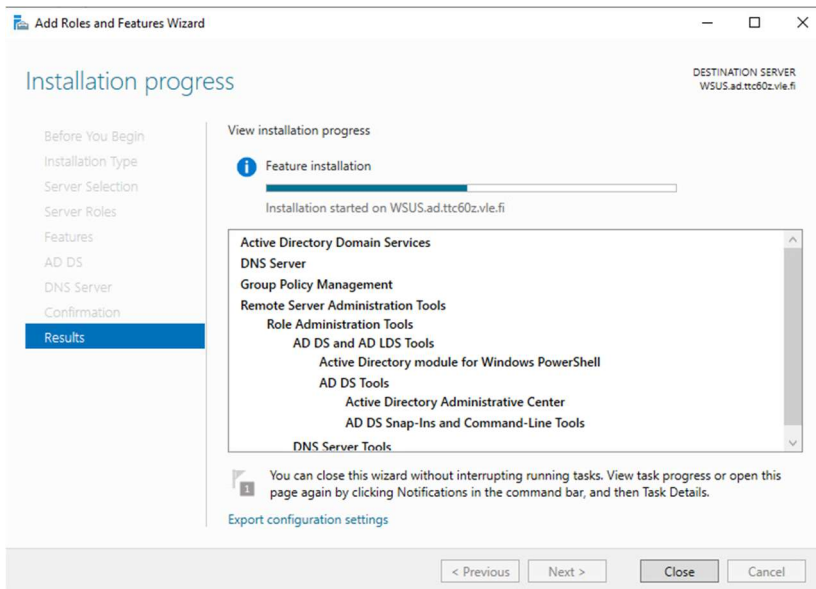
Server Name	Severity	Title	Category
DC01	Warning	The directory partition CN=Configuration,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition DC=DomainDnsZones,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition DC=ForestDnsZones,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition CN=Schema,CN=Configuration,DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	The directory partition DC=ad,DC=ttc60z,DC=vle,DC=fi on the domain controller DC01.ad.ttc60z.vle.fi should have been backed up within the last 8 days	Configuration
DC01	Warning	All domains should have at least two domain controllers for redundancy	Operation

Kuvio 2. BPA, AD DS.

Ylimääräisen DC:n lisääminen on tärkeää, koska jos ensisijaisen DC:n lopettaa toimintansa, koko serveri ei kaadu tähän. Sen sijasta toinen DC pystyy jatkamaan toimintaa häiriintymättä ja käyttäjät voivat esimerkiksi jatkaa verkkopalvelujen käyttämistä (ittaster. 2021).

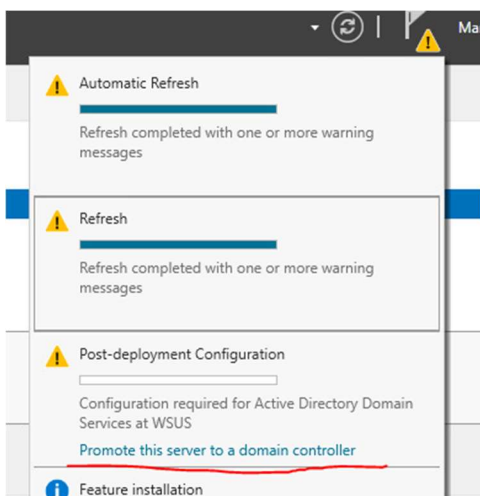
Toisen DC:n lisäämisessä meni meidän ryhmällämme hetki, sillä aluksi meidän piti perehtyä tarkemmin labraympäristöön ja eri DC vaihtoehtoihin. Päädyimme käyttämään Servers-netissä olevaa WSUS-konetta toisena domain controllerina (ks. Liite 1.). WSUS-koneelle piti asentaa Server Managerin kautta monia eri servicejä, jotta toisen DC:n lisääminen onnistuisi tähän koneelle. Käytimme asennusapuna ohjevideota YouTubesta, jota seuraamalla pystyy lisätä DC:n, ja mikä kertoo tarkemmin mitä asetuksia tarvitsi konfiguroida DC:n asennukseen (MSFT WebCast. 2019).

Oikealta yläkulmasta Server Managerista löytyy Toolsien alta **Add Roles and Features**, josta valitaan Active Directory Domain Services asennettavaksi. Tämän lisäksi asennamme myös DNS Serverin ja Group Policy Managementin toiseen DC:hen, jotta pystyisimme käyttämään niitä myöhemmin tarvittaessa (ks. kuvio 3).



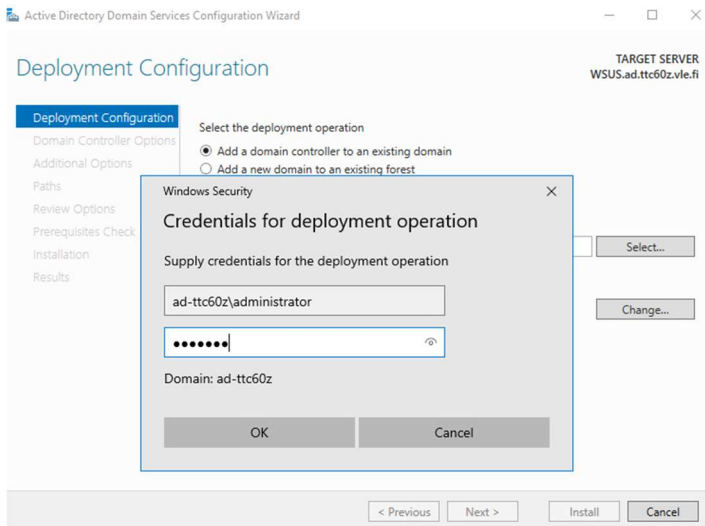
Kuvio 3. Installing features to second controller.

Kun Active Directory Domain Services asennus ja konfigurointi toiselle DC:lle on valmis, domain kontrolleriksi ylentäminen onnistui ilmoituksien kautta (ks. kuvio 4).



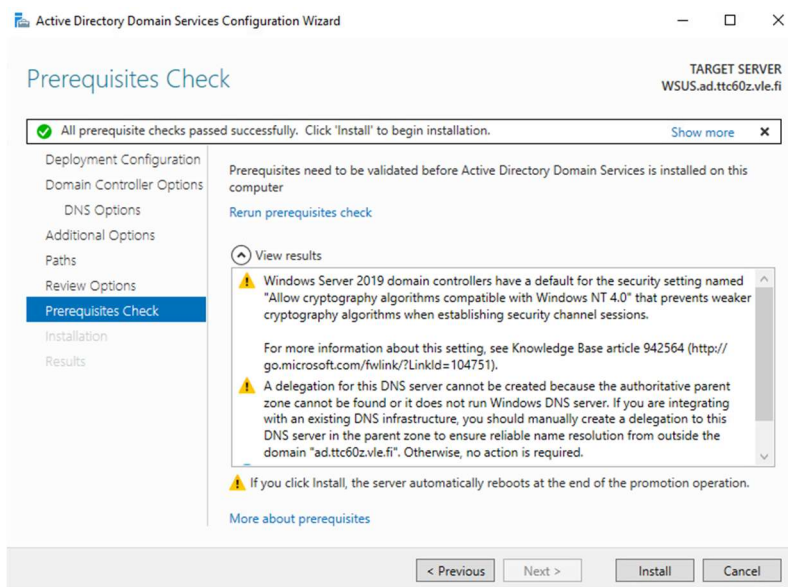
Kuvio 4. Promoting to domain controller.

Ennen kuin WSUS-koneen pystyi ylentämään DC:ksi, tämä tarvitsi konfigurointia ja varmistamista, että meillä oli oikeudet ylentää WSUS-kone toiseksi DC:ksi. Kuvasta näkyy, miten meidän piti laittaa kredentiaalit ennen ylentämistä (ks. kuvio 5).



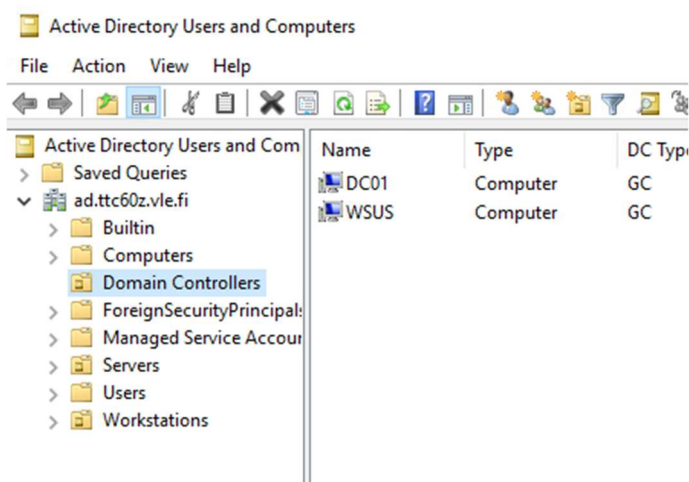
Kuvio 5. Credentials for the domain controller.

Lopussa tehtiin vielä viimeinen '**Prerequisites Check**', että toisen DC:n asennus ja konfigurointi onnistui WSUS-koneelle (ks. kuvio 6).



Kuvio 6. Checks passed.

Kun asennus ja konfigurointi olivat valmiita, WSUS tuli näkyviin Active Directoryn Domain Controllers kansiossa, mikä tarkoittaa, että se on nyt meidän ympäristössämme käytössä toisena DC:nä ja Analyzerin antama warning on myös kadonnut. Analyzerista unohtui ottaa kuva tässä vaiheessa, mutta myöhemmässä vaiheessa kun varmuuskopiointi on lisätty, Analyzer on tyhjä (ks. kuvio 7.).

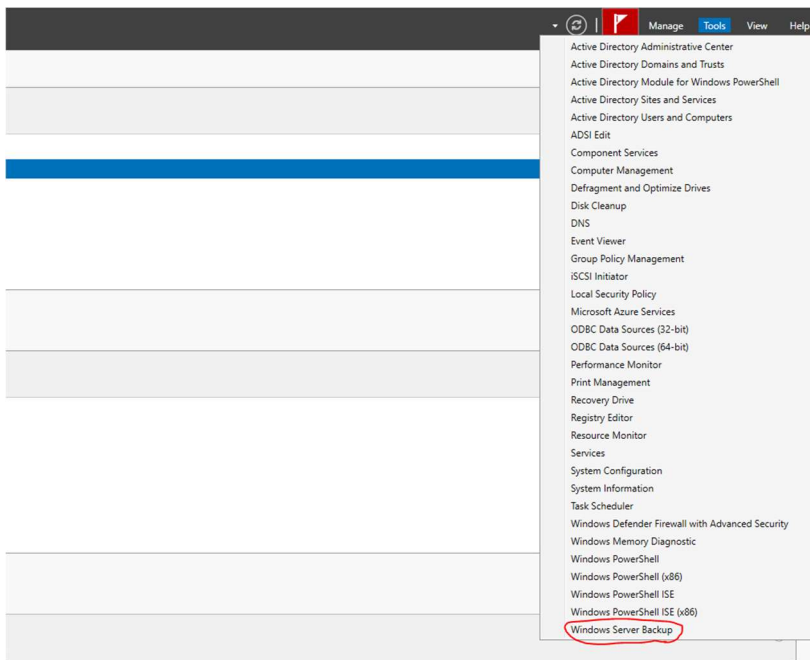


Kuvio 7. Second Domain Controller.

2.5 File and Storage Services koventaminen, Varmuuskopioinnin luominen

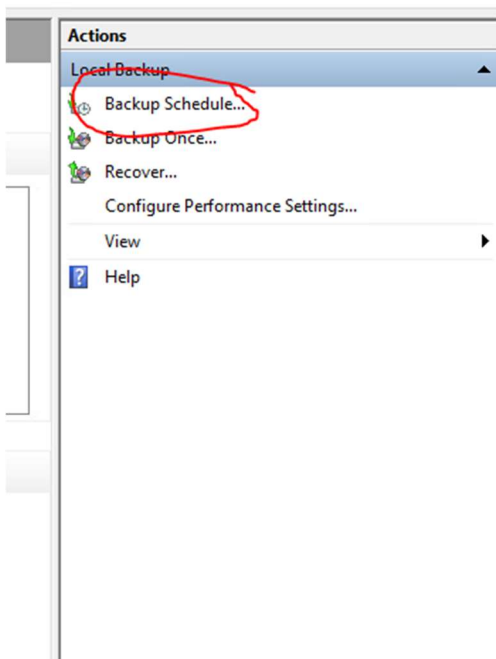
Aloimme korjaamaan seuraavaksi warningeja ja erroreita mitä BPA File And Storage Services tuotti. Suurin osa näistä oli varmuuskopioimisen puute, ja sen konfigurointi standardien mukaiseksi, joten aloimme korjaamaan tätä BPA:n ohjeiden mukaan.

Tässä labrassa käytimme WSUS-koneen varmuuskopioinnin kohteena ympäristöön kuuluvaa ja samassa Zonessa olevaa SRV01-laitetta, joka toimii tiedostopalvelimena tässä labrassa, ja varmaan tulevaisuuden labroissakin. Yleisesti varmuuskopiointi kannattaa tehdä johonkin mikä ei ole näin lähellä varmuuskopioitavaa, koska joissain tapauksissa monet verkossa lähellä olevat koneet voivat sammua ja menettää tärkeitä tiedostoja samaan aikaan. Backup-servicenä käytimme Windowsin omaa palvelua, joka löytyy kätevästi Server Managerin Tools-palkista (ks. kuvio 8).



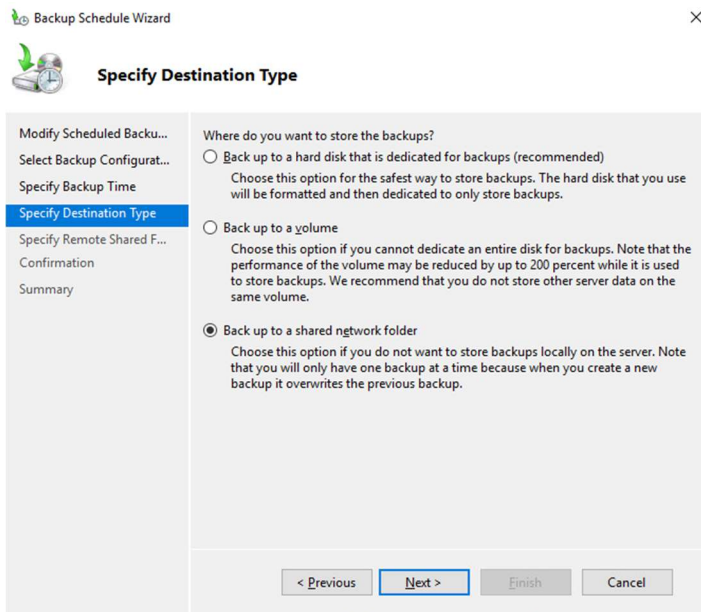
Kuvio 8. Windows Server Backup.

Windowsin oma backup-service on suhteellisen helppokäyttöinen ja selkeä. Windows Server Backup näkymän oikealla näkyy ”actions”-osa, josta valitaan Backup Schedule (ks. kuvio 9).



Kuvio 9. Backup Schedule.

Varmuuskopiointi on hyvä aikatauluttaa, jotta se toimii automaattisesti ja säännöllisesti. Asetimme Full Server varmuuskopioimisen aamukuudeksi joka päivälle. Tämän jälkeen valitsimme Destination Typen, joka oli tässä tapauksessa Shared Network Folder eli jaettu verkkokansio. Verkkokansiona toimii hyvin SRV01, sillä se on samassa ympäristössä, joten yhdistäminen siihen sujui ongelmitta DC01:stä (ks. kuvio 10).



Kuvio 10. Shared Network Folder.

Tämän jälkeen valitsimme vielä kohteen varmuuskopiolle. Varmuuskopioinnille loimme oman kansion, jonka jälkeen sijainti määriteltiin kuvion mukaisesti (ks. kuvio 11).

Backup Schedule Wizard

Specify Remote Shared Folder

Modify Scheduled Backu...
Select Backup Configurat...
Specify Backup Time
Specify Destination Type
Specify Remote Shared F...
Confirmation
Summary

Location:

Example: \\MyFileServer\SharedFolderName
This wizard creates a folder based on the name of the server being backed up, for example MyServer-BackupFiles.

Access Control

☐ Do not inherit
This option makes the backup accessible only for the user whose credentials are provided in the next step.

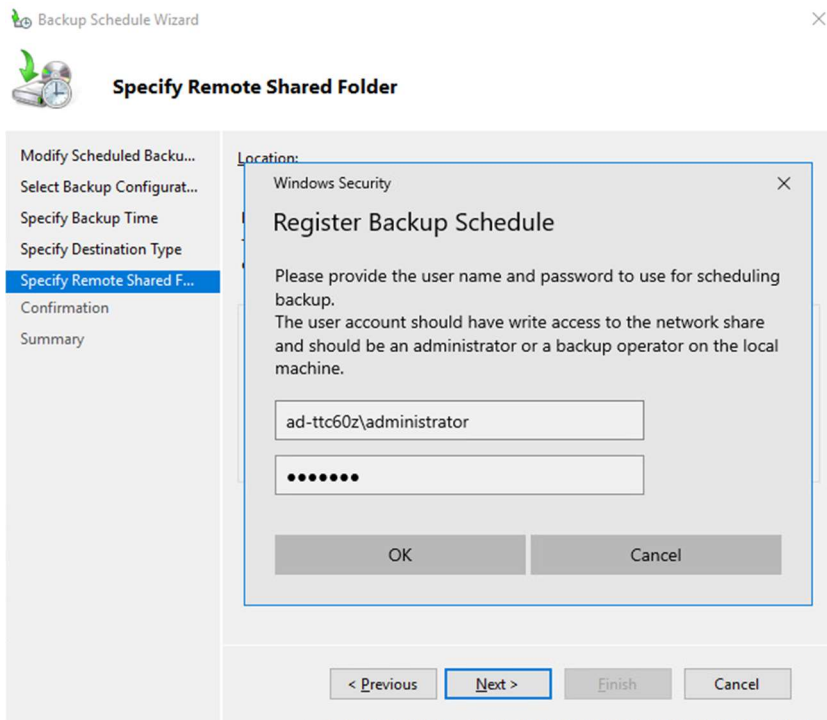
☒ Inherit
This option makes the backup accessible to everybody who has access to the specified remote shared folder.

The backed up data cannot be securely protected for this destination.
[More Information](#)

< Previous **Next >** Finish Cancel

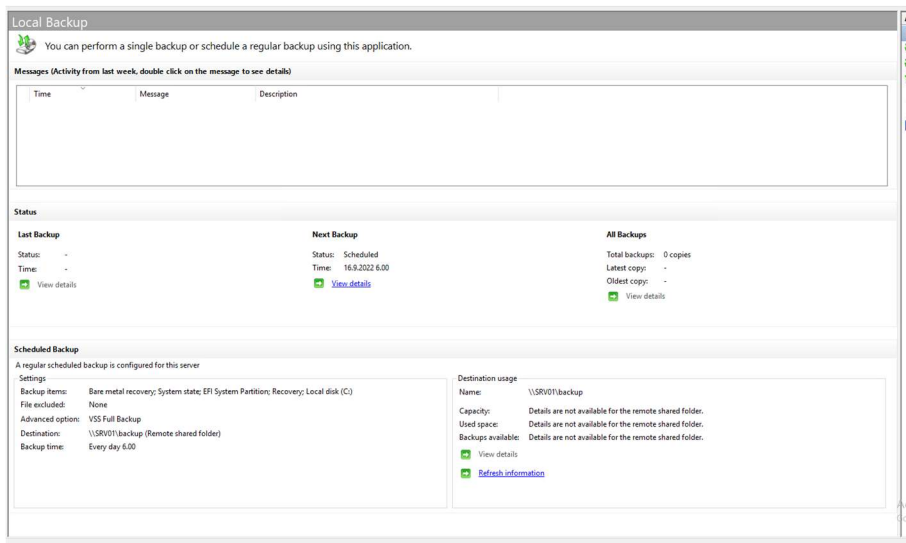
Kuvio 11. Backup location.

Kun sijainti on vahvistettu, viimeisenä vaiheena vahvistetaan kredentiaalit, kuten AD DS toisen DC:n konfiguroinnissa, jonka jälkeen varmuuskopiointi on asennettu toimimaan DC01-koneelta SRV01-koneelle (ks. kuvio 12).

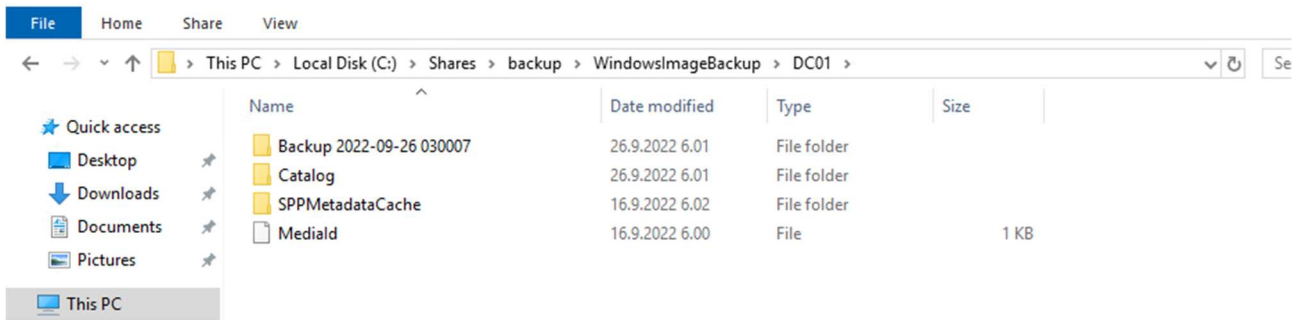


Kuvio 12. Credentials for Backup.

Nyt voimme vahvistaa varmuuskopioinnin toimivuuden katsomalla Windowsin varmuuskopiointipalvelua (ks. kuvio 13) sekä menemällä myös SRV01-laitteelle, jossa näkyy onnistunut varmuuskopio, ja myös oikea kellonaika milloin varmuuskopiointi tapahtui (ks. kuvio 14).

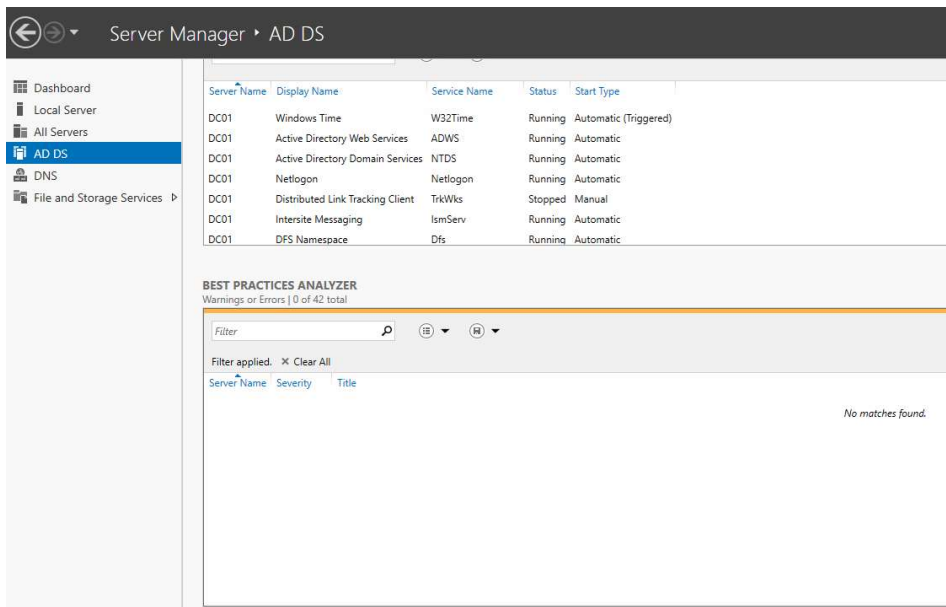


Kuvio 13. Scheduled Backup.



Kuvio 14. Backup in SRV01.

Tämän lisäksi myös AD DS:än BPA Analyzerin viimeiset backup warningit ovat kadonneet (ks. kuvio 15).



Kuvio 15. AD DS Analyzer empty

2.6 DNS koventaminen

Seuraavaksi aloimme koventamaan DC01-koneen DNS (Domain Name System) palvelua katsomalla BPA listan warningeja ja yhtä isompaa erroria. DC01-koneella oli jo valmiina asennettuna DNS, mutta tämän konfigurointia piti jatkaa. Aluksi aloimme korjaamaan, ”**The DNS server should have scavenging enabled**” varoitusta (ks. kuvio 16).

BEST PRACTICES ANALYZER
Warnings or Errors | 14 of 48 total

Filter

Filter applied. X Clear All

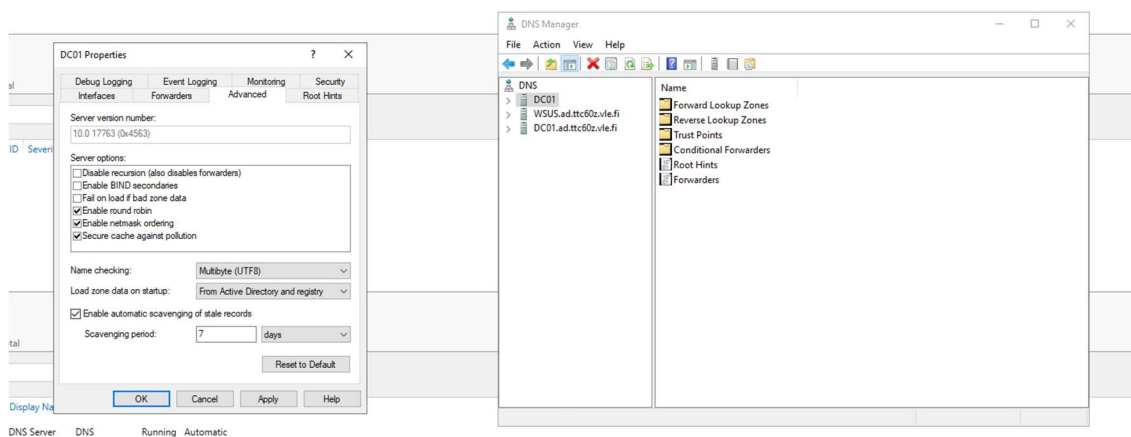
Server Name	Severity	Title	Category
DC01	Warning	DNS: The DNS server should have scavenging enabled.	Configuration
DC01	Warning	DNS: Root hint server 2001:7fe:53 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:9f:42 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:7fd:1 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:2:c must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:503:ba3e:2:30 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:2ef must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:2:d must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:84:b must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:dc3:35 must respond to NS queries for the root zone.	Configuration

Kuvio 16. BPA DNS.

2.6.1 Scavenging

Varoituksessa puhutaan termistä `scavenging` mutta mitä se on? Scavenging tarkoittaa käytännössä sitä, että kaikki vanhentuneet DNS-resurssit poistetaan, ettei ympäristöt havaitse duplikaattilaitteita samasta laitteesta useiden DNS-merkintöjen takia (Configure DNS scavenging on the Windows server. N.d.).

Scavengingin käyttöönotto oli helppoa. Tools-palkista Server Managerissa siirrytään DNS Manageriin, josta DC01:stä klikkaamalla mennään Propertiesiin ja sieltä löytyy Scavengingin käyttöönotto (ks. kuvio 17) (Configure DNS scavenging on the Windows server. N.d.).



Kuvio 17. Scavenging enabled.

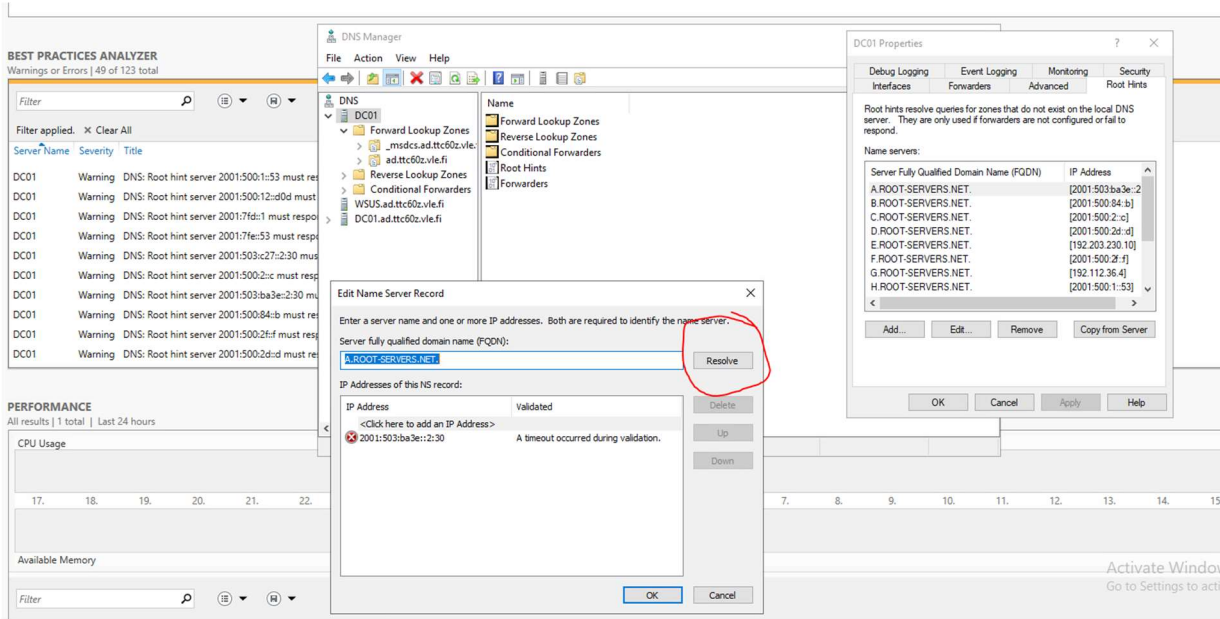
2.6.2 Root Hint Warning

Kun olimme saaneet Scavenging varoituksen korjattua, siirryimme tutkimaan useita root hint warningeja BPA:sta. Näitä varoituksia oli useita kymmeniä, mihin kaikkiin löytyi samankaltainen ratkaisu (ks. kuvio 18).

Server Name	Severity	Title	Category
DC01	Warning	DNS: Root hint server 2001:500:1::53 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:12::d0d must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:7fd::1 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:7fe::53 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:503:c27::2:30 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:2::c must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:503:ba3e::2:30 must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:84::b must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:2f::f must respond to NS queries for the root zone.	Configuration
DC01	Warning	DNS: Root hint server 2001:500:2d::d must respond to NS queries for the root zone.	Configuration

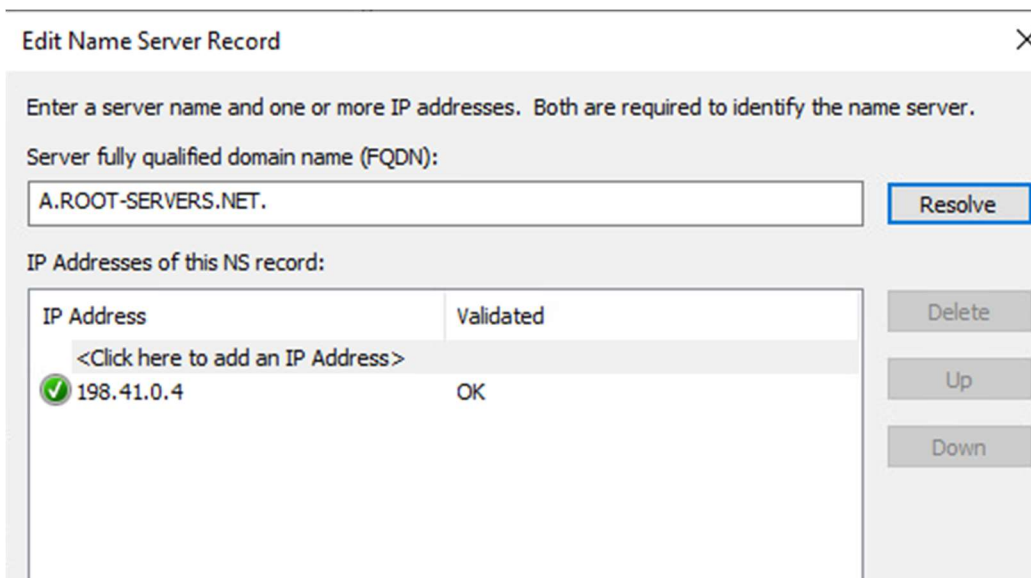
Kuvio 18. Root hint warnings.

Nämä varoitukset tarkoittavat yksinkertaisuudessaan sitä, että IP:t eivät ole oikeassa IPv4 muodossa mihin BPA:n security baseline vaatii niitä. Nämä varoitukset pystyimme korjaamaan DNS Managerista Server Managerissa. DNS managerissa mentiin uudestaan DC01:n propertiesiin, josta root hints välilehdeltä käytiin jokaisen oletus DNS:än läpi editoimalla ja painamalla resolve (ks kuvio 19) (Pervais U. 2022).



Kuvio 19. Resolving Root Hint Warnings.

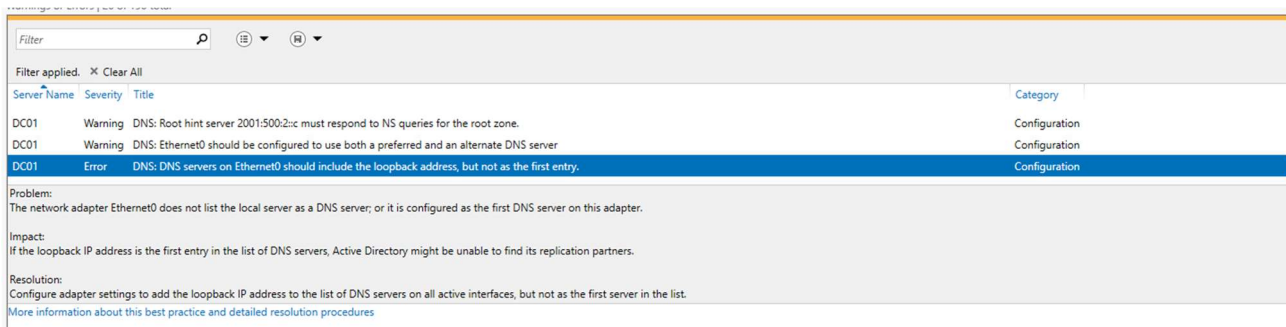
Kun nämä root hint varoitukset oli korjattu, BPA:ssa näkyi silti muutama varoitus samanlaisella teemalla, emmekä osanneet korjata näitä sillä hetkellä. Voi olla, että BPA näytti väärin, sillä resolasimme kaikki IP:t mitä löysimme DNS managerista, joista esimerkkinä ensimmäinen IP minkä korjasimme (ks. kuvio 20).



Kuvio 20. Resolved IP

2.6.3 Loopback Address Error

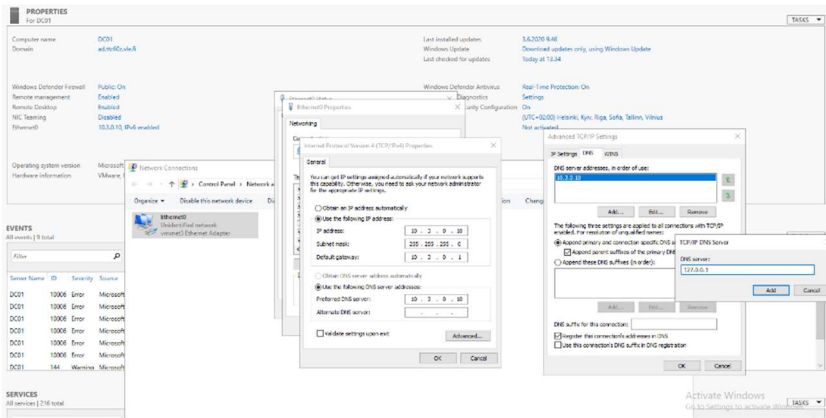
Viimeisenä DNS muutoksena aloimme ratkaisemaan BPA:sta olevaa loopback address erroria (ks kuvio 21).



Kuvio 21. Loopback Error

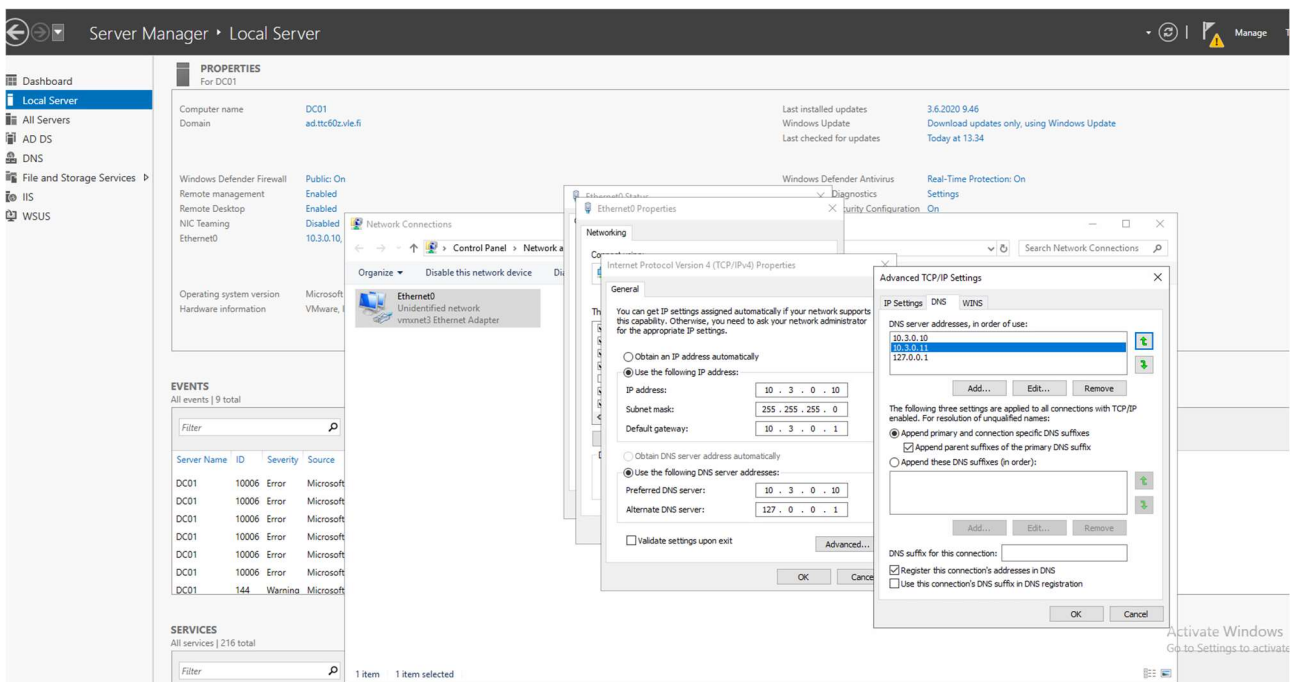
Me lisäsimme DNS asetuksiin loopback osoitteen, joka lähettää signaalin takaisin laitteisiin. Tätä osoitetta käytetään erilaisissa testeissä, esimerkiksi sen testaamiseen onko kone vielä verkossa ja päällä. Loopback ei saa myöskään olla ensimmäinen IP-listassa, joten se menee DC01:sen IP:n alapuolelle (DNS: DNS servers on should include the loopback address, but not as the first entry. 2014).

Tässä verkossa loopback osoite on 127.0.0.1 ja se lisätään painamalla Server Managerin Local Server osiossa olevaa IP:tä, joka on tässä tapauksessa 10.3.0.10. Tämän jälkeen tupla klikataan **Ethernet0**, josta mennään **Properties**, tupla klikataan **Internet Protocol Version 4 (TCP/IPv4)** ja sieltä löytyy kuvassa näkyvät ikkunat (ks. kuvio 22).



Kuvio 22. Loopback address added

Jostain syystä BPA analyzerista error ei poistunut, vaikka asetukset ovat oikein. Kyselimme myös opettajalta näistä asetuksista, ja hän varmisti, miten ne olivat oikein konfiguroitu. Yhdessä foorumissa sanottiin, että analyzer ei poista erroria jostain syystä, joten sen errorin voi sivuuttaa (DNS servers on Ethernet should include the loopback address, but not as the first entry. 2012). Lisäsimme loopback osoitteen myös toiselle domain controllerille, WSUS-koneelle, ja lisäsimme laitteiden IP:t myös toisiinsa, vaikka WSUS:än koventaminen ei ollut edellytyksenä tässä labrassa (ks. kuvio 23).



Kuvio 23. WSUS IP:n lisääminen

3 Microsoft Security Compliance Toolkit.

Kun olimme saaneet tehtyä manuaalisesti melkein kaikki warningit ja errorit mitä BPA tuotti, tajusimme että tämä ei ehkä ole paras tapa tehdä koventamista. Kyselimme opettajalta, että mitä tässä labrassa oikeasti pitäisi tehdä, ja hän vastasi osoittamalla Microsoftin Security Compliance Toolkittiä kohti.

Asensimme DC01-koneelle Microsoft Security Compliance Toolkit 1.0:n. Toolkittiin sisältyy Policy Analyzer niminen työkalu, jota voi käyttää vertaamaan esim. Microsoftin laatimaa baseline asetuksia palvelimen tällä hetkellä käytössä oleviin asetuksiin. Toolkitissä tuli myös mukana Local Group Policy Object (LGPO) työkalu, jolla voi automatisoida policyjen muuttamisen. Näiden lisäksi Toolkitin mukana tuli myös Microsoftin valmiit security baselinet Windows Server 2019:lle, mikä oli DC01-koneen versio. Siinä on valmiiksi Microsoftin suosittelemat turvalliset policyt (Microsoft Security Compliance Toolkit 1.0 - How to use. 2022).

Policy Analyzer ei ole kaikista selkein, joten selitämme tärkeät osat. Policy Analyzerin oikealla puolella näkyy Baseline, ja Effective State. Baseline on Policy Analyzeriin ladattu Security Baseline, eli mikä sen arvon pitäisi olla. Effective State on mikä on tämänhetkinen tilanne DC01-koneella. Jos

Baseline ja Effective State ei ole samat, niin se näkyy Policy Analyzerissa keltaisena. Tämän mukainen koventaminen, manuaalinen tai automaattinen, tapahtuu siten, että kummatkin Baseline ja Effective State ovat sama arvo tai muuttuja lopputilanteessa (ks. kuvio 24).

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success
Audit Policy	Account Management	Computer Account Management	Success	Success
Audit Policy	Account Management	Other Account Management Events	Success	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success and Fail...	Success
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	DS Access	Directory Service Access	Success and Fail...	Success
Audit Policy	DS Access	Directory Service Changes	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Special Logon	Success	Success
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success	Success
Audit Policy	Policy Change	Authentication Policy Change	Success	Success
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Changes	Success	No Auditing

Policy Path:
 Advanced Audit Policy Configuration
 System Audit Policies/Object Access
 Detailed File Share

Detailed File Share
 This policy setting allows you to audit attempts to access files and folders on a shared folder. The Detailed File Share setting logs an event every time a file or folder is accessed, whereas the File Share setting only records one event for any connection established between a client and file share. Detailed File Share audit events include detailed information about the permissions or other criteria used to grant or deny access.

Kuvio 24. Baseline vs Effective state.

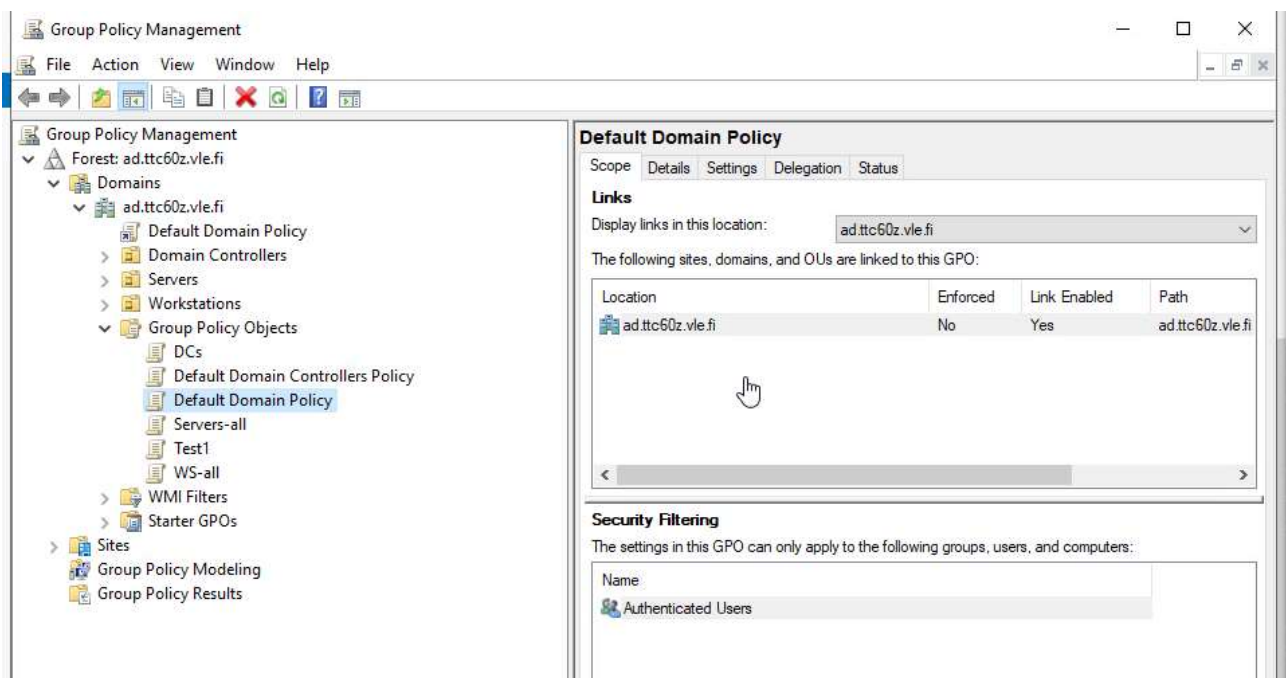
3.1 Manuaalinen Group Policy konfiguraatio

Työkalujen avulla, mitkä tulevat Toolkitin mukana, pystyisi helposti tekemään kaiken automaattisesti. Halusimme kuitenkin kokeilla ja demonstroida raportissa, miten koventamisprosessi toimisi manuaalisesti. Sitä varten valitsimme muutaman kohdan joiden avulla pystyisimme näyttämään, miten aikaa vievää ja vaikeaa tämä on tehdä manuaalisesti. Valitsimme manuaalisen konfiguroinnin kohteeksi MaximumPasswordAge ja MinimumPasswordLength (ks. kuvio 25).

EnableAdminAccount	0	1
EnableGuestAccount	0	0
LockoutBadCount	10	0
LockoutDuration	15	
LSAAnonymousNameLookup	0	0
MaximumPasswordAge	60	42
MinimumPasswordAge	1	1
MinimumPasswordLength	14	7
PasswordComplexity	1	1
PasswordHistorySize	24	24
ResetLockoutCount	15	

Kuvio 25. Policy Analyzer ja eriävät arvot mitä tulimme muuttamaan manuaalisesti.

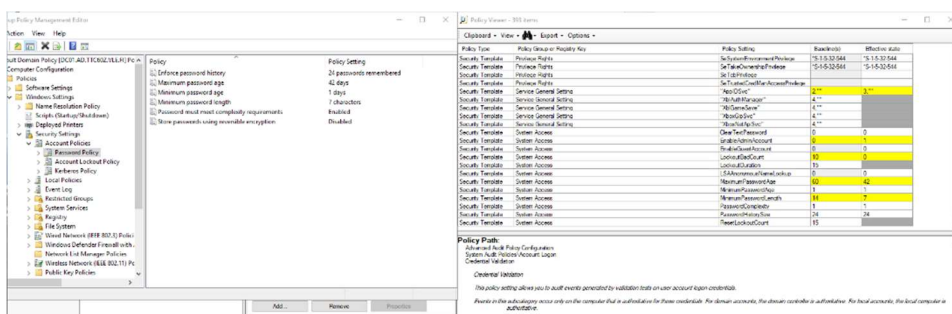
Oikeiden salasana-asetusten löytäminen oli todella vaikeaa. Yritimme etsiä monesta paikasta, esimerkiksi Local Security Policy:sta Server Managerin Toolseista. Vihdoin aloimme tutkimaan Group Policy Managementtia Server Manager Toolseista, mutta sieltäkin aluksi täysin vääristä paikoista. Lopulta oikeat salasana-asetukset löytyivät Group Policy Managementista Default Domain Policyn alta (ks. kuvio 26).



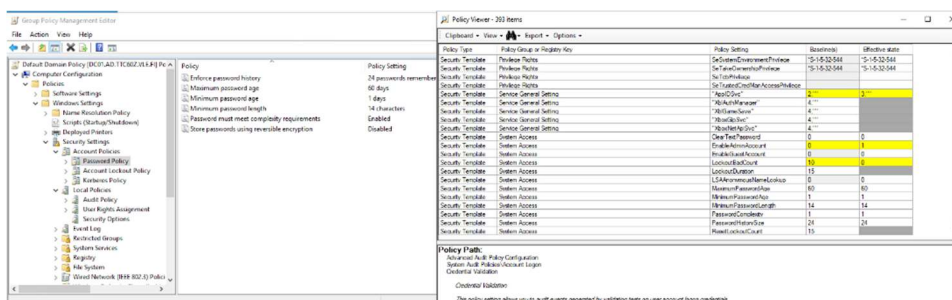
Kuvio 26. Group Policy Management, Default Domain Policy.

Jotta kaikkia Default Domain Policyn arvoja pääsee editoimaan, pitää ensiksi rightklikata halua-
maansa Group Policy Objektia, tässä tapauksessa Default Domain Policya, ja valita Edit.

Lähtötilanteessa meillä oli MaximumPasswordAge (eli salasanan vanhentumisaika) 42 päivää, kun
taas Microsoftin baseline asetuksissa suositellaan 60 päivää. Meidän alkuperäisillä asetuksillamme
oli jo jonkun verran kovennettu asetus, mutta päätimme seurata Microsoftin valmista baselinea ja
vaihtaa se 60 päivään. Vaihdoimme myös salasanan minimipituuden 7 merkistä 14 merkkiin (ks.
Kuvio 27 ja 28).



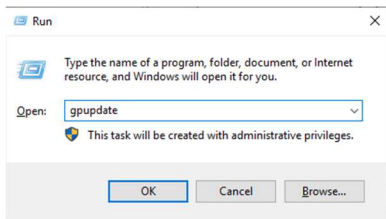
Kuvio 27. Salasana policy lähtötilanne.



Kuvio 28. Manuaalisesti muutetut salasana policyt

Jokaisen muutetun policyn jälkeen piti ajaa gpupdate (Group Policy update). Gpupdate komento
päivittää group policyt ajan tasalle, jotta Windowsin systeemeissä olevissa Policyissa ei olisi ristirii-
taa konfiguroitujen policyjen kanssa. Gpupdate komentoa käytetään avaamalla ”Run” ikkuna (Win

+ R), ja kirjoittamalla ikkunaan gpupdate. Gpupdate ei toimi, jos sitä ei aja järjestyksenvalvojana (ks. kuvio 29).



Kuvio 29. gpupdate

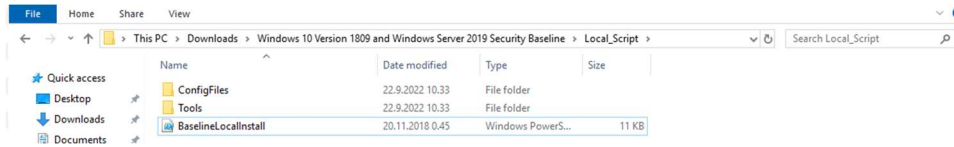
3.2 Automaattinen Group Policyjen konfiguraatio

Sen jälkeen, kun saimme kokeiltua manuaalisesti, miten näiden arvojen konfiguraatio toimii, koetimme automatisoida tämän prosessin. Eroavaisuuksia Microsoftin baselinen ja meidän laitteemme policyillä oli muutenkin meillä todella paljon, jossa olisi manuaalisesti kestänyt monia päiviä (ks kuvio. 30).

Policy Viewer - 393 items				
Clipboard View Export Options				
Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success and Fail...
Audit Policy	Account Management	Computer Account Management	Success	Success
Audit Policy	Account Management	Other Account Management Events	Success	No Auditing
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success and Fail...	Success
Audit Policy	Detailed Tracking	PNP Activity	Success	No Auditing
Audit Policy	Detailed Tracking	Process Creation	Success	No Auditing
Audit Policy	DS Access	Directory Service Access	Success and Fail...	Success
Audit Policy	DS Access	Directory Service Changes	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Account Lockout	Failure	Success
Audit Policy	Logon/Logoff	Group Membership	Success	No Auditing
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	No Auditing
Audit Policy	Logon/Logoff	Special Logon	Success	Success
Audit Policy	Object Access	Detailed File Share	Failure	No Auditing
Audit Policy	Object Access	File Share	Success and Fail...	No Auditing
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	No Auditing
Audit Policy	Object Access	Removable Storage	Success and Fail...	No Auditing
Audit Policy	Policy Change	Audit Policy Change	Success	Success
Audit Policy	Policy Change	Authentication Policy Change	Success	Success
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	No Auditing
Audit Policy	Policy Change	Other Policy Change Events	Failure	No Auditing
Audit Policy	Privilege Use	Sensitive Privilege Use	Success and Fail...	No Auditing
Audit Policy	System	Other System Events	Success and Fail...	Success and Fail...
Audit Policy	System	Security State Change	Success	Success
Audit Policy	System	Security System Extension	Success	No Auditing
Audit Policy	System	System Integrity	Success and Fail...	Success and Fail...
HKCU	Software\Policies\Microsoft\Internet Explorer\Control Panel	FormSuggest Passwords	1	
HKCU	Software\Policies\Microsoft\Internet Explorer\Main	FormSuggest Passwords	no	
HKCU	Software\Policies\Microsoft\Internet Explorer\Main	FormSuggest PW Ask	no	

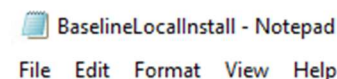
Kuvio 30. Baseline vs Effective

Windows Server 2019 Security Baseline kansioista löytyy ”**Local_Script**” niminen kansio, jonka sisällä on ”**BaselineLocalInstall**” niminen PowerShell skripti, jonka ajamalla pystyimme päivittämään Group Policyt samoiksi kuin security baseliinissa (ks. kuvio 31).



Kuvio 31. BaselineLocalInstall skripti.

Skripti tarvitsee ajamista varten parametrin, jotta se tietää minkä baseliin se asentaa. Meidän tapauksessamme koversimme Windows Server 2019 domain controlleria, joten valitsimme ”-**WS2019DomainController**” parametrin. Skriptin toimivuus vaatii myös PowerShellin järjestelmänvalvojan oikeudet sallia skriptien ajon, ja Microsoft Security Compliance Toolkitin mukana tulevan LGPO:n lgpo.exe:n sijoituksen alakansioon ”Tools”, joka on samassa paikassa kuin BaselineLocalInstall skripti. LGPO työkalulla pystyisi myös tekemään saman prosessin, mutta teimme tämän nyt BaselineLocalInstallin kautta (ks. kuvio 32).



.DESCRIPTION

Applies a Windows security configuration baseline to local group policy.

Execute this script with one of these required command-line switches to install the corresponding baseline:

```
-Win10DomainJoined      - Windows 10 v1809, domain-joined
-Win10NonDomainJoined   - Windows 10 v1809, non-domain-joined
-WS2019Member           - Windows Server 2019, domain-joined member server
-WS2019NonDomainJoined  - Windows Server 2019, non-domain-joined
-WS2019DomainController - Windows Server 2019, domain controller
```

REQUIREMENTS:

- * PowerShell execution policy must be configured to allow script execution; for example, with a command such as the following:
Set-ExecutionPolicy RemoteSigned
- * LGPO.exe must be in the Tools subdirectory or somewhere in the Path. LGPO.exe is part of the Security Compliance Toolkit and can be downloaded from this URL:
<https://www.microsoft.com/download/details.aspx?id=55319>

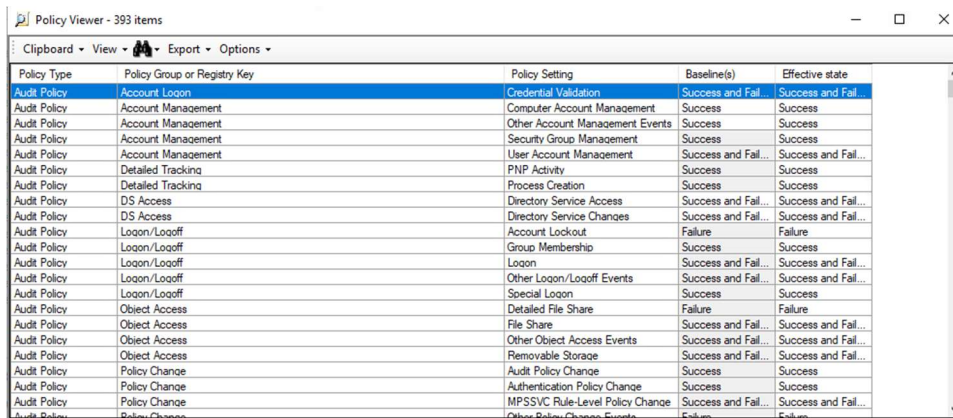
Kuvio 32. Skriptin vaatimukset

Skriptin ajon aikana ei ollut mitään ongelmia, ja saimme päivitettyä policyt DC01-koneelle (ks. kuvio 33).

```
PS C:\Users\Administrator\Downloads\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Script> .\BaselineLocalInstall.ps1 -WS2019DomainController
Logging to C:\Users\Administrator\Downloads\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Script\BaselineInstall-20220922-1226-20.log ...
-----
Windows Server 2019 - domain controller
GPOs to be installed:
  MSFT Internet Explorer 11 - Computer
  MSFT Internet Explorer 11 - User
  MSFT Windows 10 1809 and Server 2019 - Defender Antivirus
  MSFT Windows 10 1809 and Server 2019 - Domain Security
  MSFT Windows Server 2019 - Domain Controller
  MSFT Windows Server 2019 - Domain Controller Virtualization Based Security
-----
Copy custom administrative templates...
Configuring Client Side Extensions...
Running LGPO.exe /v /e mitigation /e audit /e zone
Installing Exploit Protection settings...
Applying GPO "MSFT Internet Explorer 11 - Computer"...
Running LGPO.exe /v /g ..\GPOs\{ABFB52F2-1560-4100-9103-8C10F57DC9DE}
Applying GPO "MSFT Internet Explorer 11 - User"...
Running LGPO.exe /v /g ..\GPOs\{E913422C-4F06-4D37-A739-2CD28701978E}
Applying GPO "MSFT Windows 10 1809 and Server 2019 - Defender Antivirus"...
Running LGPO.exe /v /g ..\GPOs\{FEE76283-957E-4B25-9380-2F737E13E972}
Applying GPO "MSFT Windows 10 1809 and Server 2019 - Domain Security"...
Running LGPO.exe /v /g ..\GPOs\{B9263530-926F-46F3-8382-832C31EC81B5}
Applying GPO "MSFT Windows Server 2019 - Domain Controller"...
Running LGPO.exe /v /g ..\GPOs\{FEFBD334-CF33-4078-8829-4B00DC1D1648}
Applying GPO "MSFT Windows Server 2019 - Domain Controller Virtualization Based Security"...
Running LGPO.exe /v /g ..\GPOs\{7EA149BF-56B3-42CF-AF68-3FC789510ADD}
-----
To test properly, create a new non-administrative user account and reboot.
Detailed logs are in this file:
C:\Users\Administrator\Downloads\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Script\BaselineInstall-20220922-1226-20.log
Please post feedback to the Security Guidance blog:
https://blogs.technet.microsoft.com/secguide/
-----
PS C:\Users\Administrator\Downloads\Windows 10 Version 1809 and Windows Server 2019 Security Baseline\Local_Script>
```

Kuvio 33. Ajettu skripti.

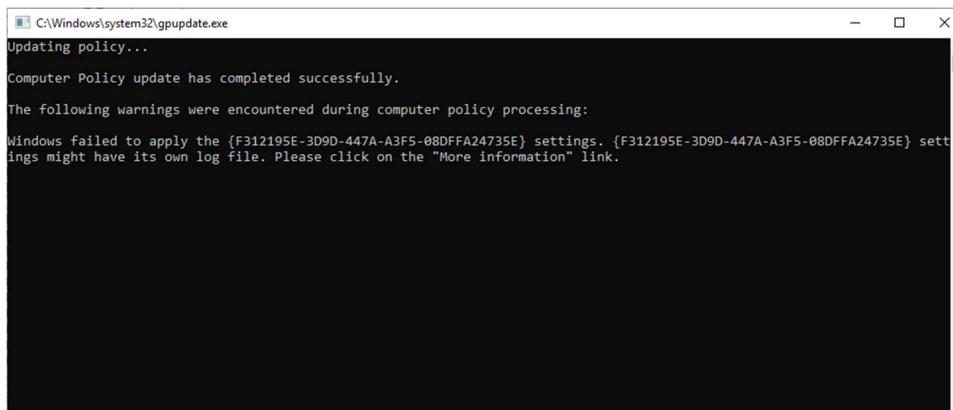
Skriptin ajon jälkeen ajoimme gpupdate:n, joka päivitti policyt onnistuneesti. Ajoimme gpupdate:n samalla lailla kuin aiemmin manuaalisen konfiguroinnin aikana (ks. kuvio 34).



Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Audit Policy	Account Logon	Credential Validation	Success and Fail...	Success and Fail...
Audit Policy	Account Management	Computer Account Management	Success	Success
Audit Policy	Account Management	Other Account Management Events	Success	Success
Audit Policy	Account Management	Security Group Management	Success	Success
Audit Policy	Account Management	User Account Management	Success and Fail...	Success and Fail...
Audit Policy	Detailed Tracking	PNP Activity	Success	Success
Audit Policy	Detailed Tracking	Process Creation	Success	Success
Audit Policy	DS Access	Directory Service Access	Success and Fail...	Success and Fail...
Audit Policy	DS Access	Directory Service Changes	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Account Lockout	Failure	Failure
Audit Policy	Logon/Logoff	Group Membership	Success	Success
Audit Policy	Logon/Logoff	Logon	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Other Logon/Logoff Events	Success and Fail...	Success and Fail...
Audit Policy	Logon/Logoff	Special Logon	Success	Success
Audit Policy	Object Access	Detailed File Share	Failure	Failure
Audit Policy	Object Access	File Share	Success and Fail...	Success and Fail...
Audit Policy	Object Access	Other Object Access Events	Success and Fail...	Success and Fail...
Audit Policy	Object Access	Removable Storage	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Audit Policy Change	Success	Success
Audit Policy	Policy Change	Authentication Policy Change	Success	Success
Audit Policy	Policy Change	MPSSVC Rule-Level Policy Change	Success and Fail...	Success and Fail...
Audit Policy	Policy Change	Other Policy Change Events	Failure	Failure

Kuvio 34. Skriptin jälkeen Policy Analyzer.

Gpupdate kuitenkin antoi virheen, **`Windows failed to apply the {F312195E-3D9D-447A-A3F5-08DFFA24735E} settings.`** (ks. kuvio 35).



```

C:\Windows\system32\gpupdate.exe
Updating policy...
Computer Policy update has completed successfully.
The following warnings were encountered during computer policy processing:
Windows failed to apply the {F312195E-3D9D-447A-A3F5-08DFFA24735E} settings. {F312195E-3D9D-447A-A3F5-08DFFA24735E} settings might have its own log file. Please click on the "More information" link.

```

Kuvio 35. gpupdate, ja virhe.

Virheestä oli vaikea löytää tietoa, mutta pienen etsimisen jälkeen oletimme, että se johtuu väärästä arvosta **`HypervisorEnforcedCodeIntegrity`**:ssä. Tähän virheeseen ei kuitenkaan pureuduttu sen tarkemmin, koska policyt päivittyivät kuitenkin, ja emme halunneet käyttää liikaa aikaa tähän yksittäiseen ongelmaan, vaan halusimme vain liikkua eteenpäin raportin kirjoittamiseen (Stenhall 2017).

Skriptin ajon jälkeen suurin osa policyistä olivat baselinen mukaisia, mutta eivät kaikki. Emme läheneet näitäkään tutkimaan syvempää, mutta luultavasti olisimme saaneet nämäkin korjattua ajan kanssa (ks. kuvio 36).

HKLM	System\CurrentControlSet\Policies\Microsoft\FVE	RD\DenyWriteAccess	1	
HKLM	SYSTEM\CurrentControlSet\Services\NTDS\Parameters	LDAPServerIntegrity	2	1
Security Template	Privilege Rights	SeDenyNetworkLogonRight	***CONFLICT***	
Security Template	Privilege Rights	SeDenyRemoteInteractiveLogonR...	"S-1-5-113"	
Security Template	Privilege Rights	SeEnableDelegationPrivilege	***CONFLICT***	"S-1-5-32-544"
Security Template	Privilege Rights	SeInteractiveLogonRight	***CONFLICT***	"S-1-5-32-544"
Security Template	Privilege Rights	SeNetworkLogonRight	***CONFLICT***	"S-1-5-11,"S-1-5-...
Security Template	Service General Setting	"XblAuthManager"	4,""	
Security Template	Service General Setting	"XblGameSave"	4,""	
Security Template	Service General Setting	"XboxGpSvc"	4,""	
Security Template	Service General Setting	"XboxNetApSvc"	4,""	
Security Template	System Access	EnableAdminAccount	0	1

Kuvio 36. Policy Analyzer Eroavaisuudet päivittämisen jälkeen.

4 Pohdinta

Labra oli alussa hämmäntävä ja lähti hitaasti liikkeelle. Ryhmänä ymmärsimme mitä tarkoittaa koventaminen, mutta miten ja mitä kovennetaan, aiheutti hämmennystä ja ihmettelyä. Alun ihmettelyn, teorian ja opettajalta kyselyn jälkeen kuva siitä, mitä kovennetaan ja miten selkeni hieman. Aloitimme käyttämällä BPA:ta (Best Practice Analyzer). Paljon oli kovennettavaa ja olisi pitänyt varmaan tutkia jotain kovennusohjetta tarkemmin ennen kuin alkoi tekemään, mutta jatkossa luultavasti labrat lähtevät selkeämmin liikkeelle, kun virheistä oppii. Ajoimme BPA:n ja lähdimme sen perusteella korjaamaan sen antamia varoituksia. Työtä oli paljon, minkä myös sivuoireena oli hankala ryhmänä pysyä perillä mitä on tehty ja miten. Hyvällä kommunikaatiolla kuitenkin saimme jaettua tekemämme ja oppimamme.

Tutkiessamme group policyjen koventamista törmäsimme Microsoftin työkaluun Microsoft Security Compliance Toolkit, joka helpotti group policyjen muuttamisessa ja vertaamisessa. Toolkitin käyttö auttoi ja nopeutti koventamista todella paljon. Microsoftin dokumentointi on hyvää ja sen avulla saimme paljon tietoa active directoryn koventamisesta.

Alun hämmennyksestä huolimatta labran lopussa olimme ajan tasalla siitä, mitä teimme ja miksi. Saimme active directoryn kovennettua niin hyvin kuin vain tämänhetkisillä tiedoilla ja taidoilla oli mahdollista ja olemme tyytyväisiä lopputulokseen.

Lähteet

Beyond Trust. What is Systems Hardening? N.d. Viitattu 20.9.2022. <https://www.beyondtrust.com/resources/glossary/systems-hardening>

Buckbee M. What is a Domain Controller, When is it Needed + Set Up. 23.06.2020. Viitattu 26.09.2022. <https://www.varonis.com/blog/domain-controller>

Configure DNS scavenging on the Windows server. N.d. Viitattu 26.9.2022. <https://documentation.n-able.com/N-central/userguide/Content/Deploying/RB-DNS-Scavenging.htm>

DNS servers on Ethernet should include the loopback address, but not as the first entry. 25.10.2012. Viitattu 26.09.2022. <https://social.technet.microsoft.com/Forums/lync/en-US/bda761a5-43ca-486b-ba6d-b16b6bd49642/dns-servers-on-ethernet-should-include-the-loopback-address-but-not-as-the-first-entry?forum=winserveressentials>

DNS: DNS servers on should include the loopback address, but not as the first entry. 29.11.2014. Viitattu 26.9.2022. <https://vschamarti.wordpress.com/2014/11/29/dns-dns-servers-on-should-include-the-loopback-address-but-not-as-the-first-entry/>

Ittaster. Adding An Additional Domain Controller To An Existing Domain | Windows Server 2019. 29.3.2021. Viitattu 26.09.2022. https://www.youtube.com/watch?v=8aR_0Fp55mg

LabraNet services for JAMK students. N.d. Viitattu 26.09.2022. <https://student.labranet.jamk.fi/instructions/>

Microsoft. Active Directory Domain Services Overview. 17.8.2022. Viitattu 20.9.2022. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview> 20.9.

Microsoft. gpupdate. 03.03.2021. Viitattu 26.9.2022 <https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate>

Microsoft. Run Best Practices Analyzer Scans and Manage Scan Results. 20.9.2021. Viitattu 20.9.2022. <https://learn.microsoft.com/en-us/windows-server/administration/server-manager/run-best-practices-analyzer-scans-and-manage-scan-results>

Microsoft. Microsoft Security Compliance Toolkit 1.0 - How to use. 21.09.2022. Viitattu 24.9.2022. <https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10>

MSFT WebCast. Adding Additional Domain Controller to an Existing Domain | Windows Server 2019. 10.6.2019. Viitattu 26.9.2022 <https://www.youtube.com/watch?v=sqHa2gN1HsY>

PCmag. Loopback address. N.d. Viitattu 26.9.2022. <https://www.pcmag.com/encyclopedia/term/loopback-address>

Pervais U. Best Practice Analyzer Root Hint Server Warnings. 17.1.2022. Viitattu 26.9.2022
<https://mushaaf.net/best-practice-analyzer-root-hint-server-warnings/>

Stenhall A. GPO error message applying settings for {F312195E-3D9D-447A-A3F5-08DFFA24735E}. 11.8.2017. Viitattu 26.9.2022. <https://www.theexperienceblog.com/2017/08/11/gpo-error-message-applying-settings-for-f312195e-3d9d-447a-a3f5-08dffa24735e/>

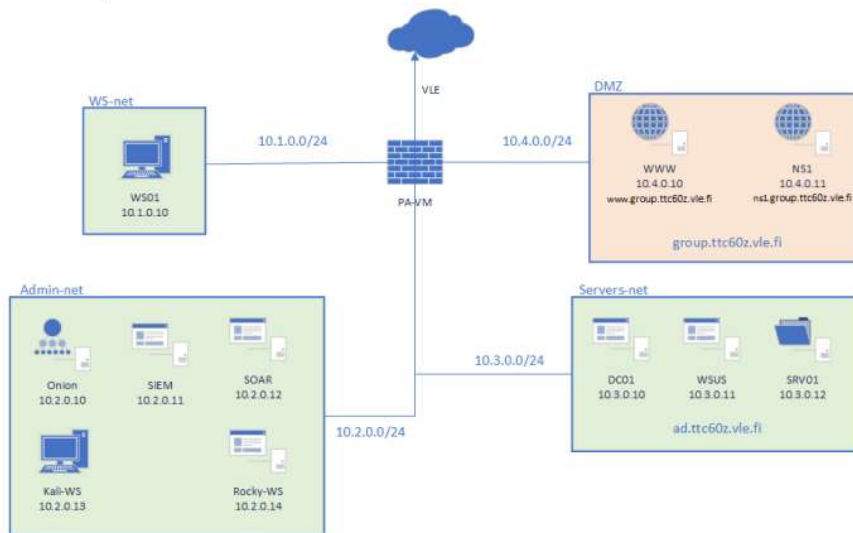
What is Backup? N.d. Viitattu 27.09.2022. <https://www.acronis.com/en-eu/blog/posts/data-backup/>

What Is DNS?. N.d. Viitattu 26.9.2022. [https://www.fortinet.com/resources/cyberglossary/what-is-dns#:~:text=The%20Domain%20Name%20System%20\(DNS,devices%20to%20locate%20the%20device.](https://www.fortinet.com/resources/cyberglossary/what-is-dns#:~:text=The%20Domain%20Name%20System%20(DNS,devices%20to%20locate%20the%20device.)

Liitteet

Liite 1. Labraympäristö

1. Ympäristö



Kuvio 1 Laboratorio ympäristö