WINDOWS-TYÖASEMAN HALLINTA HALLINTATYÖKALUILLA

Johanna Hakonen

Sisällysluettelo

Sisällysluettelo 1
1 Johdanto 2
2 Windows-palvelimen asennus 2
3 Windows-palvelimen peruskonfigurointi 4
4 Active Directory Domain Service 5
5 DHCP-Palvelin 5
6 DNS Manager 6
7 Windows 10 -työaseman liittäminen toimialueelle 6
8 ADUC – Active Directoryn rakenne 6
9 Palvelimen levyjaot 7
10 ADUC – Active Directoryn rakenteen laajennus 7
11 ADUC – Käyttäjät ja ryhmät 7
12 FSRM – Tallennusrajoitukset 8
13 Group Policy Objects 9
13.1 Offline-käyttö 9
13.2 Salasanat 9
13.3 Työasemien päivitys 9
13.4 Tiedostojen uudelleenohjaus 10
13.5 Osastokohtaiset yhteiskansiot 10
13.6 GPO-linkitys 10
14 Windows Server Backup - Varmuuskopiointi 11
15 Group Policy Objects 11
15.1 Verkkotulostin 11
15.2 Työaseman tarkistaminen 12
15.3 Tapahtumien kirjaaminen 12
15.4 Ohjauspaneelin poisto käyttäjiltä Aloitus-menusta 13
15.5 Viimeisen käyttäjän piilotus 13

16 Powershell 13
16.1 Käyttäjien haku nimen mukaan 13
16.2 Tietyn käyttäjän tietojen haku 14
16.3 Tietyn OU:n käyttäjien haku 14
16.4 Käyttäjän lisääminen 14
17 Jatkoehdotukset 15
Lähdeluettelo 16

1 Johdanto

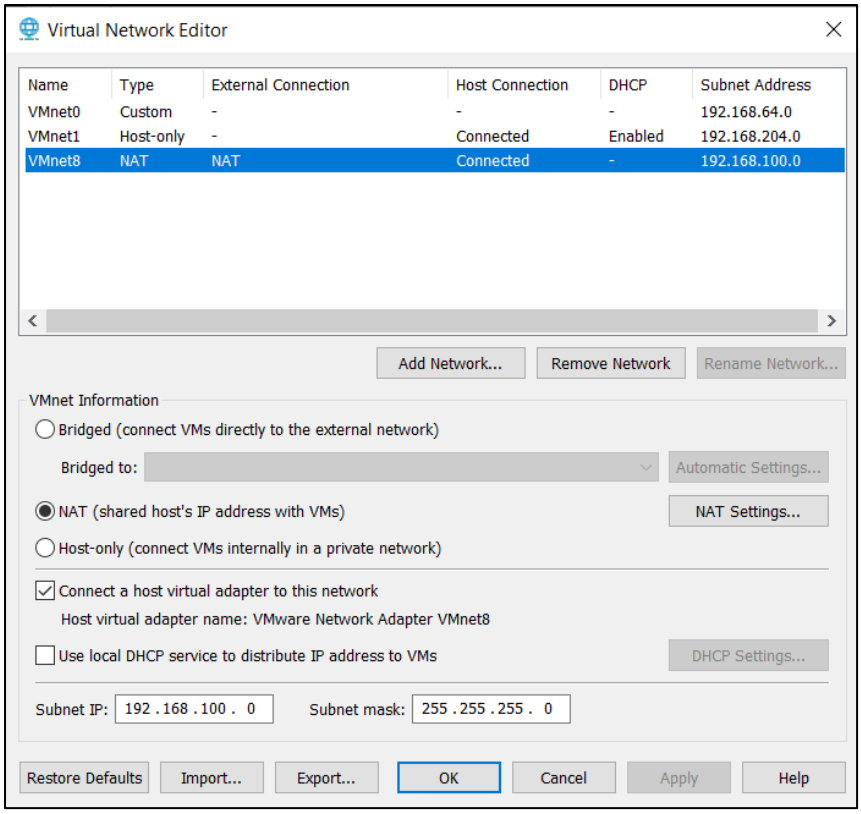
Yksi kyberuhkien hallinta- ja suojautumiskeino on laitteen hallinta hallintatyökaluilla. Ympäristönä käytettiin virtuaalikoneita VMware Workstation Pro 17 -ohjelmassa. Windows-työaseman hallintaa toimialueympäristössä toteutettiin Windows-palvelimen hallintakonsoleilla, group policyillä ja Powershellillä. Ohjeena käytettiin Windows-palvelin 2019 -materiaaleja ja Microsoft Learn -sivustoa sekä apuna ChatGPT:tä (OpenAI, 2025).

Toimialueympäristössä hallintatyökaluina käytettiin Windows-palvelimen hallintakonsoleita Server Manager, Active Directory Domain Service (ADDS), Active Directory Users and Computers (ADUC), File Server Resource Manager (FSRM), Dynamic Host Configuration Protocol (DHCP) -palvelin, Domain Name System (DNS) Manager, Windows Server Backup, Print Management, Event Viewer ja Group Policy Management Console (GPMC). Powershellia harjoiteltiin tehtävien automatisoinnissa.

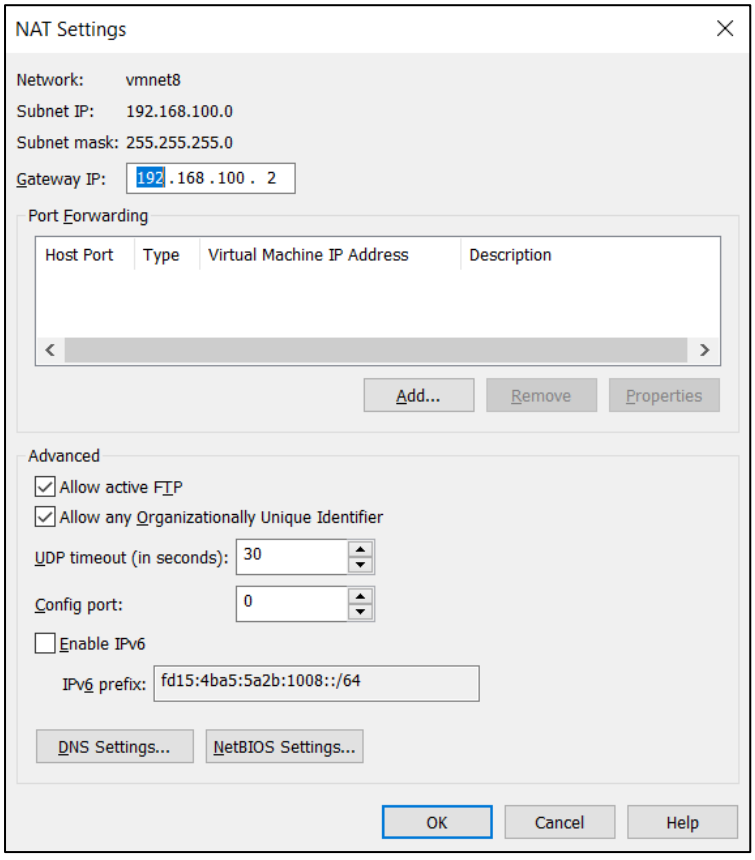
2 Windows-palvelimen asennus

Ensin muutetaan verkkoasetukset (VMWareworkstation > Edit > Virtual Network Editor) siten, että NAT-yhteyden DHCP-palvelu pois päältä (Kuva 1). Verkon IP-alue on 192.168.100.0/24. Kuva 2 on esitetty NAT-asetukset: Gateway IP-osoite on 192.168.100.2.

Opetusmateriaalista poiketen ei asenneta täysin uutta virtuaalikonetta vaan Windows-palvelimena käytetään osittain valmista srv1win2022_AmiDom-virtuaalikonetta server22-physio, jonka levyn koko on 100 GB ja muisti on 4 GB. Prosessorien määräksi vaihdetaan kahden tilalle neljä ja lisätään uusi 60 GB kovalevy. Admistrator-tunnuksen salasana on P@ssw0rd. VMware Toolsit päivitettiin heti. Koneesta tehtiin snapshot 20250129.



Kuva 1.Verkkoasetukset.

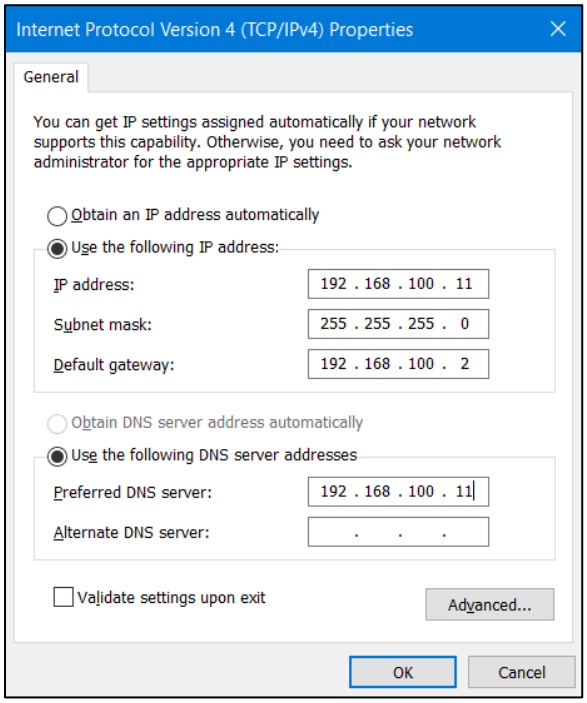


Kuva 2. NAT-asetukset.

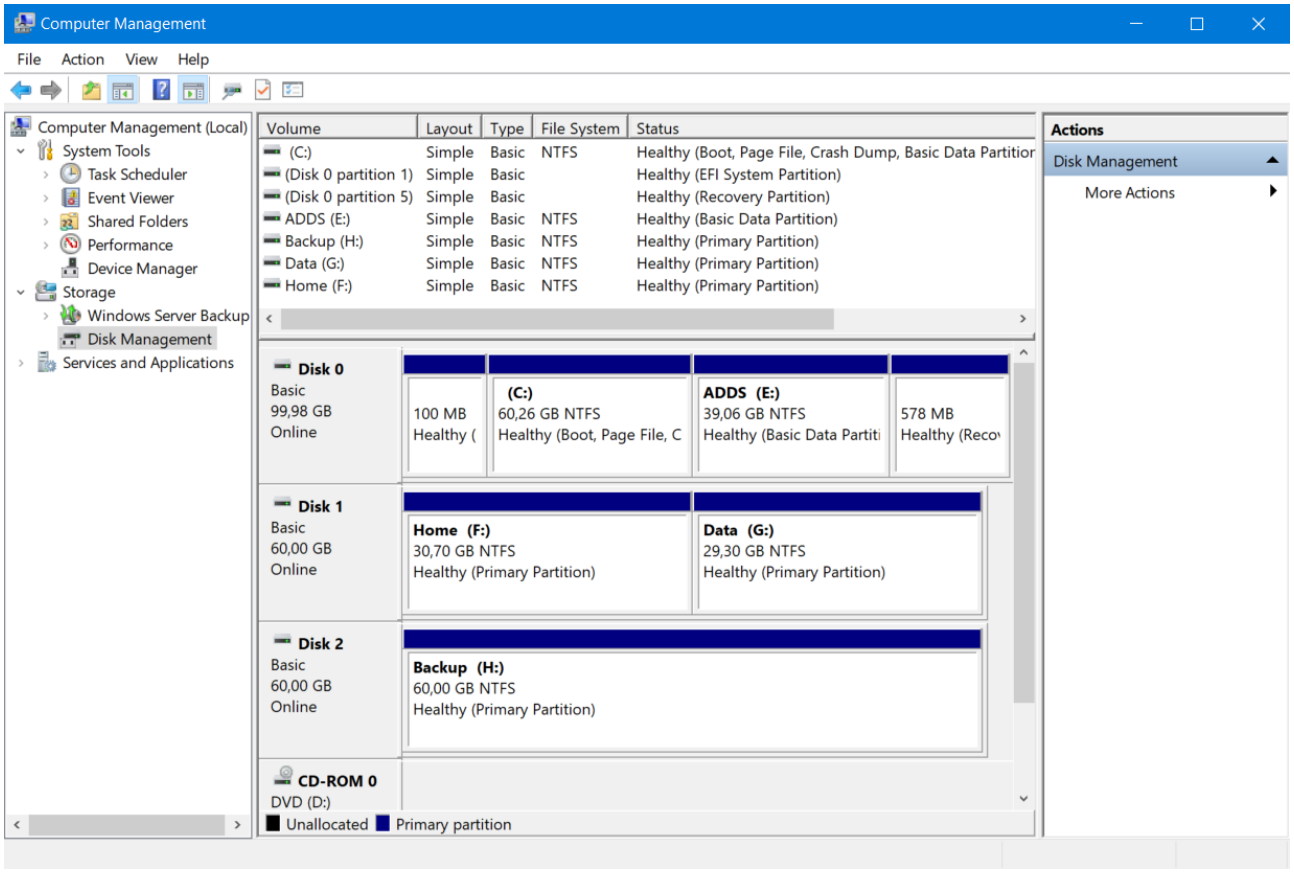
3 Windows-palvelimen peruskonfigurointi

Palvelin toimii erittäin hitaasti ja kaatui heti alkuun, kun konfiguraatioita alettiin tehdä. Palvelimen nimi voitaisiin vaihtaa (Server Manager > Local Server > Properties > Computer Name) mutta pidettiin se Server01:nä. IPv4-osoite voitaisiin vaihtaa (Local Server > Properties > Ethernet0 > Network Connections > Ethernet0 > Ethernet0 Properties > Properties > Internet Protocol Version 4 (TCP/IPv4) Properties) mutta pidettiin asetukset alkuperäisinä (Kuva 3).

Levyt otettiin käyttöön ja alustettiin (Server Manager > Tools > Computer Management > Storage > Disc Management) Kuva 4 mukaiseksi. Alkuun ohjelma pyytää alustamaan Levyn 1 ja valitaan osiointityyliksi Master Boot Record (MBR) kuten oppimateriaalissa. Pienennettiin Levyn 0 C-levyä (Shrink Volume) 40 GB, jotta saatiin Active Directorylle tilaa 39,06 GB. Tehtiin ADDS E-levy New Simple Volume Wizardilla lokitiedostoja ja tietokantaa varten. Jaettiin myös Levy 1 Home- ja Data-levyihin, molemmat noin 30 GB. Otettiin palvelimesta snapshot 20250130 ja varmuuskopioitiin ulkoiselle kovalevylle. Lisättiin vielä kolmas 60 GB kovalevy varmuuskopiointia varten, otettiin se käyttöön ja alustettiin.



Kuva 3. Palvelimen Internet Protocol Version 4 (TCP/IPv4) -ominaisuudet.



Kuva 4. Palvelimen osiointi.

4 Active Directory Domain Service

Active Directory Domain Service (ADDS) on jo valmiina virtuaalikoneessa. Jos ei olisi, se asennettaisiin lisäämällä rooli (Server Manager > Tools > Add Roles and Features) Wizardilla. Ohjeita oli vaikea soveltaa, koska niissä kaikki tehdään alusta asti. Käytetyssä virtuaalikoneessa on jo NDTS- ja SYSVOL-kansiot luotu C:\Windows-kansioon, vaikka ohjeissa ne tehtiin itse tehtyyn ADDS-osioon Active Directory Domain Services Configuration Wizardilla.

5 DHCP-Palvelin

DHCP-palvelin asennettiin lisäämällä rooli (Server Manager > Tools > Add Roles and Features) Wizardilla. Asennuksen jälkeen kone pyytää varoituskolmiolla viimeistelemään DHCP:n konfigurointi ja tehtiin se. Tehtiin uusi alue (Tools > DHCP > IPv4 > New Scope…), josta työasemat saavat IP-osoitteet. Alueen nimeksi laitettiin Wks ja kuvaukseksi Työasemat. Oppimateriaalissa ohjataan tekemään alue sadalle työasemalle ja käytettiin tässä samaa määrää, jos Physio tulee laajentumaan tulevaisuudessa. Alueeksi laitettiin siis 192.168.100.100–192.168.100.199. Maskina on 24 eli 255.255.255.0. Varausajaksi laitettiin kahdeksan päivää. Konfiguroitiin DHCP-optiot. Reitittimen IP-

osoitteeksi laitettiin 192.168.100.2. Domain Name and DNS Servers -kohtaan laitettiin palvelimen nimeksi Server01 ja klikataan Resolve, jolloin löytyi IP-osoite 192.168.100.11. Aktivoitiin alue.

6 DNS Manager

Tehtiin osoitetietue ohjeiden mukaan (Server Manager > Tools > DNS) valitsemalla amidom.local kohdassa Forward Lookup Zones ja valitsemalla New Host (A or AAAA). Annettiin nimi WKS100 ja IP-osoite 192.168.100.100.

7 Windows 10 -työaseman liittäminen toimialueelle

Windows-työasemana käytetään wks1win10_22H2_x64-virtuaalikonetta wks1-physio. Päivitettiin VMware Toolsit heti. Windows Update teki automaattisesti päivitykset. Ethernet-asetuksista nähtiin, että kone löysi automaattisesti amidom-toimialueen ja DHCP jakoi automaattisesti osoitteen (192.168.100.128).

Kirjauduttiin toimialueeseen (Asetukset > Järjestelmä > Tietoja > Nimeä tämä tietokone uudelleen (lisäasetus) > Järjestelmän ominaisuudet > Muuta…) muuttamalla jäsenyys työryhmästä toimialueeksi amidom.local ja antamalla Tietokoneen nimi ja toimialuemuutokset -kohdassa tietokoneen tilille oikeus kirjautua toimialueelle (Administrator, P@ssw0rd). Käynnistettiin tietokone uudelleen ja kirjauduttiin Administrator-tunnuksella sisään. Kirjauduttiin palvelimeen sisään ja tarkistettiin (Server Manager > Tools > DHCP > server1.amidom.local > IPv4 > Scope [192.168.100.0] Wks > Address Leases), että wks1 löytyy listasta. Aloitettiin automaattiset päivitykset ja sammutettiin kone. Otettiin snapshotit 20250131 palvelimesta ja työasemasta, ja varmuuskopioitiin molemmat ulkoiselle kovalevylle.

8 ADUC – Active Directoryn rakenne

Käynnistettiin palvelin ja päivitettiin VMware Tools. Suoritettiin Windows Updaten ehdottamat päivitykset.

Tarkistettiin, että työasemassa on automaattiset IP-asetukset käytössä (Asetukset > Verkko ja internet > Muuta sovitinasetuksia > Ethernet0 > Ominaisuudet: Ethernet0 > Ominaisuudet > Internet Protocol Version 4 (TCP/IPv4) > Ominaisuudet > Ominaisuudet: Internet Protocol Version 4 (TCP/IPv4)).

Tehtiin AD:lle rakennetta (Server Manager > Tools > Active Directory Users and Computers (ADUC)) ohjeen mukaan. Otettiin käyttöön Advanced Features (View). Luotiin amidom.local-toimialueen alle Physio-organisaatioyksikkö (OU), jonka alle luotiin IT-, Hoitajat-, Ryhmät ja Tietokoneet-organisaatioyksiköt.

9 Palvelimen levyjaot

Tehtiin kotikansiojako ja osastokohtainen jako mallikäyttäjää varten (Server Manager > Tools > Computer Management > Shared Folders) kuten alla on kuvattu.

Luotiin Home (F:) -asemalle Home-kansio (Home) ja tehtiin sille piilojako (Properties > Sharing > Advanced Sharing…: Share this folder: Share name: Home$). Vaihdetaan oikeuksia siten, että Everyonen tilalle haetaan Authenticated User (Permissions: Add… > Select Users, Computers, Services, or Groups > Enter the object names to select: Authenticated Users). Annetaan täydet oikeudet valitsemalla Full Control. Poistetaan ryhmät CREATOR OWNER ja Users sekä lisätään Authenticated User katkaisemalla ensin periytyminen (Security > Advanced… > Advanced Security Settings for Home > Disable inheritance > Block Inheritance: Convert inherited permissions into explicit permissions on this object) ja poistamalla/lisäämällä sitten käyttäjät (Security > Edit > Remove/Add…). Vaihdettiin vielä vain Read & execute -oikeudet Authenticated Userille (Advanced > Advanced Security Settings for Home: Authenticated User > Edit > Permission Entry for Home: Applies to: This folder only).

Lisäksi luotiin Data (G:) -asemalle Yhteinen-kansio. Jaettiin se (Properties > Sharing > Advanced Sharing…: Share this folder: Share name: Yhteinen) ja vaihdetaan oikeuksia siten, että Everyonen tilalle haetaan Authenticated User (Permissions: Add… > Select Users, Computers, Services, or Groups > Enter the object names to select: Authenticated Users). Annetaan täydet oikeudet valitsemalla Full Control.

Sammutettiin palvelin ja työasema, otettiin snapshotit (20250202) ja varmuuskopioitiin ulkoiselle kovalevylle.

10 ADUC – Active Directoryn rakenteen laajennus

Käynnistettiin palvelin ja päivitettiin VMware Tools. Suoritettiin Windows Updaten ehdottama päivitys Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1666.0).

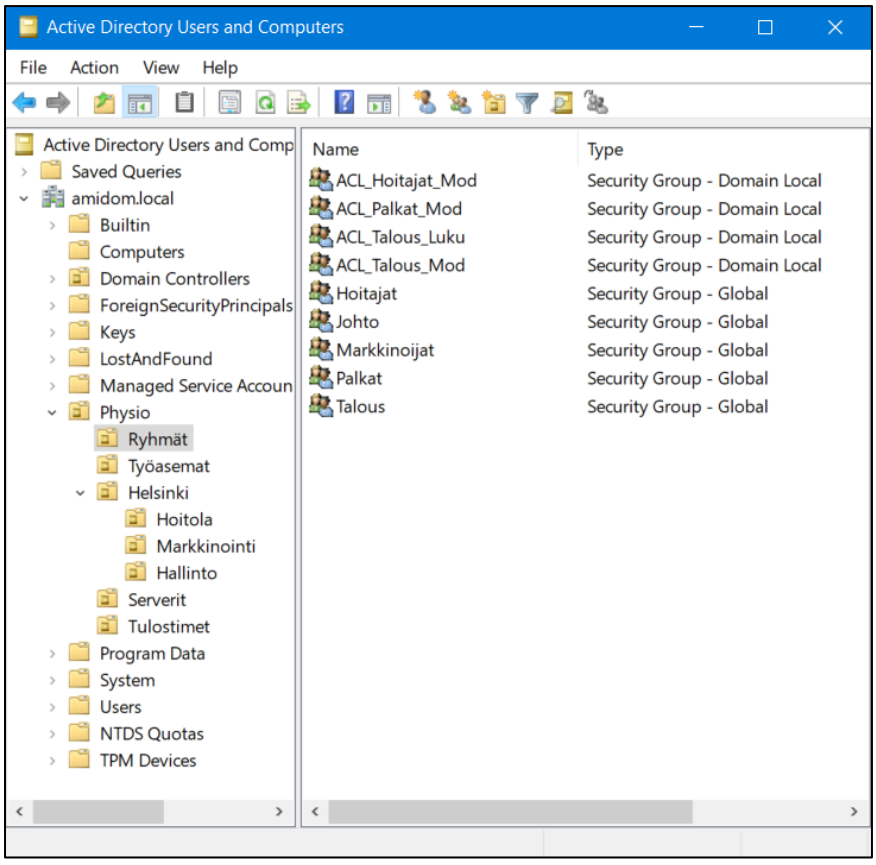
Laajennettiin AD:n rakennetta tulevaisuutta ajatellen. Lisättiin Physio-organisaatioyksikköön yksiköt (Server Manager > Tools > Active Directory Users and Computers) Helsinki, Tulostimet ja Serverit. Tietokoneet-yksikkö nimettiin uudelleen Työasemat-yksiköksi. Poistettiin IT-yksikkö. Hoitajat-yksikkö siirrettiin Helsinki-yksikön alle nimellä Hoitola ja lisättiin sinne myös Hallinto- ja Markkinointi-yksiköt.

11 ADUC – Käyttäjät ja ryhmät

Luotiin mallikäyttäjä Helsinki-yksikön Hoitola-yksikköön (New > User > New Object – User). Etunimeksi laitettiin _template, sukunimeksi hoitola ja User logon nameksi template.hoitola. Seuraavassa ruudussa valittiin ”Account is disabled”. Käyttäjän kotikansioksi määritellään H: (Properties > _template hoitola Properties > Profile: Home Folder: Connect) ja To: \\server01\home$\%username%. Home (F:) -aseman Home-kansioon ilmestyi template.hoitola-kansio.

Määriteltiin Physio-yksikön Ryhmä-yksikköön Global-ryhmä Hoitajat (New > Group > New Object – Group) ja Domain Local -ryhmä ACL_Hoitajat_Mod, jolla tehdään pääsylistoja verkkojakoihin. Lisättiin mallikäyttäjä Hoitajat-ryhmään (Properties > Hoitola Properties > Members > Add…). Lisättiin myös Hoitajat -ryhmä ACL_Hoitajat_Mod-ryhmään (Properties > Hoitola Properties > Member of > Add…). Luotiin käyttäjä Henni Hieroja mallikäyttäjän pohjalta eli kopioidaan _template hoitola (Copy… > Copy object – User) ja annettiin nimi ja käyttäjänimi henni.hieroja. Seuraavassa ruudussa annetaan salasanaksi P@ssw0rd ja poistetaan valinta ”Account is disabled”. Kirjauduttiin käyttäjällä työasemaan, päivitettiin VMware Tools ja tarkistettiin, että tehty kotikansio löytyy.

Tehtiin Ryhmät-organisaatioyksikön alle vielä Global -ryhmät Palkat, Talous, Markkinoijat ja Johto sekä Domain Local -ryhmät ACL_Palkat_Mod, ACL_Talous_Mod, ACL_Talous_Luku (Kuva 5). Palkat-ryhmä liitetään ACL_Palkat_Mod-ryhmän alle, Johto- ja Talous-ryhmät ACL_Talous_Mod-ryhmän alle ja Markkinoijat-ryhmä ACL_Talous_Luku-ryhmän alle. Muihin ryhmiin kuin Hoitajat ei lisätä käyttäjiä, koska ne on tehty laajentumista varten.



Kuva 5. Active Directoryn rakenne.

12 FSRM – Tallennusrajoitukset

Tehtiin kotikansioihin talletusrajoitus 100 MB. Asennettiin ensin File Server Resource Manager (Server Manager > Manage > Add Roles and Features > Add Roles and Features Wizard > Installation type: Role-based or feature-based installation >> Server Roles: File and Storage Services > File and iSCSI

Services > File Server Resource Manager > Add Features > Confirmation > Install). Avataan se (Server Manager > Tools) ja luodaan tallennusrajoitus (Quota Management > Quotas > Create Quota…: Quota path: F:\Home, Auto apply template and create quotas on existing and new subfolders, 100 MB Limit).

Sammutettiin palvelin ja työasema, otettiin snapshotit (20250203) ja varmuuskopioitiin ulkoiselle kovalevylle.

13 Group Policy Objects

Käynnistettiin palvelin ja suoritettiin Windows Updaten ehdottama päivitys Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1685.0).

13.1 Offline-käyttö

Työasemia voidaan hallita ryhmäkäytännöillä (Group Policy Objects, GPO). Lisättiin objekti, jolla sallitaan työaseman offline-käyttö (Server Manager > Tools > Group Policy Management). Group Policy Objects -kohdassa on valmiina Default Domain Controllers Policy ja Default Domain Policy. Klikattiin edellä mainittua ja saatiin ilmoitus, että tämän GPO:n luvat SYSVOL-kansiossa poikkeavat AD:n luvista ja annettiin lupa muuttaa ne vastaaviksi. Sama tehtiin jälkimmäiselle. Sitten jatkettiin oppimateriaalin mukaisesti lisäämällä uusi GPO Offline_salli Group Policy Objects -kohdan alle ja editoitiin sitä (Edit > Computer Configuration > Policies > Administrative Templates > Network > Offline Files > Standard-välilehti: Allow or Disallow use of the Offline Files feature > Edit: Enabled).

13.2 Salasanat

Physion tietoturvapolitiikan mukaan salasanojen tulee olla vähintään seitsemän merkkiä pitkiä ja ne vanhenevat 30 päivän välein. Kolmea edellistä salasanaa ei saa käyttää uudelleen. Muokattiin salasanoihin liittyvää GPO:ta (Default Domain Policy > Edit > Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy). Enforce password history -kohtaan vaihdettiin 24 tilalle 3 ja Maximum password age -kohtaan 42 tilalle 30. Minimum password length oli jo valmiiksi 7.

13.3 Työasemien päivitys

Työasemat hakevat päivitykset joka päivä klo 19. Lisättiin uusi GPO Windows_updates Group Policy Objects -kohdan alle ja editoitiin sitä (Edit > Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update > Standard-välilehti: Configure Automatic Updates > Edit). Valitaan Enabled, Auto download and schedule for install, Scheduled install time 19:00.

13.4 Tiedostojen uudelleenohjaus

Käyttäjän omat tiedostot tallentuvat palvelimella sijaitsevaan kotikansioon. Lisättiin uusi GPO Dokumenttien_siirto Group Policy Objects -kohdan alle ja editoitiin sitä (Edit > User Configuration > Policies > Windows Settings > Folder Redirection > Documents > Properties). Valitaan Setting: Basic - Redirect everyone's folder to the same location, Root Path: \\server01\home$.

13.5 Osastokohtaiset yhteiskansiot

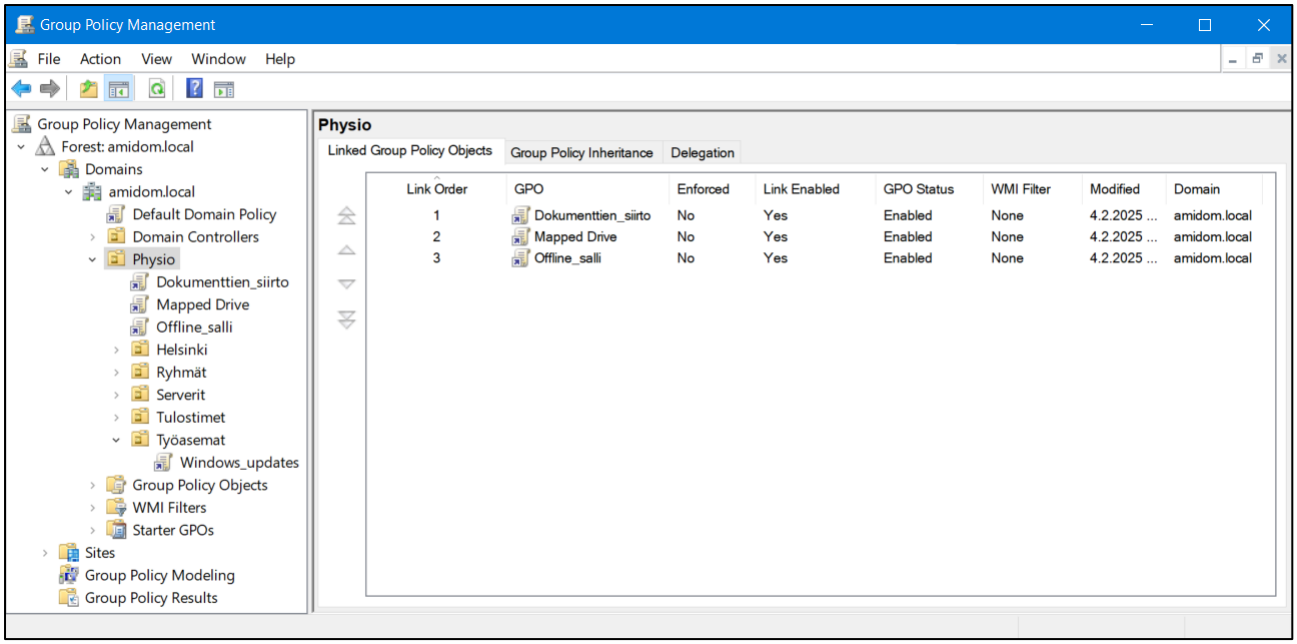
Physiolla on yhteinen verkkohakemisto, joka näkyy automaattisesti käyttäjillä. Sen alla ovat osastokohtaiset yhteiskansiot, joihin on pääsy ainoastaan osaston työntekijöillä, ja käyttäjät voivat tallentaa omia tiedostojaan osastokohtaisiin kansioihin muttei yhteiseen. Lisättiin uusi Mapped Drive -GPO Group Policy Objects -kohdan alle ja editoitiin sitä (Edit > User Configuration > Preferences > Windows Settings > Drive Maps > Preferences-välilehti). Tehtiin uusi Mapped Drive, johon valittiin Location: \\server01\yhteinen, Reconnect, Label as: Yhteinen, Drive Letter: Use first available, starting at Y.

Tehtiin vielä osastokohtaiset asetukset eli määritettiin NTFS-oikeudet. Luotiin ensin Data (G:) -asemalle Yhteinen-kansioon Hoitajat-, Palkat-, Johto-, Talous- ja Markkinointi-kansiot. Määriteltiin Hoitajat-kansioon pääsevät henkilöt (Properties > Security-välilehti). Kansiota ei tarvinnut jakaa, koska Yhteinen-kansio on jo jaettu. Poistettiin siis ryhmä Users sekä lisätään ACL_Hoitajat_Mod katkaisemalla ensin periytyminen (Security > Advanced… > Advanced Security Settings for Hoitajat > Disable inheritance > Block Inheritance: Convert inherited permissions into explicit permissions on this object) ja poistamalla/lisäämällä sitten käyttäjät (Security > Edit > Remove/Add…). Annettiin ACL_Hoitajat_Mod-ryhmälle Modify-oikeus.

Sama tehtiin muille kansioille. ACL_Talous_Mod-ryhmälle annettiin Modify-oikeudet Johto- ja Talous-kansioon. ACL_Talous_Luku-ryhmälle annettiin Read & Execute-oikeudet Markkinointi-kansioon. ACL_Palkat_Mod-ryhmälle annettiin Modify-oikeudet Palkat-kansioon.

13.6 GPO-linkitys

Kun GPO:t oli luotu, lähdettiin levittämään niitä edelleen Group Policy Management-konsolissa. Työasemiin liitettiin (Link an Existing GPO…) Windows_updates -GPO ja koko Physioon liitetään muut juuri tehdyt GPO:t (Kuva 6).



Kuva 6. Ryhmäkäytännöt (GPO).

14 Windows Server Backup - Varmuuskopiointi

Varmistettiin osastokohtaiset kansiot luomalla varmuuskopionti. Ensin asennettiin Windows Server Backup -hallintakonsoli (Server Manager > Manage > Add Role and Features > Features: Windows Server Backup > Install) ja avattiin se (Server Manager > Tools > Windows Server Backup). Määritettiin varmuuskopiointi joka ilta klo 23 (Local Backup > Actions > Backup Schedule… > Select Backup Configuration: Custom > Select Items for Backup > Add Items > Select Items: G:\Yhteinen > Specify Backup Time: Once a Day, 23:00 > Specify Destination Type: Backup to a volume > Select Destination Volume > Add > Add Volume: Backup (H:)).

Sammutettiin palvelin, otettiin snapshot 20250204 ja tallennettiin varmuuskopio ulkoiselle kovalevylle.

15 Group Policy Objects

15.1 Verkkotulostin

Käynnistettiin palvelin ja päivitettiin VMware Tools.

Ensin asennettiin Print Management -hallintakonsoli (Server Manager > Manage > Add Role and Features > Add Roles and Features Wizard > Installation type: Role-based or feature-based installation > Server Roles: Print and document Services > Role Services: Print Server). Asennettiin palvelimelle paikallinen tulostin (Tools > Print Management > Print Servers > Server01 (local) > Printers > Add Printer… > Network Rrinter Installation Wizard > Add a TCP/IP or… > Printer Address: Type of Device:

TCP/IP Device, IP address ja Port Name 192.168.100.20, Auto detect… pois päältä > Printer Driver: Install a new driver > Printer Installation: Generic IBM Graphics 9pin > Printer name and Sharing Settings: Share Name: IBM1, Location: Helsinki). Valittiin vielä List in the directory (Properties).

Asennettiin verkkotulostin kaikille työasemille. Lisättiin uusi GPO Tulostin Group Policy Objects -kohdan alle (Tools > Group Policy Management) ja editoitiin sitä (Edit > User Configuration > Preferences > Control Panel Settings > Printers > New > Shared Printer > Share path: browse: \\SERVER01\Generic IBM Graphics 9pin > Set this printer as the default printer).

15.2 Työaseman tarkistaminen

Tarkistettiin palvelimen asetukset vielä oppimateriaalin mukaisesti. Siirrettiin työasema Computer-kohdasta Työasemiin (Server Manager > Tools > Active Directory Users and Computers). Palvelin sijaitsee Domain Controllers-kohdassa, joten poistetaan Serverit-OU. Poistetaan myös turha Tulostimet-OU.

Päivitettiin GPO-muutokset palvelimessa komentokehotteessa (gpupdate /force). Käynnistetään työasema, kirjaudutaan Henni Hierojana sisään. Päivitettiin VMware Tools ja asennettiin Suojaustietojen päivitys tuotteelle Microsoft Defender Antivirus – KB2267602 (versio 1.421.1715.0). Resurssienhallinnasta löytyy verkkosijainneista henni.hieroja-kansio H-levyltä ja Yhteinen (Y:)-levy. Tehtiin Tiedostot-kansioon henni1-tekstitiedosto, johon kirjoitetaan ”testi” ja jonka pitäisi näkyä myös henni.hieroja-kansiossa, mutta ei näkynyt. Käytiin läpi Dokumenttien_siirto-GPO, päivitettiin uudestaan (gpupdate /force) palvelimella ja käynnistettiin työasema uudestaan, jonka jälkeen siirto toimii. Tehtiin Yhteinen-kansion Hoitajat-kansioon testi-tekstitiedosto, johon kirjoittaminen onnistui. Muihin Yhteinen-kansion kansioihin ei päästy sisälle kuten ei pitänytkään. Verkkotulostin löytyy Ohjauspaneelista.

Sammutettiin työasema ja palvelin sekä otettiin snapshotit 20250205 ja varmuuskopioitiin ulkoiselle kovalevylle.

15.3 Tapahtumien kirjaaminen

Käynnistettiin palvelin ja päivitettiin VMware Tools.

Muokattiin Default Domain Controllers Policy GPO:ta toteuttamaan sekä onnistuneiden että epäonnistuneiden toimialueelle kirjautumisten tarkistus (Server Manager > Tools > Group Policy Management > Domain Controllers > Default Domain Controllers Policy > Edit > Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy > Audit account logon events > Define these policy settings: Success ja Failure > Audit Logon Events > Define These Policy Settings: Success ja Failure). Annettiin komentokehotteessa komento gpupdate.exe /force. Luotiin sekä onnistuneita että epäonnistuneita kirjautumisia käyttämällä vääriä ja oikeita salasanoja. Käynnistettiin työasema ja yritettiin kirjautua pari kertaa Henni Hierojan tunnuksella väärällä salasanalla. Kirjauduttiin ulos ja takaisin palvelimelle Administrator-tunnuksella ja oikealla salasanalla. Tarkasteltiin kirjautumisia Event Viewerillä (Server Manager > Tools > Event Viewer > Windows Logs > Security) ja epäonnistuneet kirjautumiset näkyivät Audit failurena: Event ID:llä 4771 Kerberos Authentication Service: Kerberos pre-authentication failed.

Loki on täynnä logon/logout-merkintöjä silloinkin, kun ei kirjauduta, johtuen ehkä virtuaaliympäristöstä.

15.4 Ohjauspaneelin poisto käyttäjiltä Aloitus-menusta

Lisättiin uusi Poista Control Panel -GPO Group Policy Objects -kohdan alle (Server Manager > Tools > Group Policy Management) ja editoitiin sitä (Edit > User Configuration > Policies > Administrative Templates > Start Menu and Taskbar > Remove programs on Settings menu: Enable). Linkitetään GPO koko Physioon (Link an Existing GPO…). Annettiin komentokehotteessa komento gpupdate.exe /force. Ohjauspaneeli ei näkynyt Henni Hierojalla Aloitus-valikosta mutta sen saa haulla edelleen käyttöön, joten poistetaan GPO hyödyttömänä.

15.5 Viimeisen käyttäjän piilotus

Viimeksi työasemaan kirjautuneen käyttäjän tunnus ei pitäisi olla näkyvissä kun seuraava käyttäjä kirjautuu. Lisättiin uusi Hide last logged user -GPO Group Policy Objects -kohdan alle (Server Manager > Tools > Group Policy Management) ja linkitettiin se Työasemat -yksikköön (Link an Existing GPO…). Editoitiin sitä (Edit > Computer Configuration > Policies > Windows Settings >Security Settings > Local Policies > Security Options> Interactive logon: Don’t display last signed-in, Enable). Annettiin komentokehotteessa komento gpupdate.exe /force kaksi kertaa ja käynnistettiin työasema kaksi kertaa, minkä jälkeen asetus tuli voimaan ja edellistä käyttäjää ei enää näkynyt.

Sammutettiin työasema ja palvelin sekä otettiin snapshotit 20250206 ja varmuuskopioitiin ulkoiselle kovalevylle.

16 Powershell

Powershell on komentotulkki ja -kieli, jolla voidaan automatisoida hallintatehtäviä (Microsoft, Microsoft Learn PowerShell, 2025), kuten käyttäjätilien luominen, päivitysten hallinta tai lokien tarkastelu. Harjoiteltiin sen käyttöä esimerkkien (Microsoft, Microsoft Learn, Windows, PowerShell, ActiveDirectory, 2025) ja ChatGPT:n avulla.

16.1 Käyttäjien haku nimen mukaan

Kokeiltiin komentoa, jolla haetaan kaikki käyttäjät, joilla on ”henni” nimessä:

```
Get-ADUser -Filter 'Name -like "*henni*"' | Format-Table Name,SamAccountName -A
```

Tuloksena saatiin:

```
Name        SamAccountName
```

Henni Hieroja henni.hieroja

16.2 Tietyn käyttäjän tietojen haku

Kokeiltiin komentoa, jolla saadaan Hennin tiedot:

Get-ADUser -Identity henni.hieroja -Properties *

Tässä esitellään vain osa tuloksista:

CanonicalName : amidom.local/Physio/Helsinki/Hoitola/Henni Hieroja

DisplayName : Henni Hieroja

DistinguishedName : CN=Henni Hieroja,OU=Hoitola,OU=Helsinki,OU=Physio,DC=amidom,DC=local

HomeDirectory : \\server01\home$\henni.hieroja

MemberOf : {CN=Hoitajat,OU=Ryhmät,OU=Physio,DC=amidom,DC=local}

ObjectCategory : CN=Person,CN=Schema,CN=Configuration,DC=amidom,DC=local

ObjectClass : user

PrimaryGroup : CN=Domain Users,CN=Users,DC=amidom,DC=local

SamAccountName : henni.hieroja

UserPrincipalName : henni.hieroja@amidom.local

16.3 Tietyn OU:n käyttäjien haku

Kokeiltiin komentoa, jolla haetaan tiettyyn OU:hun kuuluvat käyttäjät:

Get-ADUser -Filter * -SearchBase "OU=Hoitola,OU=Helsinki,OU=Physio,DC=amidom,DC=local"

Tuloksena saatiin oikeat Henni Hieroja ja mallikäyttäjä.

16.4 Käyttäjän lisääminen

Lisättiin käyttäjä Henri Fyssari ChatGPT:n avulla:

Määritä template-käyttäjä ja uuden käyttäjän tiedot

$templateUser = Get-ADUser -Identity "template.hoitola" -Properties *

$newUserSam = "henri.fyssari" # Uuden käyttäjän käyttäjätunnus

$newUserName = "Henri Fyssari" # Uuden käyttäjän koko nimi

```
$newUserOU = "OU=Hoitola,OU=Helsinki,OU=Physio,DC=amidom,DC=local"  # Kohde-OU

# Luo uusi käyttäjä kopioimalla templatesta tietyt arvot

New-ADUser -SamAccountName $newUserSam `

   -Name $newUserName `

   -UserPrincipalName "$newUserSam@amidom.local" `

   -GivenName $templateUser.GivenName `

   -Surname $templateUser.Surname `

   -DisplayName $newUserName `

   -Title $templateUser.Title `

   -Department $templateUser.Department `

   -Office $templateUser.Office `

   -EmailAddress "$newUserSam@amidom.local" `

   -Path $newUserOU `

   -AccountPassword (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force) `

   -Enabled $true

Add-ADGroupMember -Identity "Hoitajat" -Members $newUserSam
```

Onnistumista tarkasteltiin komennolla:

```
Get-ADUser -Filter 'Name -like "*henri*"' | Format-Table Name,SamAccountName -A
```

Tuloksena saatiin:

```
Name        SamAccountName

Henri Fyssari henri.fyssari
```

Henri Fyssari löytyi myös ADUC:sta, mutta etunimi ja sukunimi olivat suoraan mallikäyttäjältä. Vaihdettiin ne oikeiksi komennolla:

```
Set-ADUser -Identity henri.fyssari -Replace @{GivenName="Henri"; sn="Fyssari"}
```

Käynnistettiin työasema ja kirjautuminen onnistui henri.fyssari-tunnuksella.

Sammutettiin työasema ja palvelin sekä otettiin palvelimesta snapshot 20250207 ja varmuuskopioitiin ulkoiselle kovalevylle.

17 Jatkoehdotukset

Käyttöoikeuksien hallintaa ja delegointia voisi vielä tehdä. Restricted Groups Policya voidaan käyttää delegoitaessa järjestelmänvalvojan oikeuksia työasemille. Group Policy Objecteja voisi vielä lisätä,

esimerkiksi ohjelmien poisto ja asennus, siirrettävien tallennusvälineiden käytön esto sekä sen varmistus, ettei käyttäjä pääse käsiksi tietoturva- ja palomuuriasetuksiin. Powershellia voisi harjoitella lisää.

Toimialueympäristön lisäksi voitaisiin suunnitella laitehallinta pilveen. Hallintaa voitaisiin siis toteuttaa pilvipalveluna M365 Admin Centerin kautta. Tällöin ympäristönä toimisi Microsoft Developer E5 -testiympäristö.

Lähdeluettelo

Microsoft. (7. Helmikuu 2025). *Microsoft Learn PowerShell*. Noudettu osoitteesta https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.5

Microsoft. (7. Helmikuu 2025). *Microsoft Learn, Windows, PowerShell, ActiveDirectory*. Noudettu osoitteesta https://learn.microsoft.com/en-us/powershell/module/activedirectory/?view=windowsserver2019-ps

OpenAI. (20. Tammikuu 2025). *ChatGPT*. Noudettu osoitteesta https://chatgpt.com/