AD – KÄSIKIRJA

1 Käsitteet

AD - Active Directory - Hakemistopalvelu
Keskitetty järjestelmä, joka hallinnoi käyttäjiä, tietokoneita ja verkkoresursseja.

DC - Domain Controller - Toimialueen ohjain
Toimialueen ohjain on AD-palvelin, joka kontrolloi koko yritys- tai organisaatioverkkoa. Ilman toimialueen ohjainta Active Directory -verkko ei toimisi.

OU - Organizational Unit
Organisaatioyksikkö on Active Directoryn looginen kansio, jolla ryhmitellään käyttäjiä, tietokoneita ja muita objekteja. Sen avulla voidaan kohdistaa ryhmäkäytäntöjä ja delegoida hallintaoikeuksia. OU helpottaa suurten IT-ympäristöjen hallintaa, mutta ei määritä käyttöoikeuksia itsessään.

GPO - Group Policy Object
Group Policy Object on kokoelma asetuksia, joilla hallitaan Windows-käyttäjien ja -tietokoneiden toimintaa. Sitä käytetään Active Directory -ympäristössä. GPO voidaan kohdistaa käyttäjiin, tietokoneisiin tai organisaatioyksiköihin. Sen avulla voidaan esimerkiksi estää USB-laitteet tai määrittää salasanasäännöt. GPO helpottaa keskitettyä IT-hallintaa.

DNS - Domain Name System
Domain Name System (DNS) on järjestelmä, joka muuntaa verkkotunnukset (esim. www.example.com) IP-osoitteiksi (esim. 192.0.2.1). Ilman DNS:ää käyttäjien pitäisi muistaa verkkosivujen IP-osoitteet. DNS helpottaa internetin käyttöä tekemällä osoitteista ymmärrettäviä ihmisille. Se toimii hajautetusti ja nopeasti eri puolilla maailmaa. DNS on olennainen osa internetin toimintaa.

LDAP - Lightweight Directory Access Protocol
LDAP on kevyt hakemistopalveluprotokolla, jota käytetään tietojen hakemiseen ja hallintaan hakemistopalvelimilta. Sitä käytetään esimerkiksi käyttäjätietojen hallintaan yritysverkoissa (kuten Active Directoryssa). LDAP mahdollistaa keskitetyn kirjautumisen ja käyttäjähallinnan.

FSMO - Flexible Single Master Operations
FSMO on joukko erityisiä rooleja, joita käytetään Active Directoryssa hallitsemaan tietokannan yhdenmukaisuutta ja estämään ristiriitoja.

FSMO-roolit jakautuvat useisiin rooleihin, kuten:

- **Schema Master** – hallitsee skeeman muutoksia
- **Domain Naming Master** – hallitsee verkkotunnuksen nimimuutoksia
- **RID Master** – jakaa tunnuksia (RID) käyttöön
- **PDC Emulator** – toimii pääasiallisena aikapalvelimena ja varmistaa yhteensopivuuden vanhempien Windows-versioiden kanssa
- **Infrastructure Master** – huolehtii tietojen synkronoinnista eri alueiden välillä

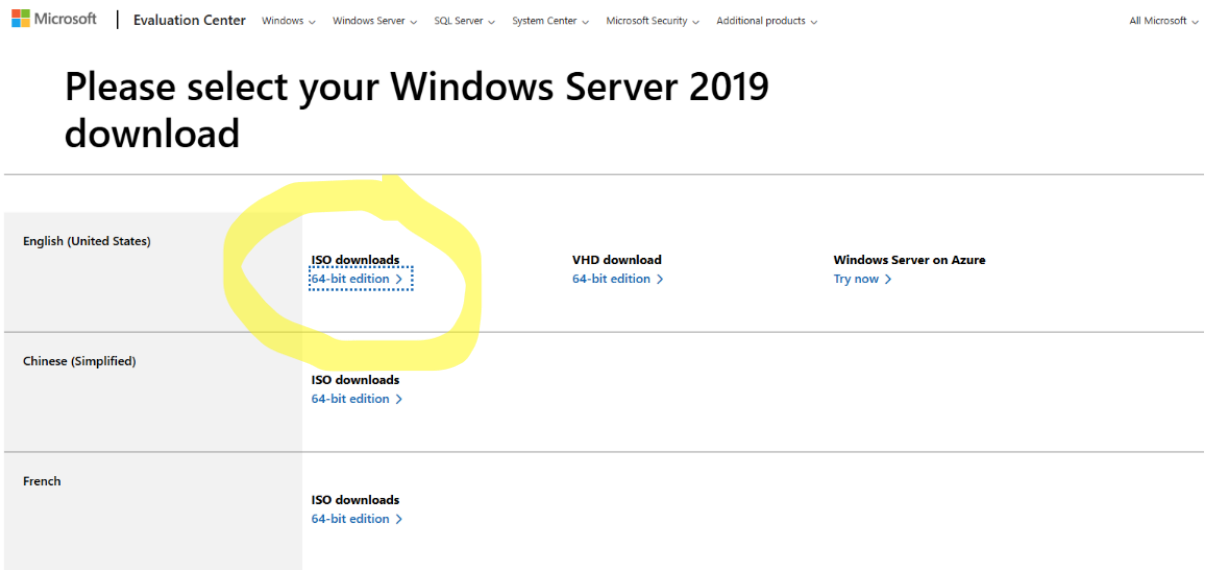
FSMO-roolit ovat tärkeitä Active Directoryn toiminnan varmistamiseksi.

GC - Global Catalog
Global Catalog on erityinen tietokanta, joka sisältää tiivistetyt tiedot kaikista Active Directoryn objekteista koko verkossa. GC nopeuttaa hakemista ja mahdollistaa käyttäjien ja resurssien etsimisen eri toimialueilta. Se on tärkeä monidomaini-ympäristöissä, joissa se parantaa hakutulosten nopeutta ja varmistaa oikeuksien hallinnan. NTDS - NT Directory Services

RSoP - Resultant Set of Policy
RSoP on työkalu, joka näyttää, miten ryhmäkäytännöt (Group Policy) vaikuttavat tiettyyn käyttäjään tai tietokoneeseen. Se laskee ja näyttää, mitkä politiikat ovat voimassa käyttäjän tai laitteen tilanteen mukaan, ottaen huomioon kaikki periytymiset ja päällekkäiset asetukset. RSoP:tä voidaan käyttää vianmääritykseen ja varmistamaan, että oikeat politiikat ovat käytössä.

2 Windows Serverin asennus

1. Lataa Microsoftin nettisivulta Windows Server ISO-tiedosto. Valitse vaihtoehto, joka on ympyröitynä kuvassa.



2. Avaa Hyper-V ja luo uusi virtuaalikone ISO-tiedostoa käyttäen.

Ohjeet virtuaalikoneen luontiin:

Luo uusi virtuaalikone

1. **Aloita uuden virtuaalikoneen luominen:**
    - Klikkaa oikealla puolella olevasta valikosta New ja valitse Virtual Machine.

2. **Seuraa ohjatun työkalun vaiheita:**
    - Nimi ja sijainti:
        - Anna virtuaalikoneelle nimi (esim. "WindowsServerVM").
        - Valitse haluamasi tallennuspaikka, jossa virtuaalikoneen tiedostot säilytetään. Oletusarvoisesti tiedostot tallennetaan C:\ProgramData\Microsoft\Windows\Hyper-V.
    - Generaatio:
        - Valitse Generation 1 (yhteensopivuus vanhempien käyttöjärjestelmien kanssa) tai Generation 2 (suositeltava nykyaikaisille käyttöjärjestelmille ja UEFI-bootille). Generation 2 tukee UEFI:ta ja Secure Bootia, mutta se saattaa vaatia yhteensopivia käyttöjärjestelmiä.

- Muisti:
  - Määritä virtuaalikoneelle muistimäärä (esim. 4 GB). Voit valita myös "Use dynamic memory for this virtual machine" -valinnan, jolloin muistia varataan dynaamisesti tarpeen mukaan.

- Verkkoyhteys:
  - Valitse verkko. Yleensä voit valita oletusverkon, jos Hyper-V on liitetty tietokoneeseesi.

- Virtuaalikova levy:
  - Valitse "Create a virtual hard disk" ja määritä sen koko (esim. 40 GB).
  - Voit myös valita olemassa olevan virtuaalikovan (jos sinulla on sellainen).

- Asennusvaihtoehdot:
  - Valitse asennustapa:
    - Install an operating system from a bootable image file: Valitse tämä, jos haluat asentaa käyttöjärjestelmän ISO-tiedostosta.
    - Liitä lataamasi ISO-tiedosto tähän.

3. **Viimeistele ja luo virtuaalikone:**
   - Tarkista asetukset ja klikkaa Finish.

4. Käynnistä virtuaalikone

- Virtuaalikone on nyt luotu ja näkyy Hyper-V Managerissa.
- Valitse virtuaalikone ja klikkaa Start (Käynnistä).
- Klikkaa Connect (Yhdistä), jolloin virtuaalikone avautuu ja voit aloittaa käyttöjärjestelmän asennuksen.

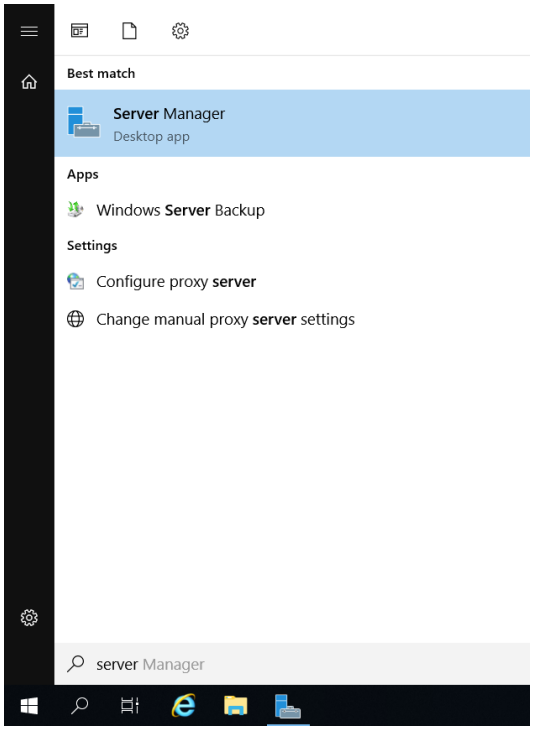
5. Asenna käyttöjärjestelmä

- Valitse valikosta ”Windows Server Desktop Experience” ja seuraa normaalisti käyttöjärjestelmän asennusprosessia.

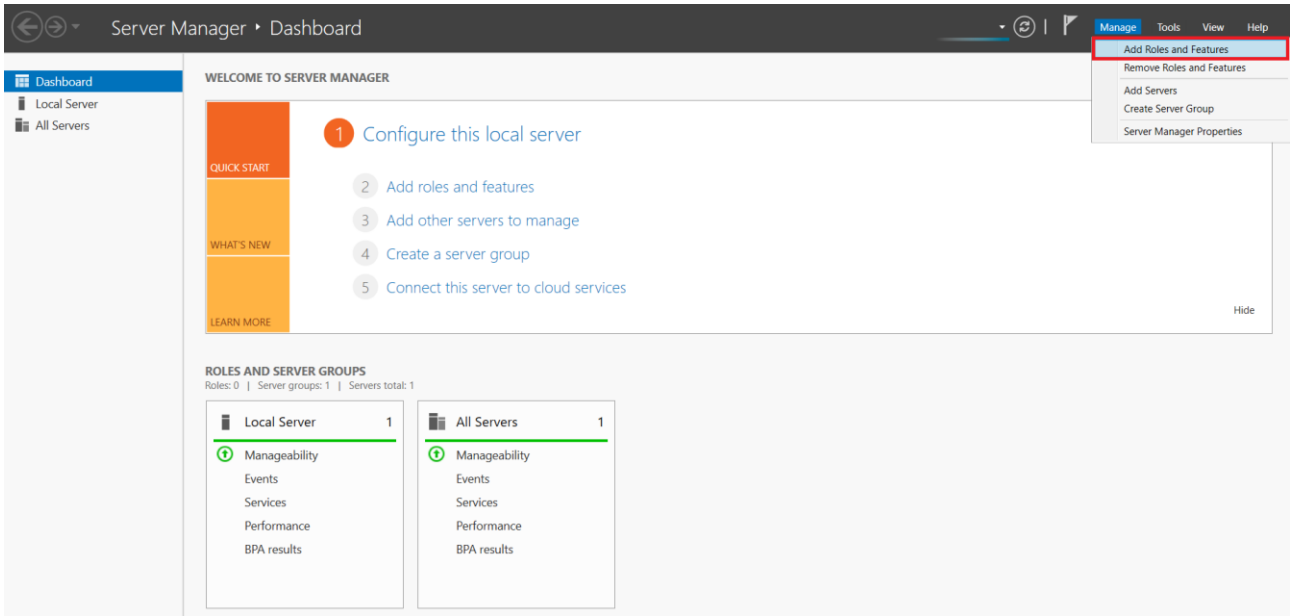
3 Palvelinroolit

Palvelinroolien päälle laittaminen ja Palvelimen promotoiminen DC-palvelimeksi.
Tein tämän käyttäen alla olevia ohjeita.

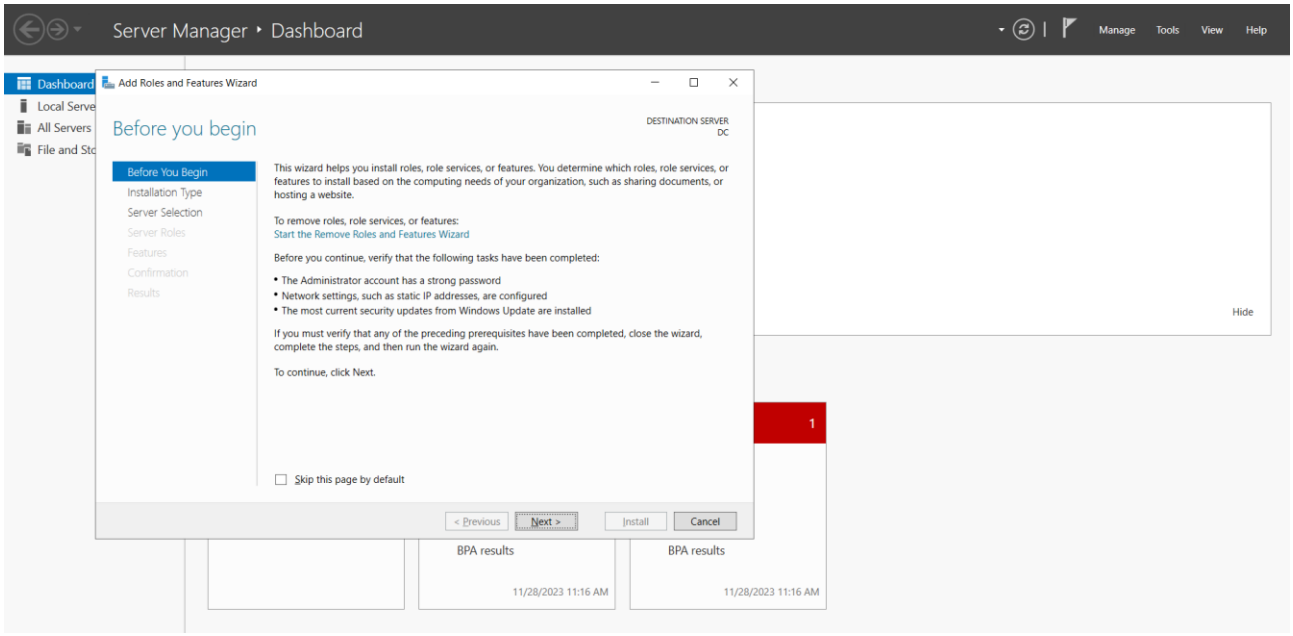
1. Avaa Server Manager



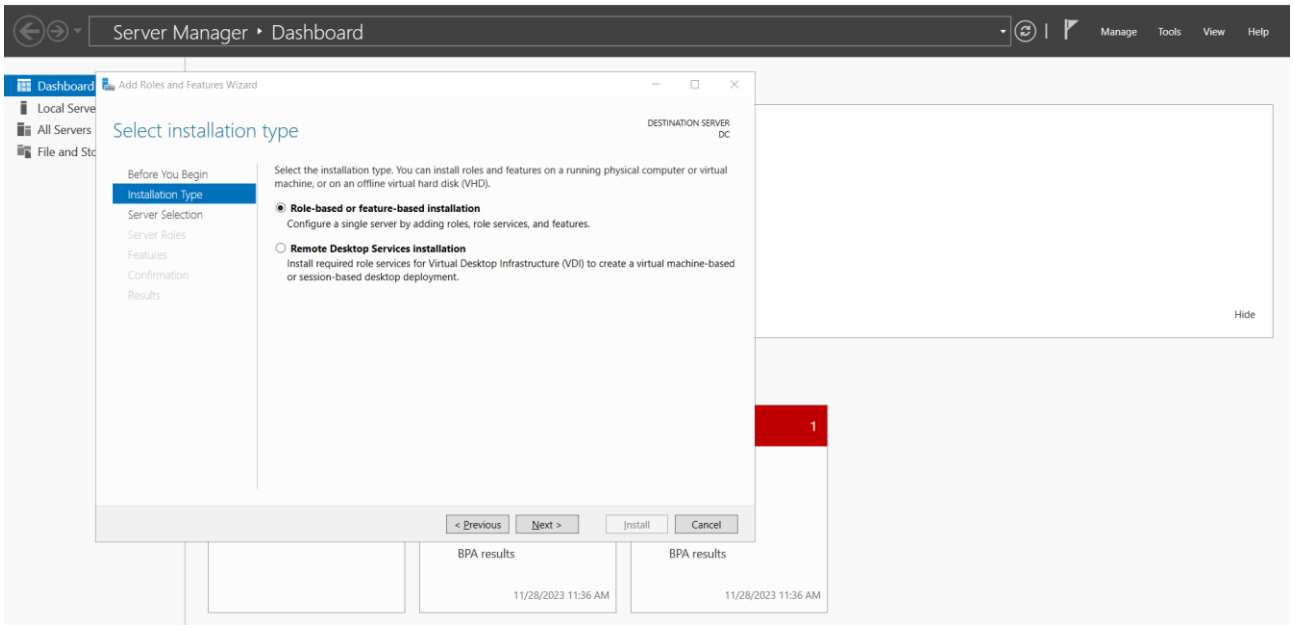
2. Valitse **“Manage”** oikealta ylävalikosta ja sitten valitse **”Add roles and features”**.



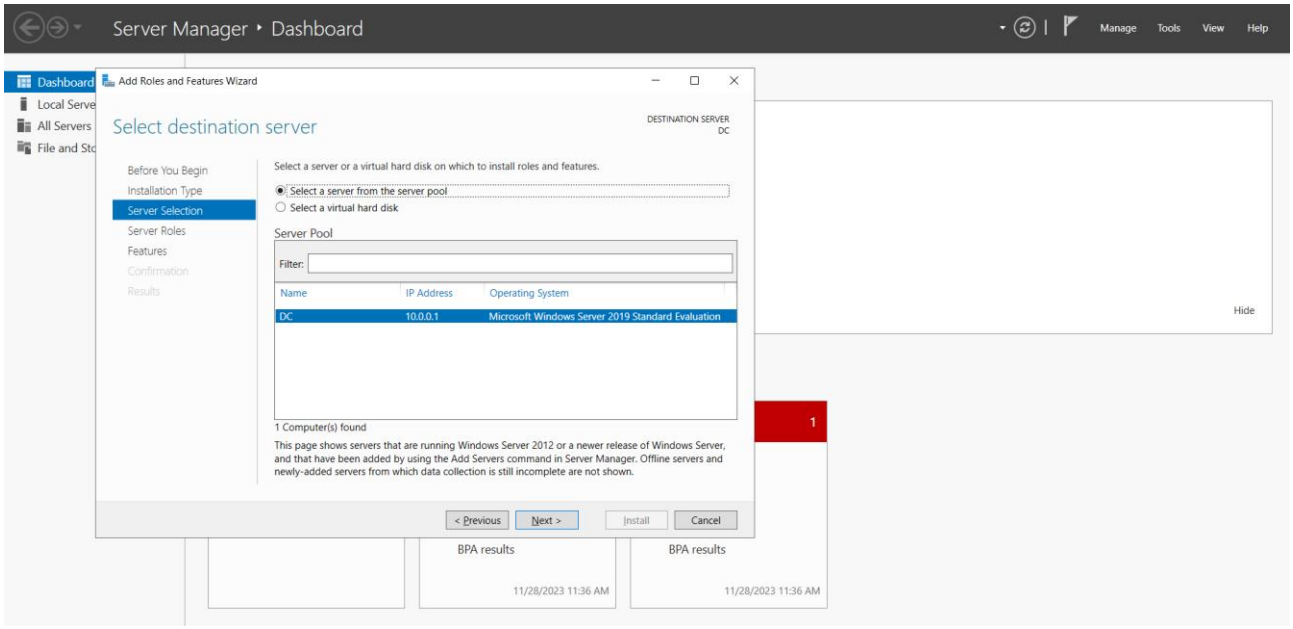
3. Tarkista tarvittavat tehtävät ja paina **”Next”**.



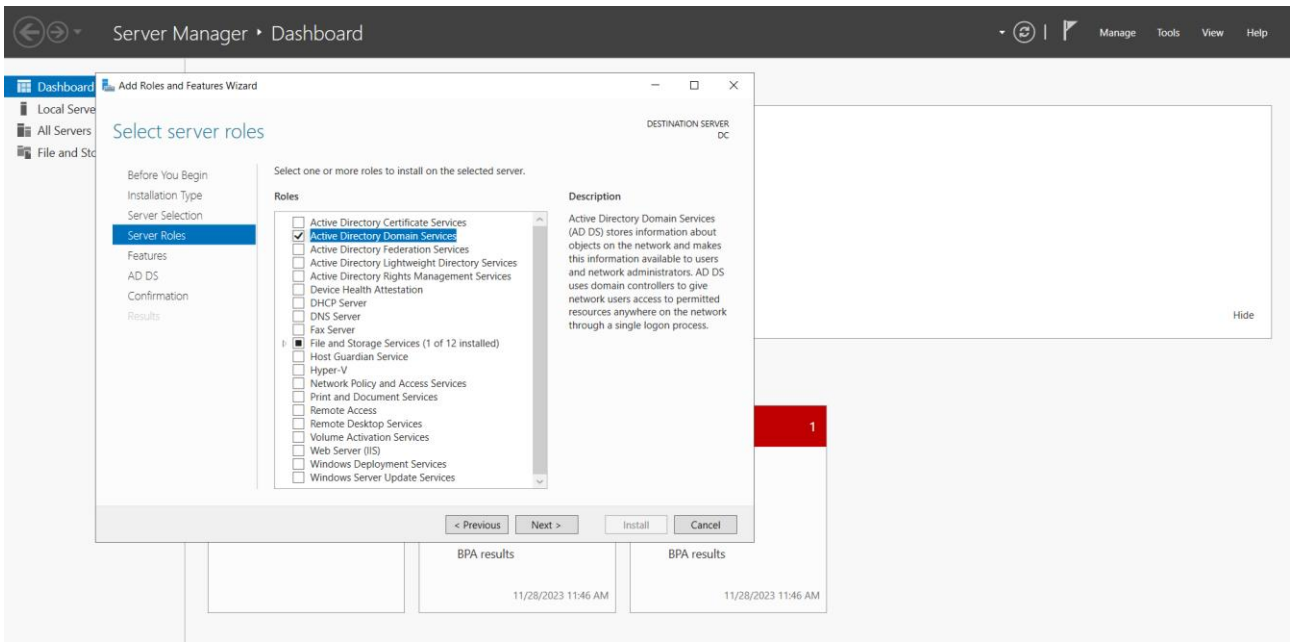
4. Valitse asennustapa:” Role**-based or feature based installation”** ja paina **“Next”**.



5. Määritä palvelinvalintasi ja roolisi: Valitse palvelimesi kohdasta **”Server Pool”** ja paina **”Next”**.



6. Valitse palvelinroolit: **“Active Directory Domain Services”** ja **“DNS Server”** ja paina **“Next”**.

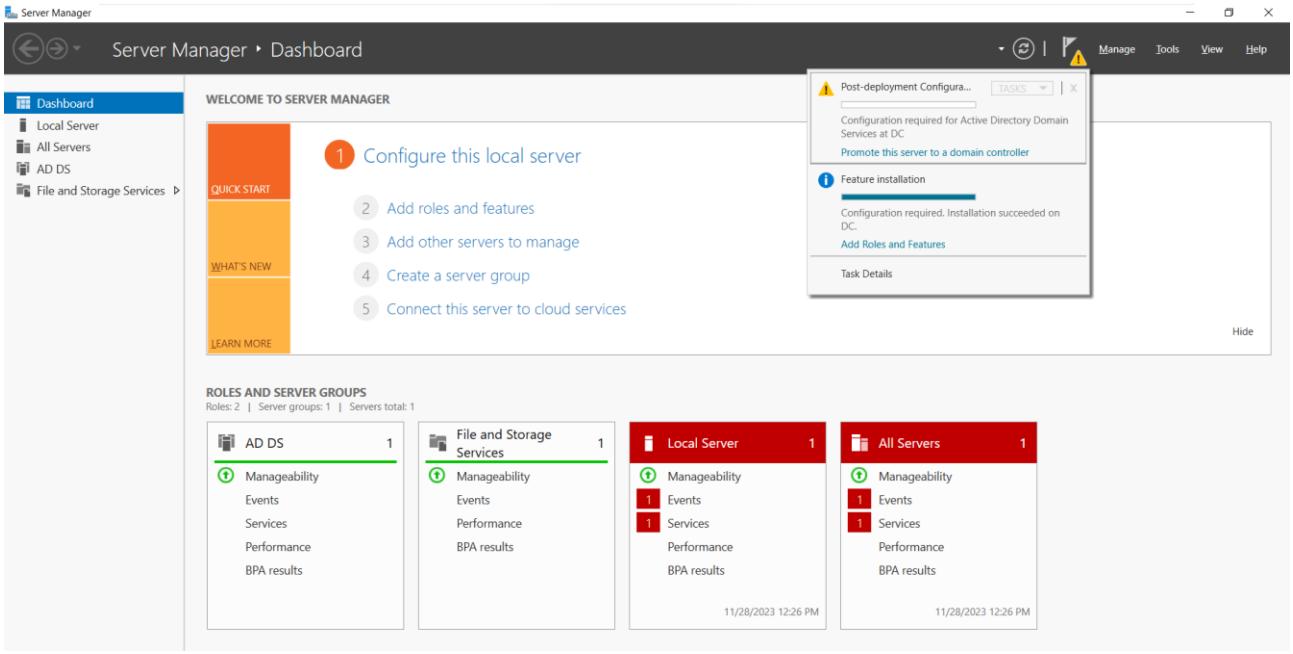


7. Asennuksen yhteenvedon vahvistus: Paina **”Install”** - painiketta. Kun asennus on valmis paina **”Close”**.

Palvelimen promotoiminen DC-palvelimeksi:

Root domain name: METSANVARTIJA.COM
NetBIOS-nimi: METSANVARTIJA

1. Avaa ”Server Manager”. Etsi oikeasta yläkulmasta lippukuvake, napsauta sitä ja valitse sitten ” **Promote this server to a domain controller”**.

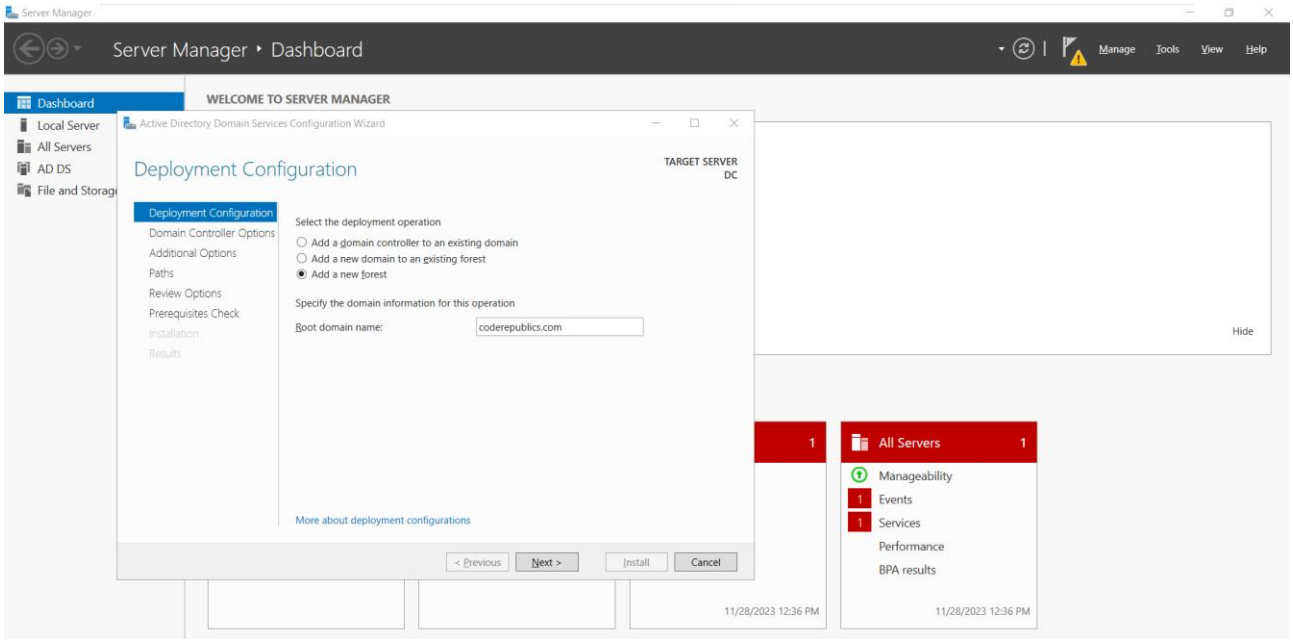


2. Valitse käyttöönottoasetukset:

Käyttöönoton määritysten ponnahdusikkunassa on kolme vaihtoehtoa: liittyminen olemassa olevaan verkkotunnukseen, uuden verkkotunnuksen lisääminen olemassa olevaan metsään tai uuden metsän lisääminen.

- **Add a domain controller to an existing domain:** Tällä asetuksella suoritetaan lisätoimialueen ohjauskoneen asennus olemassa olevaan toimialuerakenteeseen.
- **Add a new domain to an existing forest:** Tällä asetuksella asennetaan aliverkkotunnus olemassa olevaan verkkotunnusrakenteeseen.
- **Add a new forest:** Tällä asetuksella asennetaan uusi verkkotunnus.

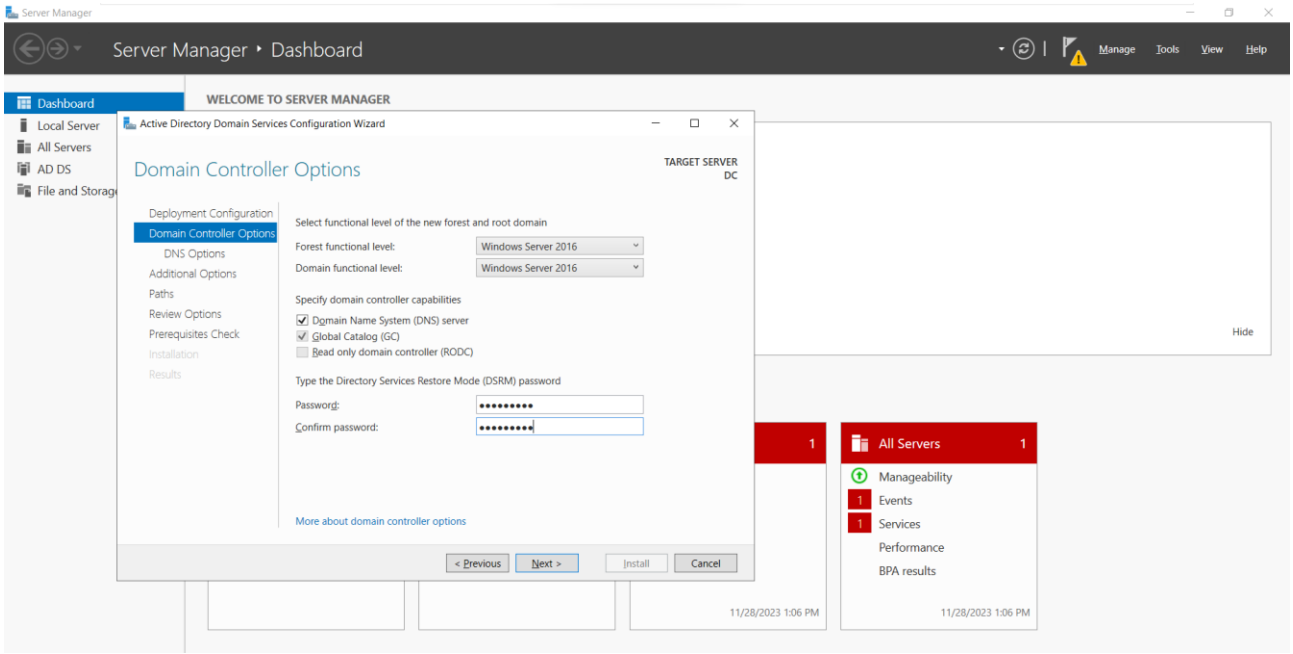
Koska asennamme verkkomme ensimmäistä toimialueen ohjainta, valitse viimeinen vaihtoehto. Napsauta ” **Add a new forest”** .



3. Valitse toimialue ja metsän toiminnallinen taso:

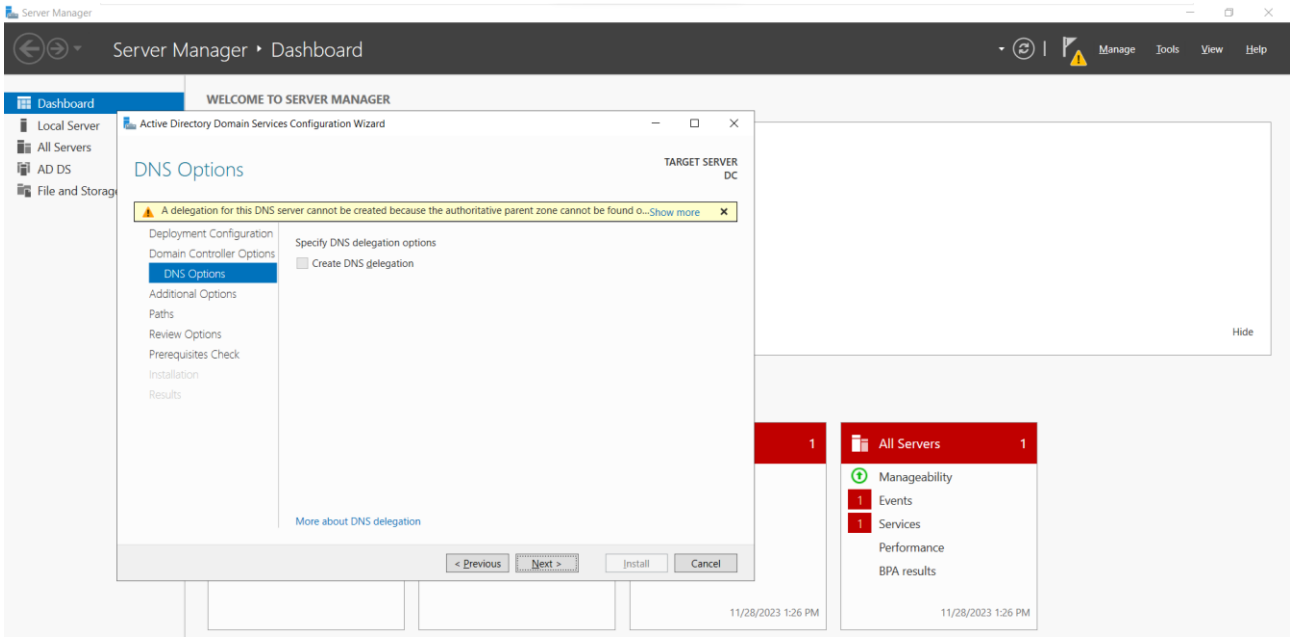
Toiminnalliset tasot määrittelevät Active Directory -toimialuepalveluiden (AD DS) toimialueilla tai metsissä käytettävissä olevat ominaisuudet. Ne myös määrittävät, mitä Windows Server -käyttöjärjestelmiä voit käyttää toimialueen tai metsän ohjauskoneissa.

Huomautus: Toiminnalliset tasot eivät vaikuta siihen, mitä käyttöjärjestelmiä voit käyttää toimialueeseen tai metsään liitetyillä työasemilla ja jäsenpalvelimilla. Valitse vanhempia vaihtoehtoja vain, jos toimialueellasi tai metsässäsi on vanhempia toimialueen ohjaimia.



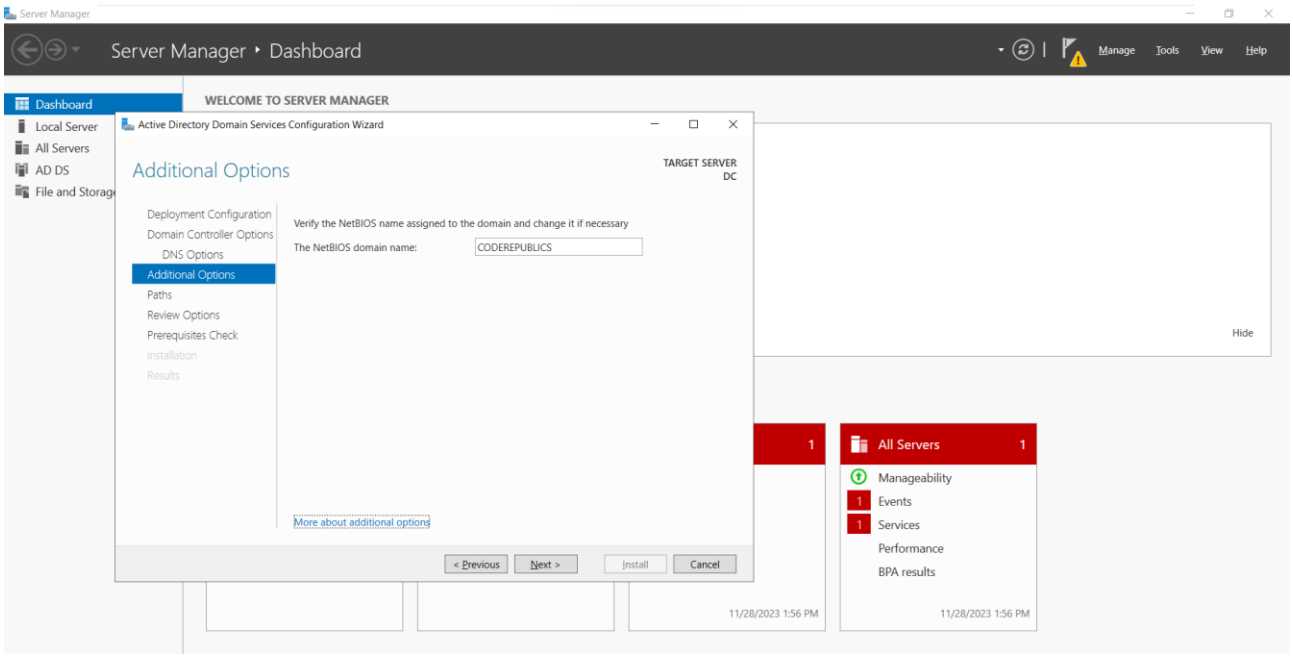
4. DNS-delegointi:

DNS-asetuksessa näet nyt varoitusviestin ”A delegation for this DNS server cannot be created because the authoritatable parent zone cannot be found...” (Tämän DNS-palvelimen delegointia ei voida luoda, koska auktoriteettista päävyöhykettä ei löydy...). Tämä varoitus johtui DNS-palvelimen puuttumisesta ympäristöstä, eikä valtuutusta Coderepublics.com-vyöhykkeen käyttämiseen ulkoisesta ympäristöstä (Internetistä) ole myönnetty tällä DNS-palvelimella. Voit ohittaa tämän varoituksen, koska kyseessä on ensimmäisen metsäsi verkkotunnus.



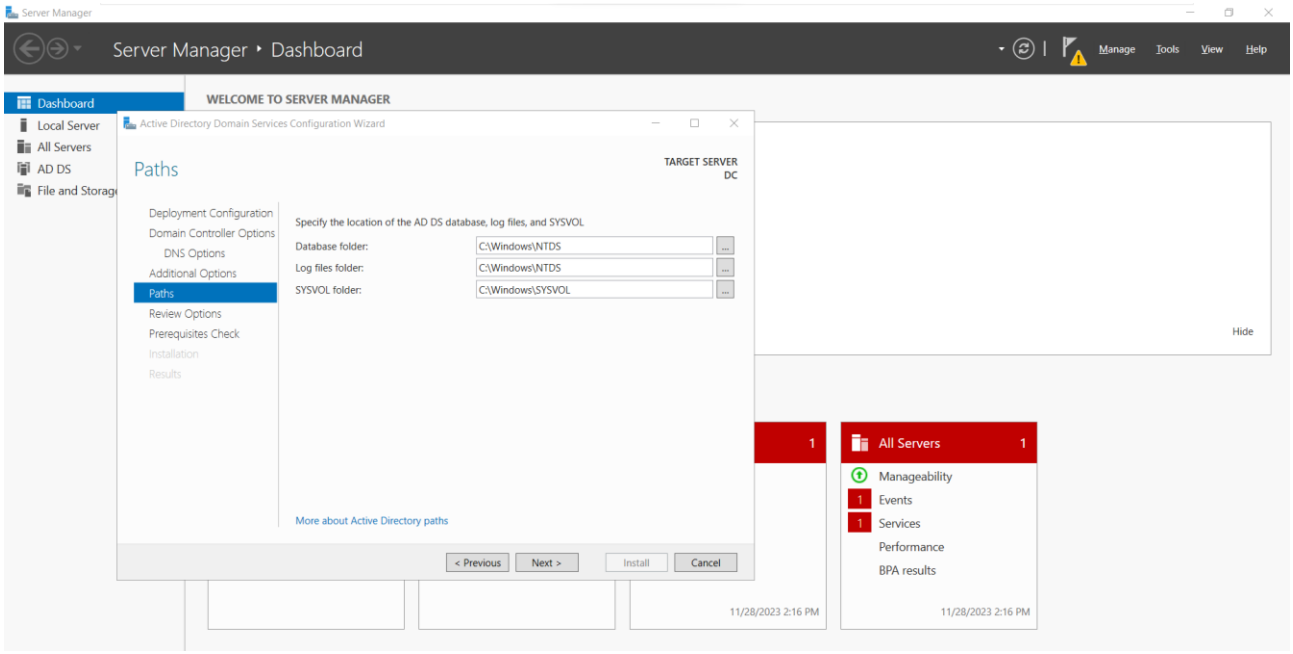
5. Valitse NetBIOS-nimi:

Se on lyhenne sanoista Network Basic Input / Output System. NetBIOS-nimi pysyy samana kuin verkkotunnuksen määritysvaiheessa määritimme.



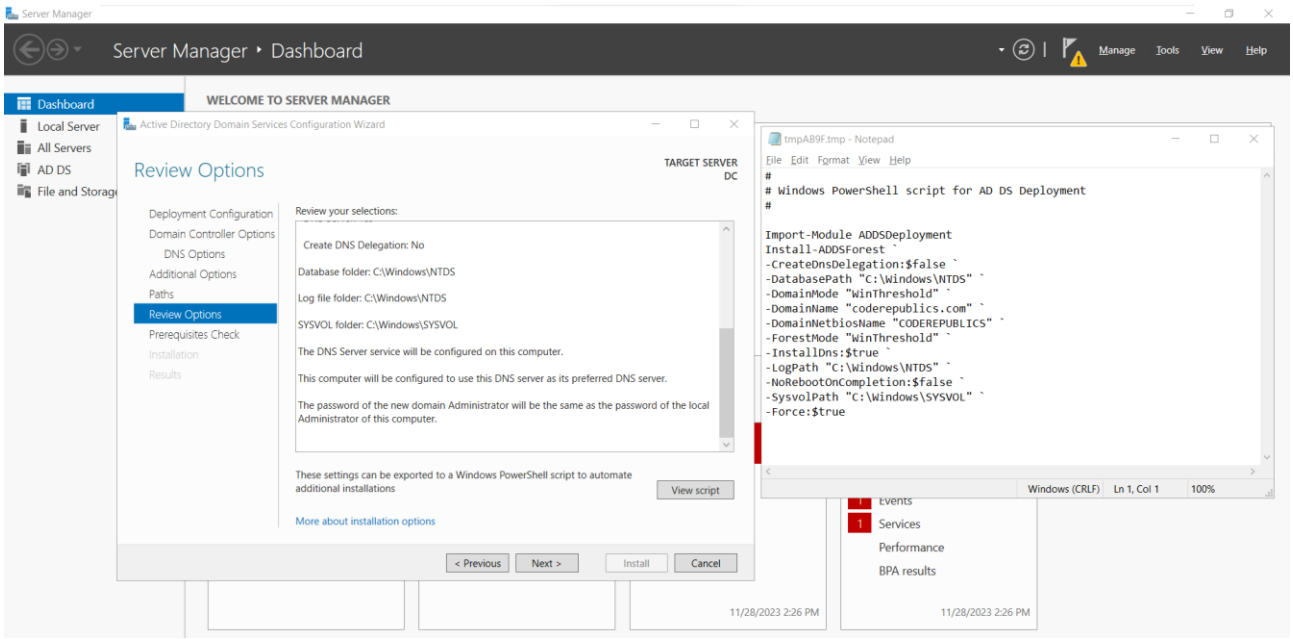
6. Polun valinta:

- **Tietokannan kansio:** Active Directory tallentaa tietonsa NTDS.DIT-tiedostoon, joka sijaitsee järjestelmän päähakemiston NTDS-kansiossa, yleensä C:\Windows\NTDS-kansiossa.
- **Lokitiedostokansio:** Täällä sijaitsee NTDS.dit-tietokannan lokitiedosto.
- **SYSVOL-kansio:** Jaettu kansio, joka tallentaa ryhmäkäytäntötiedot sekä kirjautumis- ja uloskirjautumisskriptit.



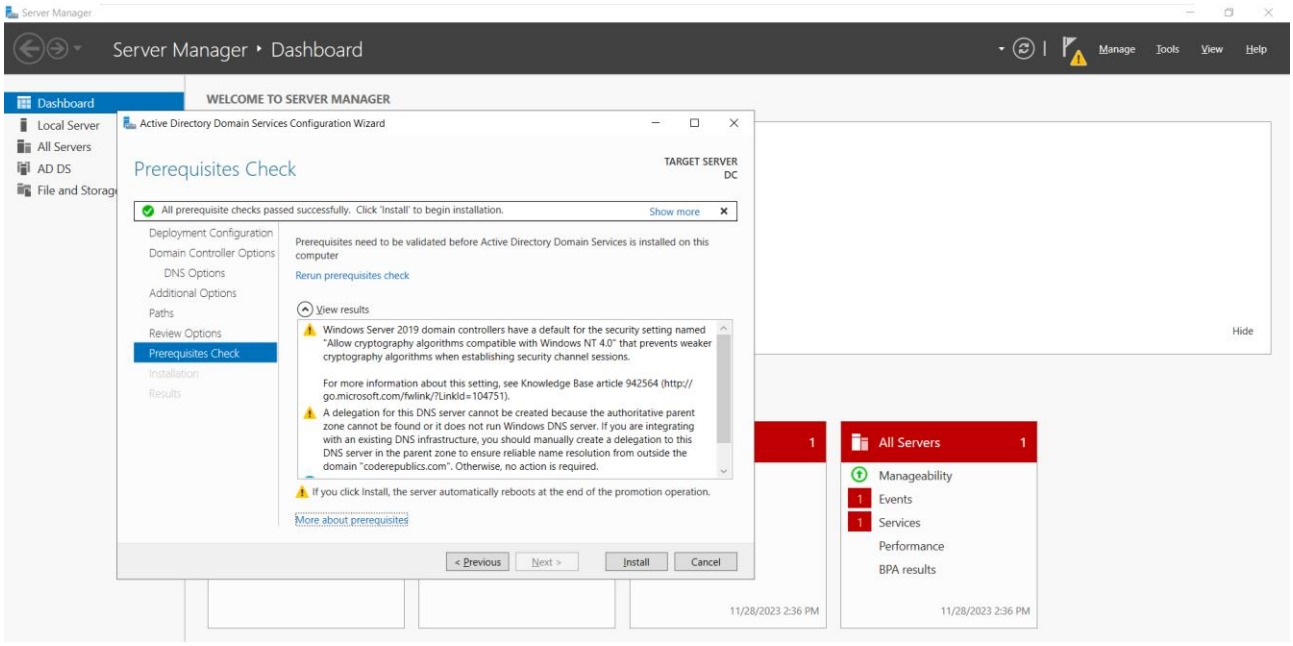
7. Arviointivaihtoehto:

Täällä näet tekemäsi asetuksen tai muutoksen. Voit myös napsauttaa "näytä skripti" -painiketta (PowerShell-skripti Active Directoryn asentamiseksi).

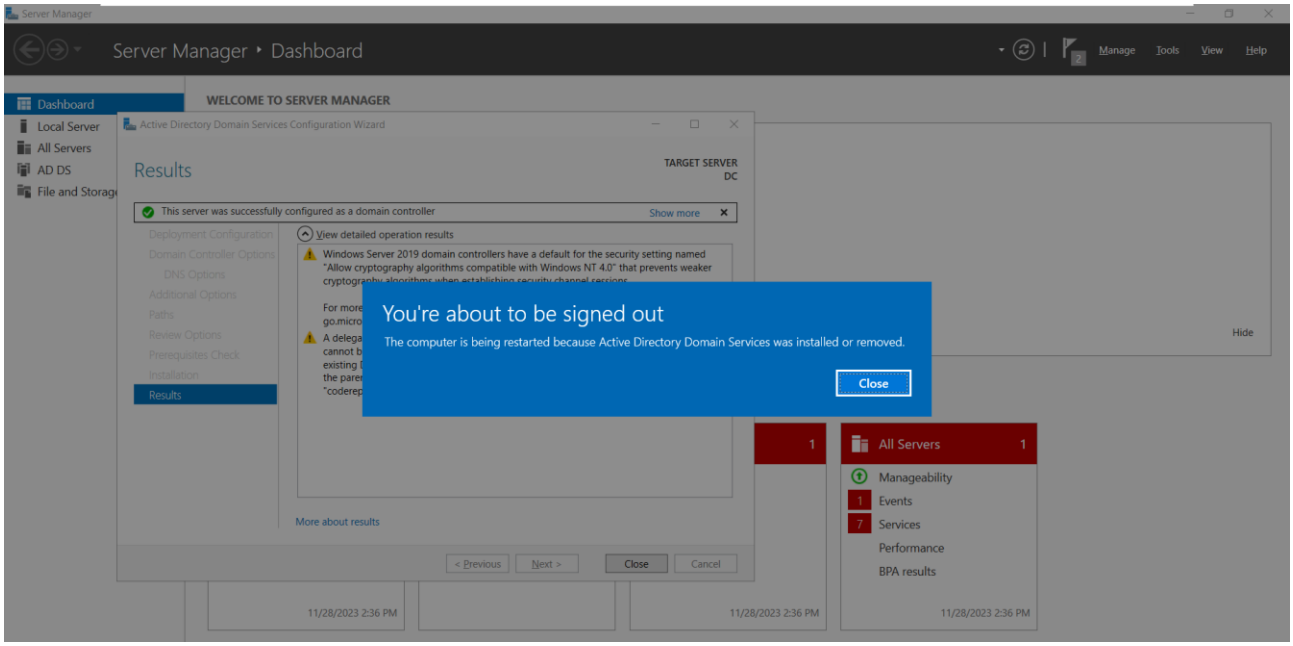


8. Edellytysten tarkistus:

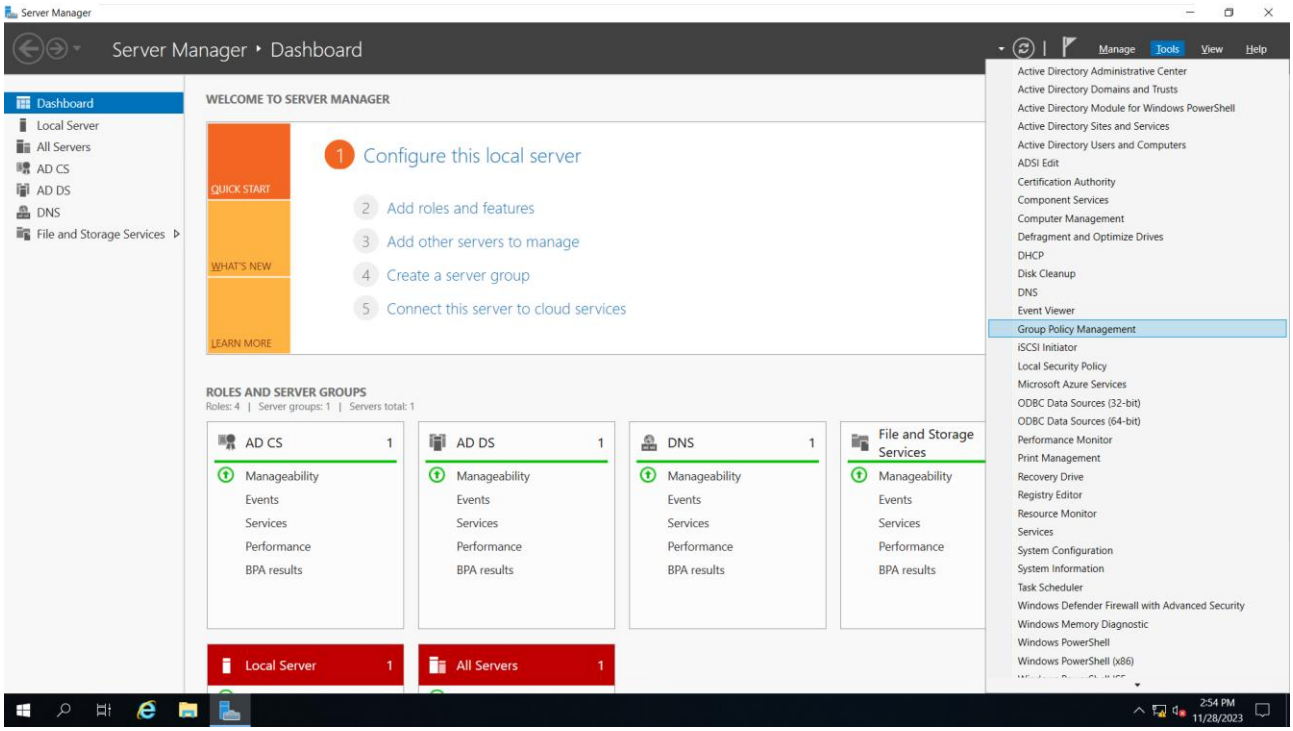
Tämä on yksi viimeisistä vaiheista ennen palvelimen asentamista ja edistämistä Domeeni ohjaimena. Jos kaikki on kunnossa ilman virheitä, voit napsauttaa asennuspainiketta. Näin vältät tietoturvailmoitukset ja DNS-delegoinnin varoituksen. Varmista vain, että ruudussa on vihreä rasti, jossa lukee *"Kaikki esivaatimukset tarkistukset suoritettiin onnistuneesti"*.



Asennus vie aikaa ja palvelin käynnistyy automaattisesti uudelleen asennuksen valmistuttua.

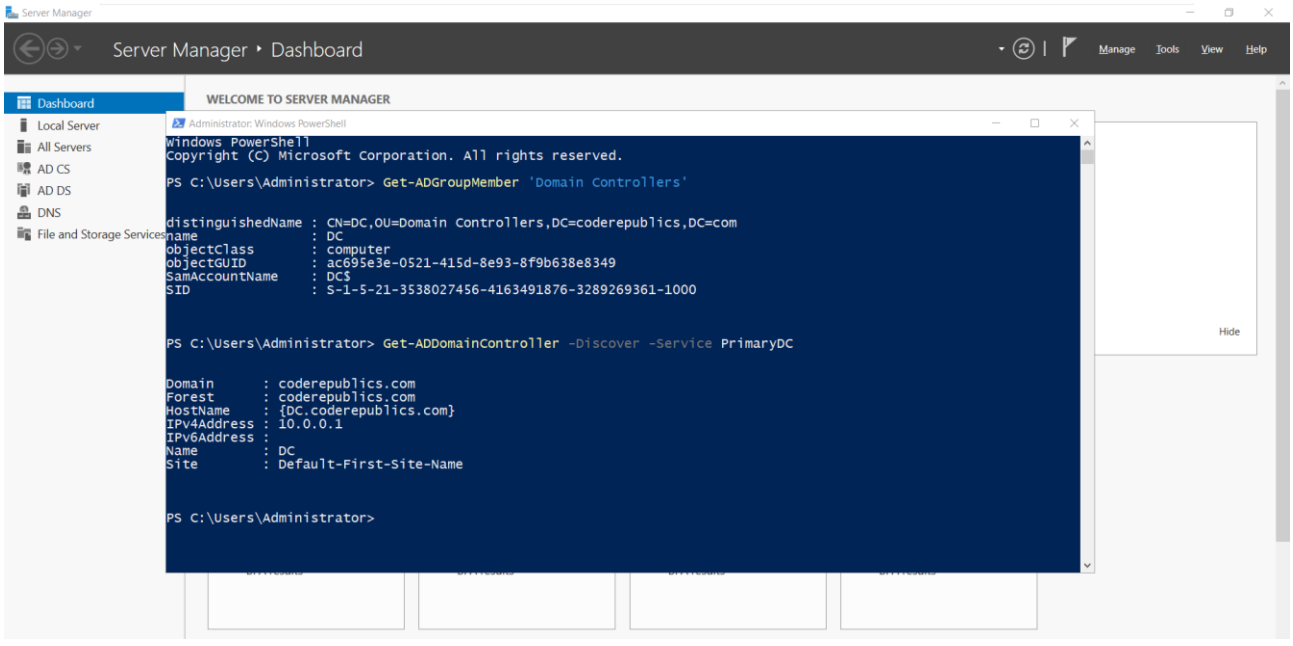


Kun järjestelmä on käynnistynyt uudelleen, kirjaudu sisään järjestelmänvalvojan tunnuksilla ja avaa **”Server Manager”** ja valitse sitten **”Tools”**. Näet ryhmäkäytäntöjen hallinnan. Tämä on ominaisuus, jonka valitsimme vaiheessa. **”6. Select features”**, Tämä tarkoittaa, että palvelin on onnistuneesti siirretty toimialueen ohjauskoneeksi.



Saadaksesi tietoja toimialueen ohjauskoneestasi, nämä komennot näkyvät PowerShellissä.

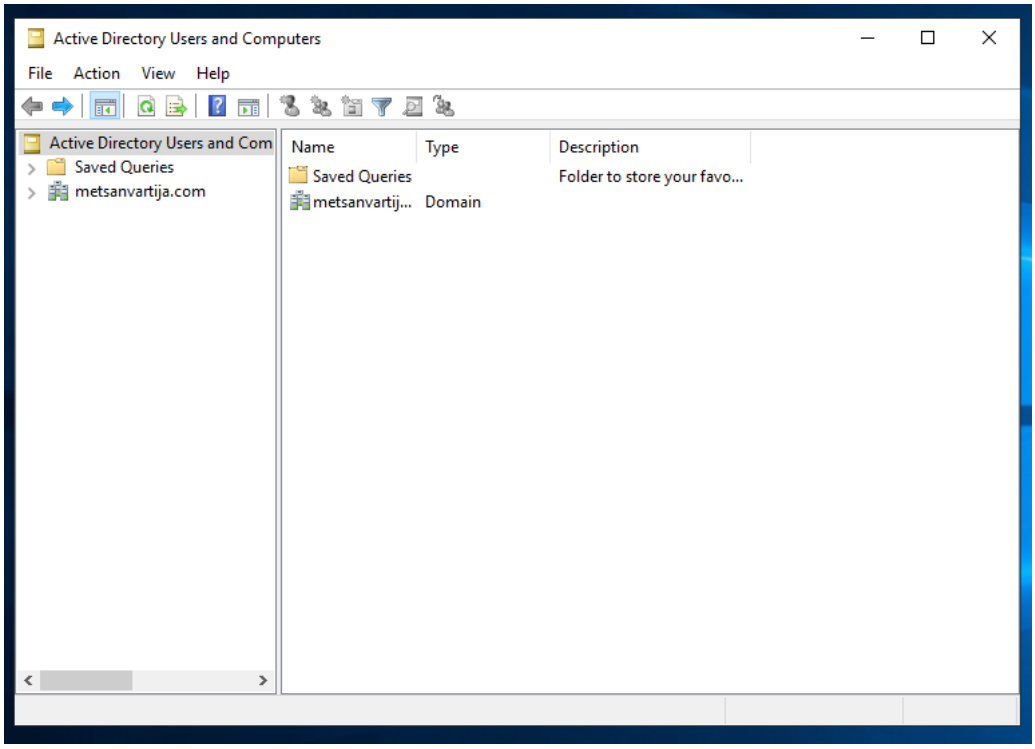
- *Get-ADGroupMember 'Domain Controllers'*
- Get-ADDomainController -Discover -Services PrimaryDC



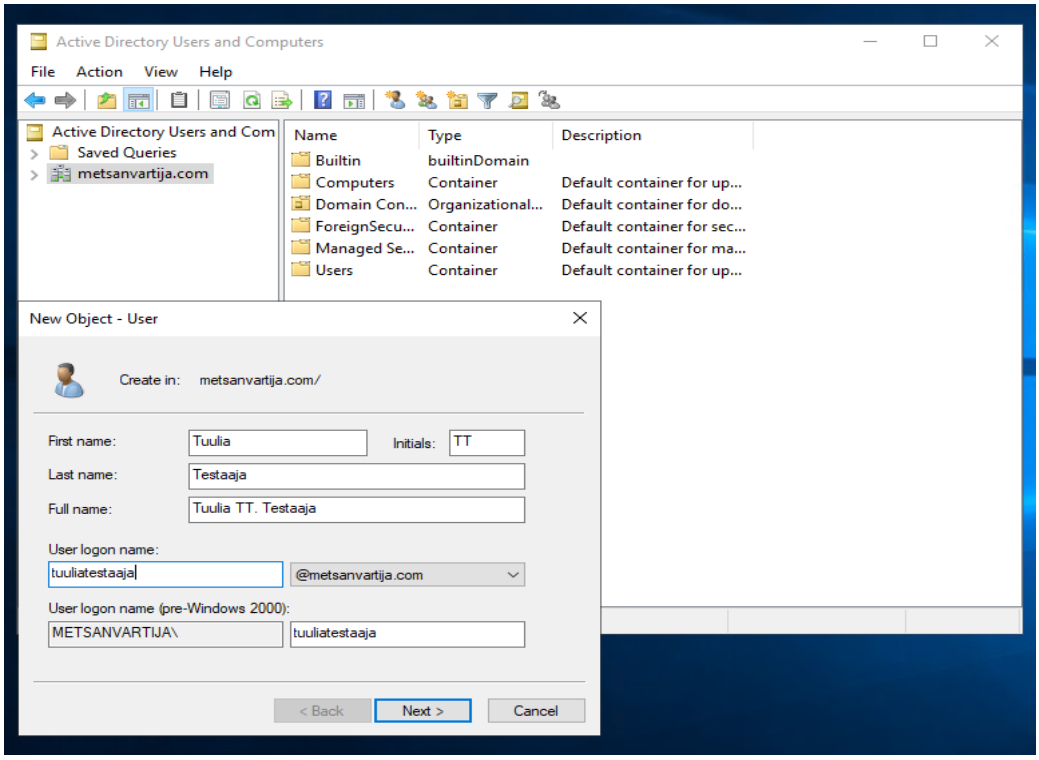
4 Käyttäjien luominen

Loin käyttäjät tämän ohjevideon mukaan:
https://www.youtube.com/watch?v=UPDDuZP_zi0

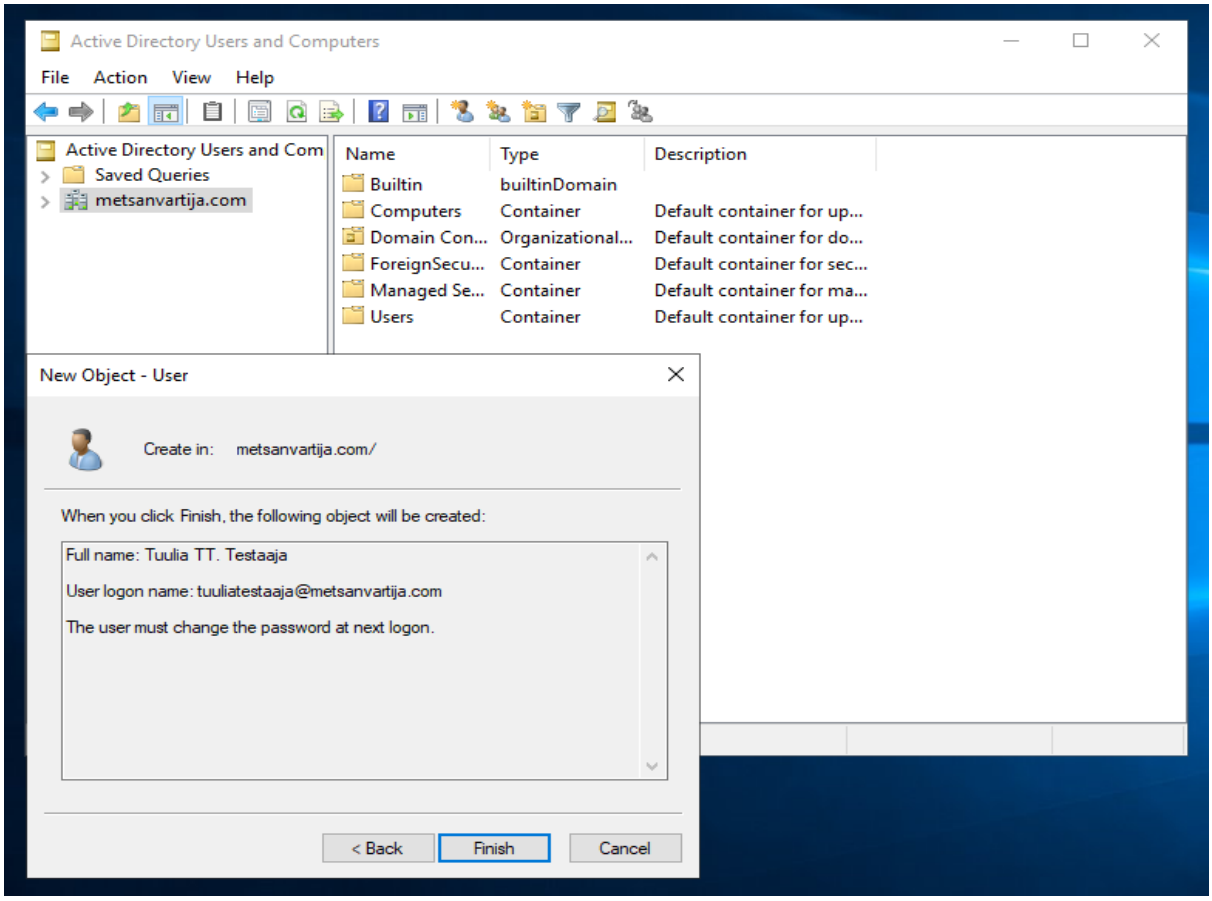
1. Avasin Domain Controllerin ja valitsin metsanvartija.com Domainin.



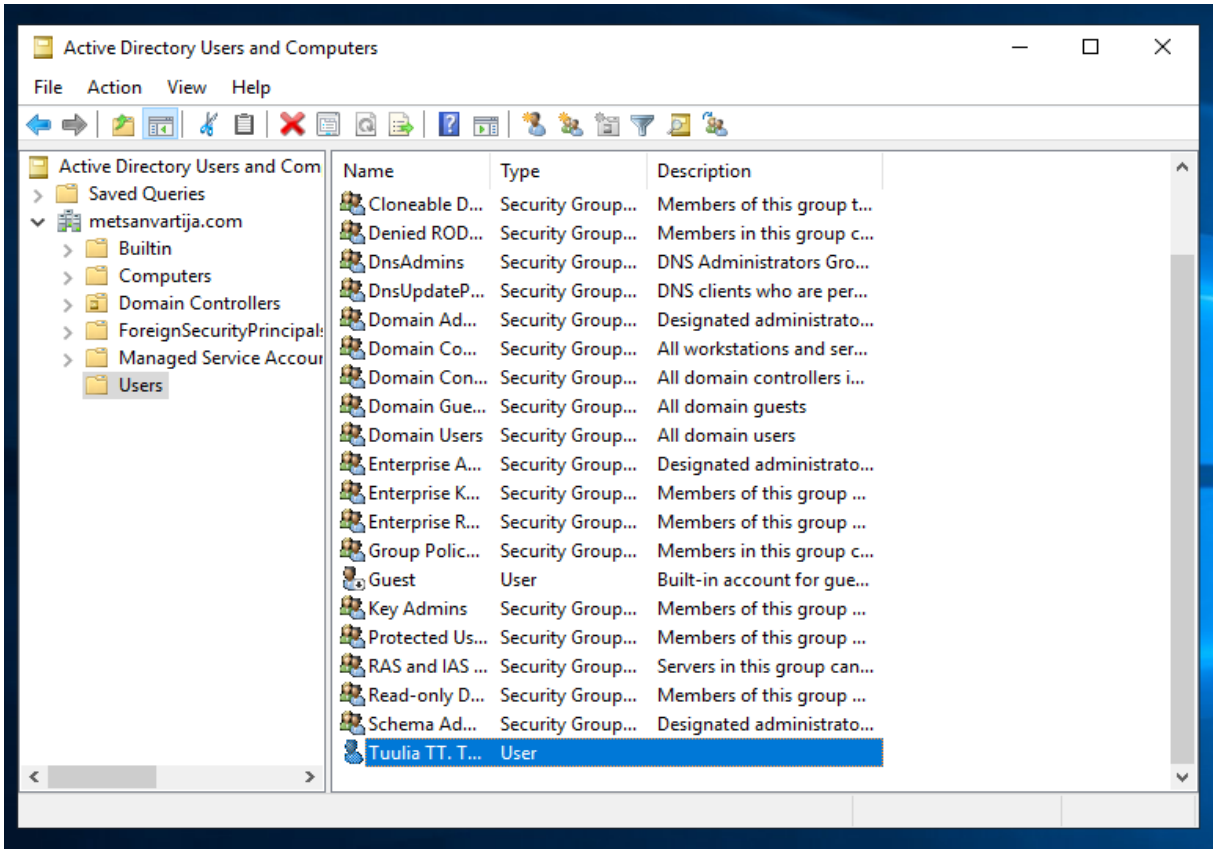
2. Lisäsin uuden käyttäjän: Tuulia Testaaja – Salasana: 5Ala5ana2025!



3. Käyttäjä luotu kansioon ”Users”.



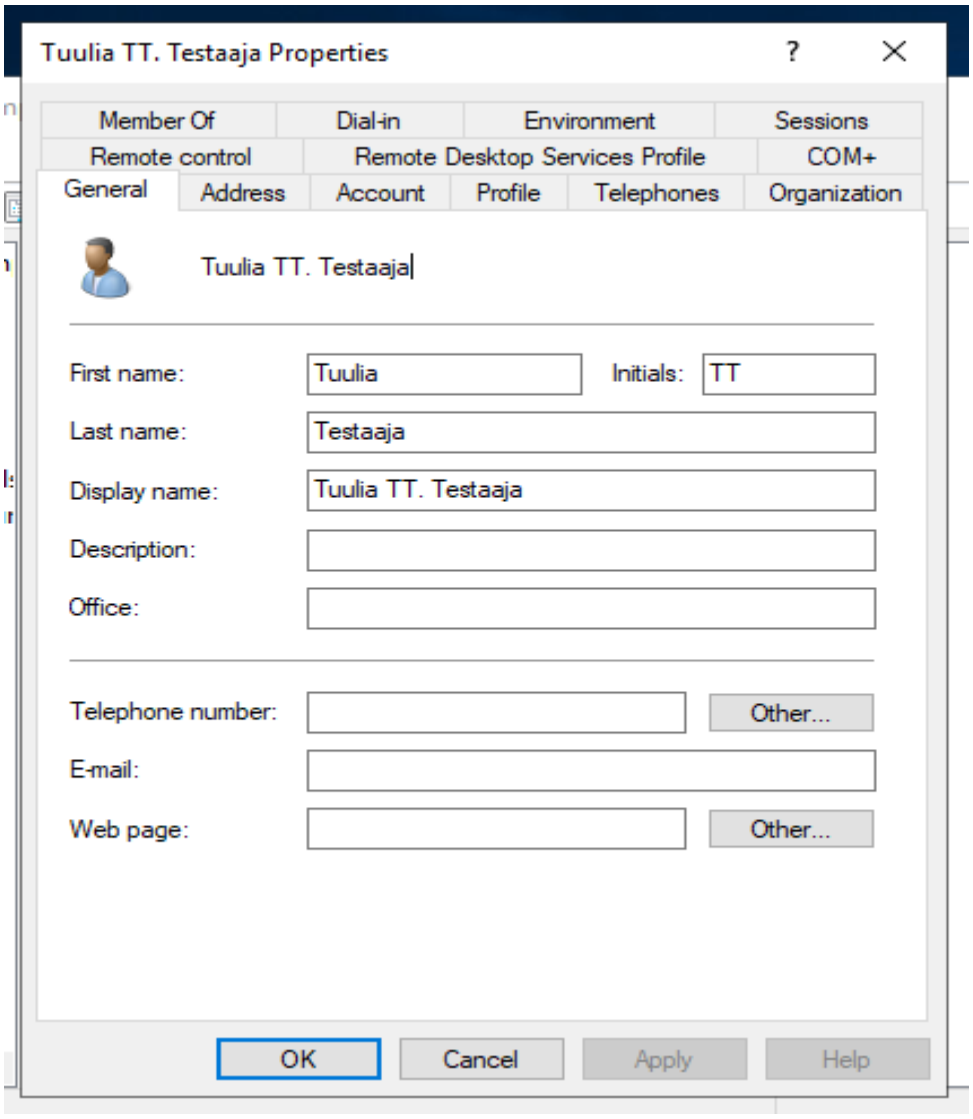
4. Käyttäjä ”Tuulia Testaaja” löytyy oikeasta paikasta.



5. Tutustuin käyttäjätilin ominaisuuksissa näkyviin välilehtiin.

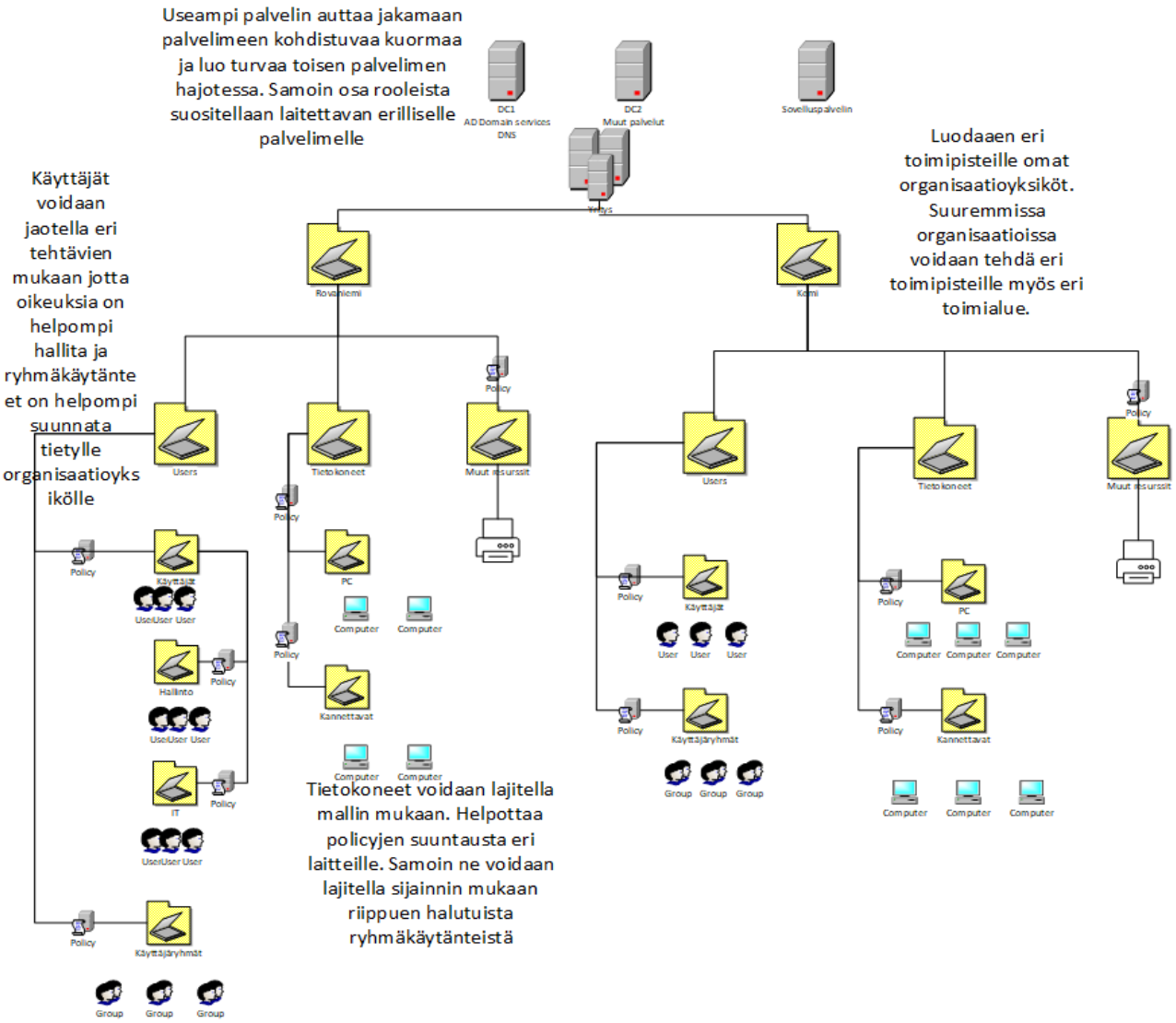
- Account-välilehti: Voit hallita käyttäjän tilin voimassaoloa ja salasanaa.
- Profile-välilehti: Käyttäjälle laitetaan kotihakemisto ja logonscripti tältä välilehdeltä.

  Logonscripti: Logonskripti (kirjautumisskripti) on automaattisesti kirjautumisen yhteydessä suoritettava skripti, jolla voidaan määrittää mm. verkkolevyt, tulostimet ja käyttäjäasetukset.

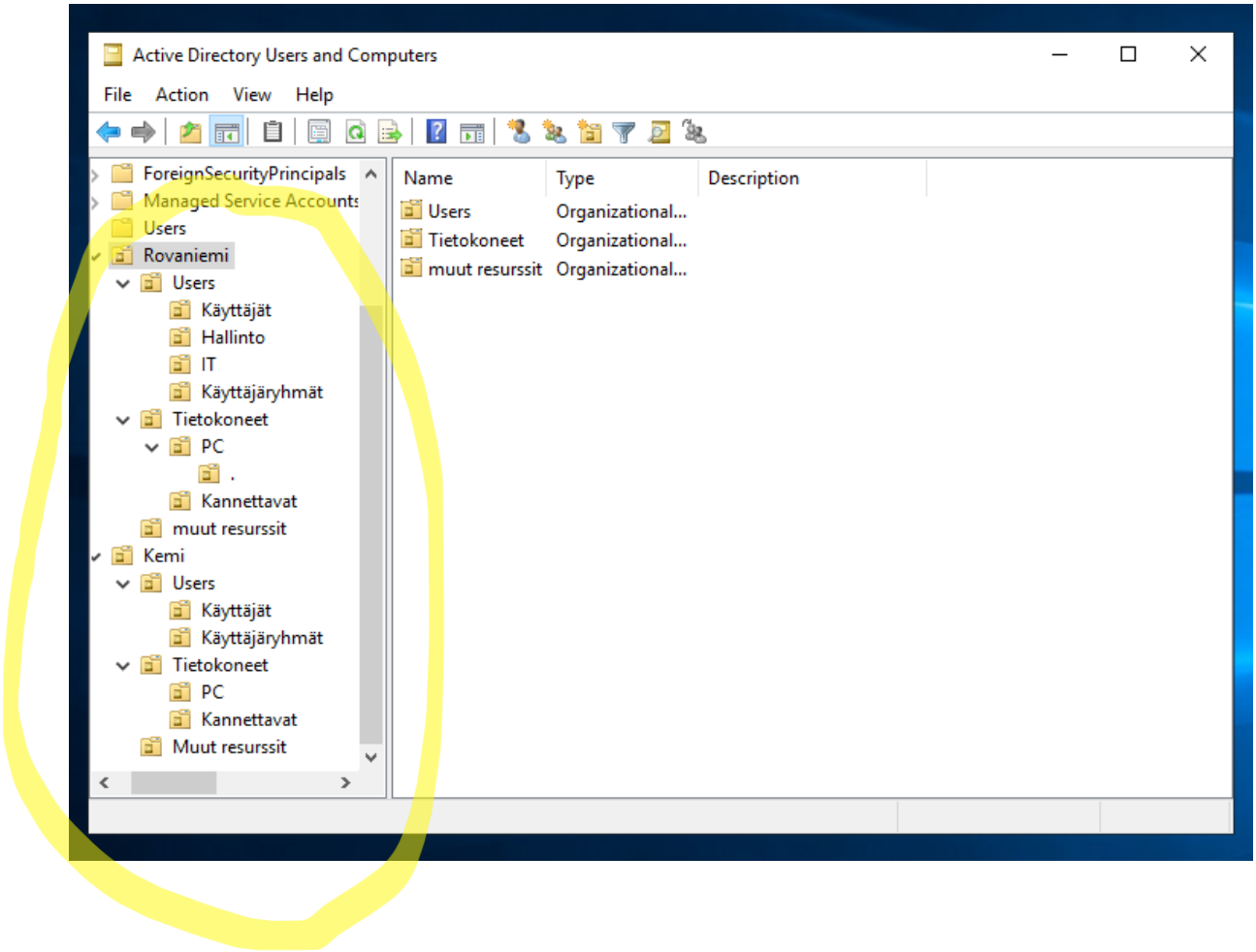


5 OU:t eli Organizational Units

Paula Springaren (TIVI22ROITT), tekemä esimerkki kuva AD:sta. Kuvassa on selitetty Organisaatio Unit:tien käyttöä, eli kerrottu miten Organisaatio Unitien avulla AD:n rakenteesta saadaan helposti hallittava.



Loin samanlaisen OU:n rakenteen, kuin Paulalla. Alla olevassa kuvassa näkyy tulos ympyröitynä.



OU:ita käytetään Active Directoryssa järjestämään käyttäjät ja koneet loogisiin ryhmiin, jolloin niitä voidaan hallita helpommin, kohdistaa ryhmäkäytäntöjä tarkasti ja delegoida hallintaoikeuksia eri tiimeille.

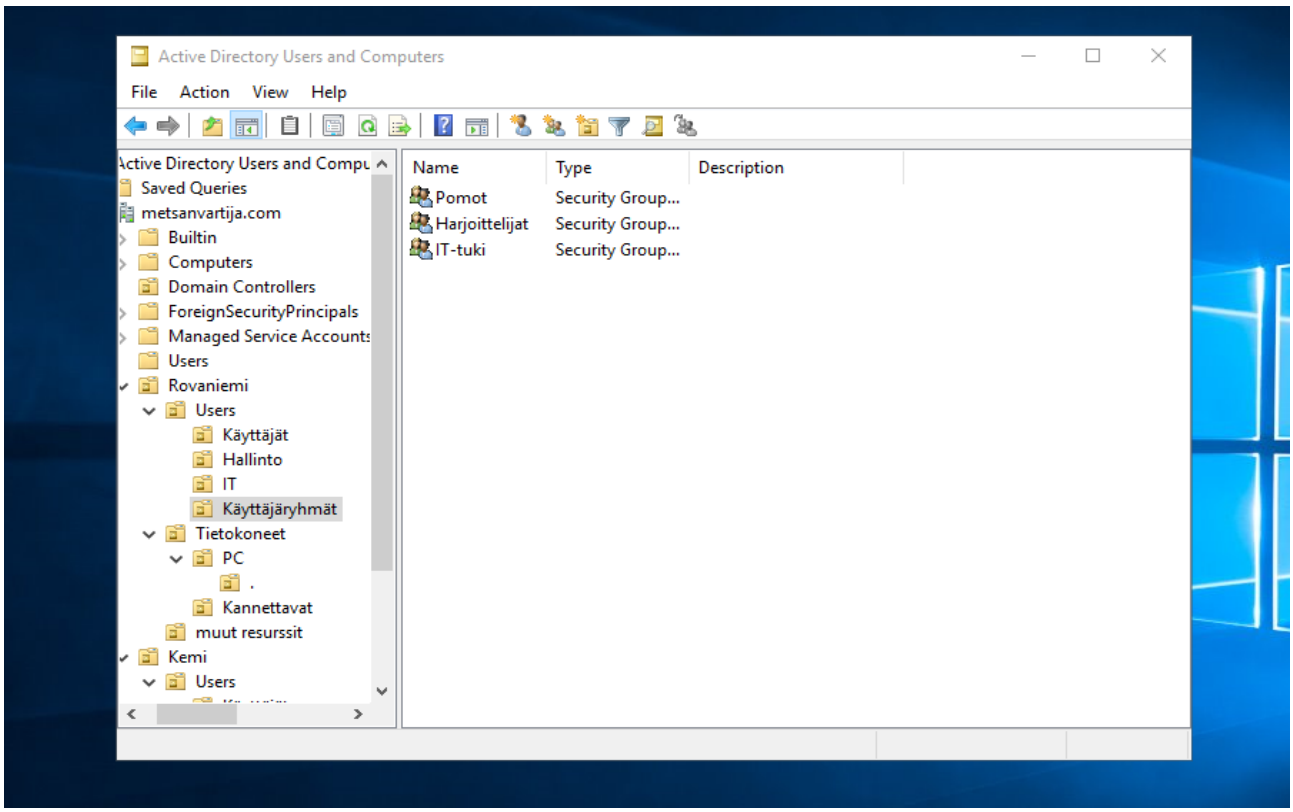
OU:t helpottavat hallintaa seuraavasti:

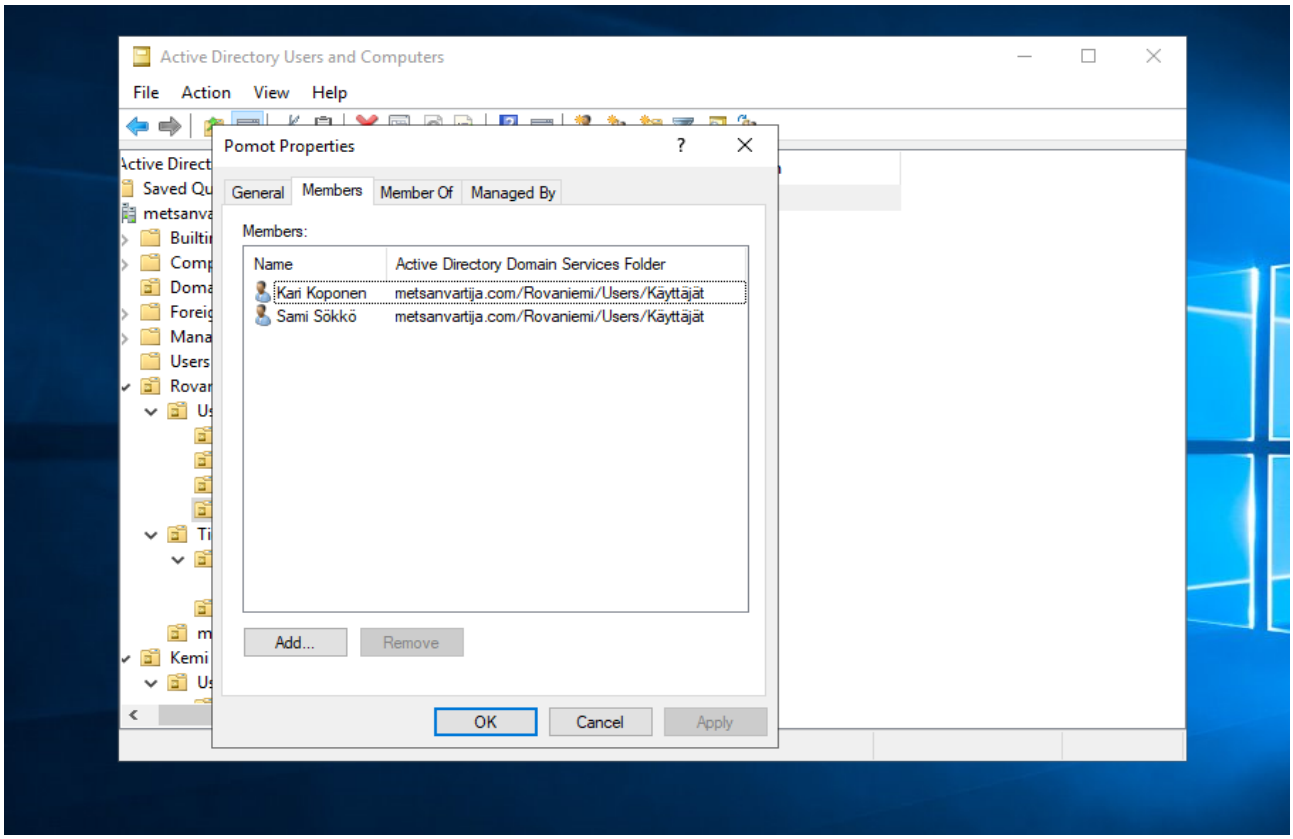
- **Ryhmäkäytännöt** voidaan kohdistaa tarkasti tiettyihin käyttäjiin tai koneisiin.
- **Hallintaoikeuksia** voidaan delegoida vain tiettyyn OU:hun ilman pääsyä muualle.
- Ne tuovat **selkeyttä ja rakennetta**, erityisesti suurissa ympäristöissä.
- Helpottavat **automaatiota ja massatoimintoja** (esim. skriptit, ohjelmistojakelut).

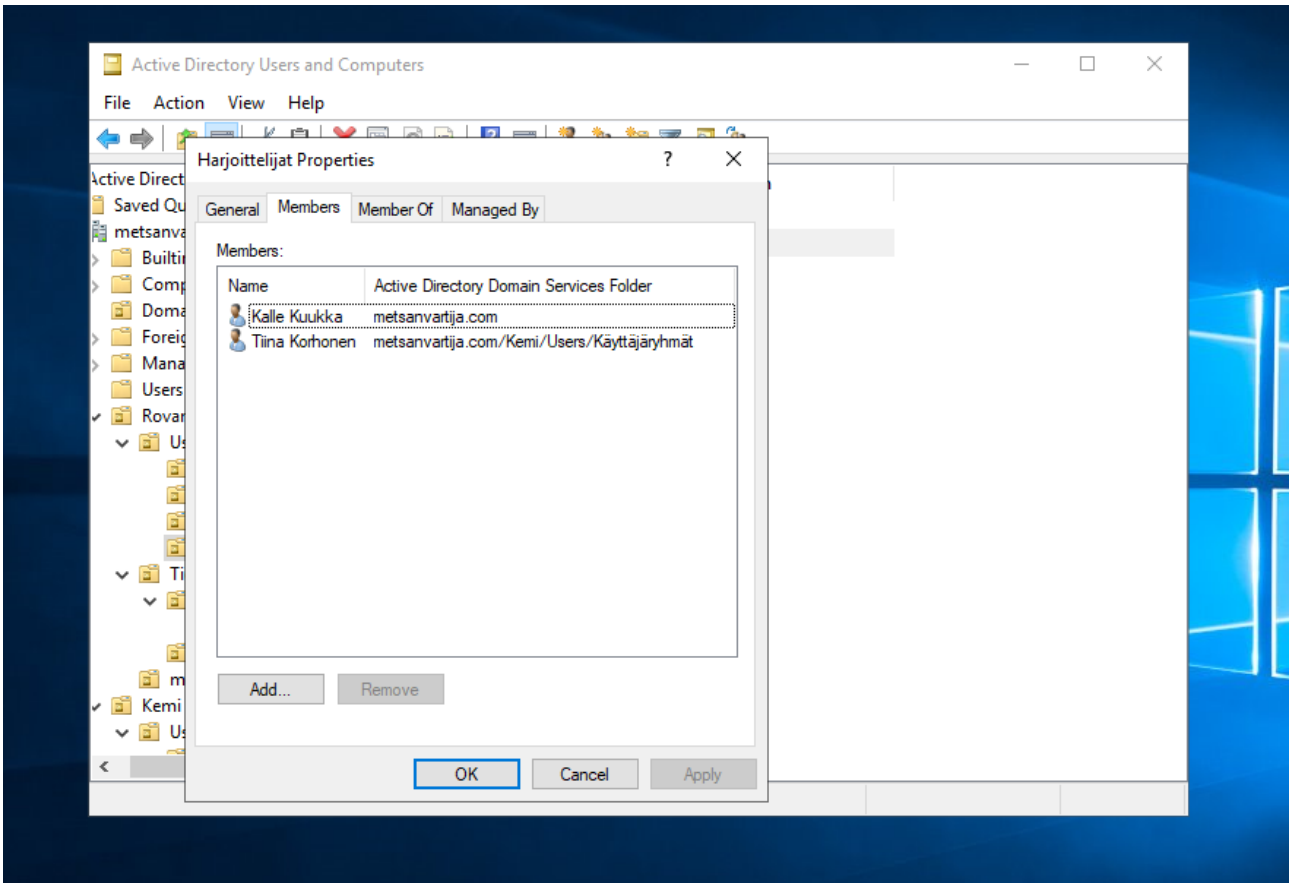
6 Käyttäjäryhmät

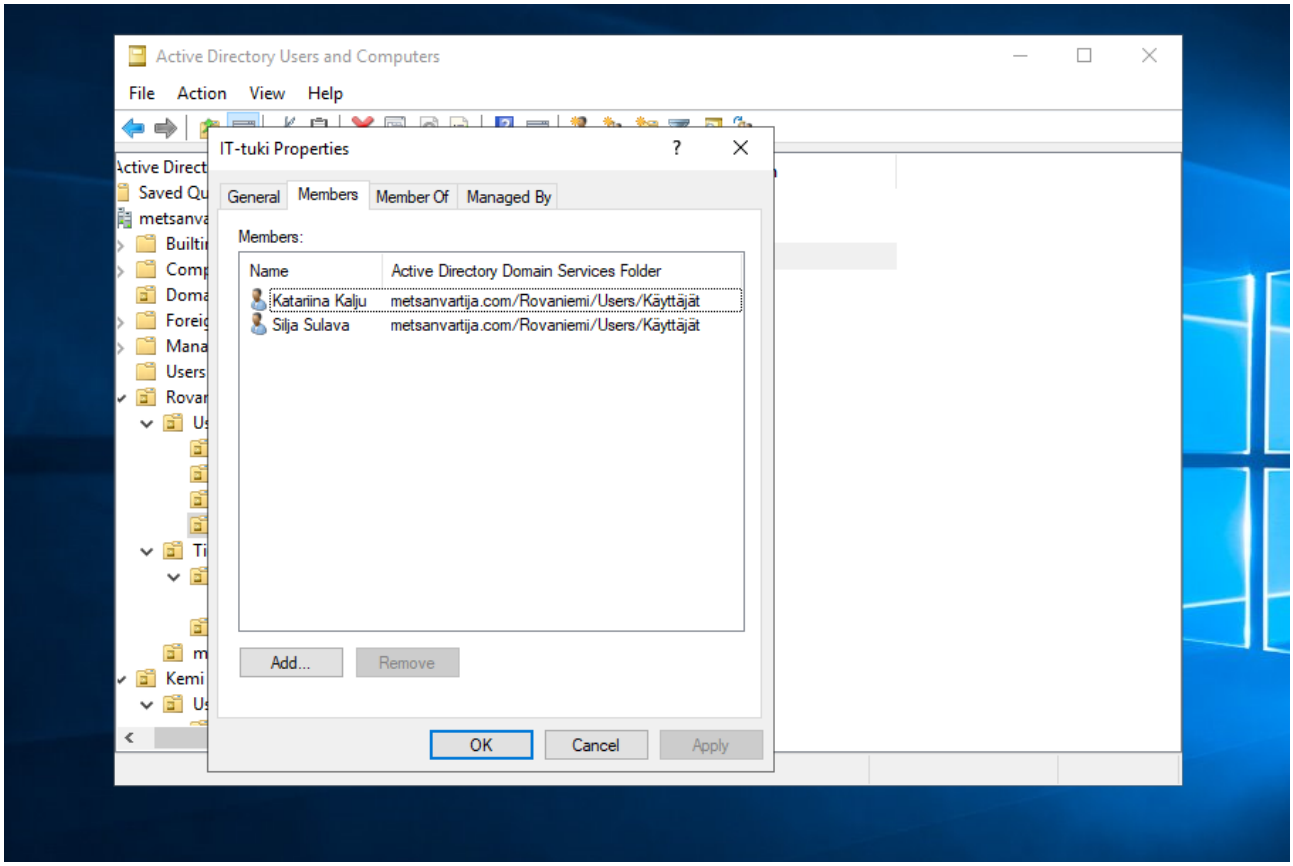
Lisäsin käyttäjäryhmät ja niihin käyttäjät, alla olevan ohjevideon mukaan:

[How to Create OU, Users and Groups on Active Directory 2019 - YouTube]





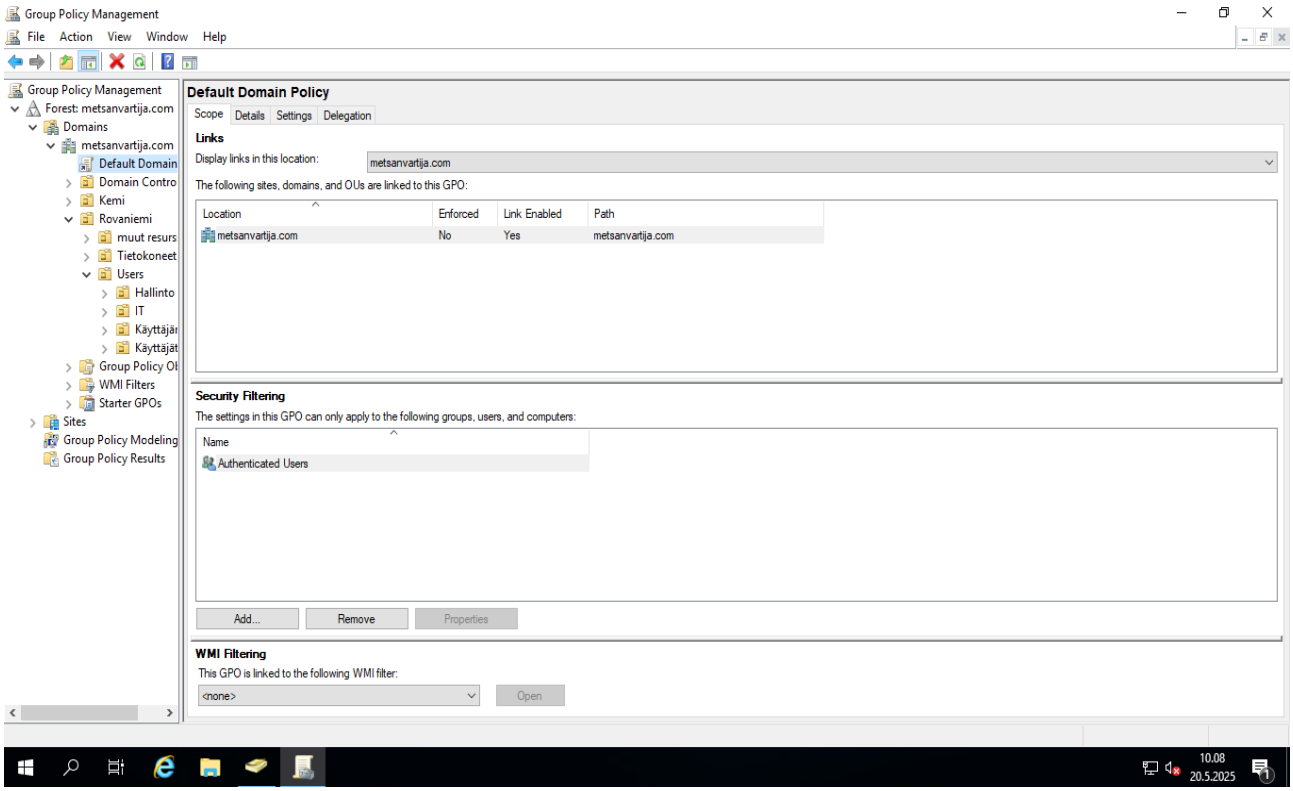

Active Directory Users and Computers
File Action View Help
Harjoittelijat Properties
General Members Member Of Managed By
Members:
Name Active Directory Domain Services Folder
Kalle Kuukka metsanvartija.com
Tiina Korhonen metsanvartija.com/Kemi/Users/Käyttäjäryhmät
Add... Remove
OK Cancel Apply


Active Directory Users and Computers
File Action View Help
IT-tuki Properties
General Members Member Of Managed By
Members:
Name Active Directory Domain Services Folder
Katariina Kalju metsanvartija.com/Rovaniemi/Users/Käyttäjät
Silja Sulava metsanvartija.com/Rovaniemi/Users/Käyttäjät
Add... Remove
OK Cancel Apply

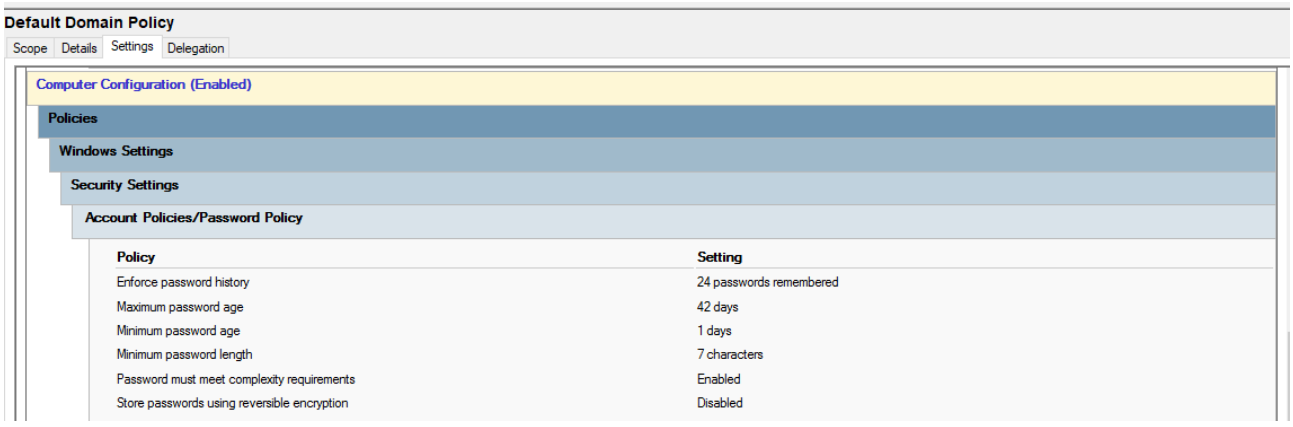
7 Group Policy Management työkalu

Avasin Group Policy Management-työkalun ja sieltä Default domain Policy. Muutin salasanojen asetuksia kohdassa ”Account Policies/Password Policy”.

Ohjevideot:
https://www.youtube.com/watch?v=rEhTzP-ScBo
https://www.youtube.com/watch?v=H4_5ak61S74



Aiemmat asetukset:



Uudet muokatut asetukset:

Account Policies/Password Policy

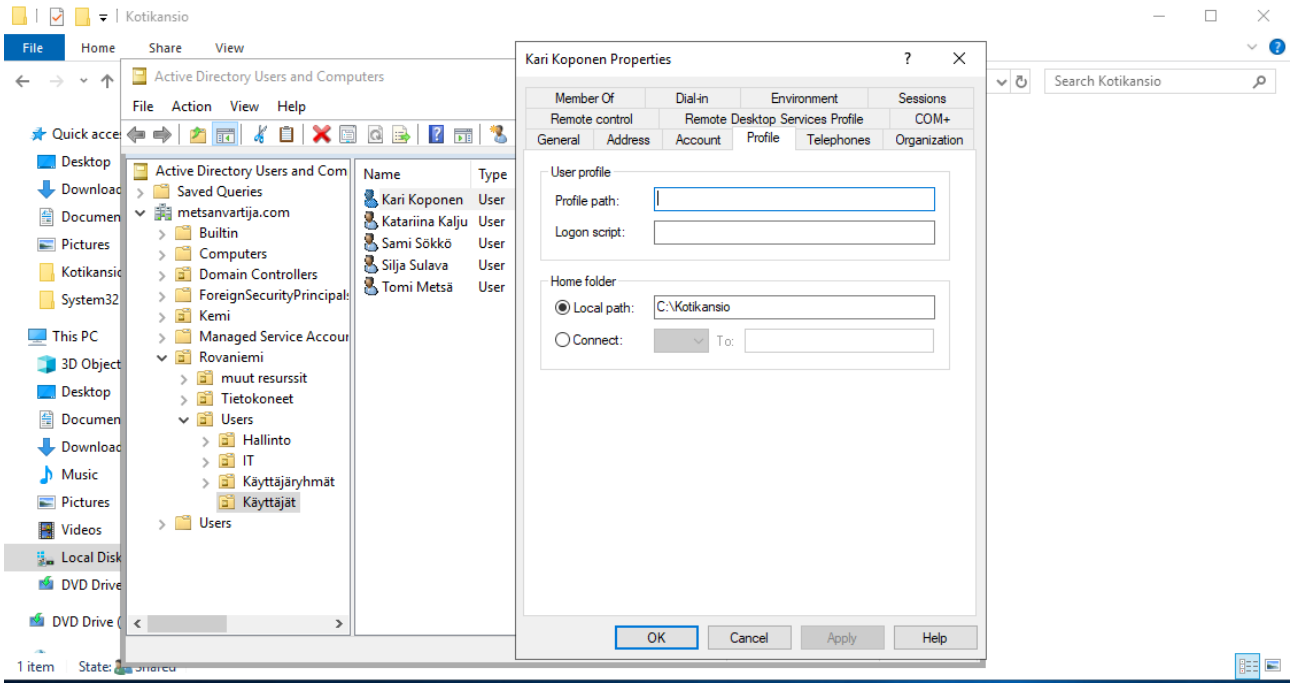
Policy	Setting
Enforce password history	20 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

8 Jaetut kansiot

Tein seuraavat tehtävät käyttäen alla olevaa ohjetta:

https://lucit.sharepoint.com/:w:/r/sites/Pipojengi-TIVI24IT-tuki/_layouts/15/Doc.aspx?sourcedoc=%7B20C98921-F255-4E48-A2B2-509D5AFA6328%7D&file=AD-teoria.docx&action=default&mobileredirect=true

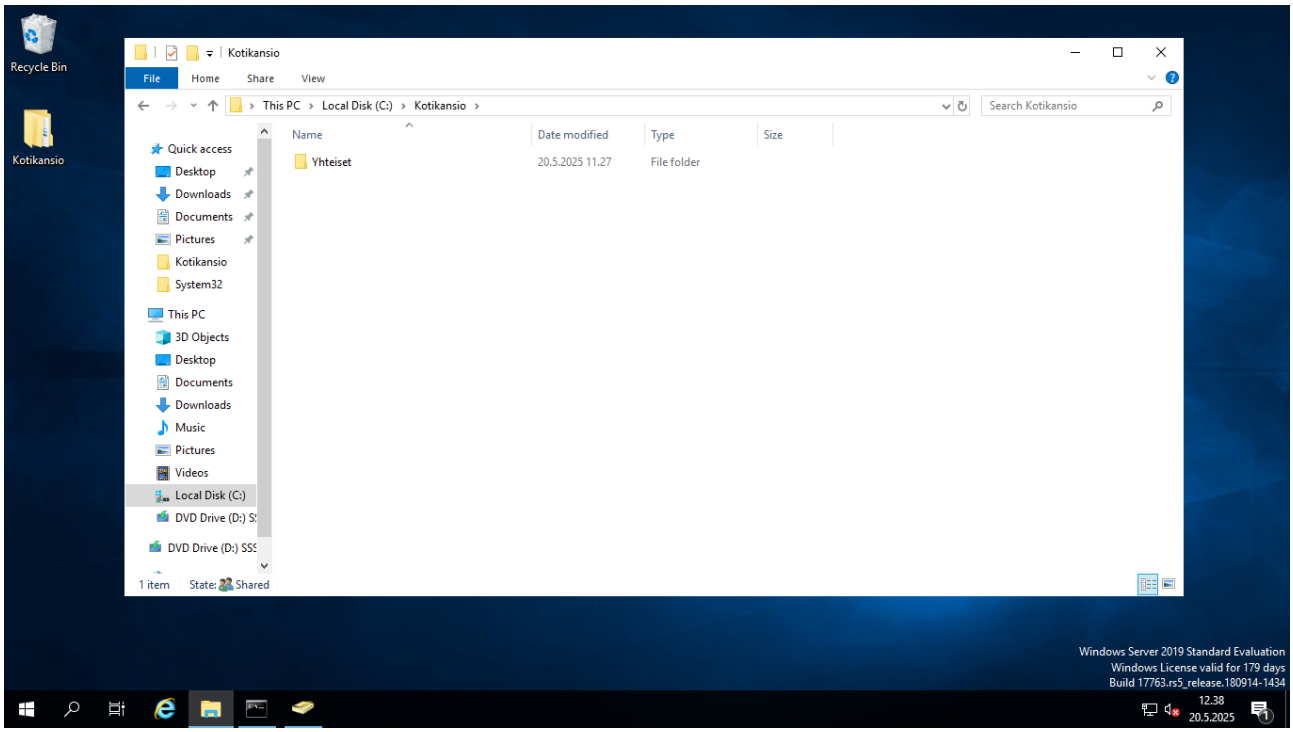
1. **Tee yhdelle käyttäjistäsi kotihakemisto**
2. **Lisää samalle käyttäjälle yhteinen jaettu kansio**
3. **Kopioi käyttäjä uudeksi käyttäjäksi, mitä huomaat?**



1. Tein Kotihakemiston käyttäjälle ”Kari Koponen”. Sen nimi on ”Kotikansio”.

2. Lisäsin kotihakemistoon jaetun kansion nimeltään ”Yhteiset”.

3. Kopioin Käyttäjän ”Kari Koponen” uudeksi käyttäjäksi nimeltään ”Kari Kakkonen”. huomaan, että uudella käyttäjällä on kaikki samat asetukset, kuin alkuperäisellä. Kopioiminen helpottaa ja nopeuttaa samanlaisten käyttäjien lisäämistä.


Recycle Bin
Kotikansio
Kotikansio
File
Home
Share
View
This PC › Local Disk (C:) › Kotikansio ›
Search Kotikansio
Quick access
Desktop
Downloads
Documents
Pictures
Kotikansio
System32
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) S
DVD Drive (D:) SSS
1 item
State: Shared
Name
Date modified
Type
Size
Yhteiset
20.5.2025 11.27
File folder
Windows Server 2019 Standard Evaluation
Windows License valid for 179 days
Build 17763.rs5_release.180914-1434
12.38
20.5.2025