

4.2. AD ja Powershell

Monday, September 22, 2025 20:59

Ohje löytyy täältä:

<https://medium.com/@botgonbayar/building-seoras-user-base-creating-30-users-ous-and-security-groups-b4a22e2f1d73>

Active Directory jotakin ominaisuutta - START HERE;

1. GPO – Group Policy Object

Mikä GPO on?

- GPO = ryhmäkäytäntöobjekti, jolla voidaan hallita käyttäjien ja koneiden asetuksia keskitetysti AD:ssä.
- Käytetään erityisesti:
 - Turvallisuusasetuksiin (esim. salasanakäytänöt, lukitukset)
 - Käyttöliittymärajoituksiin (esim. työpöytä, Käynnistä-valikko)
 - Sovellusasetuksiin (esim. sallitut ohjelmat, skriptit, ohjelmien asennus)

2. GPO: Salasanakäytäntö (Password Policy)

Salasanapolitiikat määritetään GPO:ssa esimerkiksi näin:

Asetus Tarkoitus

Minimum password length Vähimmäispituus, esim. 12 merkkiä

Complexity requirements Pakottaa käyttämään:

- Isoja ja pieniä kirjaimia
- Numeroita
- Erikoismerkkejä |
 - | Maximum password age | Montako päivää salasana on voimassa (esim. 90) |
 - | Minimum password age | Kuinka nopeasti voi vaihtaa salasanan |
 - | Password history | Estää saman salasanan käytön (esim. 10 edellistä tallessa) |

☞ Nämä löytyvät GPO:ssa:

Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy

3. GPO: Työpöydän asetukset (Desktop Restrictions)

Tämän avulla voidaan rajoittaa tai ohjata käyttäjän työpöytäkokemusta. Esimerkiksi:

Asetus Vaikutus

Estä taustakuvalta vaihtaminen Käyttäjä ei voi vaihtaa työpöydän taustaa

Piilota "This PC" Estää käyttäjää selamaasta tiedostoja

Poista tehtäväpalkin asetukset Ei voi muuttaa tehtäväpalkkia

Rajoita Käynnistä-valikkoja Estää sovellusten kiinnittämisen, jne.

Automaattinen taustakuva Aseta yrityksen brändin mukainen tausta

Estä komentorivi (cmd) Estää komentokehoteen käytön

4. GPO: Sovellusasetukset ja sovellusrajoitukset

GPO:lla voit myös määritellä:

- Salitut sovellukset (AppLocker / Software Restriction Policies)
 - Estää käyttäjää ajamasta mitä tahansa .exe-tiedostoja
 - Salit vain tiettyt ohjelmat (esim. Microsoft Word, Teams)
- Skriptit (logon/logooff)
 - Aja automaattisesti esim. kirjaudu- tai uloskirjautumiskriptejä

5. OU ja GPO-linkitys

Mikä on OU (Organizational Unit)?

- OU = Organisaatioyksikkö
- Looginen kansiorakenne AD:ssä, johon sijoitetaan käyttäjiä, koneita, ryhmiä jne.
- Esim.:
 - YritysXC Corp > Users > Sales
 - YritysXC Corp > Computers > Laptops

Mikä on "Linkitetty GPO OU-tasolla"?

- GPO voidaan "linkittää" tiettyyn OU:hun.
- GPO vaikuttaa vain niihin objekteihin (käyttäjät/koneet), jotka sijaitsevat kyseisessä OU:ssa.

Esimerkki:

- GPO "SalesRestrictions" linkitetään OU: Sales
- Vain myyntitiimin käyttäjiin sovelletaan tätä GPO:ta

AD DS (active directory domain services) sisältyvät ominaisuudet:

AD DS (Active Directory Domain Services) toimii yrityksen keskitettynä hakemistopalveluna

Mitä AD DS mahdollistaa – mitä sen "alla" tapahtuu?

Toiminto	Selitys
• Käyttäjien hallinta	Luodaan, poistetaan ja hallitaan käyttäjätunnusia. Jokaisella käyttäjällä on oma identiteetti domainissa (esim. user@yritysxc.local).
• Organisaatioyksiköt (OU)	Looginen kansiorakenne käyttäjiä ja koneiden ryhmittelyyn (esim. Sales, IT, Management).
• Käyttöoikeudet ja valtuutukset	Määritetään mihin resursseihin (tiedostoihin, kansioihin, tulostimiin) käyttäjällä tai ryhmällä on pääsy.
• Ryhmäjäsenyydet (Groups)	Käyttäjät lisätään ryhmiin, joille annetaan oikeuksia. Esim. HR Read Access -ryhmä saa luko-oikeudet HR-kansioon.
• Group Policy Objects (GPO)	Määritetään käyttäjien ja koneiden asetuksia keskitetysti. Esim: <ul style="list-style-type: none">- Salasanavaatimukset- Työpöydän lukitus- Ohjelmarajoitukset- Skriptit
• DNS-integraatio	AD DS sisältää usein DNS-palvelun, joka ratkaisee domain-nimiä (esim. server01.yritysxc.local).

<input checked="" type="checkbox"/> Työasemien ja palvelinten liittäminen	Koneet liitetään domainiin → niistä tulee domain-jäseniä ja ne hallitaan keskitetysti.
<input checked="" type="checkbox"/> Replikointi	Jos on useita domain controllerereita (DC), ne jakavat tiedot keskenään automaattisesti.
<input checked="" type="checkbox"/> Todennus (Authentication)	Käyttäjien kirjautumiset varmistetaan Kerberos-protokollalla → AD tarkistaa, onko salasana oikein, ja mitä oikeuksia käyttäjällä on.

Active Directory Domain Services (AD DS) on alusta, jonka "alla" tapahtuvat:

- Käyttäjähallinta
- Ryhmät
- Oikeudet
- Organisaatioyksiköt
- GPO:t
- DNS-palvelut
- Domain-koneiden hallinta
- Keskitetty kirjautuminen ja todennus

Ja kaikki tämä tapahtuu joko fyysisessä tai virtuaalisessa palvelimessa, jota kutsutaan **Domain Controlleriksi (DC)**.

Active Directory Domain Services (AD DS) - Domain Controller (DC)

AD DS ja DC (Domain Controller) eivät ole täysin eri asia, mutta ne eivät myöskään ole sama asia.
Ne liittyvät tiiviisti toisiinsa, mutta toinen on **palvelu**, ja toinen on **palvelin, joka ajaa tätä palvelua**.

AD DS vs DC

Käsite	Selitys
AD DS (Active Directory Domain Services)	Microsoftin hakemistopalvelu, joka mahdollistaa käyttäjähallinnan, GPO:t, kirjautumisen, ryhmät, jne. Tämä on toiminallispuisto/palvelu , jota Windows Serverissä voidaan asentaa.
DC (Domain Controller)	Tarkoitus: Hakemistopalvelu käyttäjien, koneiden, ryhmienv jne. hallintaan Palvelin, joka ajaa AD DS -roolia. Se tarjoaa AD DS -toiminnot verkossa (kirjautuminen, GPO, DNS jne). Tarkoitus: Fyysisen tai virtuaalinen kone, joka ajaa AD DS:ää ja vastaa AD-toiminnoista

AD DS on palvelu, DC on palvelin (toinen esim. AD DS = postipalvelu, DC = postitoimisto). DC ei voi olla DC ilman AD DS:ää. Ja AD DS ei toimi ilman DC:tä, joka sitä ajaa.

Toinen esim vertauksena:

- AD DS (Active directory domain services) joka toimi kuin pääkonttorina
 - Hallitsee ja hoitaa keskitetyt kaiken hallinnan: käyttäjät, ryhmät, oikeudet, salasanat ja muut laitteet
 - Hallitsee koko organisationsa rakenteen ja sijainti voi olla esim. Helsinki
 - Tämä pätee myös AD DS voi hallinnoida sivullisia DC
- DC (Domain controller) - joka toimii kuin sivutoimistona
 - Joka on palvelin, esim. Sivutoimisto voi olla muualla toimistolla, ja joka sisältää kopioita AD DS tiedoista ja tästä kutusta an replikaatioksi.
 - Tämä voi toimia itsenäisesti, jos yhteys pääkonttorissa tapahtuu poikkeavaa esim. Katkosta
 - Sivutoimisto toimii paikallisesti esim. Turku/Tampere/Rovaniemi - sivutoimistona: työntekijät kirjautumiset, datat, tiedostot ja jne.
 - DC voi synkronoida tietoje kesken, et esim. Pääkonttorissa tulee uusia/poistuvia käyttäjiä - niin sivutoimisto saa sen tiedoston.

DC sisältää – ominaisuudet AD DS:n lisäksi

1. AD DS-palvelu

- Tämä on se ydin: käyttäjien, ryhmien, salasanojen ja oikeuksien hallinta.
- DC ei ole DC ilman AD DS:ää – se on kuin vartija ilman porttia.

2. DNS-palvelu (Domain Name System)

- DC toimii usein myös DNS-palvelimena.
- Tämä mahdollistaa nimen (esim. *tietokone1.firma.local*) muuntamisen IP-osoitteiksi.
- Ilman DNS:ää AD DS ei toimi kunnolla.

3. Replikaatio

- DC:t voivat **synkronoida tietonsa** muiden DC-palvelimien kanssa.
- Tämä takaan, että käyttäjätiedot ja oikeudet pysyvät ajan tasalla eri toimipisteissä.

4. Kirjautumispalvelu (Kerberos & NTLM)

- DC hoitaa **autentikoinnin**: kun käyttäjä kirjautuu, DC tarkistaa salasanan ja antaa käyttöoikeudet.
- Käytössä on Kerberos-protokolla (modernimpia) tai NTLM (vanhempi).

5. Group Policy -hallinta

- DC voi jakaa **ryhmäkäytäntöjä (Group Policies)**, joilla määritetään esim. työpöydän asetukset, sovellusten estot, salasanaehdot.
- Tämä on yksi AD DS:n tärkeimmistä hallintatyökaluista.

6. Global Catalog

- DC voi toimia **Global Catalog -palvelimena**, joka sisältää osan koko AD:n tietokannasta.
- Tämä nopeuttaa hakua ja kirjautumista suurissa ympäristöissä.

7. FSMO-roolit (Flexible Single Master Operations)

- Tietyt DC:t hoitavat erityisiä tehtäviä, kuten:
 - **Schema Master** (AD:n rakenteen hallinta)
 - **RID Master** (käyttäjätunnusten jakaminen)
 - **PDC Emulator** (aikapalvelin, NTLM-tuki)
 - jne.

Ominaisuus	AD DS	DC
Käyttäjien ja ryhmien hallinta	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (AD DS:n kautta)
DNS-palvelu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (yleensä mukana)
Replikaatio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kirjautumisen tarkistus	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Group Policy -jakelu	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Global Catalog	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (valinnainen)
FSMO-roolit	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> (valitut DC:t)

AD DS rakenne linux tree mallina:

secora.local (Domain Root)
└ Secora Corp (Company Root OU)

```

    |-- Users
    |   |-- Administrators      # Tier 0 & 1 admins
    |   |-- IT Staff            # Tier 2 and regular IT users
    |   |-- Management          # Executives and managers
    |   |-- Finance              # Finance department
    |   |-- HR                  # Human Resources
    |   |-- Sales                # Sales team
    |   |-- General Staff        # Other employees
    |-- Computers
    |   |-- Servers              # All server systems
    |   |-- Workstations
    |       |-- Executive        # C-level workstations
    |       |-- IT                # IT department computers
    |       |-- General           # Standard user workstations
    |   |-- Laptops               # Mobile devices
    |-- Groups
    |   |-- Security Groups     # Access control groups
    |   |-- Distribution Lists   # Email distribution
    |-- Service Accounts
    |-- Resources
        |-- Shared Folders        # File share resources

```

```
#####
#####
```

Työelämässä - AD DS, GPO ja muu käyttö

Monissa työpaikoissa saatetaan kysyä, osaoko käyttää **Active Directoryä (AD)** tai onko siitä kokemusta. Miksi?

- **Vastaus:** Perusosaaminen AD:stä on hyödyllistä, ja joissain yrityksissä sen käyttö on edelleen keskeinen osa IT-infrastruktuuria.
- **Käytöltävät vaihtelevat:** Osa organisaatioista on siirtyneet kokonaan pilvipalveluihin (esim. Azure AD), osa käyttää hybridimallia (paikallinen palvelin + pilvi), ja jotkut hyödyntävät edelleen täysin paikallista AD-ympäristöä.

Keskseinen osa AD:n hallinta osuu:

- GPO:t ovat käytännössä se tapa, **miten hallitset keskitetyt käyttäjät ja tietokoneita** AD-ympäristössä. Jos sinulla on Windows-verkko, jossa on kymmeniä tai satoja koneita tai käyttäjiä, ei ole järkevää säättää asetuksia käsin konekohtaisesti.

- Mihin GPO:ta käytetään?

- **Tietoturvan parantamiseen** (esim. salasanasäännöt, lukitusajat)
- **Käyttöjärjestelmän asetusten määrittelyseen** (esim. poista ohjauspaneeli käytöstä)
- **Käyttäjäympäristön hallintaan** (esim. työpöydän kuvalaajasetukset, kirjautumisskriptit)
- **Resurssien jako** (esim. verkkokaasemien mapitus)
- **Tulostimien asetus käyttäjille**
- **Ohjelmien asennus tai esto**
- **Windows-päivitysten hallinta**

Active Directory ei ole vain käyttäjähallintaa — se on **keskitetty hallintajärjestelmä**, joka tuo:

- **Tehokkuutta:** Asetukset ja resurssit hallitaan yhdestä paikasta.
- **Turvallisuutta:** Käytöönoikeudet ja poliittiat ovat hallittavissa tarkasti.
- **Valvontaa ja auditointia:** Tapahtumat ja muutokset voidaan seurata.
- **Etä- ja lähihallinta:** Toimii sekä fyysisille että etäkäytössä oleville laitteille.

Esim. **USB-porttien käytön rajoittaminen tai estäminen** on yleinen käytäntö erityisesti Yhdysvalloissa ja kansainvälisissä yrityksissä, joissa tietoturva on kriittinen osa toimintaa. Tällainen rajoitus voidaan toteuttaa suoraan **Active Directoryn kautta käytämällä GPO-asetuksia (Group Policy Objects)**.

Jos USB-tikkujen käyttö on välttämätöntä, voidaan sallia vain **tietyt hyväksytyt laitteet**, kuten yrityksen omat **salatut USB-tikut**. Nämä estetään ulkopuolisten tai tuntemattomien laitteiden käytön ja parannetaan tietoturva merkittävästi.

```
#####
#####
```

Koskien AD:n OU (organization units) - START HERE:

OU (Organizational Unit) toimii Active Directoryssä ja miten sen avulla voidaan rakentaa järkevä ja hallittava rakenne organisaation – kuten myyntiosaston ja tiimienv – ympärille.

Mikä on OU?

Organizational Unit (OU) on Active Directoryn looginen säiliö, johon voit:

- järjestellä käyttäjiä, tietokoneita, ryhmiä ja muita OU:ita
- soveltaa ryhmäkäytäntöjä (GPO)
- delegoida hallintaoikeuksia (esim. tiiminvetäjät voivat hallita omia tiimiään)

OU on siis kuin kansio AD:n sisällä, jonka avulla voit **organisoida resurssit loogisesti ja hallittavasti**.

- **OU = hallinnan ja rakenteen yksikkö Active Directoryssä**
- **Ryhmiä = käytetään oikeuksien ja resurssien hallintaan**
- Myyntiimeille **OU-rakenne** on tehokas, etenkin jos halutaan antaa tiiminvetäjille hallinta
- Ryhmät toimivat hyvin oikeuksien myöntämisessä ja sähköpostin jakelussa
- **Paras käytäntö:** käytä **OU:ta hallintaan ja ryhmiä oikeuksiin**

```
#####
Esim.1 Pieni malli OU rakenne
```

```

-----  

YritysXC.local  

└── OU=Myynti  

    ├── OU=Tiimi1  

    ├── OU=Tiimi2  

    └── OU=Tiimi3
-----
```

- Käyttäjät ja tietokoneet sijoitetaan omiin OU:iinsa.
- Tiiminvertäjille voidaan delegoida hallintaoikeudet omaan OU:hun (esim. Tero voi luoda käyttäjiä Tiimi1-OU:ssa, mutta ei muissa).
- Eri GPO:t voidaan kohdistaa tiimeittäin, esim. työpöydän tausta, kirjautumisviestit, tai ohjelmistorajotukset.

Esim.2 Pieni malli OU rakenne

```
-----
YritysXC.local
└── OU=Myynti
    ├── Group=Tiimi1
    ├── Group=Tiimi2
    └── Group=Tiimi3
```

- Kaikki käyttäjät ovat samassa OU:ssa.
 - Tiimejä erotellaan **ryhmien avulla** (security groups).
 - GPO:t voidaan kohdistaa ryhmiin kautta, mutta se on hieman monimutkaisempaa (tarvitsee WMI-suodattimia tai GPO:n kohdistamista ryhmiille).
 - Hallinta ei ole niin hienojakoinen kuin OU:illa.
-

Active Directory -hallintaa — ryhmien tyypit ja laajuudet (scope + type) määrittävät **mihin ryhmään voidaan käyttää ja missä ympäristössä**.

Pääominaisuudet:

- **Group Type** – *Mihin ryhmään käytetään*
- **Group Scope** – *Missä ryhmä toimii (ja keihin jäseniin se voi viitata)*

Tyypit:

Security group (turvaryhmä)

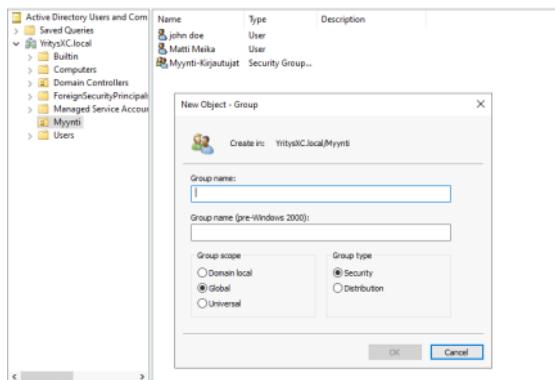
- Käytetään **oikeuksien hallintaan** (file share, NTFS, GPO, tulostin jne.)
- Esimerkki: "HR-Fileshare-Access"
- Voi käyttää oikeuksien määrittämiseen myöntämiseen **ACL-tasolla** (Access Control List)
- Voi käyttää myös sähköpostjakeluun
- Käytetään lähes aina

Distribution group (jakeluryhmä)

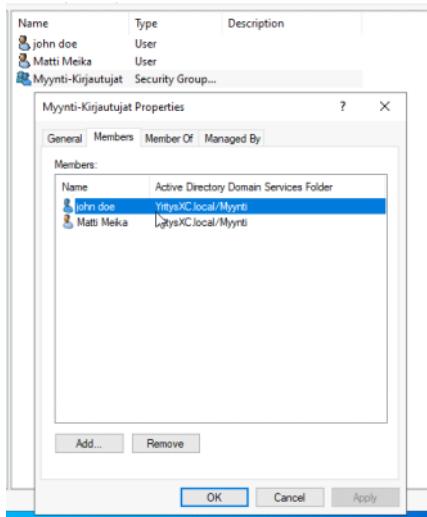
- Käytetään **vain viestintään**, esim. Exchange-sähköposti: "Kaikki työntekijät"
- Ei voi käyttää oikeuksien määrittämiseen (ei toimi NTFS, GPO, ACL jne.)
- Kevyempi (ei turvallisuuskontekstiä)
- Ei käytetä, jos haluat myöntää käyttöoikeuksia
- Käytetään vain, jos pelkkä viestintä

2. Group Scope (Ryhmin laajuus)

Scope	Mihin resurssiin voi käyttää	Keitä voi lisätä jäseniksi	Toimii missä
Domain Local	Vain omassa domainissa	Käyttäjät/ryhmät mistä tahansa forestista	Käyttö vain omassa domainissa
Global	Kaikissa domaineissa	Vain oman domainin käyttäjät ja globaalit ryhmät	Toimii koko metsässä (forest)
Universal	Kaikissa domaineissa	Käyttäjät ja ryhmät mistä tahansa domainista	Kaikki domainit (ja sitten myös Exchange)



Ryhmin alta sitten voi lisätä käyttäjiä ryhmään tai poistaa jos on poistunut henkilö.



PIENI ESIM: JA TILANNEKUVA

Tilannekuva: Myyntiosasto

Myyntiosasto (OU=Myynti) jakaantuu kolmeen toimintayksikköön, joilla on omat tiimit ja resurssit:

1. **Tiimi-Tampere:** vastaa Pirkanmaan asiakkuuksista
 2. **Tiimi-Helsinki:** pääkaupunkiseudun myynti
 3. **Tiimi-Verkkokauppa:** verkkomyynti ja asiakaspalvelut
- Jokaisella on:
- Oma OU käyttäjille (hallinnan ja GPO-delegoinnin vuoksi)
 - Oma Security Group (Global): tiimin jäsenydet
 - Oma Security Group (Domain Local): resurssien oikeudet
 - Esimerkiksi: jaettu kansio tai myyntisovellus (FS01, APP01 jne.)

LINUX TREE RAKENNE:

```

OU=Myynti,DC=YritysXC,DC=local
└── OU=Tiimi-Tampere
    ├── Users
    │   ├── CN=tuula.tammeri (user)
    │   └── CN=kim.koskinen
    ├── Groups
    │   ├── GG-Tiimi-Tampere-Kayttajat      (Global Group)
    │   └── DL-FS01-Tampere-Share-Access    (Domain Local Group)
    └── Resources
        └── \FS01\Tampere          (Shared Folder)
            └── Oikeus: DL-FS01-Tampere-Share-Access (Read/Write)

    └── OU=Tiimi-Helsinki
        ├── Users
        │   ├── CN=salla.saarinen
        │   └── CN=antti.arvola
        ├── Groups
        │   ├── GG-Tiimi-Helsinki-Kayttajat    (Global Group)
        │   └── DL-FS01-Helsinki-Share-Access (Domain Local Group)
        └── Resources
            └── \FS01\Helsinki
                └── Oikeus: DL-FS01-Helsinki-Share-Access (Read Only)

    └── OU=Tiimi-Verkkokauppa
        ├── Users
        │   ├── CN=jonna.jarvi
        │   └── CN=leevi.liinna
        ├── Groups
        │   ├── GG-Verkkokauppa-Kayttajat      (Global Group)
        │   └── DL-APP01-WebApp-Access         (Domain Local Group)
        └── Resources
            └── APP01: WebApp - käyttöoikeudet
                └── Oikeus: DL-APP01-WebApp-Access (App käyttäjät)

```

Powerhell käyttöä Active directory:ssä - START HERE

PowerShell on erittäin tehokas työkalu Active Directory -hallintaan, etenkin automatisointiin, kuten:

- Käyttäjien luonti / poisto (onboarding & offboarding)
- Ryhmien hallinta
- Koneiden liittäminen domainiin
- Salasanojen vaihtaminen
- Oikeuksien antaminen
- Raportointi (esim. viimeisin kirjautuminen)

PIENI INFO: tämä onkin virtualisointi koskien windows serverin käytöö - jossa käytetään PowerShell skriptiä ja komennon käytöö - niin ei tarvitse kirjautua sisään ja ensimmäisen avatessa on jo "administrator" level taso ja oikeudet. Ei tarvitse erikseen kirjautua ja joskus saattaa syöttää kirjautumisen sisään.

Vaatiiko PowerShell jotain kirjautumista tai oikeuksia?

- **Tarvitset käyttöoikeudet (yleensä AD-järjestelmänvalvoja)**
 - Vähintään: oikeudet kysiseen OU:hun ja käyttäjäobjekteihin
 - Suositeltavaa: käyttää erillistä AD-admin-tiliä
- **PowerShell-moduuli täytyy olla asennettuna:**
 - RSAT: Active Directory module (Windowsissa)
 - Komento: Import-Module ActiveDirectory
 - Vaatii ADDS-työkalut asennettuna
- PowerShell-komennot **ajetaan sillä käyttäjätilillä**, jolla olet kirjautunut – tai erikseen määritetyllä tilillä.

❖ Mitä voit tehdä? (Automatisointi)

Onboarding-esimerkki (uuden työntekijän luonti):

```
New-ADUser -Name "matti.meikalainen" ` 
-GivenName "Matti" ` 
-Surname "Meikalainen" ` 
-SamAccountName "matti.meikalainen" ` 
-UserPrincipalName "matti.meikalainen@yritysxc.local" ` 
-Path "OU=Myynti,DC=yritysxc,DC=local" ` 
-AccountPassword (ConvertTo-SecureString "Välialainen1!" -AsPlainText -Force) ` 
-Enabled $true ` 
Add-ADGroupMember -Identity "GG-Tiimi-Tampere-Kayttajat" -Members "matti.meikalainen"
```

Offboarding-esimerkki (työntekijän poistaminen):

```
# Poista käyttäjä ryhmistä
Get-ADUser "matti.meikalainen" | Get-ADPrincipalGroupMembership | Remove-ADGroupMember -Members "matti.meikalainen" -Confirm:$false
```

```
# Disable käyttäjätunnus
Disable-ADAccount -Identity "matti.meikalainen"
```

```
# Siirrä arkistoointi-OU:hun
Move-ADObject -Identity "CN=matti.meikalainen,OU=Myynti,DC=yritysxc,DC=local" ` 
-TargetPath "OU=PoistetutKayttajat,DC=yritysxc,DC=local"
```

MINI HARJOITUS - START HERE;

uusi käyttäjä **John Smith** Active Directoryyn, sijoitetaan hänet **OU=Myynti** -yksikköön, ja annetaan hänen peruskäyttöoikeudet – PowerShellin avulla.

Oma demo , mutta nice - ja silti pitää kirjautua sisään active directory moduuliin kuitenkin

The screenshot displays two windows side-by-side. On the left is the 'Active Directory Users and Computers' snap-in, showing a tree view of the directory structure and a list of users (John Doe, John Smith, Matti Meka) under the 'Myynti' organizational unit. On the right is a ChatGPT interface with a title 'PowerShell-komento käyttäjän luontiin'. It contains a PowerShell script block with comments explaining the steps to create a new user 'John Smith' in the 'Myynti' OU and add them to a specific group. The script uses 'New-ADUser' and 'Add-ADGroupMember' cmdlets.

```
# Tuo AD-moduuli
Import-Module ActiveDirectory
```

```
# Luo uusi käyttäjä
New-ADUser ` 
-Name "John Smith" ` 
-GivenName "John" ` 
-Surname "Smith" ` 
-SamAccountName "john.smith" ` 
-UserPrincipalName "john.smith@yritysxc.local" ` 
-Path "OU=Myynti,DC=yritysxc,DC=local" ` 
-AccountPassword (ConvertTo-SecureString "Tervetuloa1!" -AsPlainText -Force) ` 
-ChangePasswordAtLogon $true ` 
-Enabled $true ` 
-Description "Myyntiosasto – Tampereen tiimi"
```

```
# Lisää ryhmään (valinnainen)
Add-ADGroupMember -Identity "GG-Tiimi-Tampere-Kayttajat" -Members "john.smith"
```

```

Windows PowerShell
copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

S C:\Users\Administrator> Import-Module ActiveDirectory
S C:\Users\Administrator> New-ADUser -Name "John Smith" -GivenName "John" -Surname "Smith" -SamAccountName "john.smith" -UserPrincipalName "john.smith@rytysxc.local" -Path "OU=Myynti,DC=rytysxc,DC=local" -AccountPassword (ConvertTo-SecureString "Tervetuloa1!" -AsPlainText -Force) -ChangePasswordAtLogon $true -Enabled $true -Description "Myyntiosasto - Tampere tiimi"
S C:\Users\Administrator>

```

```

# PowerShell-komento käyttäjän luontiin
powershell

# Tuo AD-moduuli
Import-Module ActiveDirectory

# Luo uusi käyttäjä
New-ADUser -Name "John Smith" -GivenName "John" -Surname "Smith" -SamAccountName "john.smith" -UserPrincipalName "john.smith@rytysxc.local" -Path "OU=Myynti,DC=rytysxc,DC=local" -AccountPassword (ConvertTo-SecureString "Tervetuloa1!" -AsPlainText -Force) -ChangePasswordAtLogon $true -Enabled $true -Description "Myyntiosasto - Tampereen tiimi"

# Lisää ryhmään (valinnainen)
Add-ADGroupMember -Identity "GG-Tiimi-Tampere-Kayttajat" -Members "john.smith"

```

Tässä alhaalla on esim. Käyttäjän tarkistaminen:

```
$Get-ADUser -Identity "john.smith" | Select Name, Enabled, DistinguishedName
```

```

PS C:\Users\Administrator> Get-ADUser -Identity "matti.meika" | select name
name
-----
Matti Meika

PS C:\Users\Administrator> Get-ADUser -Identity "matti.meika" | select name, type
name      type
-----  -----
Matti Meika  User

PS C:\Users\Administrator>

```

```

# Mitä tämä tekee?
• Luo käyttäjän John Smith
• Asettaa salasanan (joka pitää vaihtaa ensimmäisellä kirjautumisella)
• Aktivoi tunnusken
• Sijoittaa käyttäjän OU=Myynti alle
• Lisää hänet ryhmään GG-Tiimi-Tampere-Kayttajat (jos sellainen on olemassa)

# Tarkistus
arkista että käyttäjä löytyy:
powershell
Get-ADUser -Identity "john.smith" | Select Name, Enabled, DistinguishedName

```

Seuraavaksi ryhmän luonti & Ryhmien luonti Active Directoryssä PowerShellillä on **nopea ja yksinkertainen**, ja se on oleellinen osa käyttäjien hallintaa – etenkin kun käytetään AGDLP-mallia (Global, Domain Local, jne.).

MALLI: \$New-ADGroup -Name "<RyhmnNimi>" -GroupScope <Scope> -GroupCategory <Typpi> -Path "<OU-polku>"

🔗 Luo ryhmä myyntiosastolle

Luodaan uusi **Global-ryhmä** nimeltä GG-Myynti-TiimiTampere-Kayttajat, joka sijaitsee OU=Myynti.

```
New-ADGroup `

-Name "GG-Myynti-TiimiTampere-Kayttajat" `

-SamAccountName "GG-Myynti-TiimiTampere-Kayttajat" `

-GroupScope Global `

-GroupCategory Security `

-Description "Tampereen myyntitiimin käyttöjäryhmä" `

-Path "OU=Myynti,DC=rytysxc,DC=local"
```

```

Windows PowerShell
copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

S C:\Users\Administrator> New-ADGroup -Name "Kotkan myynti" -SamAccountName "Kotkan myynti" -GroupScope Global -GroupCategory Security -Description "Kotkan myynti" -Path "OU=Myynti, DC=rytysxc, DC=local"
S C:\Users\Administrator>

```

```

# Malli: $New-ADGroup -Name "<RyhmnNimi>" -GroupScope <Scope> -GroupCategory <Typpi>

# Luo ryhmä myyntiosastolle
New-ADGroup `

-Name "GG-Myynti-TiimiTampere-Kayttajat" `

-SamAccountName "GG-Myynti-TiimiTampere-Kayttajat" `

-GroupScope Global `

-GroupCategory Security `

-Description "Tampereen myyntitiimin käyttöjäryhmä" `

-Path "OU=Myynti,DC=rytysxc,DC=local"

# Toinen esimerkki: Domain Local -ryhmä resurssioikeuksia varten
New-ADGroup `

-Name "DL-FS01-MyyntiShare-RW" `

-GroupScope DomainLocal `

-GroupCategory Security `

-Description "Myyntiyhdistön luku- ja kirjoitusoikeus FS01 joettuun kansioon" `

-Path "OU=Myynti,DC=rytysxc,DC=local"

```

🔗 Toinen esimerkki: Domain Local -ryhmä resurssioikeuksia varten

```

New-ADGroup ` 
-Name "DL-FS01-MyyntiShare-RW" ` 
-GroupScope DomainLocal ` 
-GroupCategory Security ` 
-Description "Myyntiryhmän luku- ja kirjoitusoikeus FS01-jaettuun kansioon" ` 
-Path "OU=Myynti,DC=yritysxc,DC=local"

```

```

PS C:\Users\Administrator> New-ADGroup ` 
>> -Name "Dilli-Myyntishare-RW" ` 
>>> -GroupScope DomainLocal ` 
>>> -GroupCategory Security ` 
>>> -Description "Myyntiryhmän luku- ja kirjoitusoikeus kansioon" ` 
>>> -Path "OU=Myynti,DC=yritysxc,DC=local" ` 
New-ADGroup : The specified local group already exists
At line:1 char:1
+ New-ADGroup
+ ~~~~~~
    + CategoryInfo          : NotSpecified: (CN=Dilli-Myyntishare-RW,OU=Myynti,DC=yritysxc,DC=local) [New-ADGroup], ADException
    + FullyQualifiedErrorId : ActiveDirectoryServer:1379,Microsoft.ActiveDirectory.Management.Commands.NewADGroup
PS C:\Users\Administrator> New-ADGroup ` 
>> -Name "Dilli-Myyntishare-RW" ` 
>>> -GroupScope DomainLocal ` 
>>> -GroupCategory Security ` 
>>> -Description "Myyntiryhmän luku- ja kirjoitusoikeus kansioon" ` 
>>> -Path "OU=Myynti,DC=yritysxc,DC=local" ` 
At line:1 char:1
+ New-ADGroup
+ ~~~~~~
The output stream for this command is already redirected.
At line:1 char:1
+ New-ADGroup
+ ~~~~~~

```

ryhmät tai käyttäjät.

Syy: Ryhmä luotu oletuskansioon "Users", ei OU:hun "Myynti".
PowerShellin tulosteessa näkyy selvästi:

```

powershell
DistinguishedName : CN=Dilli-Myyntishare-RW,CN=Users,DC=YritysXC,DC=local

```

Tämä tarkoittaa, että ryhmä on luotu AD:n oletussijaintiin CN="Users" container, eli OU="Myynti" -kansioon.

Ratkaisu: siirrä ryhmä oikeaan OU:hun
Jos haluat ryhmän näkyvän Myynti-OU:ssa ADUC:ssa muiden ryhmien kanssa, siirrä se sinne seuraavasti PowerShellillä:

```

powershell
Move-ADObject ` 
-Identity "CN=Dilli-Myyntishare-RW,CN=Users,DC=YritysXC,DC=local" ` 
-TargetPath "OU=Myynti,DC=YritysXC,DC=local"

```

* Tämän jälkeen päivitys (F5) ADUC-näkymä ↓ nyt ryhmän pitäisi näkyä "Myynti"-OU:ssa muiden ryhmien rinnalla.

Tarkista käytössä olevat OU:t näin:

Jos haluat varmistaa, että OU on oikein kirjoitettu,

New-ADGroup `
-Name "Myynti-Tiimikotka-Käyttäjät" `
-GroupScope Global `
-GroupCategory Security `
-Path "OU=Myynti,DC=yritysxc,DC=local"

Tarkista käytössä olevat OU:t näin:

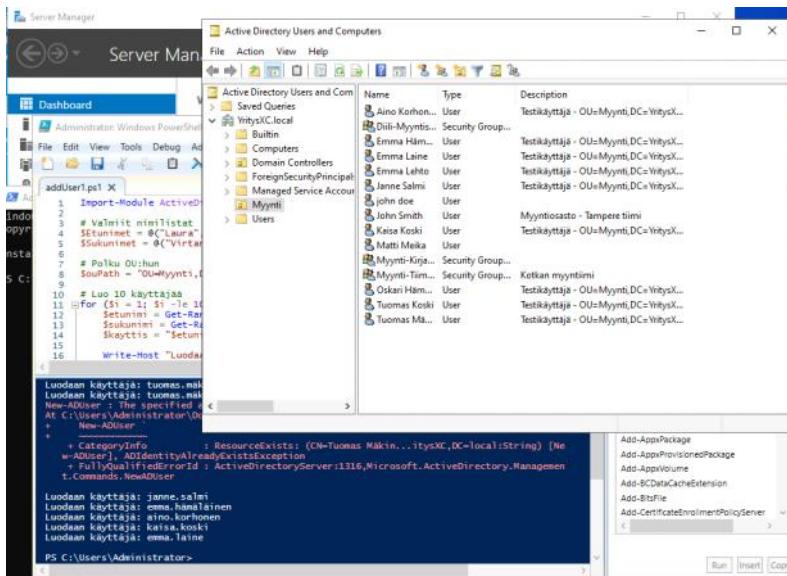
Jos haluat varmistaa, että OU on oikein kirjoitettu, käytä:

```

powershell
Get-ADOrganizationalUnit -Filter * | Select Name, DistinguishedName

```

Tämä näyttää kaikki OU:t ja niiden tarkan polun.



Ylemmässä kuvassa suoritin perus Powershell skriptinsä, että luo esim. 10 satunnaista nimeä ja perus copy-paste, ja antaa sen runnua tuossa (sinisen powershell terminal) alla. Skriptin osuuksien on alhaalla

```
#####
Powershell skripti ja luo 10 satunnaista AD käyttäjää :

Import-Module ActiveDirectory

# Valmitit nimilistat
$Etunimet = @("Laura", "Mikko", "Aino", "Janne", "Emma", "Tuomas", "Saara", "Oskari", "Kaisa", "Antti")
$Sukunimet = @("Virtanen", "Korhonen", "Mäkinen", "Hämäläinen", "Laine", "Heikkinen", "Koski", "Järvinen", "Lehto", "Salmi")

# Polku OU:hun
$ouPath = "OU=Myynti,DC=YritysXC,DC=local"

# Luo 10 käyttäjää
for ($i = 1; $i -le 10; $i++) {
    $etunimi = Get-Random -InputObject $Etunimet
    $sukunimi = Get-Random -InputObject $Sukunimet
    $kayttis = "$etunimi.$sukunimi".ToLower()

    Write-Host "Luodaan käyttäjä: $kayttis"

    New-ADUser `

        -Name "$etunimi $sukunimi" `

        -GivenName $etunimi `

        -Surname $sukunimi `

        -SamAccountName $kayttis `

        -UserPrincipalName "$kayttis@yritysxc.local" `

        -Path $ouPath `

        -AccountPassword (ConvertTo-SecureString "Tervetuloa1!" -AsPlainText -Force) `

        -Enabled $true `

        -ChangePasswordAtLogon $true `

        -Description "Testikäyttäjä - $ouPath"
}

#####
```

 Lisää käyttäjiä ryhmään

`Add-ADGroupMember -Identity "GG-Myynti-TiimiTampere-Kayttajat" -Members "john.smith"`

Muistutus ryhmien käyttööperiaatteista:

Tyyppi	Käyttötarkoitus
◦ Global	Käyttäjien jäsenyydet – lisätään muihin ryhmiin
◦ Domain Local	Resurssien käytööikeudet (esim. jaetut kansiot)
 Universal	Käytetään metsäympäristössä useiden domainien välillä
 Security	Oikeuksia varten
 Distribution	Vain sähköpostilistat (ei oikeuksia)

Powershell - moduulin kirjautuminen

Windows Serverissä, jossa on Active Directory Domain Services (AD DS) -rooli asennettuna, Active Directory -moduuli (ActiveDirectory) on esiasennettu ja valmiina käytettäväksi. Tämä tarkoittaa, että:

- Ei tarvitse erillistä kirjautumista AD-moduuliin
 - Ei oleensä tarvitse edes Import-Module-komentoa erikseen, koska moduuli **ladataan automaattisesti**, kun suoritat ensimmäisen AD-komennon (esim. Get-ADUser).
 - Voi heti käyttää PowerShellissä AD-komentoja, kuten: \$Get-ADUser -Identity john.smith

Digitized by srujanika@gmail.com

Lisää käyttäjiä ja tiettyyn OU:n alle

Tämä on yksi käyttjän lisäminen, että mihin yksikköön OU alle laitettaan

```
New-ADUser ` 
-Name "Jisoo Kim" ` 
-GivenName "Jisoo" ` 
-Surname "Kim" ` 
-SamAccountName "jisookim" ` 
-UserPrincipalName "jisoo.kim@Yritysxc.local" ` 
-Path "OU=Users,OU=Asia,DC=Yritysxc,DC=local" ` 
-AccountPassword (ConvertTo-SecureString "Salainen123!" -AsPlainText -Force) ` 
-Enabled $true
```