4. user ja ryhmät luonti

Monday, October 6, 2025 13:27

Käyttäjä luonti - START HERE;

Luodaan tähän vm (windows server) ympäristön alle siis toinen käyttäjä - ettei turha luoda uutta VM 10/11 konetta käyttöön - koska muuten joutuisi konffata DHCP ja muuta.

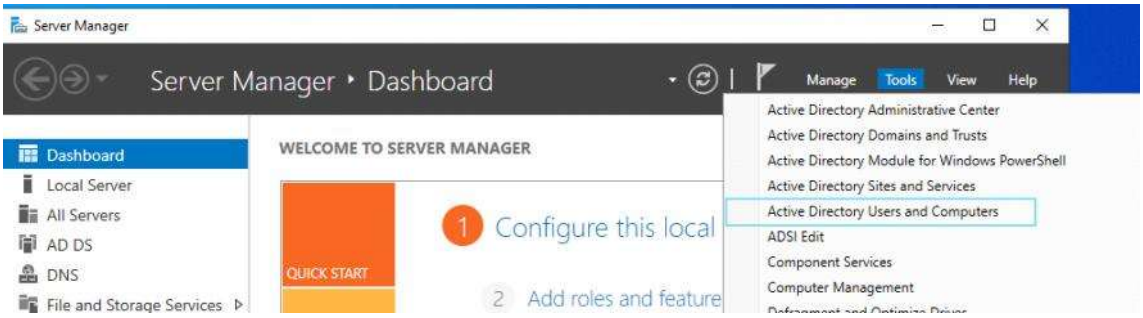
Voidaan **kirjautua ulos ja vaihtaa käyttäjätunnusta** aivan normaalisti, vaikka kyseessä olisi sama domain (esim. yritysxc.local) ja kone olisi liitetty siihen.

- Esim. Päätili "yritysxc.loca\administrator"
- Vara tai muu tunnus: "yritysxc.local\matti.meikalainen"
- Molemmissa on sama passu ja säilytetään ne: P@ssw0rd (nolla)

Tämä voisi toimia myös jos Windows serveri on WIn10 mallinen, ja jos kirjautuu Matti meikäläisen tunnarilla windows 10 tai 11 versiolla.

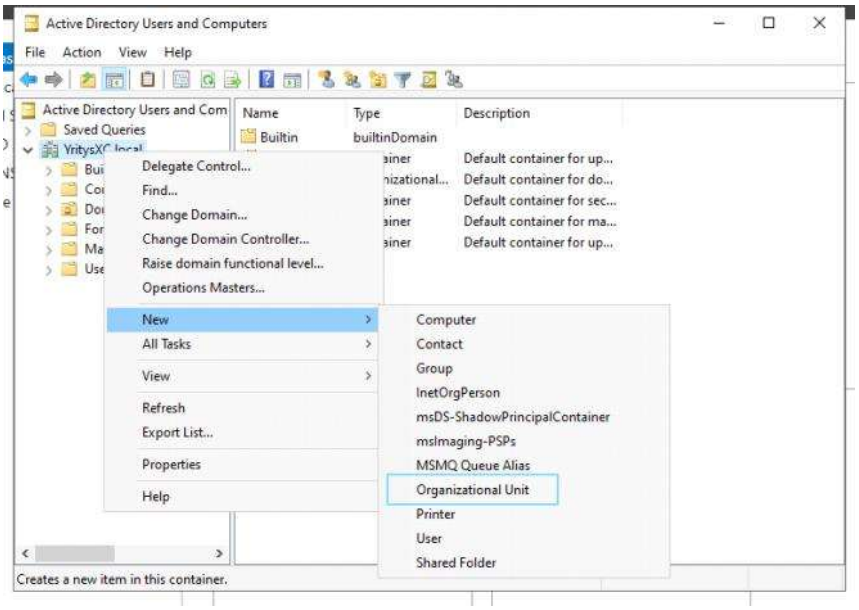
OMA TOIMINTA - START HERE;

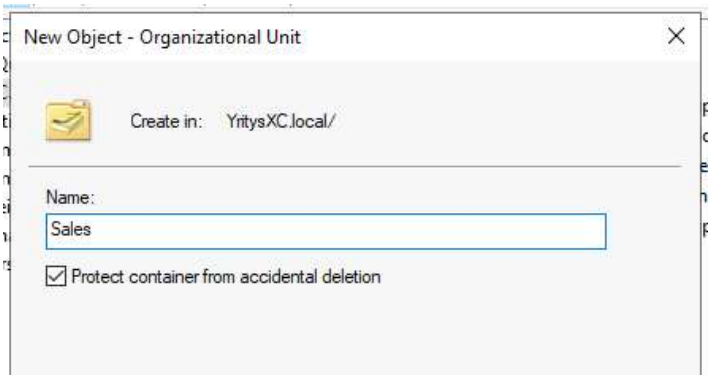
Ihan normaalisti domain administraton alta luodaan se uusi käyttäjä , ja normaalisti tulee jotakin error:in juttua.



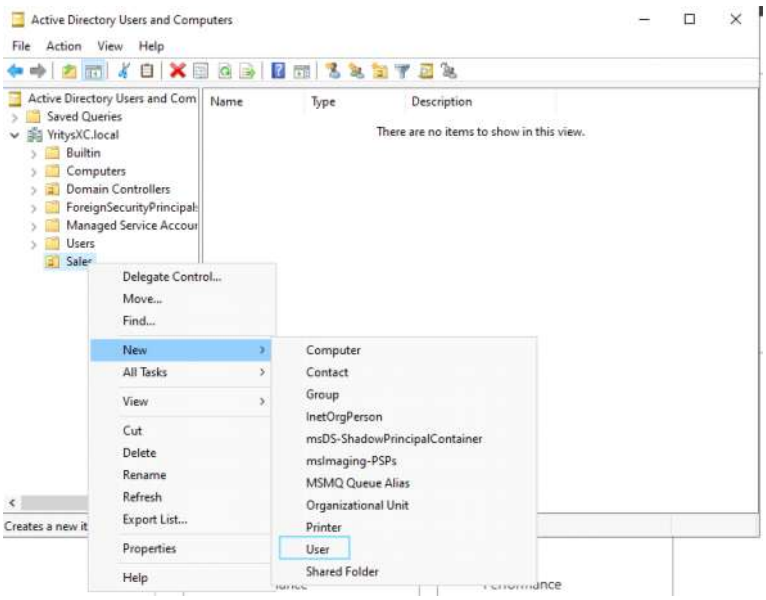
Tähän luodaan kansio ja ikään kuin organisaation yksikkö.

- **Organizational Unit" (OU)** Windowsin **Active Directoryssa (AD)** tarkoittaa **organisatorista yksikköä**, ja se toimii eräänlaisena **säiliönä tai ryhmittymänä** AD:n objekteille. Jossain termistössä tätä käytetään **hakemisrorakenne** tai "kansio", jossa objekteja säilytetään ja hallitaan.





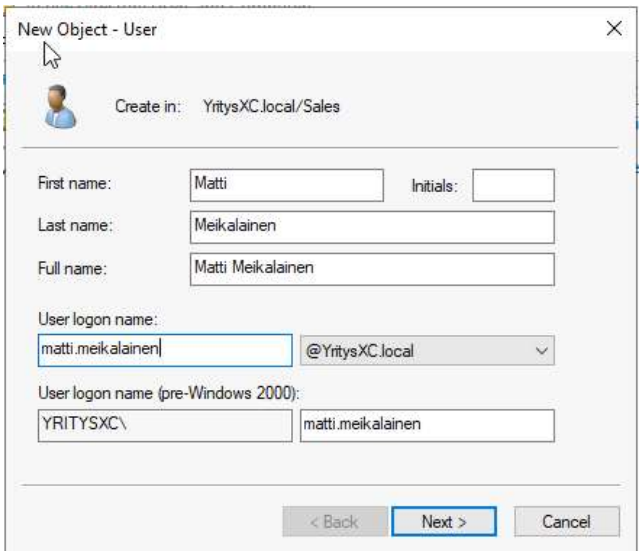
Esim. Tämä "Sale" OU luoneen jälkeen se tulee näkyviinsä tonne "Group policy management" asetuksien alle - ja sitä voi esim. Sieltä asettaa erilliset asetuksensa



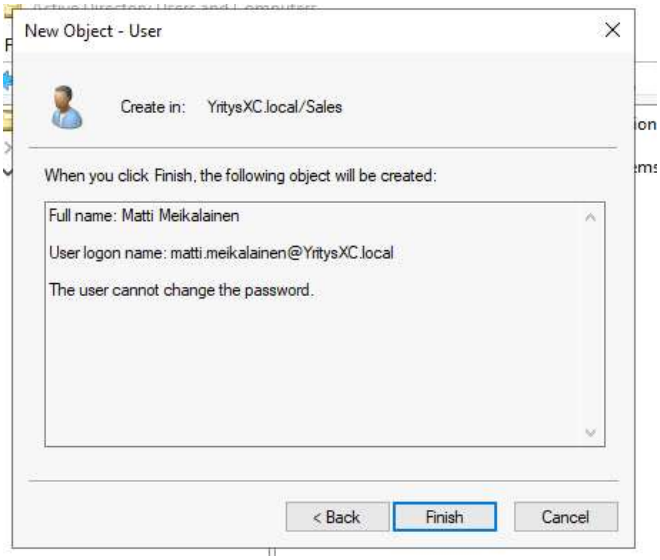
Loin uuden käyttäjän:

- Matti Meika

Nimellä ei ole väliä ja jos on testi tunnus - sekin riittä esim. Etunimi: testi ja sukunimi: testi

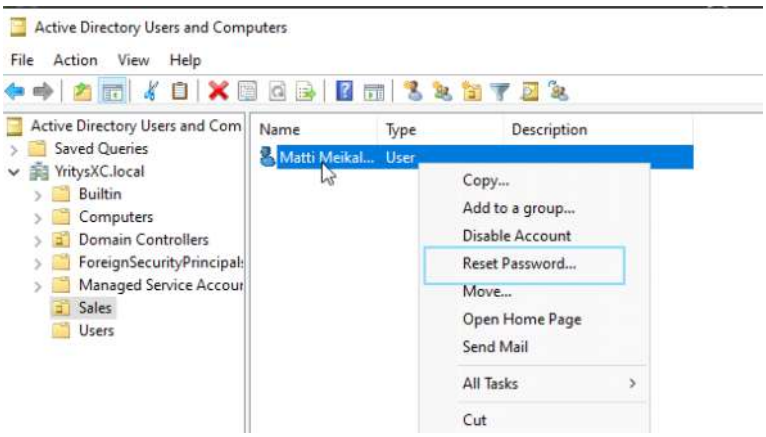


Tässä väliin tulee syöttää joku salasana , niin asetin "P@ssw0rd" ja tulee asettaa esim. Ensimmäisen kirjauttumisen jälkeen tulee resetoida salasanasa.

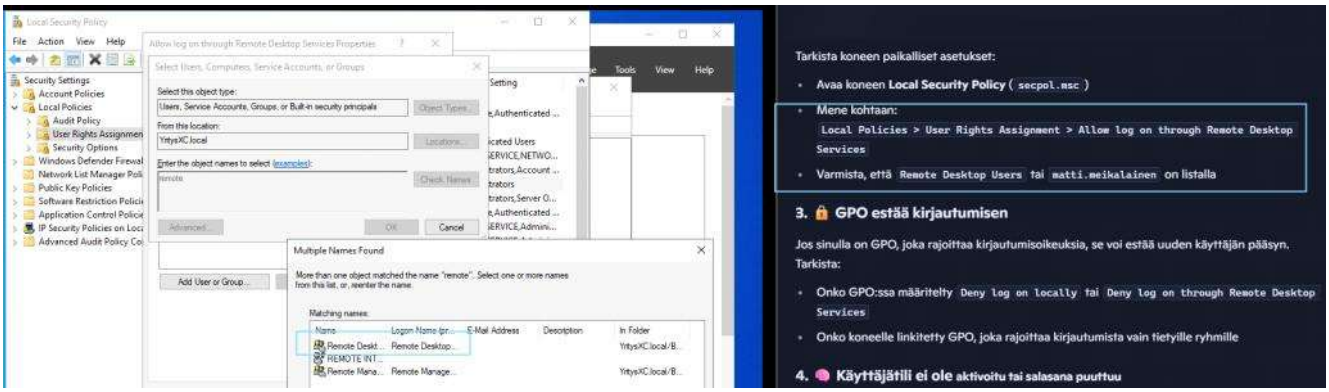


Jos käyttäjä itse (Matti Meikä) ei muista salasansa esim. Resetoidun jälkeen niin pää administrator voi resetoida.

- Tämän kauttakin voidaan resetoida esim. Jos on poistunut käyttäjä (irtisanonut ja lähtenyt firman alta)

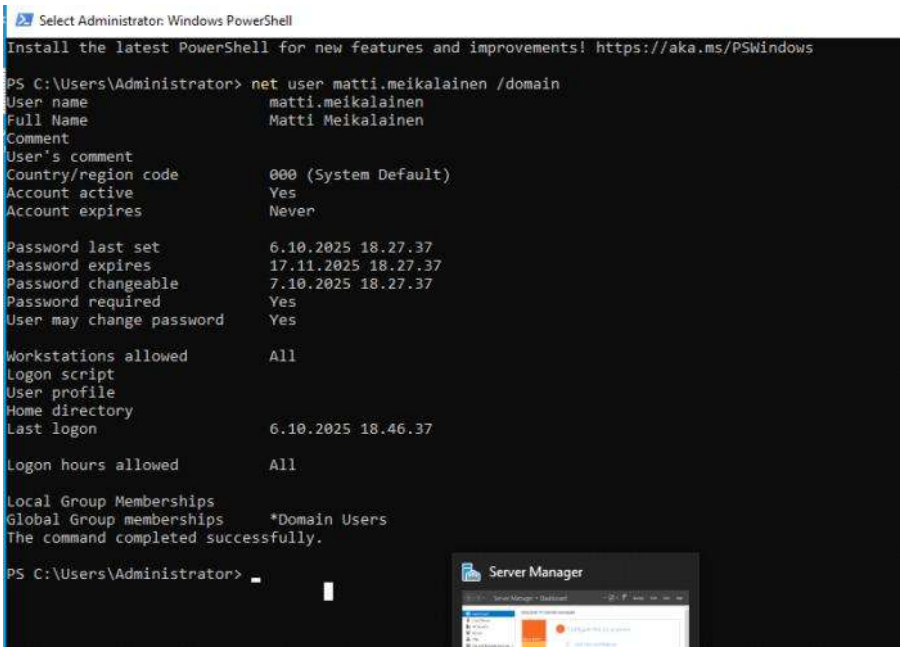


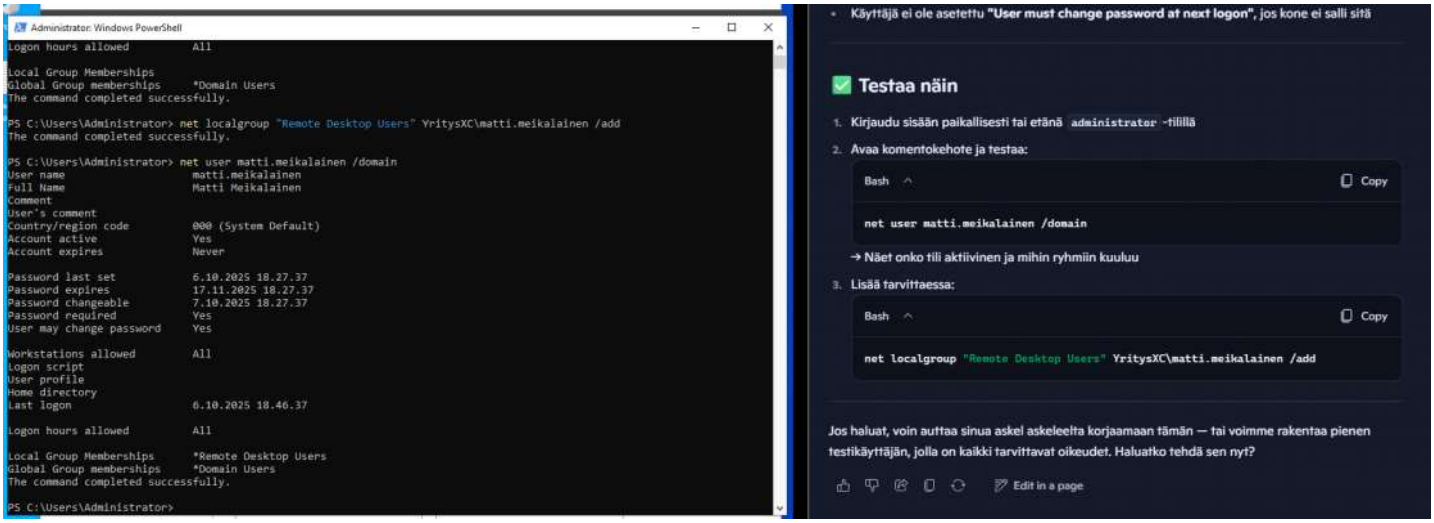
TÄSSÄ VÄLISSÄ OLI SEKAANUSTA TARKISTUSTA - IGNORE PART



Tämä on hyvä tarkistus kohde, että tarkistaa onko lisätty ja mitä oikeutta käyttäjällä on - sama koskien onko hän domain listan alla.

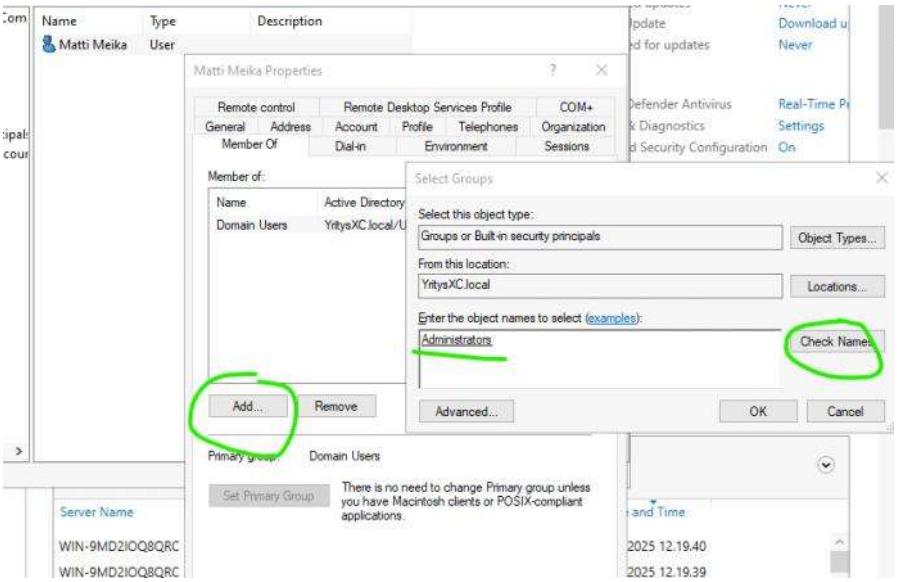
- Tämä pitää suorittaa windows serverin SEN powershell terminaalissa.





Takaisin toimintaa - START HERE;

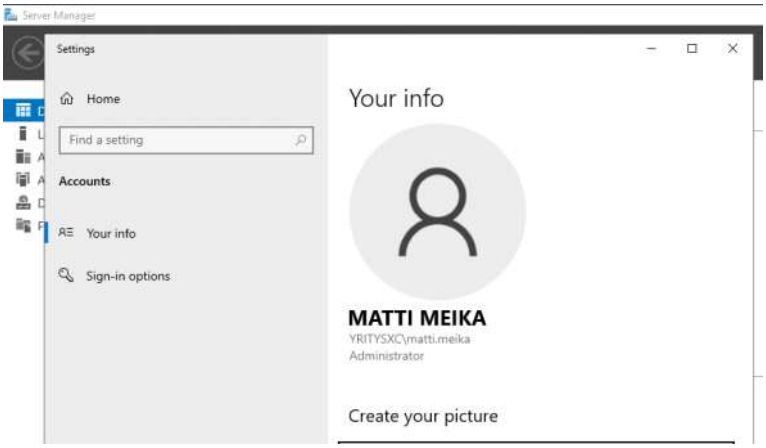
Kokeilin käyttäjästä (oikea hiiren klikkaus) --> Properties ja alta "member of" lisätä esim. Oikeuden. Syötä kentään esim. "ad" ja klikkaa "check names" niin se automaattisesti antaa "administrators" oikeuden käyttäjälle.



Tässä välissä vaihdoin käyttäjänsä ja kirjauduin toisella tunnuksella (change user). Normaalisti ensimmäisen kirjauttuessa se Windows pyyttää normaalisti vaihtamaan salasansa.

TUNNUS:
- Matti.meika
- Uusi passu: Pr0Tectme-

Kirjauttuminen voi mennä näillä vaihtoehdoilla ja toimii:
- matti meika
- matti.meika@YritysXC.local



PIENI YHTEENVETO - START HERE;

Tämä on yksi tapa antaa käyttäjälle järjestelmänvalvojan (administrator) oikeudet Windows Server -ympäristössä – esimerkiksi lisäämällä käyttäjä ryhmään *Administrators* kohdassa **"Member Of"**.

HUOM! Tämä ei ole suositeltu tapa tietoturvan näkökulmasta. Jos kaikille käyttäjille annetaan järjestelmänvalvojan oikeudet, he voivat tehdä muutoksia Windows Serverin asetuksiin, mikä voi johtaa virheisiin, järjestelmän epävakauteen tai jopa tietoturvariskeihin.

☑ Käytä tätä vain erityistapauksissa ja varmista, että käyttäjä todella tarvitsee pääkäyttäjätason oikeuksia.

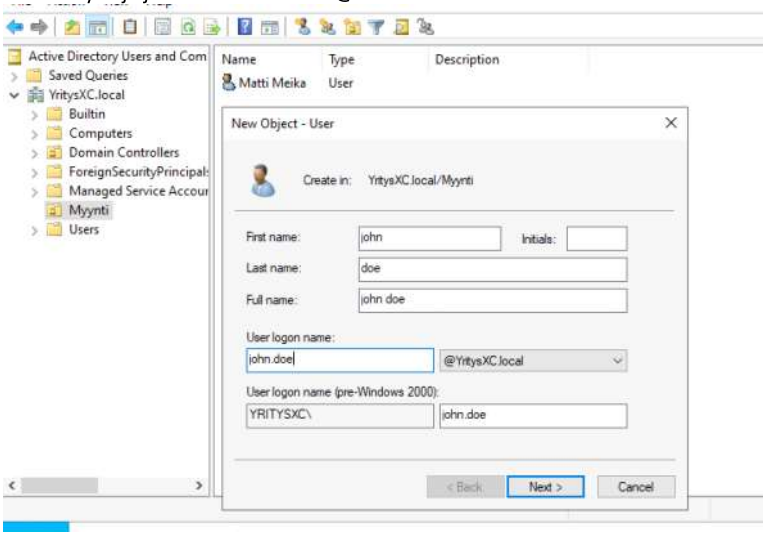
##
##

Kokeillaan luoda uusi käyttäjä - START HERE;

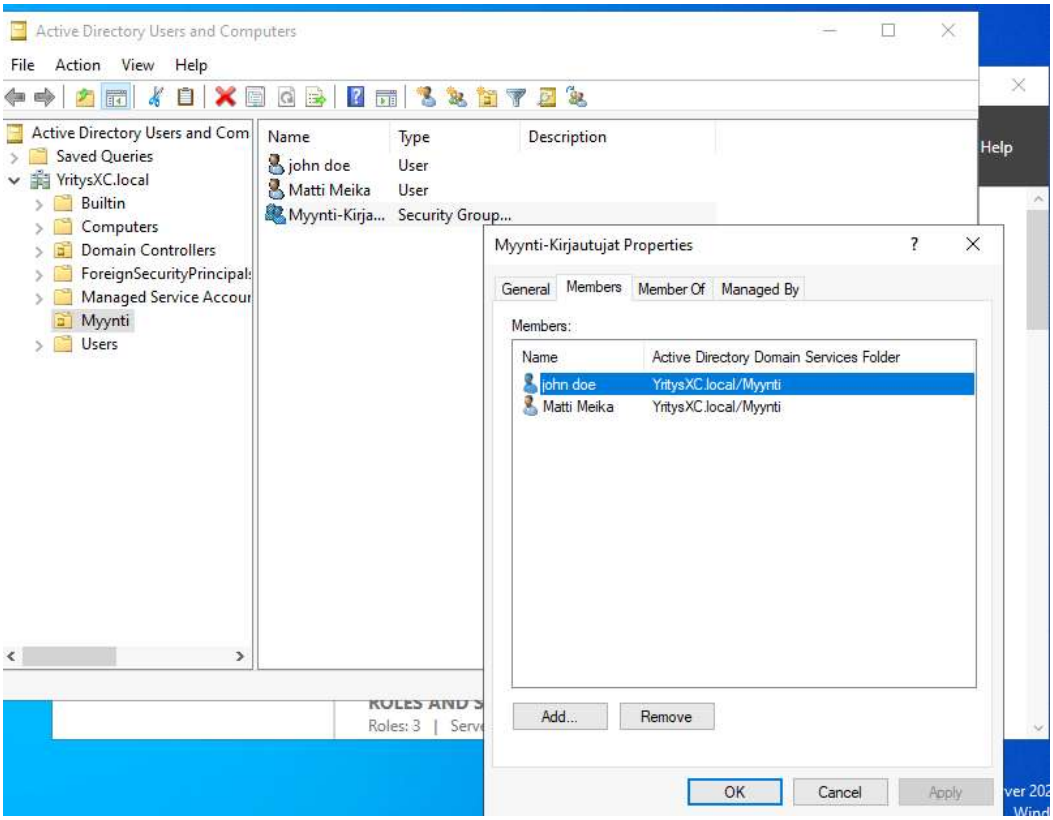
Muutamia ja ehkä vähä isompi haaste itselle, kun ideana oli/on saada esim. Samaan VM (windows serveriin) aseman alle kirjautua toisella tunnuksella, mutta tekoälyn jeesaamista ja saatiin syynsä miksi.

Syy on toisessa kappaleessa, mutta tähän kappaleseen koskien mitä tapahtui ja miksi näin suoritettiin, että vähä saisi ymmärrystä.

Luotu käyttäjä ja oletus salasana "P@ssw0rd"



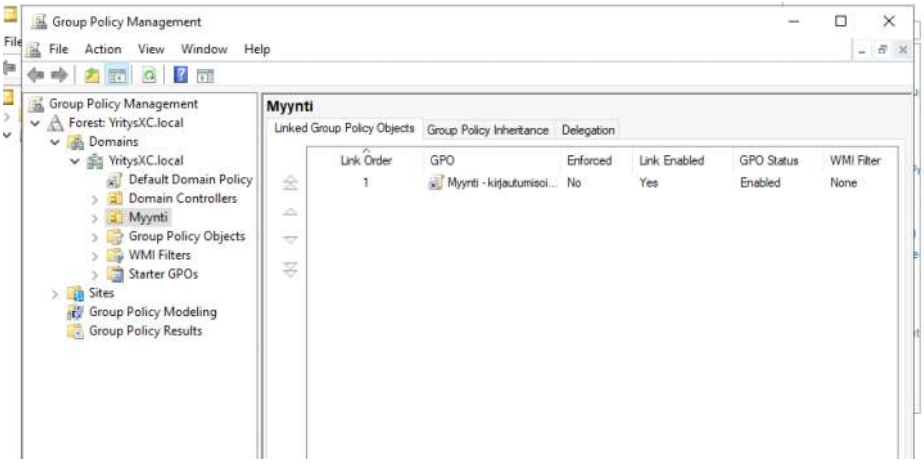
Tästä piti varmistaa, että on lisätty "Myynti (OU)" sisään se ryhmä erikseen, jotta se toimii. Vähä kuin yksikkö (OU) , "myynti-

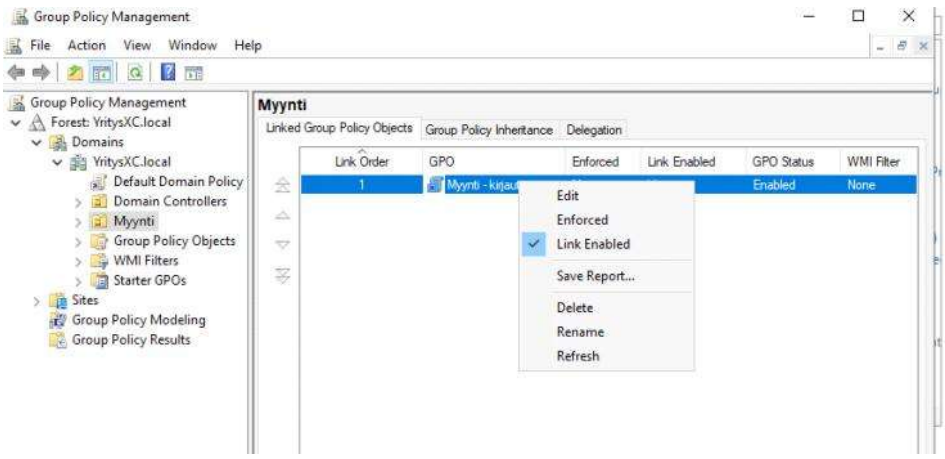


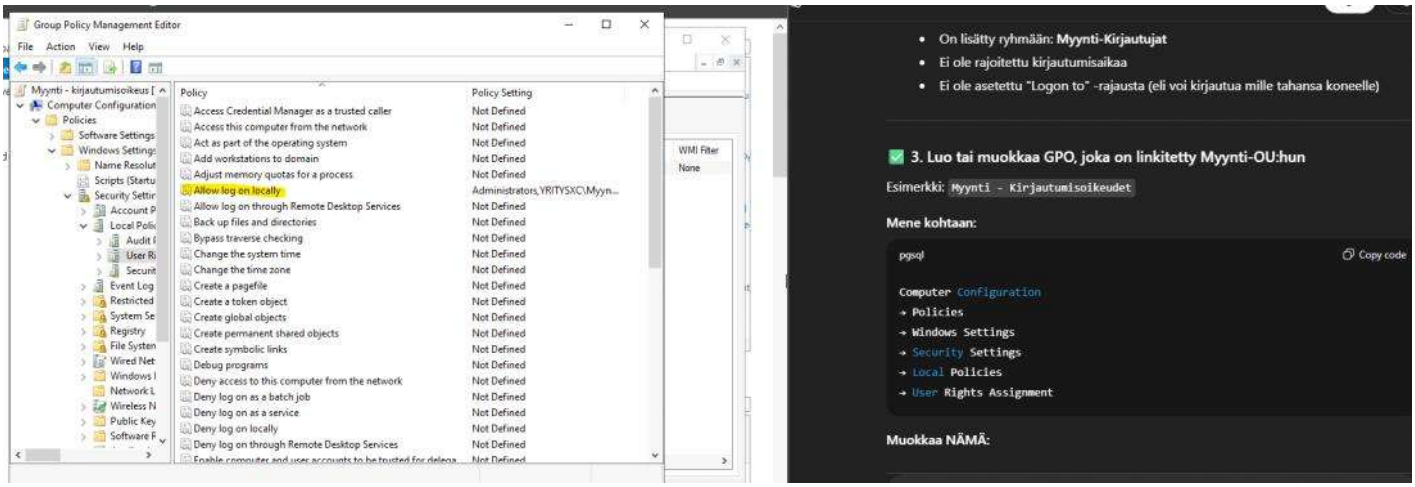
Tässä alettiin tarkistaa ja konffiguroida asetusta, jotta se sallii sen "Myynti -kirjautumisen" ryhmänsä

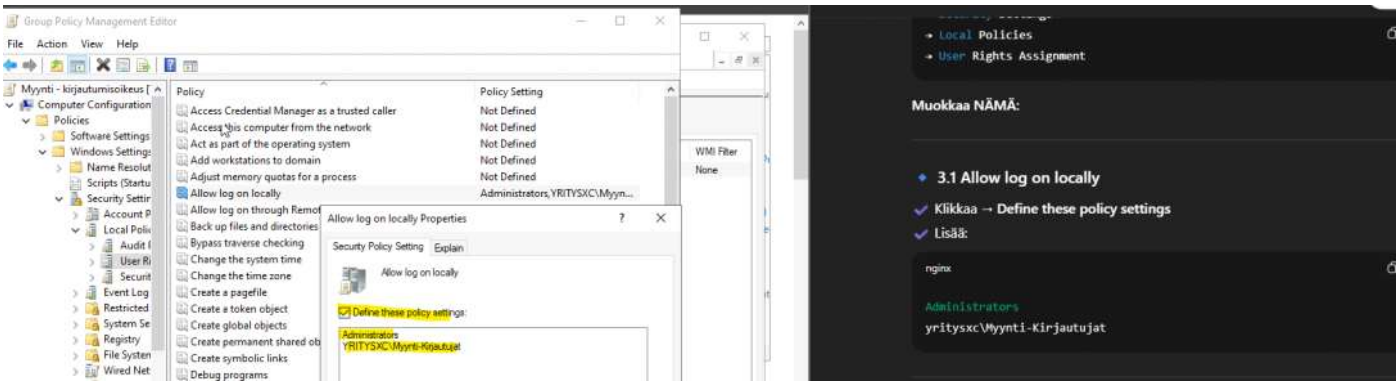
GPO: esim. Myynti – Kirjautumisoikeudet

→ Avaa se Group Policy Managementista ja muokkaa

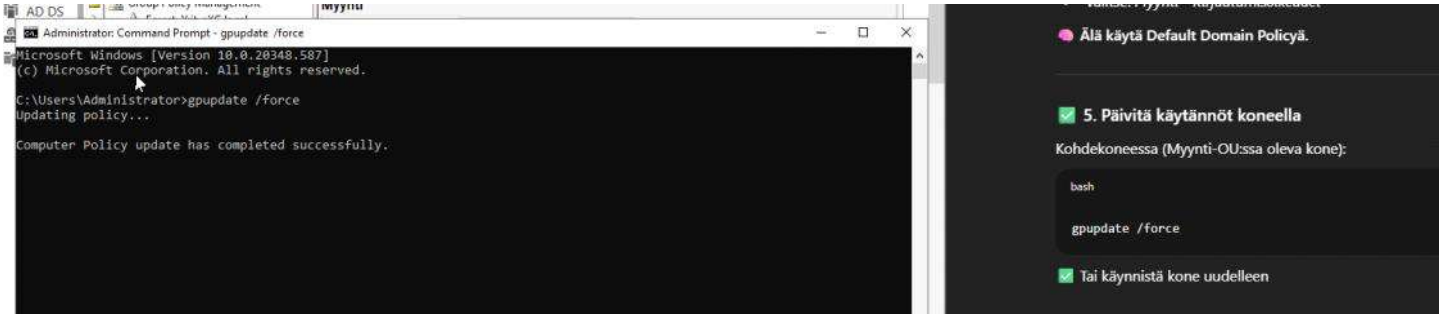








Komennolla ($gupdate /force) toimii cmd:ssä ja ehkä jopa powershell - että päivittää kaikki AD DS ja muut policy asetuksien päivitykset, tai uudelleen buuttaa windows serverinkin voi mahdollista toimia.

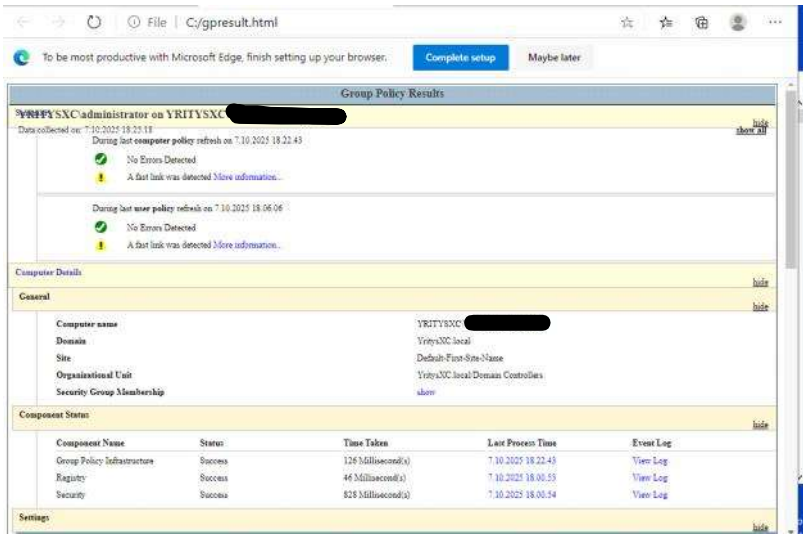


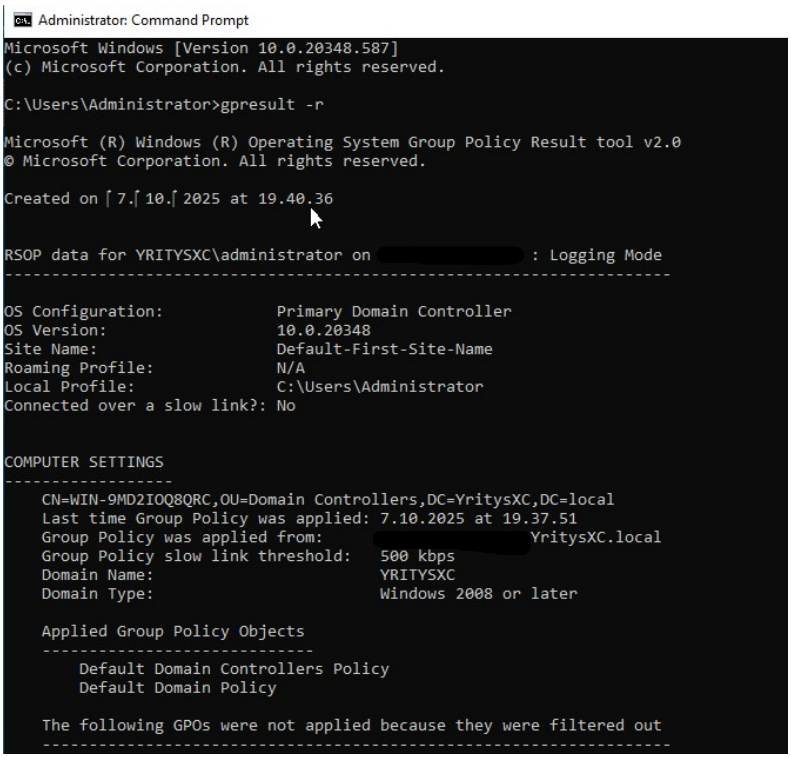
USEITA SYITÄ JA SELVITTÄMINEN

Jos syitä on tosi paljon, että vaikea sanoa ja turha joutua käydä jokaisen policy-asetuksensa lävitse. Nopeitan ja mahdollisesti helpompi syöttää komentoa, josta tulostaa vähä kuin html ja lokituksensa, mitä tässä on oikein tapahtunut ja mitä ollaaan konfiguroitu.

On pari metodia

- yksi on tulostaa html muodossa
- cmd:ssä normi output muodossa





SYY miksi ei toimi - START HERE;

Nyt tulostetaan syy, mutta tässä harjoituksen ideana on/oli tässä windows serverin (VM) ulos kirjautumisella mennään toisella tunnuksella oiskin myynti/laskutus tai muu henkilön tunnuksella - että säästyy esim. Työasema ja vm koneiden käyttö. Kuitenkin konffauksessa ja tämän menetelmä on huono ja miksi, vastaus on alhaalla.

Tämä on se result ouput osuus eli cmd:stä:

```
C:\Users\Administrator>gpresult /r
Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© Microsoft Corporation. All rights reserved.
Created on 7.10.2025 at 18.26.27

RSOP data for YRITYSXC\administrator on [redacted] : Logging Mode
-----------------------------------------------------------------------
OS Configuration:            Primary Domain Controller
OS Version:                  10.0.20348
Site Name:                   Default-First-Site-Name
Roaming Profile:             N/A
Local Profile:               C:\Users\Administrator
Connected over a slow link?: No

COMPUTER SETTINGS
------------------
    CN=[redacted],OU=Domain Controllers,DC=YritysXC,DC=local
```

```
    Group Policy was applied from:      [redacted].YritysXC.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        YRITYSXC
    Domain Type:                        Windows 2008 or later
    Applied Group Policy Objects
    ----------------------------
        Default Domain Controllers Policy
        Default Domain Policy
    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)
    The computer is a part of the following security groups
    ------------------------------------------------------
        BUILTIN\Administrators
        Everyone
        BUILTIN\Pre-Windows 2000 Compatible Access
        BUILTIN\Users
        Windows Authorization Access Group
        NT AUTHORITY\NETWORK
        NT AUTHORITY\Authenticated Users
        This Organization
        [redacted]
        Domain Controllers
        NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
        Authentication authority asserted identity
        Denied RODC Password Replication Group
        System Mandatory Level

USER SETTINGS
--------------
    CN=Administrator,CN=Users,DC=YritysXC,DC=local
    Last time Group Policy was applied: 7.10.2025 at 18.25.36
    Group Policy was applied from:      [redacted].YritysXC.local
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        YRITYSXC
    Domain Type:                        Windows 2008 or later
    Applied Group Policy Objects
    ----------------------------
        N/A
    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)
    The user is a part of the following security groups
    ---------------------------------------------------
        Domain Users
        Everyone
        BUILTIN\Administrators
        BUILTIN\Users
        BUILTIN\Pre-Windows 2000 Compatible Access
        NT AUTHORITY\INTERACTIVE
        CONSOLE LOGON
        NT AUTHORITY\Authenticated Users
        This Organization
        LOCAL
        Group Policy Creator Owners
        Domain Admins
        Enterprise Admins
        Schema Admins
        Authentication authority asserted identity
        Denied RODC Password Replication Group
        High Mandatory Level
C:\Users\Administrator>
```

################

Mitä tässä oikein lukekaan?

Koneessa lukee näin (WIN-9MD2IOQ8QRC) on Domain Controller (DC)

- OS Configuration: Primary Domain Controller
  CN=WIN-9MD2IOQ8QRC,OU=Domain Controllers,DC=YritysXC,DC=local

Mitä tuo rivi tarkoittaa?

Purettuna:

- CN=[redacted]= Koneen (Computer Object) nimi

- **OU=Domain Controllers** = Tämä kone sijaitsee **"Domain Controllers"** -nimisessä **Organizational Unitissa (OU)** Active Directoryssä
- **DC=YritysXC,DC=local** = Domainisi nimi: YritysXC.local

- SYY:
  Tämä tarkoittaa, että kone, johon yrität kirjautua john.doe-käyttäjällä, on domain controller.
  Tavalliset käyttäjät EIVÄT voi kirjautua domain controllerille.

🔓 Miksi tämä on tärkeää?

- **Normaalit käyttäjät**, kuten john.doe, **eivät saa kirjautua domain controlleriin (DC)**, ellei heillä ole **erityisiä oikeuksia** tai he ovat **admin-ryhmissä**.
- GPO-asetukset kuten "Allow log on locally" ja "Allow log on through RDP" eivät yksin riitä, koska **DC:llä on erityiset rajoitukset**.

🎯 Ratkaisuvaihtoehdot

☑ Vaihtoehto 1: Käytä toista konetta, joka EI ole domain controller

- Luo toinen **Windows 10/11-virtuaalikone (tai palvelin)**, liitä se domainiin YritysXC.local
- Yritä kirjautua sinne käyttäjällä yritysxc\john.doe
- Tämä toimii, kunhan GPO:t on oikein (kuten aiemmin määriteltiin)

👉 **Tämä on normaali ja suositeltu tapa testata AD-kirjautumista**

⚠ Vaihtoehto 2: Jos Haluat Pakottaa Pääsyn DC:lle (ei suositeltu harjoittelussa)

- Voit antaa ryhmälle Myynti-Kirjautujat oikeuden kirjautua myös domain controllerille, muokkaamalla **Default Domain Controllers Policy** -GPO:ta

  Group Policy Management
  → Forest → Domains → YritysXC.local → Domain Controllers → Default Domain Controllers Policy

  Computer Configuration
  → Policies
  → Windows Settings
  → Security Settings
  → Local Policies
  → User Rights Assignment

  Ja lisää (molempiin kenttään siis)
  - Allow log on locally
  - Allow log on through Remote Desktop Services

  ➕ Lisää ryhmä: yritysxc\Myynti-Kirjautujat
  ❗ **VAROITUS:** Tämä ei ole suositeltavaa oikeassa tuotantoympäristössä eikä harjoittelussakaan pidemmän päälle, koska se rikkoo periaatetta:
  "Vain adminit kirjautuvat domain controllereille."

Suosituksena rakentaisi uuden VM koneensa eli Windows 10/11 koneensa käyttöön ja kirjautuu sisään, että sillä kautta liittää sen työasemaan. Näin saattaisiin ja varmistettua liittyneen yrityksen domain (yritysxc.local)alle.

MINI YHTEENVETO:

Tässä konfigurointi asetuksessa kokoajan yritettiin **kirjautua koneelle, joka on domain controller**, ja siksi gpresult /r -tulosteessa näkyi tämä rivi:

- *CN=[redacted]OU=Domain Controllers,DC=YritysXC,DC=local*

Kyseinen windows serveri ja kone on "domain controller", koska sijaitsee OU:ssa ja siksi tavallinen käyttäjä (john.doe ja aikaisepi Matti Meika) ei pääsy koskaan kirjautua. Tavallisilla käyttäjillä ei ole oikeutta kirjautua Domain Controlleriin, **eikä pidäkään olla** — paitsi jos heille annetaan erikseen erikoisoikeudet (ei suositeltavaa).

Paras keinona on luoda uusi VM ohjelma ja erikseen omana windows 10/11 ja sillä kirjautua sisään, että liittää samaan verkon ympäristöön ja sillä varmistuksena on liitetty active directory yrityksen local yhteyteen.

##
##

Miksi tavallinen käyttäjä ei saa kirjautua Domain Controllerille (DC)?

🔐 Perusvastaus:

Koska **domain controller on yrityksen sydän**, ja sille pääsyn tulisi olla **erityisesti rajattua vain järjestelmänvalvojille (admin)**.

Tämä ei ole pelkkä suositus — se on osa **parhaita käytäntöjä (best practices)** tietoturvassa ja kyberturvallisuudessa.

🧠 Teoreettinen näkökulma

1. 💾 Domain controller sisältää koko yrityksen käyttäjätunnukset, salasanat ja oikeudet

- DC ylläpitää **Active Directory** -tietokantaa
- Jokaisen käyttäjän:
  - Salasanojen tiivisteet
  - Oikeudet
  - Ryhmäjäsenyydet
  - GPO:t ja niihin liittyvät konfiguraatiot

➡️ **Jos DC vaarantuu, koko yritys on vaarantunut.**

2. 🎯 Tietoturvapolitiikan ja least privilege -periaatteen mukaan

Least privilege principle = Käyttäjällä on vain ne oikeudet, joita hän tarvitsee – ei enempää.

- Tavallinen käyttäjä ei koskaan tarvitse kirjautumisoikeutta DC:lle
- Vain ne, jotka **ylläpitävät** DC:tä (Domain Admins, IT-infra) kirjautuvat sinne

3. ⚠️ Kirjautuminen DC:lle = Mahdollinen uhkavektori

Jos tavallinen käyttäjä voi kirjautua:

- Voi yrittää nostaa oikeuksia (privilege escalation)
- Voi käyttää työkaluja, jotka pääsevät käsiksi AD-tietokantaan
- Voi päätyä haittaohjelman tai kiristysohjelman (ransomware) kohteeksi → joka pääsee DC:lle

💣 *Esimerkiksi: Haittaohjelma käyttäjän profiilissa voi iskeä suoraan ntds.dit-tiedostoon (AD:n tietokanta), jos se saa pääsyn DC:lle.*

🔐 Tietosuoja ja GDPR-näkökulma

- DC sisältää **henkilötietoja** (nimi, sähköposti, tunnus, mahdollisesti työrooli)
- GDPR:n mukaan nämä tiedot on **suojattava teknisesti ja organisatorisesti**
- Tavallinen käyttäjä, jolla on pääsy DC:lle, voi **vahingossa tai tahallaan** päästä käsiksi tietoihin, joita hän ei ole oikeutettu näkemään

🛡️ Kyberturvallisuuden näkökulma

Tavallisen käyttäjän pääsy DC:lle rikkoo:

- **Zero Trust -periaatetta** (ei luoteta kehenkään oletusarvoisesti)
- **Access Control -periaatteita** (pääsy vain roolin mukaan)
- **Vaatimuksia esim. ISO 27001, NIST, GDPR, VAHTI jne.**

🩹 Esimerkki riskistä

Käyttäjä john.doe pääsee DC:lle → lataa PowerShell-skriptin → suorittaa recon-komennon kuten Get-ADUser -Filter * → saa listan kaikista käyttäjistä → lähettää ulos sähköpostilla

➡️ Tämä on **datan vuoto**, ja **hallinnollinen virhe**, josta **sinä adminina** olisit vastuussa.