

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.

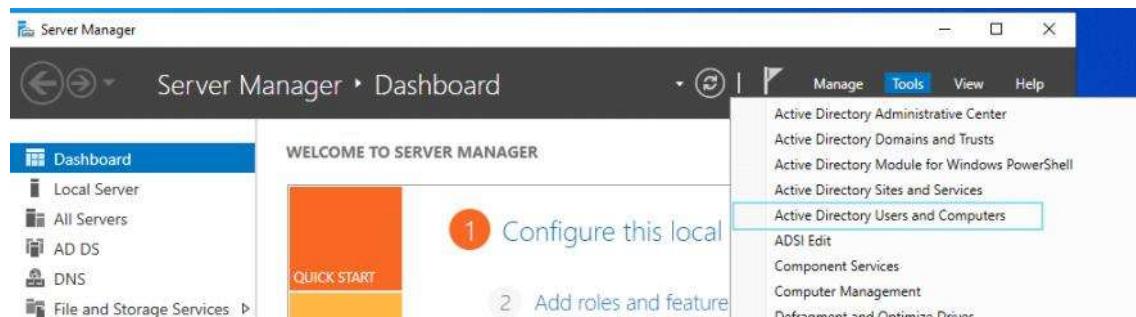
Voidaan **kirjautua ulos ja vaihtaa käyttäjätunnusta** aivan normaalisti, vaikka kyseessä olisi sama domain (esim. yritysxc.local) ja kone olisi liitetty siihen.

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

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

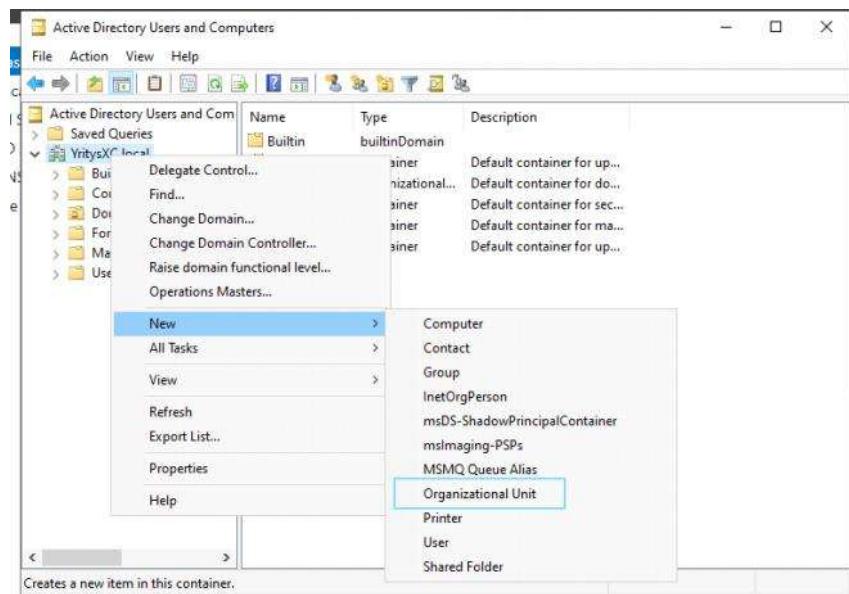
OMA TOIMINTA - START HERE;

Ihan normaalista domain administraton alta luodaan se uusi käyttäjä , ja normaalista 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 eräänlainen sääliönä tai ryhmittyminä AD:n objekteille. Jossain termistössä tättä käytetään **hakemisrakennetta** tai "kansio", jossa objekteja säilytetään ja hallitaan.



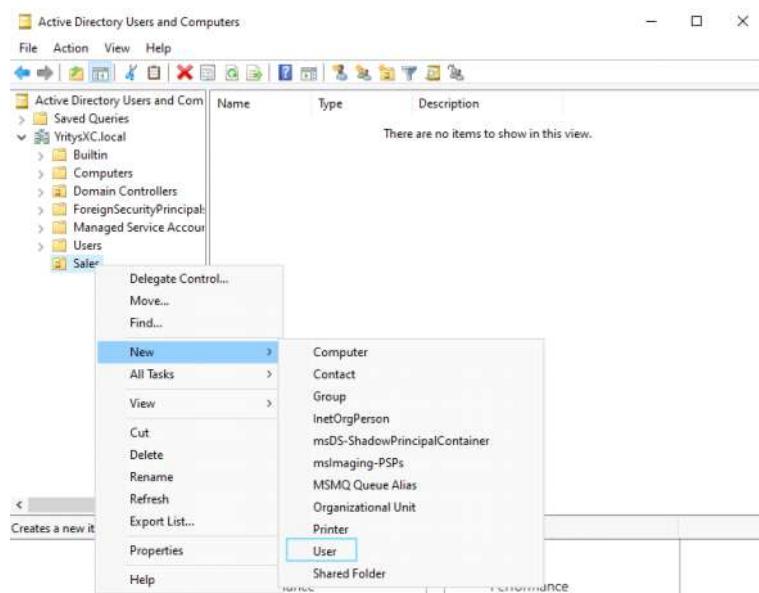
New Object - Organizational Unit

Create in: YritysXC.local/

Name: Sales

Protect container from accidental deletion

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 - sekä riittää esim. Etunimi: testi ja sukunimi: testi

New Object - User

Create in: YritysXC.local/Sales

First name: Matti Initials: [empty]

Last name: Meikalainen

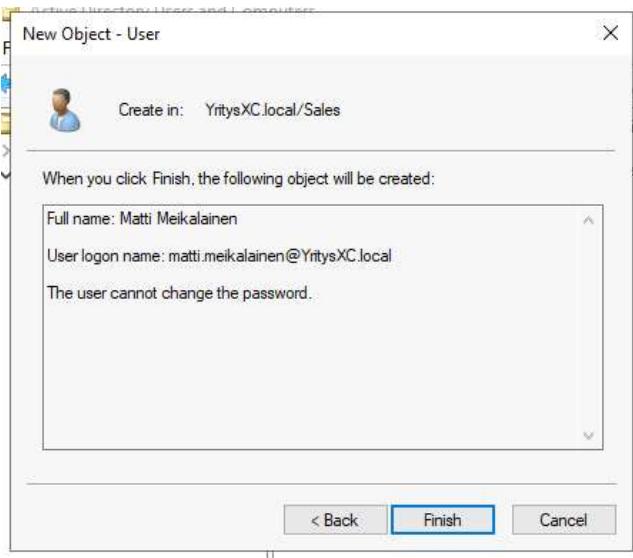
Full name: Matti Meikalainen

User logon name: matti.meikalainen @YritysXC.local

User logon name (pre-Windows 2000): YRITYSXC\matti.meikalainen

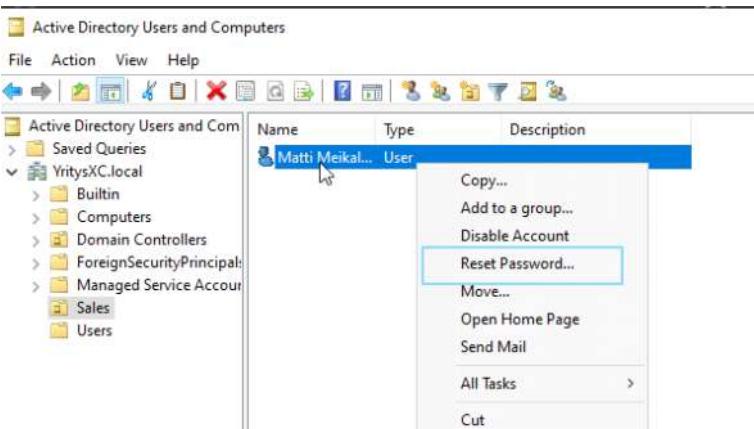
< Back Next > Cancel

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



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

Tarkista koneen paikalliset asetukset:

- Avaa koneen Local Security Policy (secpol.msc)
- Mene kohti: Local Policies > User Rights Assignment > Allow log on through Remote Desktop Services
- Varmista, että Remote Desktop Users tai matti.meikalainen on listalla

3. 🔒 GPO estää kirjautumisen

Jos sinulla on GPO, joka rajoittaa kirjautumisoikeuksia, se voi estää uuden käyttäjän pääsyn. Tarkista:

- Onko GPO:ssa määritetty Deny log on locally tai Deny log on through Remote Desktop Services
- Onko koneelle linkitetty GPO, joka rajoittaa kirjautumista vain tiettyille ryhmille

4. 🚫 Käyttäjätili ei ole aktivoitu tai salasana puuttuu

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.

Select Administrator Windows PowerShell

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

```
PS C:\Users\Administrator> net user matti.meikalainen /domain
User name          matti.meikalainen
Full Name         Matti Meikalainen
Comment
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never

Password last set   6.10.2025 18.27.37
Password expires    17.11.2025 18.27.37
Password changeable 7.10.2025 18.27.37
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon        6.10.2025 18.46.37

Logon hours allowed All

Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.
```

PS C:\Users\Administrator>

Administrator: Windows PowerShell

```
Logon hours allowed All

Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.

PS C:\Users\Administrator> net localgroup "Remote Desktop Users" YritysXC\matti.meikalainen /add
The command completed successfully.

PS C:\Users\Administrator> net user matti.meikalainen /domain
User name          matti.meikalainen
Full Name         Matti Meikalainen
Comment
User's comment
Country/region code    000 (System Default)
Account active      Yes
Account expires     Never

Password last set   6.10.2025 18.27.37
Password expires    17.11.2025 18.27.37
Password changeable 7.10.2025 18.27.37
Password required    Yes
User may change password Yes

Workstations allowed All
Logon script
User profile
Home directory
Last logon        6.10.2025 18.46.37

Logon hours allowed All

Local Group Memberships *Remote Desktop Users
Global Group memberships *Domain Users
The command completed successfully.

PS C:\Users\Administrator>
```

• Käyttäjä ei ole asetettu "User must change password at next logon", jos kone ei sali sitä

Testaa näin

1. Kirjaudu sisään paikallisesti tai etäältä `administrator`-tilillä
2. Avaa komentokehote ja testaa:

```
Bash ^ 
net user matti.meikalainen /domain
```

→ Näet onko tili aktiivinen ja mihin ryhmään kuuluu

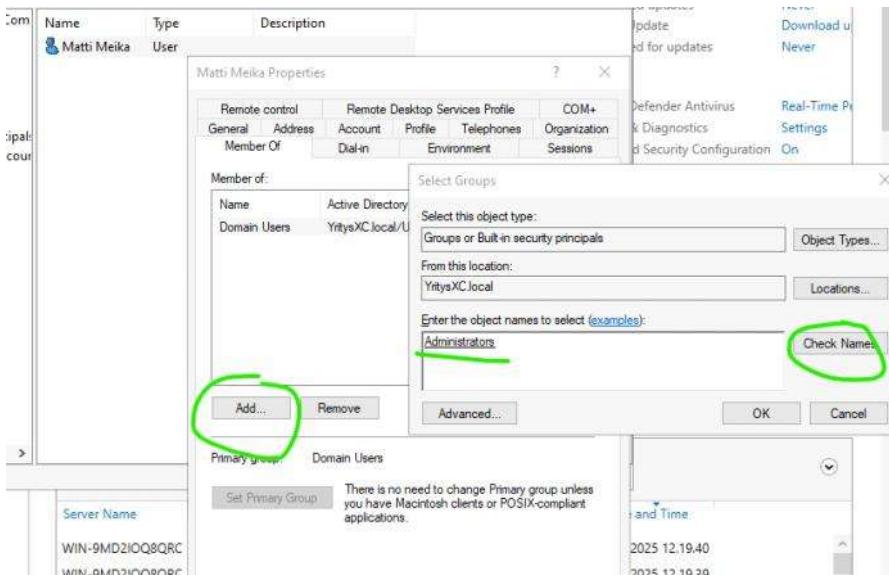
3. Lisää farvittaaessa:

```
Bash ^ 
net localgroup "Remote Desktop Users" YritysXC\matti.meikalainen /add
```

Jos haluat, voin auttaa sinua askel askeleita korjaamaan tämän — tai voimme rakentaa pienen testikäyttäjän, jolla on kaikki tarvittavat oikeudet. Haluatko tehdä sen nyt?

Takaisin toimintaan - 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.



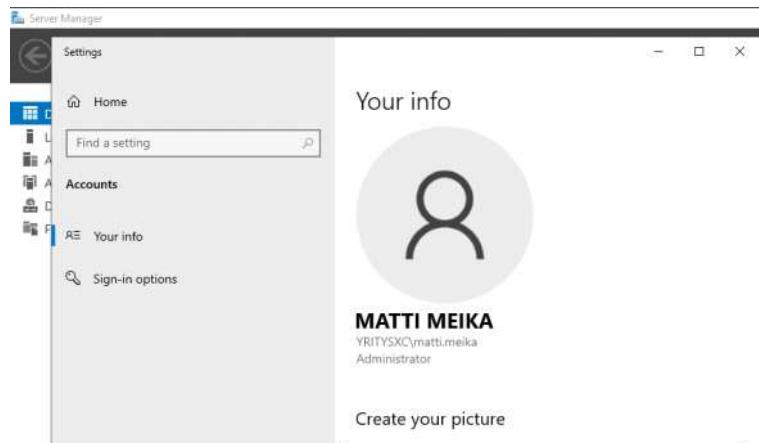
Tässä välissä vähdoxin käyttäjänsä ja kirjauduun toisella tunnuksella (change user). Normaalista ensimmäisen kirjautuessa se Windows pyytää normaalista vaihtamaan salasansa.

TUNNUS:

- Matti.meika
- Uusi passu: Pr0TECTme-

Kirjautuminen voi mennä näillä vaihtoehdolla 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;

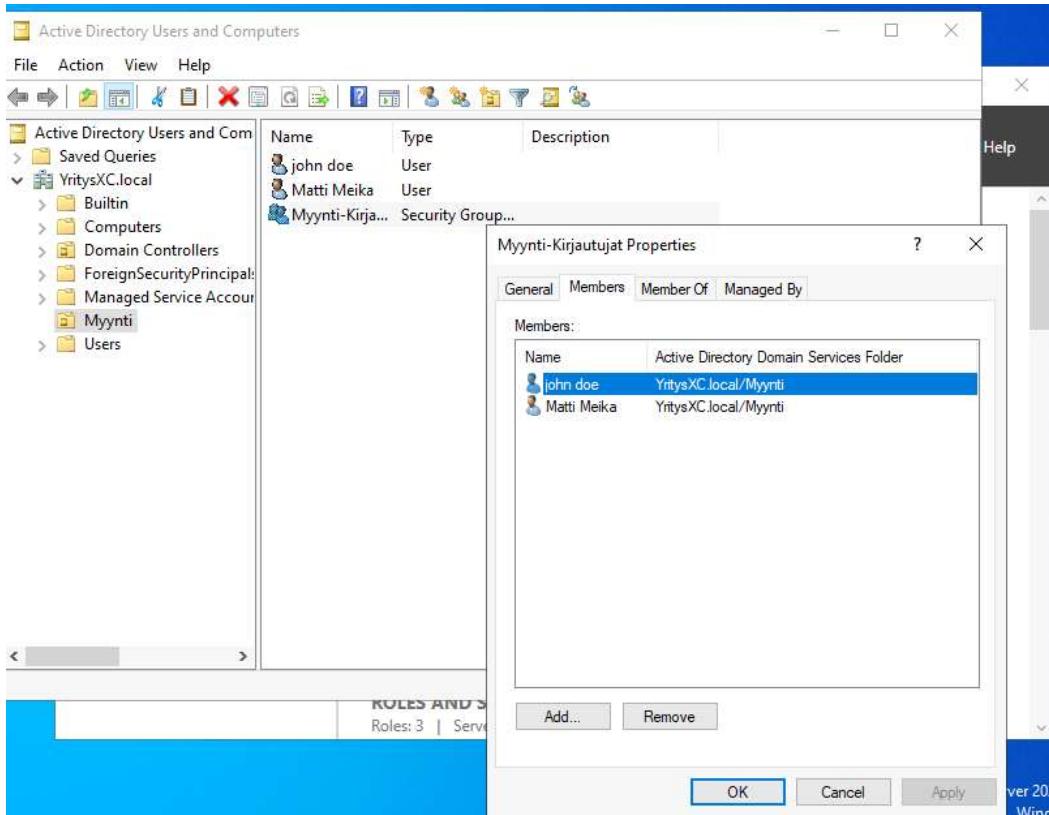
Muutamia ja ehkä vähä isompi haaste itselle, kun ideana oli/on saada esim. Samaan VM (windows serveriin) aseman alle kirjautua toisella tunnuksella, mutta tekölyn jeesaamista ja saatiin syynsä miksi.

Syy on toisessa kappaleessa, mutta tähän kappaleeseen koskien mitä tapahtui ja miksi nän suoritettiin, että vähä sasisi ymmärrystä.

Luotu käyttäjä ja oletus salasana "P@sswOrd"

A screenshot of the Active Directory Users and Computers (ADUC) management console. On the left, the navigation pane shows 'Active Directory Users and Computers' under 'View' and lists 'Saved Queries', 'YritysXC.local' (with 'Builtin', 'Computers', 'Domain Controllers', 'ForeignSecurityPrincipal', 'Managed Service Account', 'Myynti', and 'Users' subfolders), and 'Windows PowerShell'. The main window displays a table with one row: 'Name' (Matti Meika), 'Type' (User), and 'Description'. A modal dialog box titled 'New Object - User' is open, showing fields for 'First name' (john), 'Last name' (doe), and 'Full name' (john doe). Under 'User logon name', the value 'john.doe' is entered, followed by '@YritysXC.local'. Below that, 'User logon name (pre-Windows 2000)' shows 'YRITYSXC\john.doe'. At the bottom of the dialog are buttons for '< Back', 'Next >', and 'Cancel'.

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



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

GPO: esim. Myynti – Kirjautumisoikeudet

→ Avaa se Group Policy Managementista ja muokkaa

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter
1	Myynti - kirjautumiso...	No	Yes	Enabled	None

The context menu for the selected GPO includes the following options:

- Edit
- Enforced
- Link Enabled** (highlighted)
- Save Report...
- Delete
- Rename
- Refresh

The screenshot shows the Group Policy Management Editor interface. On the left, the navigation pane shows a tree structure under 'Myynti - kirjautumisoikeudet'. In the main pane, a policy setting for 'Allow log on locally' is selected. The 'Policy Setting' column shows 'Not Defined' for most items. A WMI Filter is set to 'None'. On the right, there is a detailed description of the policy setting and a note about its scope.

- On lisätty ryhmään: Myynti-Kirjautujat
- Ei ole rajoitettu kirjautumisaikaa
- Ei ole asetettu "Logon to" -rajausta (eli voi kirjautua mille tahansa koneelle)

3. Luo tai muokkaa GPO, joka on linkitetty Myynti-OU:hun

Esimerkki: Myynti - Kirjautumisoikeudet

Mene kohtaan:

ppsql

Computer Configuration

- Policies
- Windows Settings
- Security Settings
- Local Policies
- User Rights Assignment

Muokkaa NÄMÄ:

This screenshot shows the 'Allow log on locally' policy setting properties dialog box. It includes tabs for 'Allow log on locally Properties', 'Security Policy Setting', and 'Explain'. Under 'Allow log on locally Properties', the 'Define these policy settings' checkbox is checked. The 'Administrators' and 'YRITYSXC\Myynti-Kirjautujat' user accounts are listed as defined.

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.

The terminal window shows the command \$gupdate /force being run. The output indicates that the computer policy update has completed successfully.

Administrator Command Prompt - gupdate /force

Microsoft Windows [Version 10.0.20348.587]

(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gupdate /force

Updating policy...

Computer Policy update has completed successfully.

Terminal window on the right shows the command 'gupdate /force' entered in a bash shell.

Älä käytä Default Domain Policyä.

5. Päivitä käytännöt koneella

Kohdekoneessa (Myynti-OU:ssa oleva kone):

```
bash
gupdate /force
```

Tai käynnistä kone uudelleen

USEITA SYTÄ JA SELVITTÄMINEN

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

On pari metodia

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

Group Policy Results

Data collected on 7.10.2025 18:23:18
During last computer policy refresh on 7.10.2025 18:22:49

- No Errors Detected
- A fast link was detected [More information...](#)

During last user policy refresh on 7.10.2025 18:06:06

- No Errors Detected
- A fast link was detected [More information...](#)

Computer Details

General

Computer name	YRITYSX
Domain	YritysXC.local
Site	Default-First-Site-Name
Organizational Unit	YritysXC.local\Domain Controllers
Security Group Membership	slow

Component Status

Component Name	Status	Time Taken	Last Process Time	Event Log
Group Policy Infrastructure	Success	126 Millisecond(s)	7.10.2025 18:22:49	View Log
Ragutty	Success	46 Millisecond(s)	7.10.2025 18:06:59	View Log
Security	Success	818 Millisecond(s)	7.10.2025 18:00:54	View Log

Settings

7. Käynnistä kone tarvittaessa uudelleen

BONUS: Tarkista oikeuksien vaikuttus suoraan (valinnainen)

Aja koneella komento:

```
gpresult /h C:\gpresult.html
```

→ Avaa tiedosto [C:\gpresult.html](#) selaimessa

→ Etsi osio: Computer Details → User Rights Assignment

Tarkista että:

- Allow log on locally = sisältää Myynti-Kirjautujat
- Allow log on through Remote Desktop Services = sisältää Myynti-Kirjautujat

Miksi ei toimi ilman RDP-oikeutta?

Monet ajattelevat että "Allow log on locally" riittää, mutta RDP on erillinen kirjautumistapa, ja ilman oikeutta siihen, Windows estää yhteyden tähän.

```
C:\ Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

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 19:40:36

RSOP data for YRITYSX\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=WIN-9MD2IOQ8QRC,OU=Domain Controllers,DC=YritysXC,DC=local
Last time Group Policy was applied: 7.10.2025 at 19:37:51
Group Policy was applied from: YritysXC.local
Group Policy slow link threshold: 500 kbps
Domain Name: YRITYSX
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
-----
```

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 YRITYSX\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
Last time Group Policy was applied: 7.10.2025 at 18:26:21
```

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 lukeaan?

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-ryhmässä.
- 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 (molempien kenttään siis)
- Allow log on locally
 - Allow log on through Remote Desktop Services

 Lisää ryhmä: yritysxc\Myynti-Kirjautujat

! VAROITUS: Tämä ei ole suositeltavaa oikeassa tuotantoymäristössä 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. Nämä saataisiin 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 järjestelmänvalvoille (admin)**.

Tämä ei ole nelkkä 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 tiivistheet
 - Oikeudet
 - Ryhmäjäsenyydet
 - GPO:t ja niihin liittyvät konfiguraatiot

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

2. Tietoturvalain ja least privilege -periaatteeen 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

 **Esimerkki:** 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 suojaava teknisesti ja organisatorisesti
- Tavallinen käyttäjä, jolla on pääsy DC:lle, voi vahingossa tai tahallaan päästää 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 → lähettilä ulos sähköpostilla

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