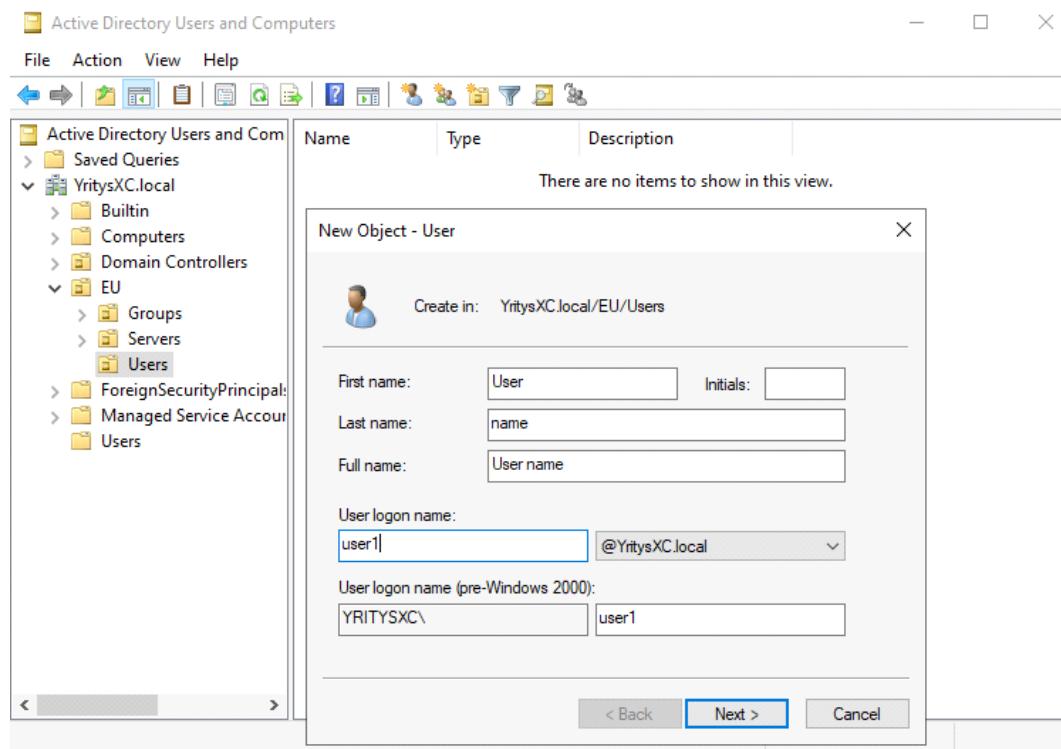


## 4.1. User 1 - login VM2 - Win10

Sunday, October 19, 2025 15:51

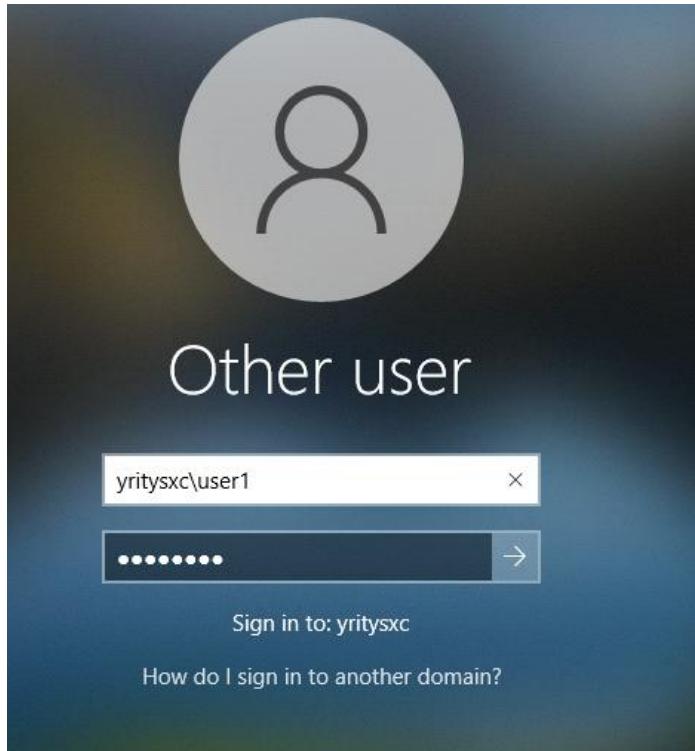
Luodaan ad toinen käyttäjä ja sillä esim. Kirjautuu samaan vm2 (windows 10) toisella tunnuksella sisään ja tämä pitäisi pelittää koska on yhdistänyt domain yritysalueelle.



User1  
P@ssw0rd

- Määritettää ensimmäisen kirjautuessa joutuu vaihtaa salasansa.

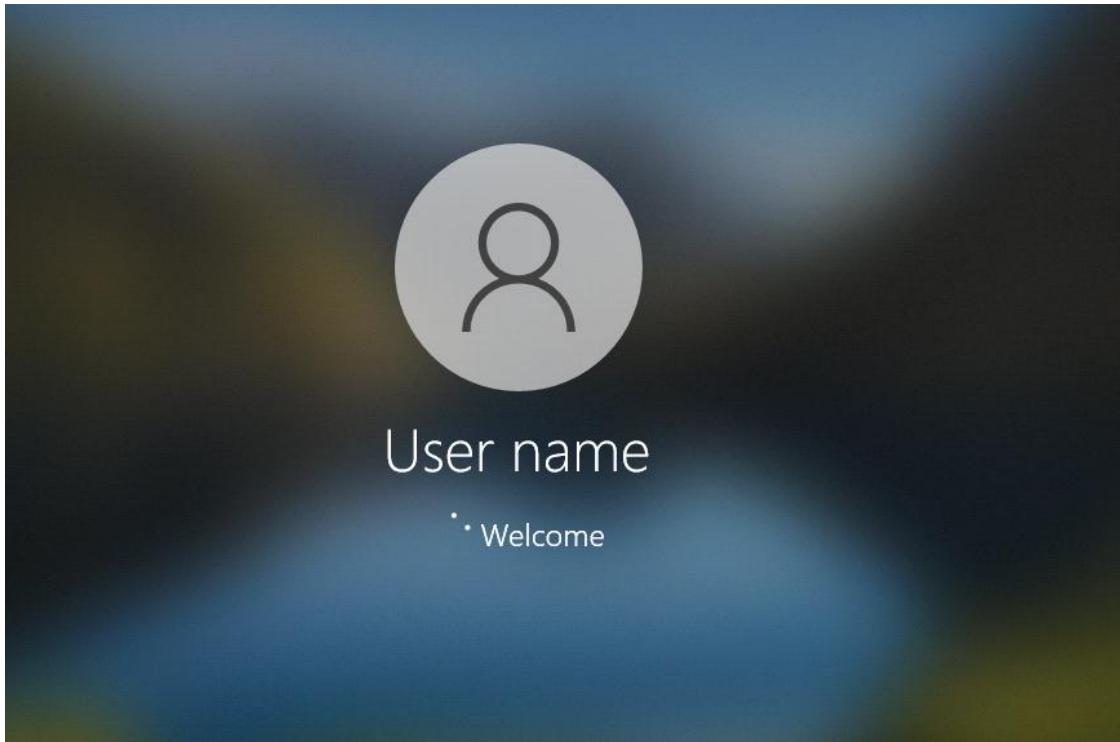
Et testaaan VM1 (windows server) alla luoneen käyttäjän --> VM2 (windows 10) ensimmäisen kirjautunutta samassa hiekkaympäristön alla vaihtaa toiseen käyttäjään et vaihda käyttis ja varmistettuna on littynyt verkosotn alueelle.



Muutettaan salasana: herneKeitto123

Jos ei muista sitä salasanaa ekana niin perus admin voi resetoida sen tarvittaessa

Ja siinä mene hetki et pääseee sisään



## Admin puoli näkymä - START HERE;

Tämä on ehkä suurin tai mahdollisesti yksi huonoista puolesta, että ei pysty tarkistaa "KUKA KÄYTTÄJÄ" on kirjauttunut "TYÖASEMAN" alle. Vaikka käyttäjä ensimmäisen kerran kirjauttuessa yhdistää yritysalueelle - niin sen kone nimi lähettää ja kuin rekisteröityy sinne ADUC (Active Directory Users and computers) alle.

- Esim. Matti M ----> Desktop XXXXXXXX

Active Directory Users and Computers

File Action View Help

DESKTOP-XXXXXX Properties

Name	Type	Description
DESKTOP-XXXXXX	Computer	Shared Desktop

General Operating System Member Of Delegation Location Managed By Dial-in

Computer name (pre-Windows 2000): DESKTOP-XXXXXX

DNS name: DESKTOP-XXXXXX.yritysXC.local

DC Type: Workstation or server

Site:

Description: Shared Desktop

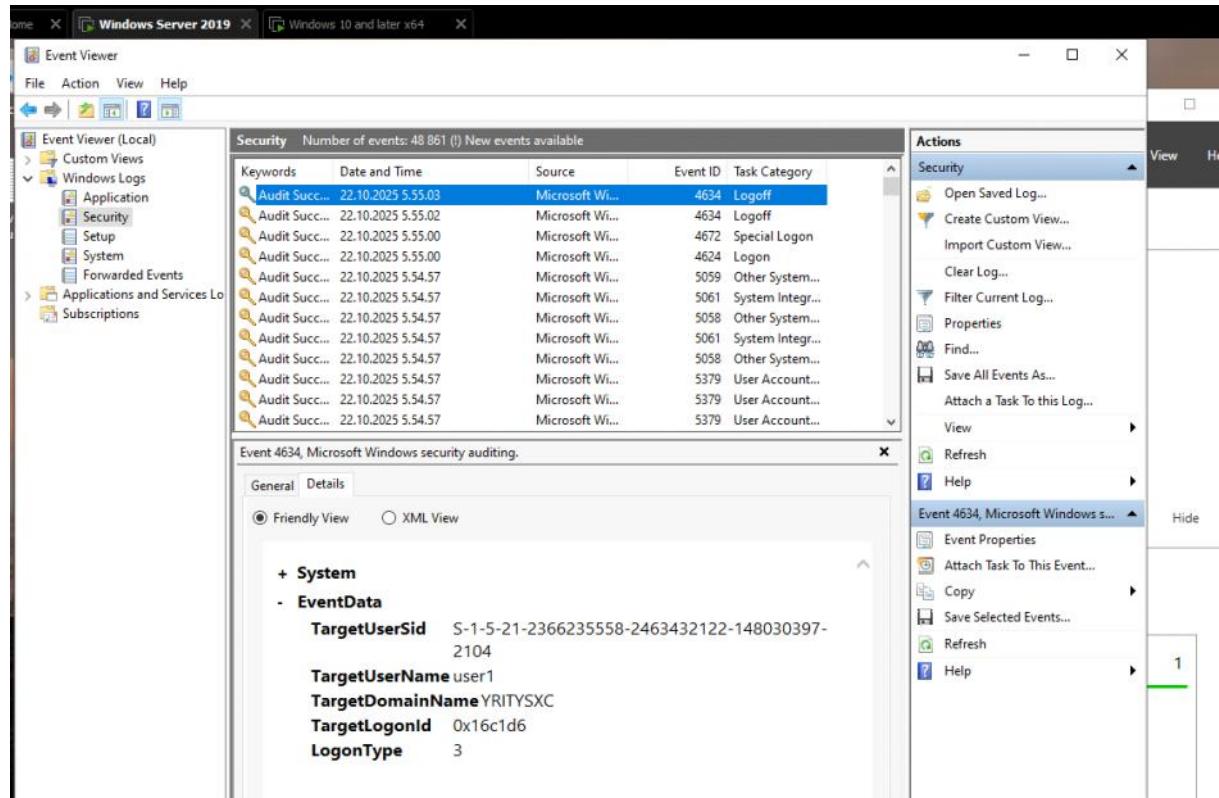
## Miten admin tarkistaa ja löytää oikean henkilön koneen omistajansa ja kirjauttuneen henkilönsä?

ADUC - active directory users and computers  
AD - active directory

Onglemansa on se windows server , ADUC / AD ei tarjoa tällaista ominaisuutta verratuna Microsoft pilvipalvelun Intune:a , että jos

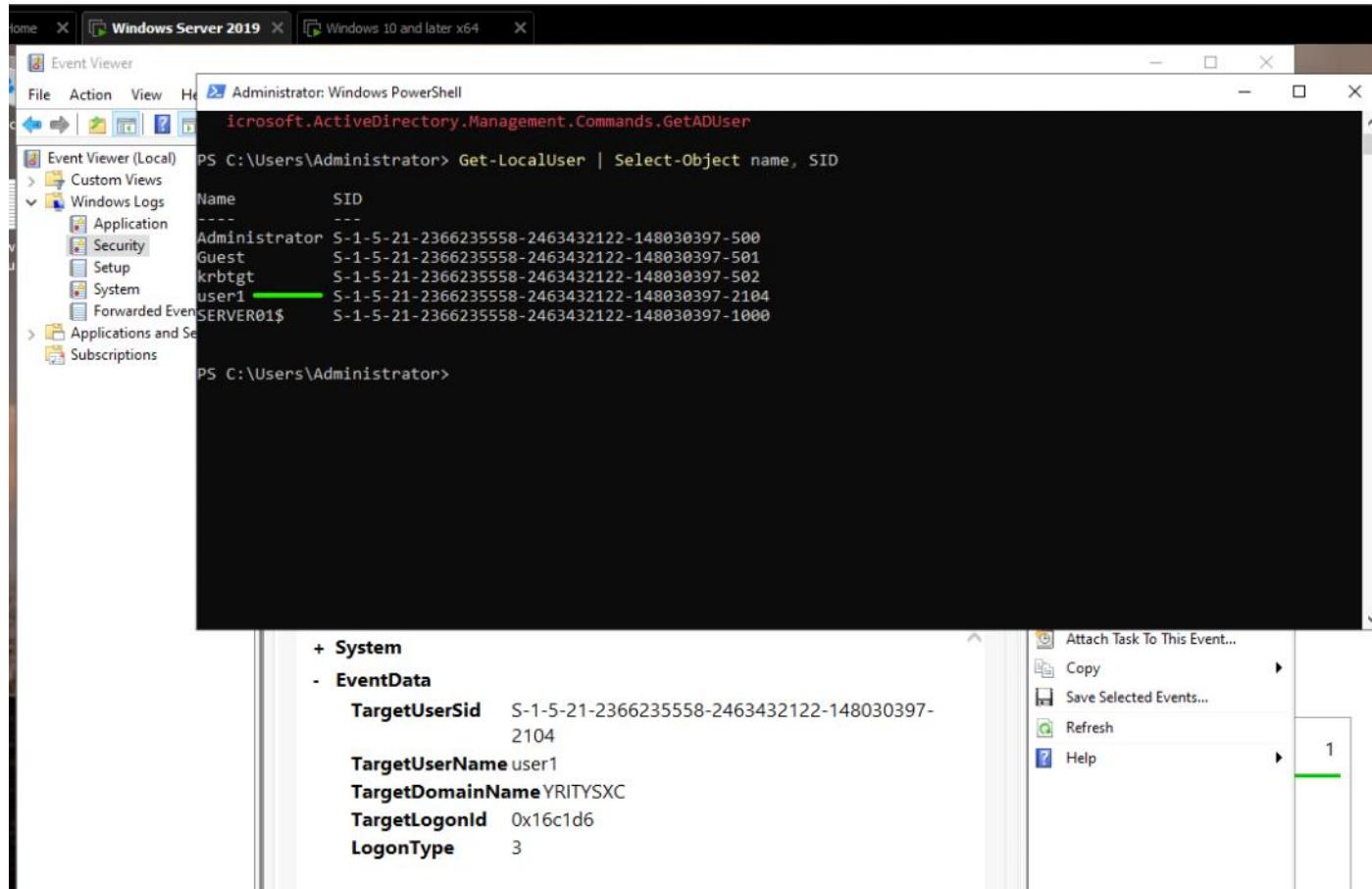
on uusi tai vanha käyttäjä kirjautuu uutteen työasemaan tai johonkin asemaan niin se henkilön nimi ja laite rekisteröityy sinne laitejärjestelmän alle.

Mahdollinen on tarkistaa Event Viewer:istä eli polku:: Event viewer >> Windows logs >> Security ja hakee haku Find ID:llä: 4624



Tästä vaan jatkaa selvittää (ylemmän kuvan) kuka on "TargetUserSid" sillä kautta ja siinä lukekin TargetUserName: user1 ja halutaan leikkista varmistaa onko se hän. Ongelman ja mahdolinen huono puolena

Ensin hakee kaikki lokaali käyttäjät ja admin itsensä ja tulostaakseen se nimi ja SID



```
Microsoft.ActiveDirectory.Management.Commands.GetADUser
PS C:\Users\Administrator> Get-LocalUser | Select-Object name, SID
Name      SID
Administrator S-1-5-21-2366235558-2463432122-148030397-500
Guest      S-1-5-21-2366235558-2463432122-148030397-501
krbtgt    S-1-5-21-2366235558-2463432122-148030397-502
user1      S-1-5-21-2366235558-2463432122-148030397-2104
SERVER01$  S-1-5-21-2366235558-2463432122-148030397-1000
PS C:\Users\Administrator>
```

+ System  
- EventData  
  **TargetUserId** S-1-5-21-2366235558-2463432122-148030397-2104  
  **TargetUserName** user1  
  **TargetDomainName** YRITYSYXC  
  **TargetLogonId** 0x16c1d6  
  **LogonType** 3

Tarkistuksena onks se just täsmälleen "user1" - ja tässä täsmentyykin

The screenshot shows the Windows Server 2019 Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Windows Logs (Application, Security, System, Forwarded Events), Applications and Services, and Subscriptions. The right pane shows a PowerShell session running as Administrator. The session output is as follows:

```
Administrator: Windows PowerShell
Name      SID
-----
Administrator S-1-5-21-2366235558-2463432122-148030397-500
Guest      S-1-5-21-2366235558-2463432122-148030397-501
krbtgt    S-1-5-21-2366235558-2463432122-148030397-502
user1      S-1-5-21-2366235558-2463432122-148030397-2104
SERVER01$  S-1-5-21-2366235558-2463432122-148030397-1000

PS C:\Users\Administrator> Get-ADUser -Identity "user1" -Properties SID
DistinguishedName : CN=User name,OU=Users,OU=EU,DC=YritysXC,DC=local
Enabled          : True
GivenName        : User
Name             : User name
ObjectClass      : user
ObjectGUID       : [REDACTED]
SamAccountName   : user1
SID              : S-1-5-21-2366235558-2463432122-148030397-2104
Surname          : name
UserPrincipalName: user1@YRITYSXC.local

PS C:\Users\Administrator>
```

Below the PowerShell output, a System event is expanded, showing the following details:

- EventData**
  - TargetUserId** S-1-5-21-2366235558-2463432122-148030397-2104
  - TargetUserName** user1
  - TargetDomainName** YRITYSXC
  - TargetLogonId** 0x16c1d6
  - LogonType** 3

On the right side of the interface, there are several context menu options: Attach Task To Task, Copy, Save Selected Event, Refresh, and Help.

Jos tosi elämässä niin tässä joko virallisen "Computers" - OU (vasenkansion) kansion alla voi olla kymmensiä tai jopa satoja koneita, josta on vaikea sanoa kuka ja kenen kone onkaan.

```
PS C:\Users\Administrator> Get-ADComputer -Filter 'Name -like "*VM*"' | Select-Object Name
PS C:\Users\Administrator> Get-ADComputer -Filter 'Name -like "*DESKTOP*"' | Select-Object Name

Name
-----
DESKTOP-S8U072N

PS C:\Users\Administrator> Get-ADComputer -Identity "DESKTOP-XXXXXX" -Properties *

AccountExpirationDate      :
accountExpires              : 9223372036854775807
AccountLockoutTime          :
AccountNotDelegated         : False
AllowReversiblePasswordEncryption : False
AuthenticationPolicy         : {}
AuthenticationPolicySilo    : {}
BadLogonCount                : 0
badPasswordTime              : 0
badPwdCount                 : 0
CannotChangePassword        : False
CanonicalName               : YritysXC.local/EU/Computers/DESKTOP-S8U072N
Certificates                : {}
CN                          : DESKTOP-S8U072N
```

(Tämä on sama komento), mutta scrollaa vähä alas ja siinä lukee se "objectSid"

The screenshot shows the Windows Server interface. On the left is the Active Directory Users and Computers (ADUC) management console. The tree view shows the structure: Event, Active Directory Users and Computers, Active Directory Users and Computers, YritysXC.local, EU, and Computers. A specific computer object, 'DESKTOP-...', is selected. The main pane displays the object's properties: Name (DESKTOP-...), Type (Computer), and Description (Shared Desktop). On the right, a Windows PowerShell window is open with administrator privileges. The command `Get-ADComputer -Identity DESKTOP-... | Select-Object \*` is run, and the output shows various attributes of the computer object, including its SID: S-1-5-21-2366235558-2463432122-148030397-2103.

Tässä ongelmansa on se **objectSid** viimeinen numero on vain vähä eri eli 2103 ja 2104 - vähä apua copilot:iltä.

Käyttäjän ja koneen SID:t:

Koneen SID:	S-1-5-21-2366235558-2463432122-148030397-2103
Käyttäjän SID:	S-1-5-21-2366235558-2463432122-148030397-2104

• Molemmat kuuluvat samaan domainiin (S-1-5-21-2366235558-2463432122-148030397), mutta viimeinen osa (-2103 vs -2104) on **objektiin yksilöllinen RID** (Relative Identifier).

- SID ei yksin kerro kirjautumisista, se auttaa **tunnistamaan objektit yksilöllisesti**.

## 💡 Mitä RID kertoo?

- RID on **uniikki tunniste** AD:n sisällä.
- Se lisätään domainin SID:n perään, jotta saadaan yksilöllinen SID jokaiselle objektiyypille (käyttäjä, ryhmä, kone).
- Esimerkiksi:
  - -500 → domainin sisäinen **Administrator**
  - -512 → **Domain Admins** -ryhmä
  - -1000 ja eteenpäin → tavalliset käyttäjät ja koneet

## 🔒 Käyttökeloisuus

- SID:tä käytetään **oikeuksien hallintaan, auditointiin, ja GPO-kohdistuksiin**.
- Jos haluat tarkistaa, mihin koneeseen käyttäjä on kirjautunut, SID ei yksin riitä – tarvitset **lokitietoja tai profiilijärkiä** koneelta.

## OMA POHDINTA OSUUS:

Tämän osalta miten tästä voisi tosi elämässä tehdäkään? Tämä koskee uusi laite tai käyttäjä luovuttaa koneensa, että admin pitää varmistaa sen koneen ID tai jollakin tunnistuksella, koska ettei sekoitu muiden koneiden kanssa ja sama idea koneeseen elinkaari. Lisäksi koskee OU yksikkön alemman kansiota ja ryhmää, että ei väliä onks firmassa tai toimistossa alle/pari/muutama 10 tai 100.

henkilöä.

hakea koneen ja nähdä omistajan:

```
$Get-ADComputer -Identity "DESKTOP-[REDACTED]" -Properties ManagedBy
```

Automatisointi ja raportointi

```
$Get-ADComputer -Filter * -Properties ManagedBy | Select-Object Name, ManagedBy
```

- Pelisäännöt adminille
- **Jokaisella koneella on omistaja** → merkintä ManagedBy
- **Koneen nimi kertoo käyttötarkoituksen**
- **Koneen tiedot dokumentoidaan** → elinkaari, takuu, käyttö
- **Käyttöönotto ja palautus ovat hallittuja prosesseja**
- **Raportointi on säännöllistä ja läpinäkyvää**

Sama pätee näiden koneesta pitää ja ehdottomasti merkitä ITSM järjestelmään, että käyttäjällä on tällainen kone käytössä