

Подключение Linux workstation к Active Directory

Используем мой [райтап](#) по поднятию домена до момента подключения рабочих станций.

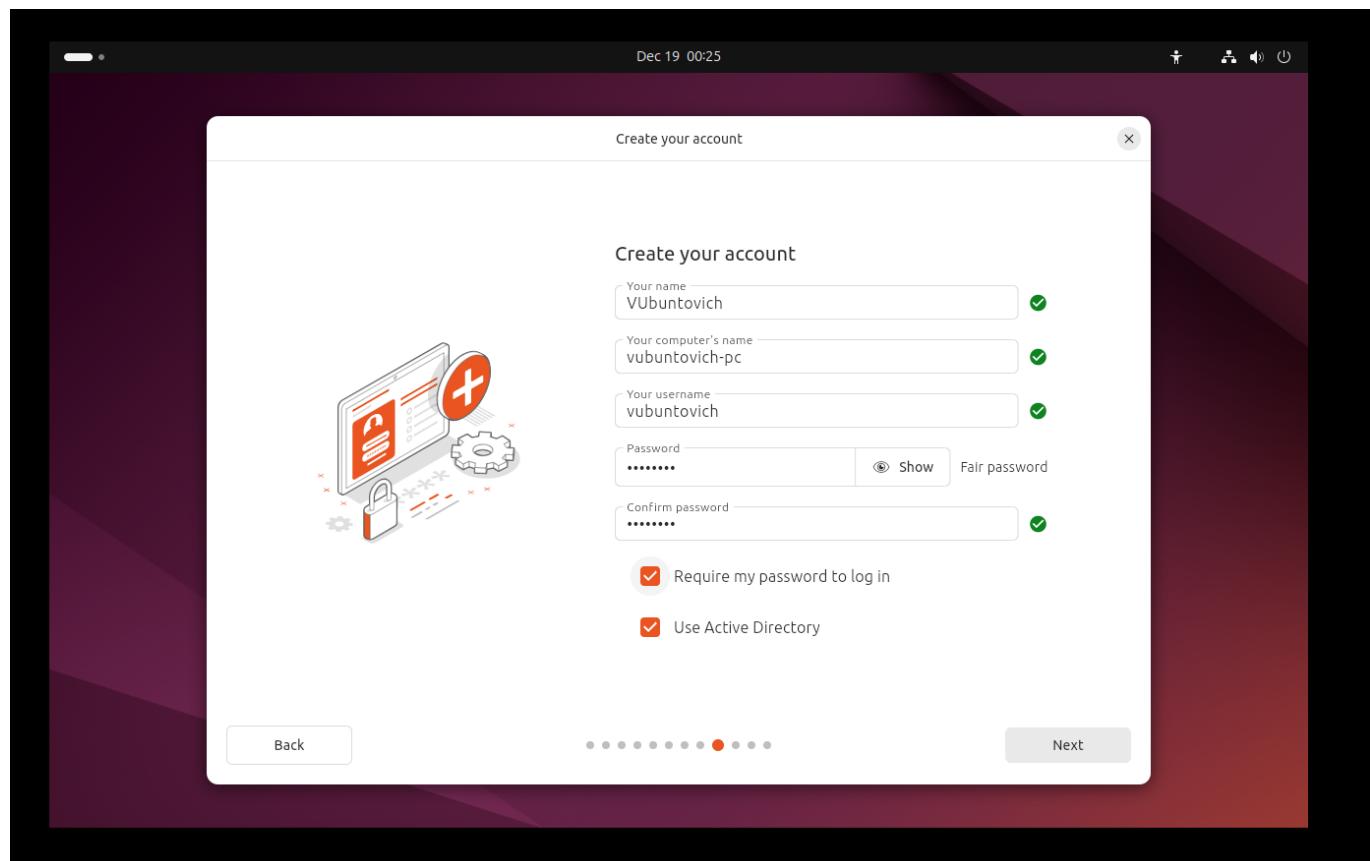
[Статья от testo-lang по раскатке домена](#)

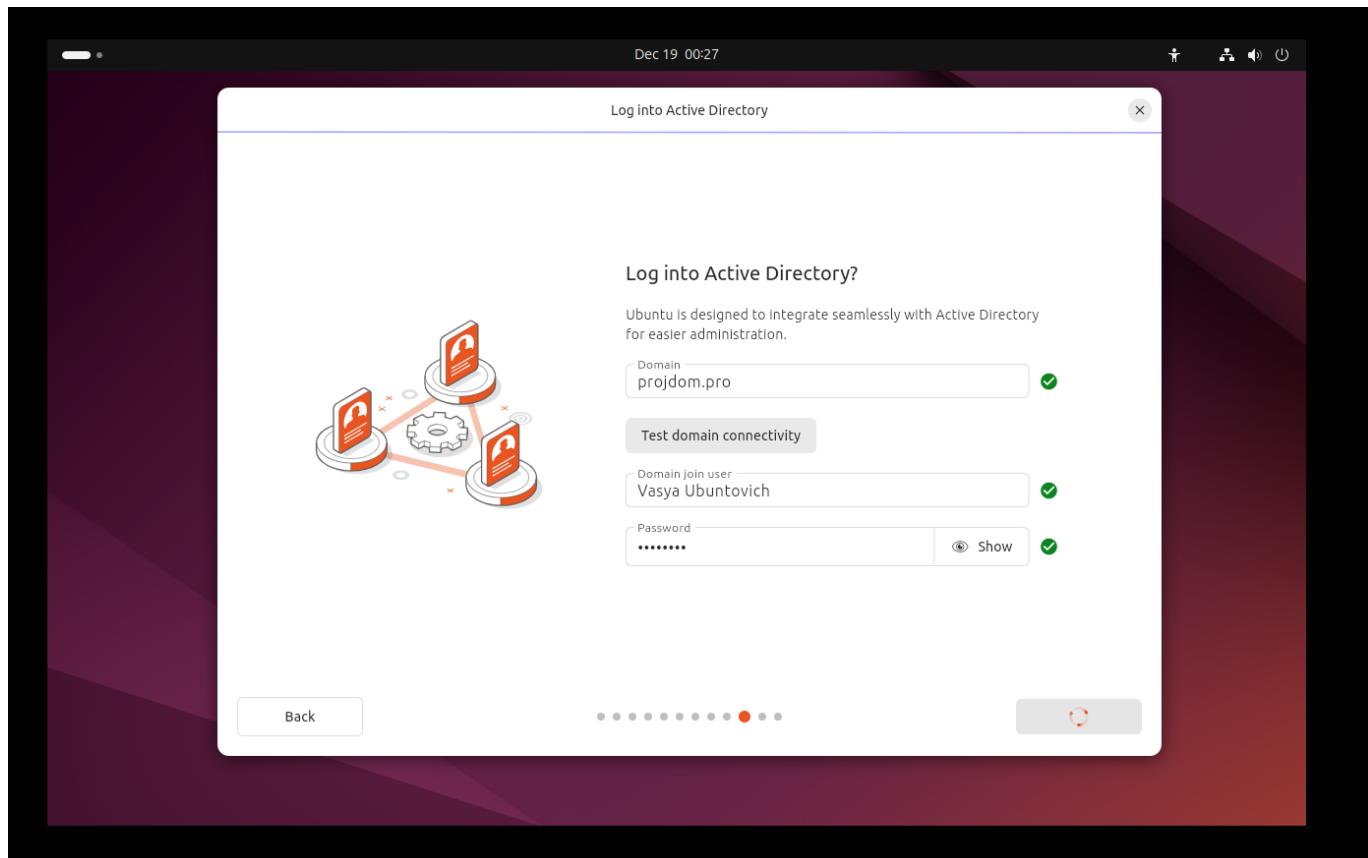
В этом райтапе сосредоточимся преимущественно на подключении линукс-машины.

Стоит отметить, что в этот раз все действия проводятся не в изолированной виртуальной сети VirtualBox, а уже на настроенной до этого локальной сети на базе маршрутизатора **MikroTik hAP ax2**. Следовательно, уже есть DHCP сервер в сети, но не смотря на это следуем best practices и назначаем доменному серверу статический IP - **192.168.88.3**.

Попытка подключения при установке.

Во время setup'ва Ubuntu 22+ есть опция сразу накатить AD на станцию. Однако несколько попыток спустя, я понял что опция зависла, поэтому решено было заняться этим уже после настройки системы. По словам LLM, то что AD не подключается при setup'e системы - норма.





Post-install подключение

Скачиваем необходимые пакеты:

```
sudo apt update
sudo apt install -y realmd sssd sssd-tools libnss-sss libpam-sss \
adcli samba-common-bin oddjob oddjob-mkhomedir packagekit
```

Затем проверяем, резолвится ли наш домен в сети:

```
realm discover projdom.pro
```

Ответ положительный, значит устройство видит домен:

```

Dec 20 14:37
vasya@vasya-desktop: ~
valid_lft forever preferred_lft forever
vasya@vasya-desktop: $ nslookup -type=SRV _ldap._tcp.projdom.pro 192.168.88.3
Server:      192.168.88.3
Address:    192.168.88.3#53

_ldap._tcp.projdom.pro  service = 0 100 389 projsrv.projdom.pro.

?
vasya@vasya-desktop: $ sudo nmcli con show
NAME           UUID                                  TYPE      DEVICE
Wired connection 1  e9c7bf1f-c1c5-36bc-b674-ce33245e2704  ethernet  ens33
lo             86e45ca7-8ce5-4a0a-9b0b-2cd5f23c4689  loopback  lo

vasya@vasya-desktop: $ sudo nmcli con mod "Wired connection 1" ipv4.dns "192.168.88.3"
vasya@vasya-desktop: $ sudo nmcli con mod "Wired connection 1" ipv4.ignore-auto-dns yes
vasya@vasya-desktop: $ sudo nmcli con up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
vasya@vasya-desktop: $ realm discover projdom.pro
projdom.pro
  type: kerberos
  realm-name: PROJDOM.PRO
  domain-name: projdom.pro
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
vasya@vasya-desktop: $

```

Поправка: write-up я пишу после того как сделал первичные действия и заново поднял виртуальные машины. После их перезагрузок Ubuntu перестала видеть домен в сети, поэтому пришлось прибегнуть к изменению авто-DNS через `nmcli` для сети роутера, к которой Ubuntu подключен:

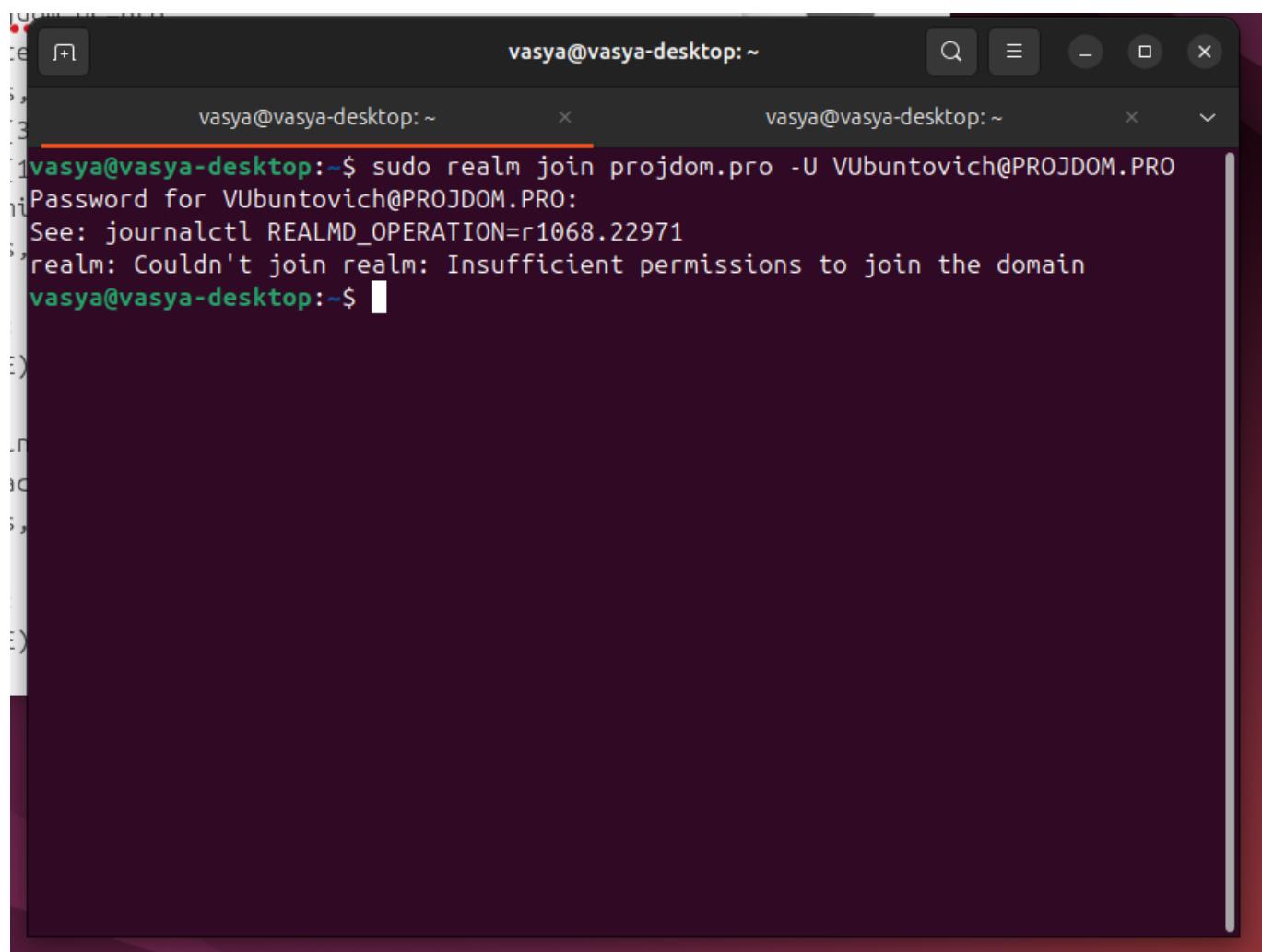
```

sudo nmcli con show
sudo nmcli con mod "Wired connection 1" ipv4.dns "192.168.88.3"
sudo nmcli con mod "Wired connection 1" ipv4.ignore-auto-dns yes
sudo nmcli con up "Wired connection 1"

```

Пытаемся вступить в домен командой:

```
sudo realm join projdom.pro -U VUbuntovich@projdom.pro
```



The screenshot shows a terminal window titled 'vasya@vasya-desktop: ~'. It contains the following command and its output:

```
vasya@vasya-desktop:~$ sudo realm join projdom.pro -U VUbuntovich@PROJDOM.PRO
Password for VUbuntovich@PROJDOM.PRO:
See: journalctl REALMD_OPERATION=r1068.22971
realm: Couldn't join realm: Insufficient permissions to join the domain
```

Терпим неудачи по некоторым факторам, которые важны:

- Разсинхронизация с сервером по времени (критично для протокола Kerberos)
- Слишком длинное имя компьютера

Рассинхрон времен

Частая боль администраторов при настройке сервисов с Kerberos. Так как я работаю уже с перезагруженными машинами, на которых решил эту проблему - вот кучка команд которые помогут настроить время на Ubuntu и Windows. Разница между хостами должна быть меньше 5 мин:

Ubuntu:

```
sudo timedatectl set-ntp true
sudo systemctl restart systemd-timesyncd
```

Windows Server

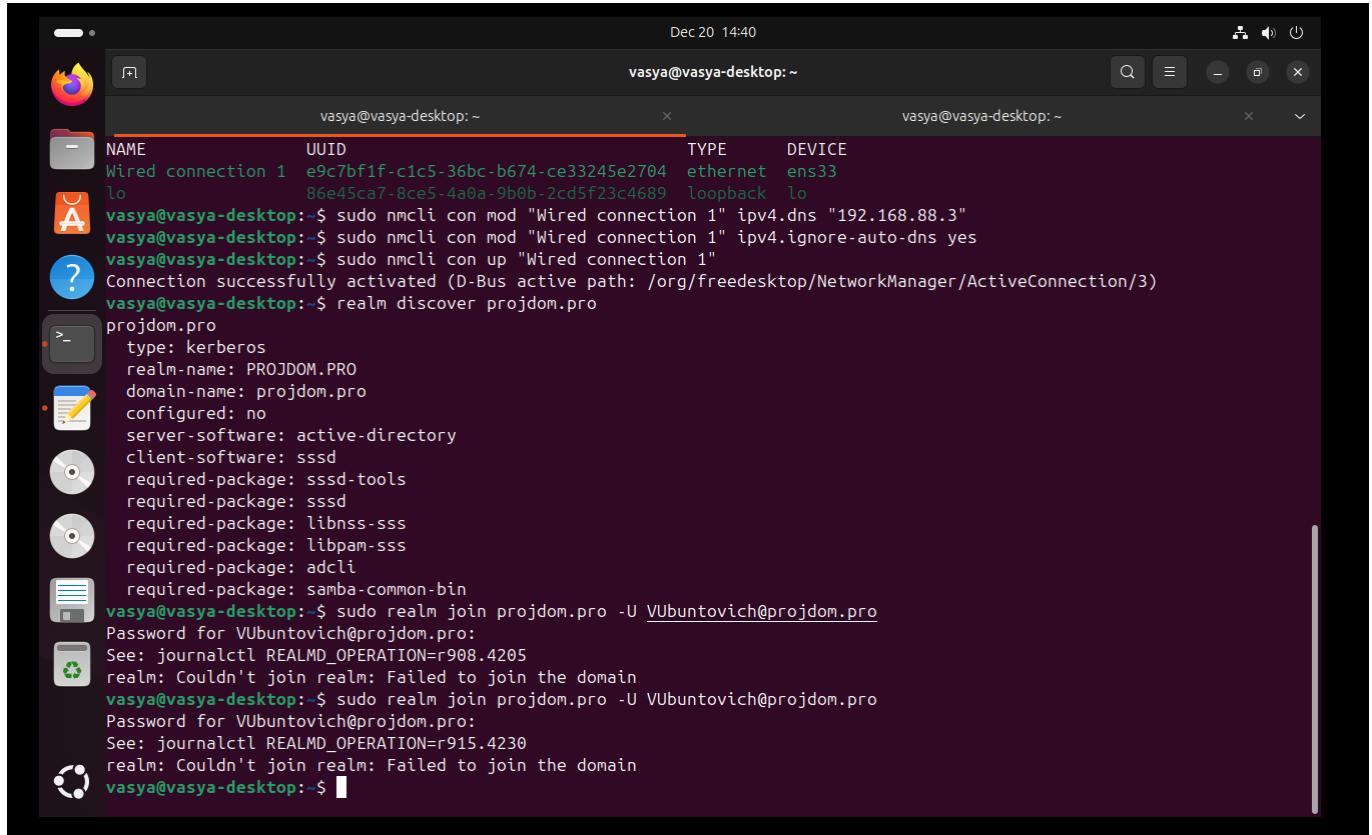
```
w32tm /stripchart /computer:localhost
# or
w32tm /query /status
```

Имя компьютера на Ubuntu

Должно быть <15 символов (NetBIOS) и не должно совпадать с существующим NetBIOS именем в AD.

До этого имя было **vasya-vmware-workstation...** что-то длинное автогенерированное, что явно больше 15 символов. Переходим в **/etc/hostname** и меняем на **vasya-desktop**.

Всё правим и идем дальше. Попытка 2:



```

Dec 20 14:40 vasya@vasya-desktop: ~
vasya@vasya-desktop: ~
NAME          UUID
Wired connection 1  e9c7bf1f-c1c5-36bc-b674-ce33245e2704  ethernet  ens33
lo            86e45ca7-8ce5-4a0a-9b0b-2cd5f23c4689  loopback  lo
vasya@vasya-desktop: $ sudo nmcli con mod "Wired connection 1" ipv4.dns "192.168.88.3"
vasya@vasya-desktop: $ sudo nmcli con mod "Wired connection 1" ipv4.ignore-auto-dns yes
vasya@vasya-desktop: $ sudo nmcli con up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
vasya@vasya-desktop: $ realm discover projdom.pro
projdom.pro
  type: kerberos
  realm-name: PROJDOM.PRO
  domain-name: projdom.pro
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: libnss-sss
  required-package: libpam-sss
  required-package: adcli
  required-package: samba-common-bin
vasya@vasya-desktop: $ sudo realm join projdom.pro -U VUbuntovich@projdom.pro
Password for VUbuntovich@projdom.pro:
See: journalctl REALMD_OPERATION=r908.4205
realm: Couldn't join realm: Failed to join the domain
vasya@vasya-desktop: $ sudo realm join projdom.pro -U VUbuntovich@projdom.pro
Password for VUbuntovich@projdom.pro:
See: journalctl REALMD_OPERATION=r915.4230
realm: Couldn't join realm: Failed to join the domain
vasya@vasya-desktop: $ 

```

```

vasya@vasya-desktop: $ sudo realm join projdom.pro -U VUbuntovich@projdom.pro --verbose
[sudo] password for vasya:
* Resolving: _ldap._tcp.projdom.pro
* Performing LDAP DSE lookup on: 192.168.88.3
* Successfully discovered: projdom.pro
Password for VUbuntovich@projdom.pro:
* Unconditionally checking packages
* Resolving required packages
* LANG=C /usr/sbin/adcli join --verbose --domain projdom.pro --domain-realm PROJDOM.PRO --domain-controller 192.168.88.3 --login-type user --login-user VUbuntovich@projdom.pro --stdin-password
* Using domain name: projdom.pro
* Calculated computer account name from fqdn: VASYA-DESKTOP
* Using domain realm: projdom.pro
* Sending NetLogon ping to domain controller: 192.168.88.3
* Received NetLogon info from: ProjSrv.projdom.pro
* Wrote out krb5.conf snippet to /var/cache/realmd/adcli-krb5-qwkPs/krb5.d/adcli-krb5-conf-hs8xZe
! Couldn't get kerberos ticket for: VUbuntovich@projdom.pro: KDC reply did not match expectations
adcli: couldn't connect to projdom.pro domain: Couldn't get kerberos ticket for: VUbuntovich@projdom.pro: KDC reply did not match expectations
! Failed to join the domain
realm: Couldn't join realm: Failed to join the domain

```

параметр **--verbose** для подробных логов о попытке входа в AD

Снова не удача. Консультируясь с LLM выходит гипотеза, что

это уже вопрос прав в AD, а не Kerberos.

1 Пользователь VUbuntovich не имеет права создавать/изменять компьютерные аккаунты в AD.

2 AD разрешает либо:

создать новый объект компьютера, либо

изменить существующий, если объект уже есть.

Но твой пользователь не имеет таких привилегий → adcli join падает.

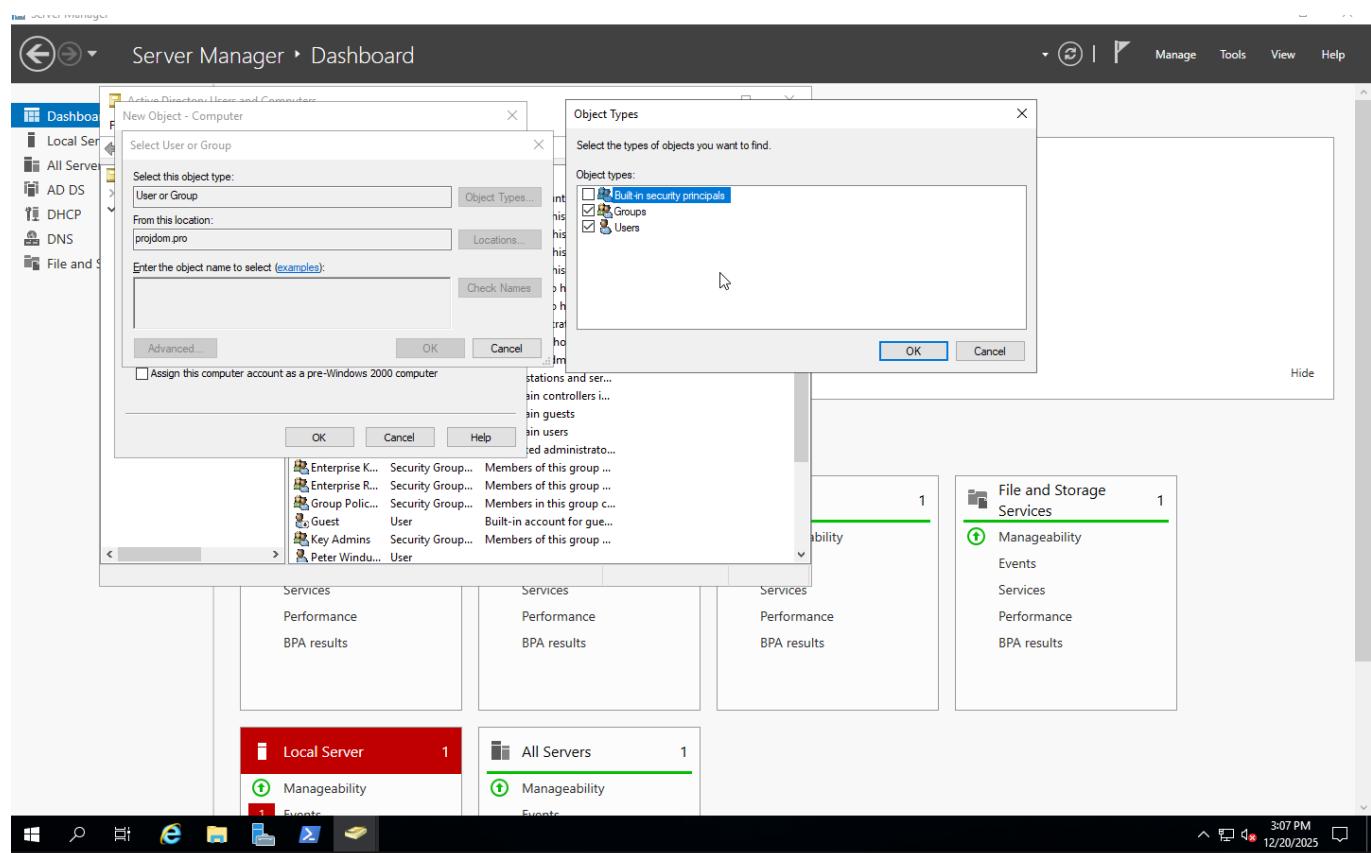
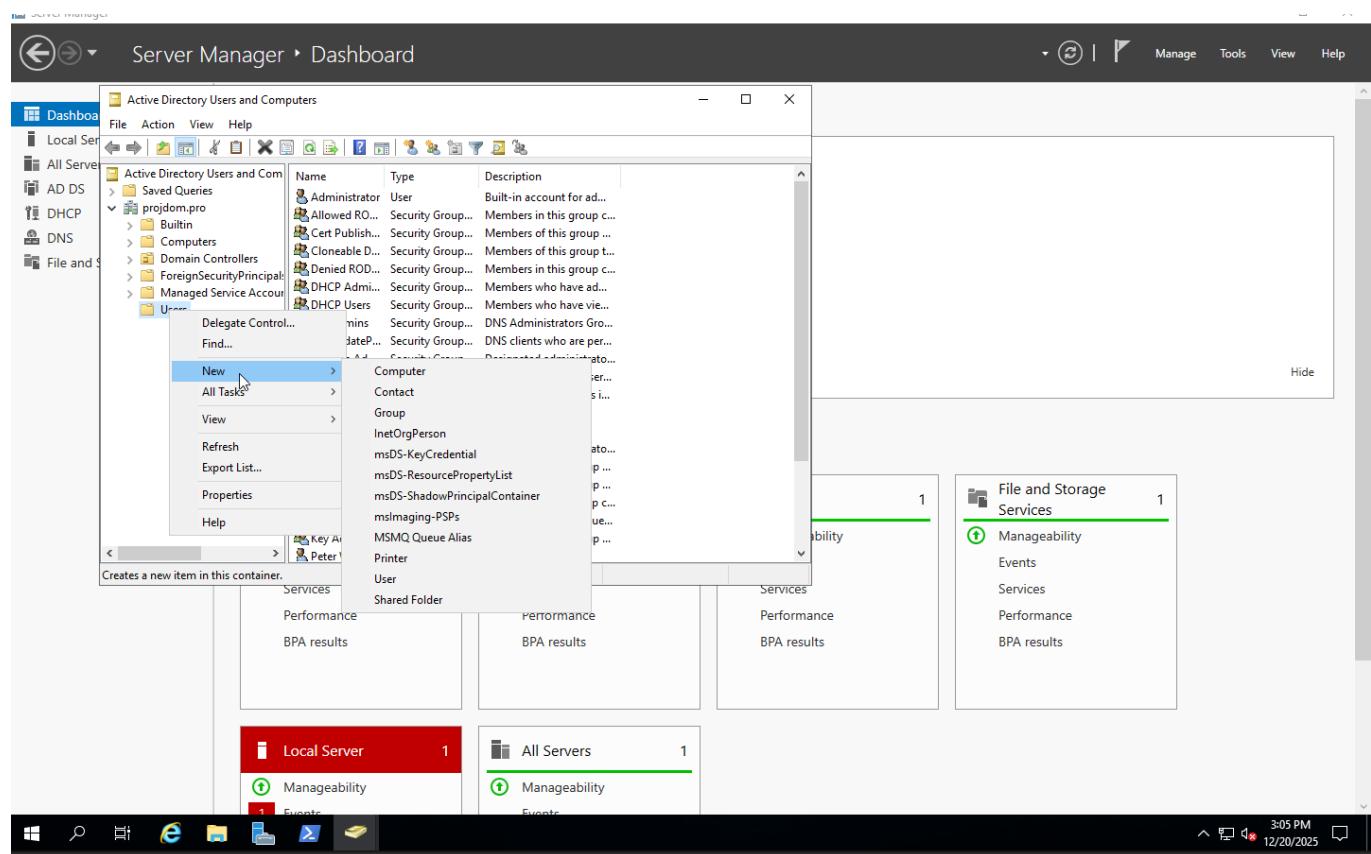
И adcli join - ручной вход - действительно падает:

```
vasya@vasya-desktop:~$ sudo adcli join --verbose projdom.pro -U VUbuntovich@projdom.pro
* Using domain name: projdom.pro
* Calculated computer account name from fqdn: VASYA-DESKTOP
* Calculated domain realm from name: PROJDOM.PRO
* Discovering domain controllers: _ldap._tcp.projdom.pro
* Sending NetLogon ping to domain controller: projsrv.projdom.pro
* Received NetLogon info from: ProjSrv.projdom.pro
* Wrote out krb5.conf snippet to /tmp/adcli-krb5-IXvlGp/krb5.d/adcli-krb5-conf-97GDcn
Password for VUbuntovich@projdom.pro:
! Couldn't get kerberos ticket for: VUbuntovich@projdom.pro: KDC reply did not match expectations
adcli: couldn't connect to projdom.pro domain: Couldn't get kerberos ticket for: VUbuntovich@projdom.pro: KDC reply did
not match expectations
vasya@vasya-desktop:~$
```

Попробуем одно из решений - создать компьютерный объект вручную в AD.

Создаем устройство компьютер в AD

Tools -> Active Directory Users and Computers



Создаем КОМП, и создаем неправильно ведь дальше ошибка. На мой взгляд тут GUI достаточно кривой у AD, чтобы разобраться, как правильно втыкать параметры, поэтому по заветам LLM используем следующие команды:

```
Remove-ADComputer vasya-desktop # удаляем прежний инстанс
New-ADComputer
```

```

-Name "VASYA-DESKTOP"
-SamAccountName "VASYA-DESKTOP$"
-DNSHostName "vasya-desktop.projdom.pro"
-Path "CN=Computers,DC=projdom,DC=pro"
-Enabled $true

# проверка
Get-ADComputer VASYA-DESKTOP -Properties DNSHostName,ServicePrincipalName |
Format-List DNSHostName,ServicePrincipalName

```

```

PS C:\Users\Administrator> New-ADComputer ` 
>> -Name "VASYA-DESKTOP" ` 
>> -SamAccountName "VASYA-DESKTOP$" ` 
>> -DNSHostName "vasya-desktop.projdom.pro" ` 
>> -Path "CN=Computers,DC=projdom,DC=pro" ` 
>> -Enabled $true
PS C:\Users\Administrator> Get-ADComputer VASYA-DESKTOP -Properties DNSHostName,ServicePrincipalName |
>> Format-List DNSHostName,ServicePrincipalName

DNSHostName      : vasya-desktop.projdom.pro
ServicePrincipalName : {}

```

```

vasya@vasya-desktop:~$ sudo realm join projdom.pro -U VUbuntovich@projdom.pro --verbose
[sudo] password for vasya:
* Resolving: _ldap._tcp.projdom.pro
* Performing LDAP DSE lookup on: 192.168.88.3
* Successfully discovered: projdom.pro
Password for VUbuntovich@projdom.pro:
* Unconditionally checking packages
* Resolving required packages
* LANG=C /usr/sbin/adcli join --verbose --domain projdom.pro --domain-realm PROJDOM.PRO --domain-controller 192.168.88.3 --login-type user --login-user VUbuntovich@projdom.pro --stdin-password
* Using domain name: projdom.pro
* Calculated computer account name from fqdn: VASYA-DESKTOP
* Using domain realm: projdom.pro
* Sending NetLogon ping to domain controller: 192.168.88.3
* Received NetLogon info from: ProjSrv.projdom.pro
* Wrote out krb5.conf snippet to /var/cache/realmd/adcli-krb5-KL3tK1/krb5.d/adcli-krb5-conf-diQQb9
! Couldn't get kerberos ticket for: VUbuntovich@projdom.pro: KDC reply did not match expectations
adcli: couldn't connect to projdom.pro domain: Couldn't get kerberos ticket for: VUbuntovich@projdom.pro: KDC reply did not match expectations
! Failed to join the domain
realm: Couldn't join realm: Failed to join the domain

```

И так не прет. Пробуем дальше. Проблема в правах пользователя, об этом говорит строка

```

adcli: joining domain projdom.pro failed: Cannot set computer password:
Access denied

```

Что предлагает LLM:

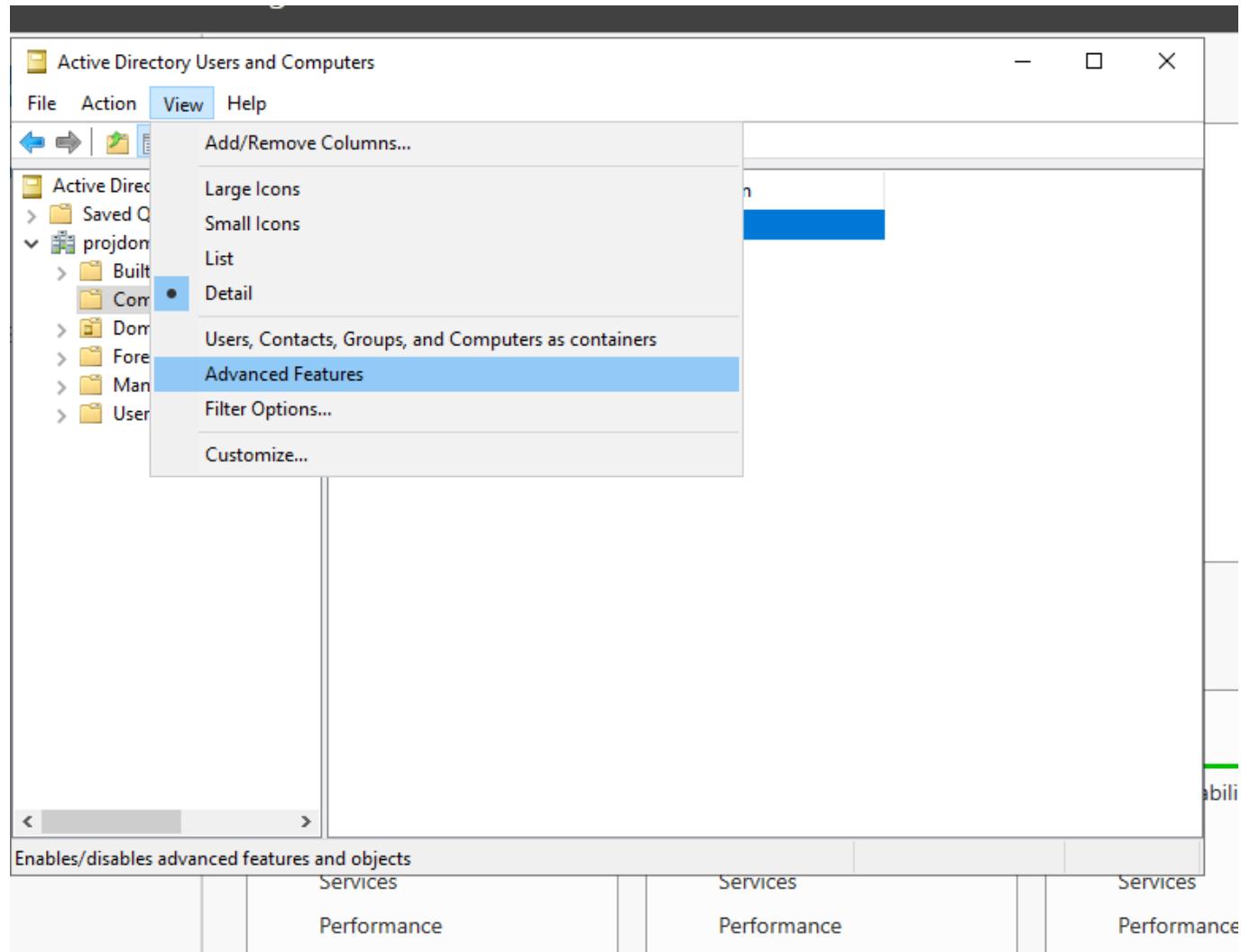
1. Использовать Domain Admin для join
2. Дать права пользователю на объект компьютера
3. Удалить объект и дать права на OU

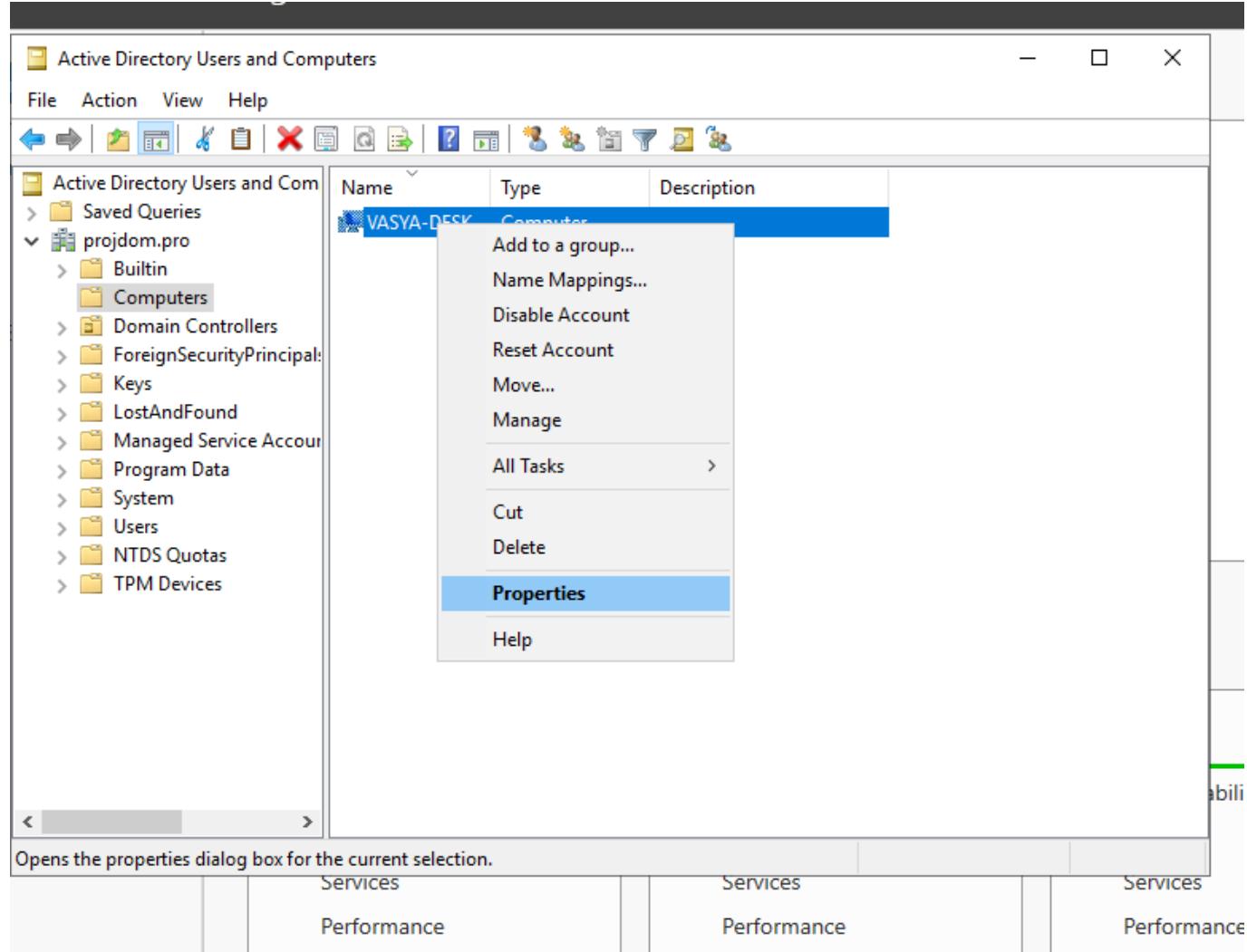
Пункты 1 и 3 на мой взгляд чушь, ведь в полевых условиях такое повышение прав - плохая практика безопасности. Поэтому выбираем вариант **2.**

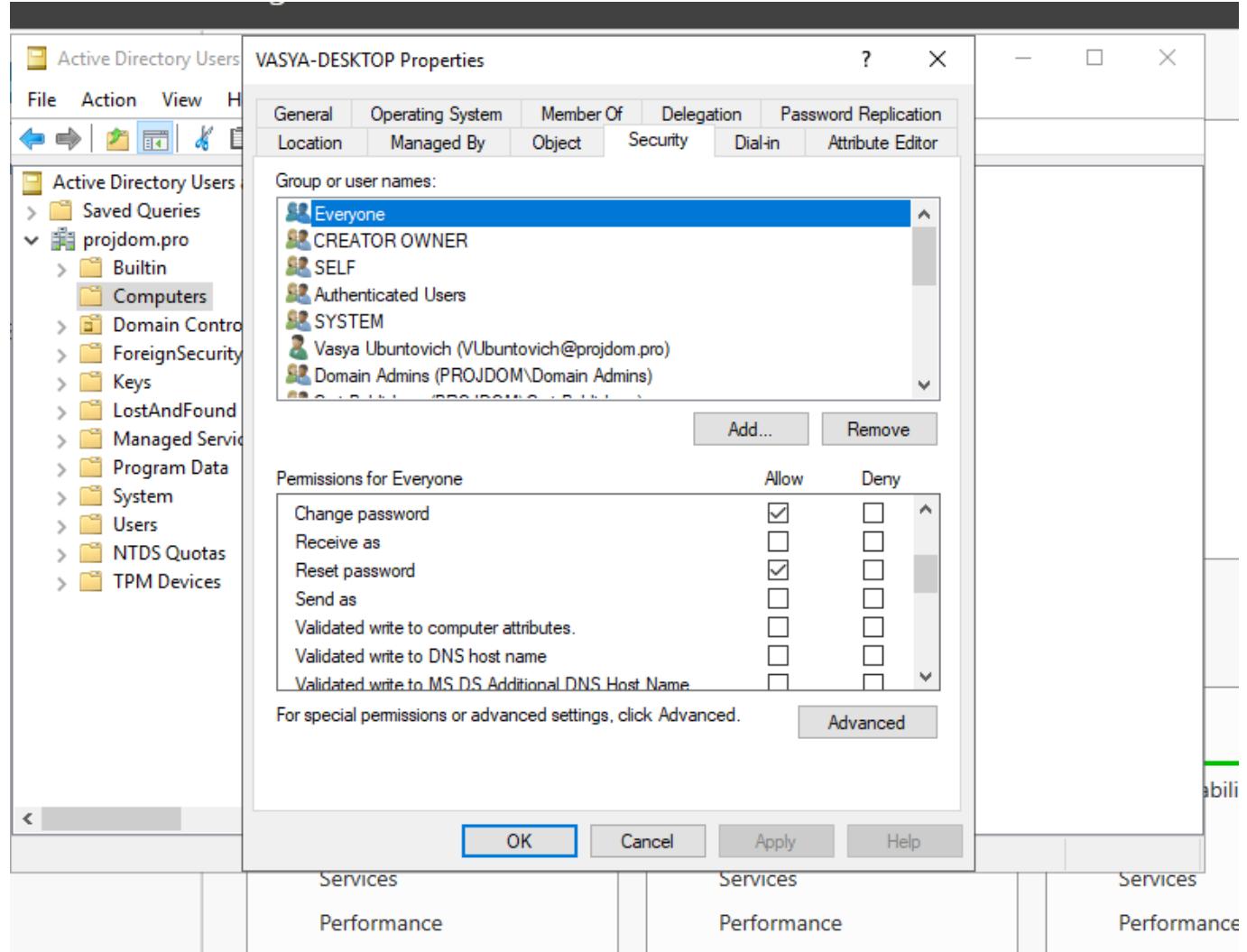
Находим снова наш компьютер:

The screenshot shows the "Active Directory Users and Computers" snap-in window. The left pane displays a navigation tree for the domain "projdom.pro". The "Computers" node is selected, showing sub-nodes for "Builtin", "Domain Controllers", "ForeignSecurityPrincipals", "Managed Service Accounts", and "Users". The right pane contains a table with three columns: "Name", "Type", and "Description". A single row is selected, showing "VASYA-DESKTOP" in the "Name" column, "computer" in the "Type" column, and an empty "Description" field. At the bottom of the window, there are tabs for "Services" and "Performance".

Name	Type	Description
VASYA-DESKTOP	computer	

Включаем Advanced View:

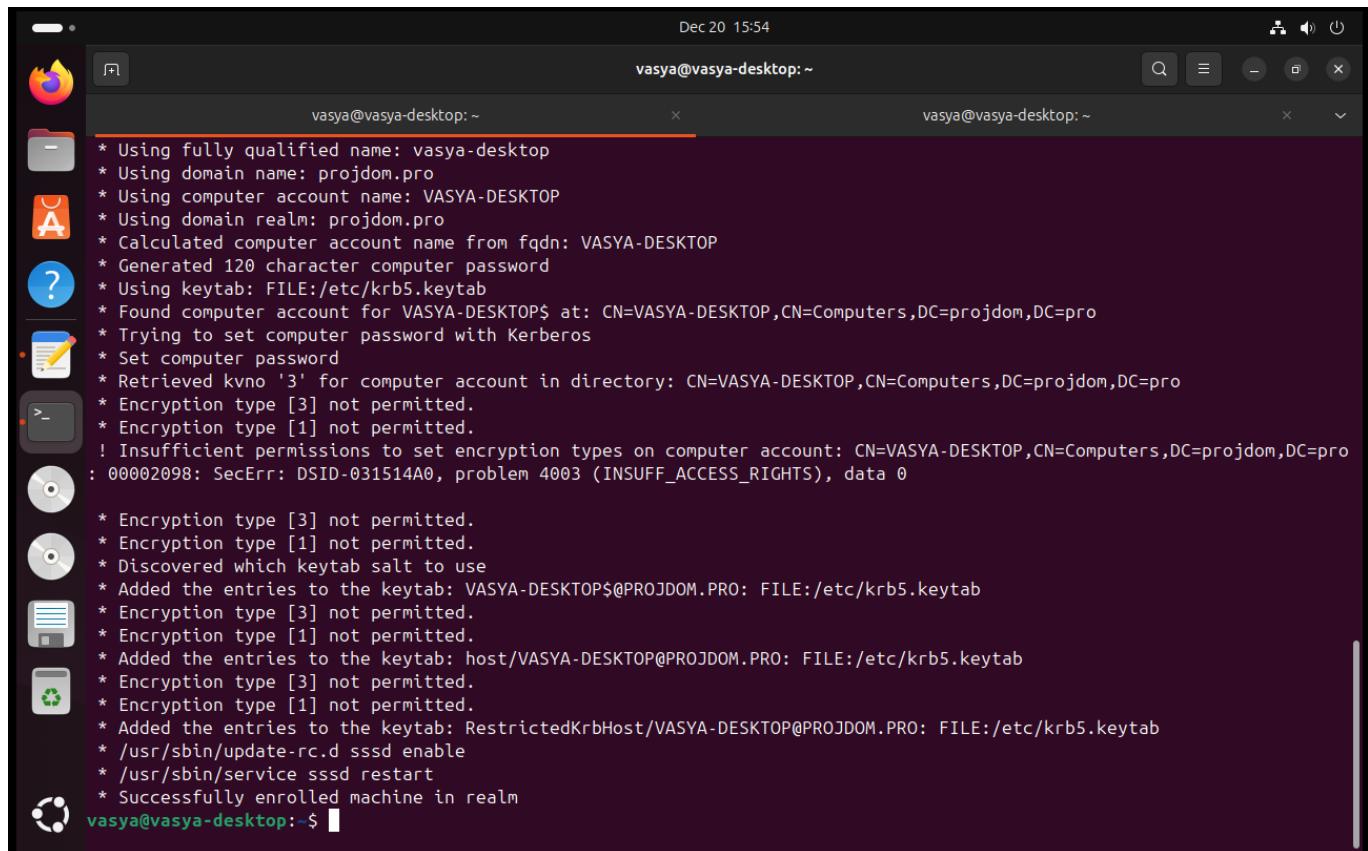




Там же тыкаем такие опции как:

- *Reset Password*
- *Validated write to DNS host name*
- *Validated write to service principal name*

Снова идем к Ubuntu и пробуем:



The screenshot shows a terminal window titled 'vasya@vasya-desktop: ~' with the following log output:

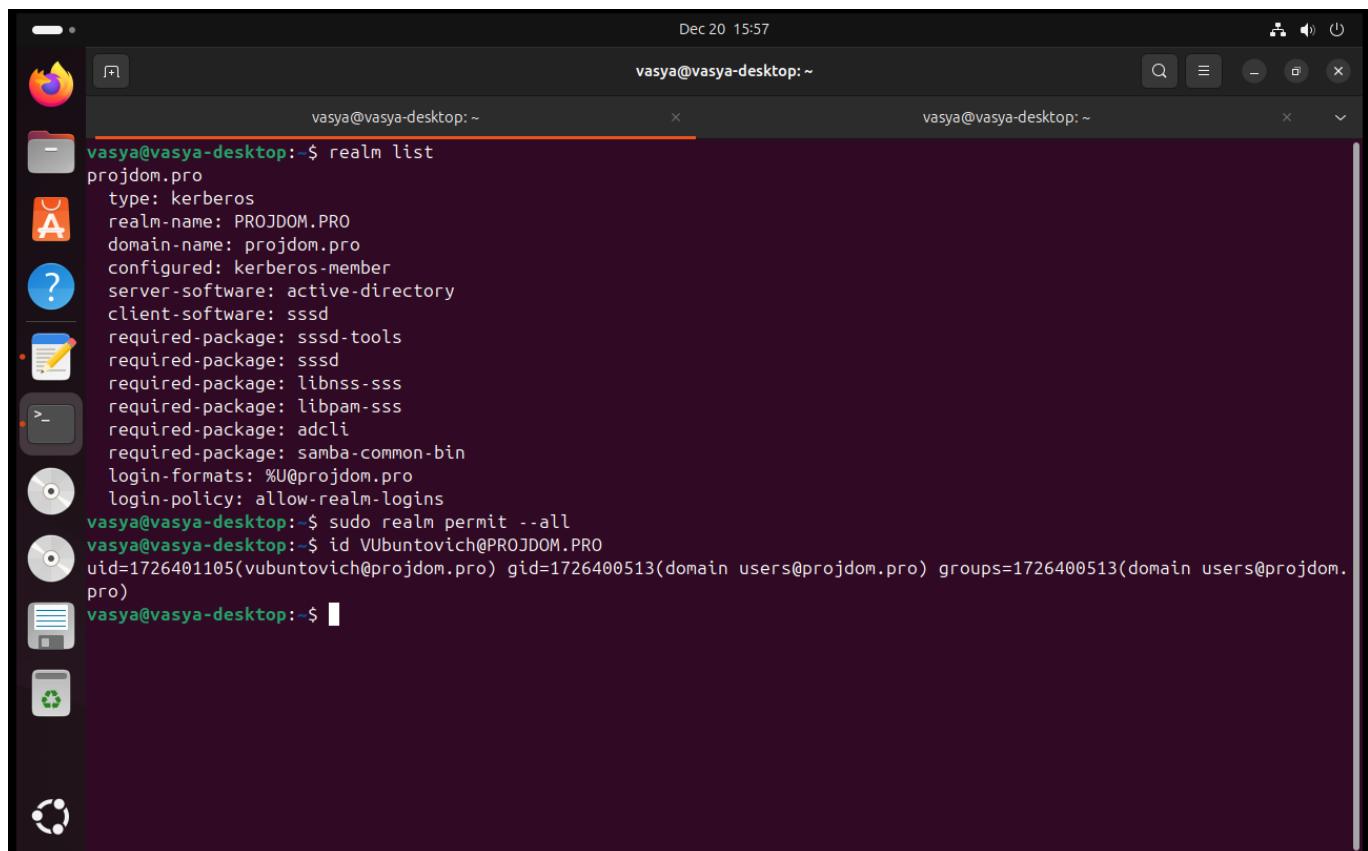
```

* Using fully qualified name: vasya-desktop
* Using domain name: projdom.pro
* Using computer account name: VASYA-DESKTOP
* Using domain realm: projdom.pro
* Calculated computer account name from fqdn: VASYA-DESKTOP
* Generated 120 character computer password
* Using keytab: FILE:/etc/krb5.keytab
* Found computer account for VASYA-DESKTOP$ at: CN=VASYA-DESKTOP,CN=Computers,DC=projdom,DC=pro
* Trying to set computer password with Kerberos
* Set computer password
* Retrieved kvno '3' for computer account in directory: CN=VASYA-DESKTOP,CN=Computers,DC=projdom,DC=pro
* Encryption type [3] not permitted.
* Encryption type [1] not permitted.
! Insufficient permissions to set encryption types on computer account: CN=VASYA-DESKTOP,CN=Computers,DC=projdom,DC=pro
: 00002098: SecErr: DSID-031514A0, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

* Encryption type [3] not permitted.
* Encryption type [1] not permitted.
* Discovered which keytab salt to use
* Added the entries to the keytab: VASYA-DESKTOP$@PROJDOM.PRO: FILE:/etc/krb5.keytab
* Encryption type [3] not permitted.
* Encryption type [1] not permitted.
* Added the entries to the keytab: host/VASYA-DESKTOP@PROJDOM.PRO: FILE:/etc/krb5.keytab
* Encryption type [3] not permitted.
* Encryption type [1] not permitted.
* Added the entries to the keytab: RestrictedKrbHost/VASYA-DESKTOP@PROJDOM.PRO: FILE:/etc/krb5.keytab
* /usr/sbin/update-rc.d sssd enable
* /usr/sbin/service sssd restart
* Successfully enrolled machine in realm
vasya@vasya-desktop:~$ 
```

Аллилуя работает.

Дальнейшая настройка



The screenshot shows a terminal window titled 'vasya@vasya-desktop: ~' with the following commands and their outputs:

```

realm list
projdom.pro
type: kerberos
realm-name: PROJDOM.PRO
domain-name: projdom.pro
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: sssd-tools
required-package: sssd
required-package: libnss-sss
required-package: libpam-sss
required-package: adcli
required-package: samba-common-bin
login-formats: %U@projdom.pro
login-policy: allow-realm-logins
sudo realm permit --all
vasya@vasya-desktop:~$ id VUbuntovich@PROJDOM.PRO
uid=1726401105(vubuntovich@projdom.pro) gid=1726400513(domain users@projdom.pro) groups=1726400513(domain users@projdom.pro)
vasya@vasya-desktop:~$ 
```

Что тут делаем?

- Чекаем что домен работает (once again)

```
realm list
```

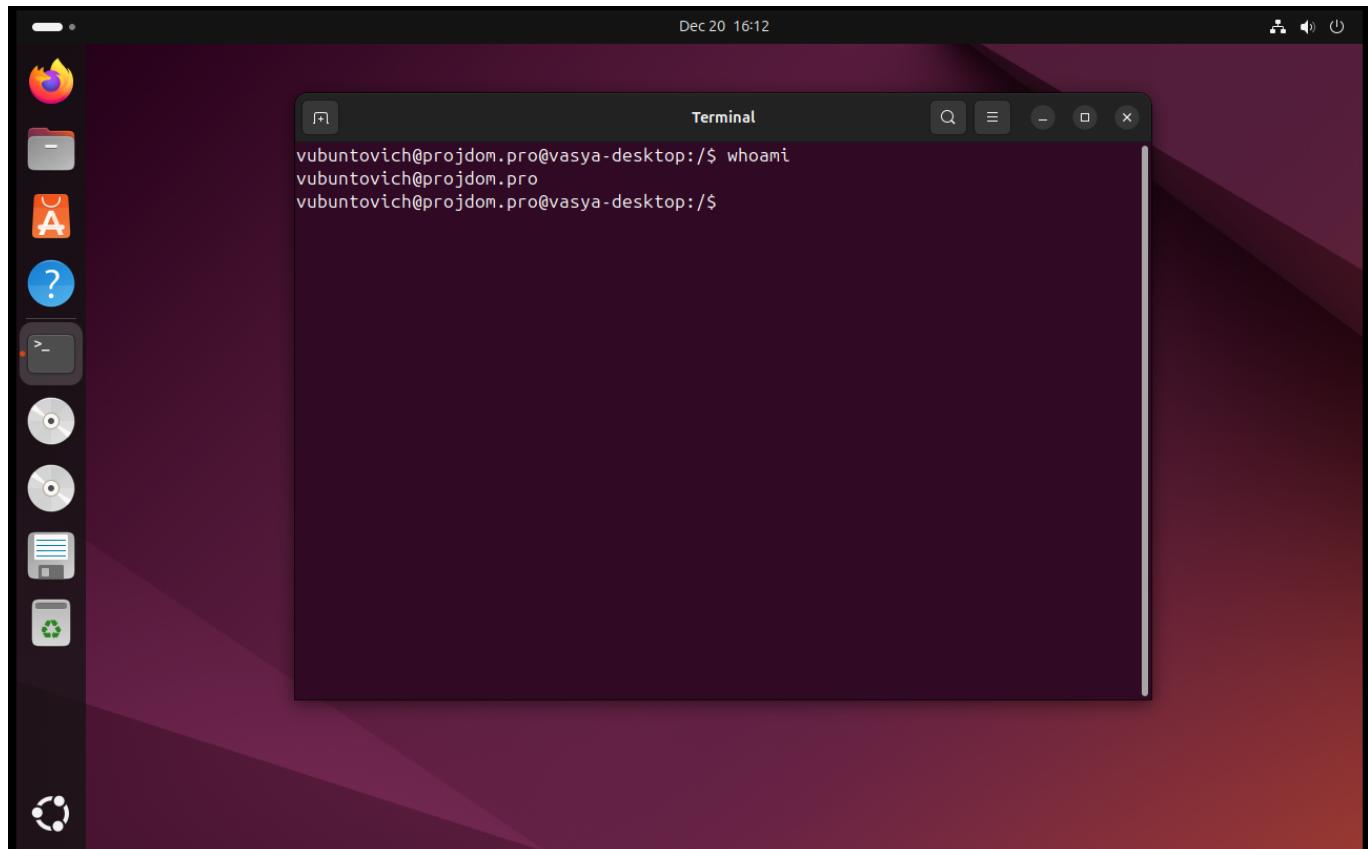
- Выдаем разрешение всем пользователям логиниться в Ubuntu (по-умолчанию никто не может, даже только что залогинившийся юзер на Ubuntu)

```
sudo realm permit --all
```

- Проверяем доступ пользователя

```
id VUbuntovich@PROJDOM.PRO
```

Теперь мы с вами можем производить LogOut из Ubuntu и войти с кредами **VUbuntovich@projdom.pro** и все будет работать:



Почему не работало?

Ответ такой:

Reset Password

- Что делает: позволяет пользователю сбросить пароль компьютера в AD.

- Почему нужно: при join Linux/Windows с помощью adcli или net ads join создаётся компьютерный пароль, который хранится в AD.
- Если пользователь не имеет права Reset Password, join не пройдёт (Access Denied).

Без него: Linux не сможет записать пароль в объект компьютера → join не проходит.

Validated write to DNS host name

- Что делает: позволяет изменять атрибут dNSHostName объекта компьютера.
- Почему нужно: при join adcli пишет в объект полное имя хоста (FQDN).

Без него: join может завершиться ошибкой, Kerberos не сможет корректно использовать SPN, а вход в домен будет проблемным.

Validated write to SPN

- Что делает: позволяет устанавливать SPN (Service Principal Names) для компьютера.
- Почему нужно: SPN нужны для Kerberos. Linux/Windows при join создаёт записи вида:

```
HOST/vasya-desktop
HOST/vasya-desktop.projdom.pro
```

Без него: Kerberos не сможет аутентифицировать машину → ошибки вроде:

```
KDC reply did not match expectations
```

Для лучших практик, уберем разрешения выданные для доступа в домен.

Также дабы избежать приколов в нейминге Linux в файлах, уберем *fully qualified names*:

```
sudo nano /etc/sssd/sssd.conf
# там находим
use_fully_qualified_names = False
#
sudo systemctl restart sssd
```

И поставим **oddjobd** для автоматического создания папок пользователей:

```
sudo apt install oddjob oddjob-mkhomedir
sudo systemctl enable oddjobd
sudo systemctl start oddjobd
sudo nano /etc/sssd/sssd.conf
# добавить или проверить
[domain/projdom.pro]
...
override_homedir = /home/%u
default_shell = /bin/bash
#
sudo systemctl restart sssd
```

Dec 20 16:31

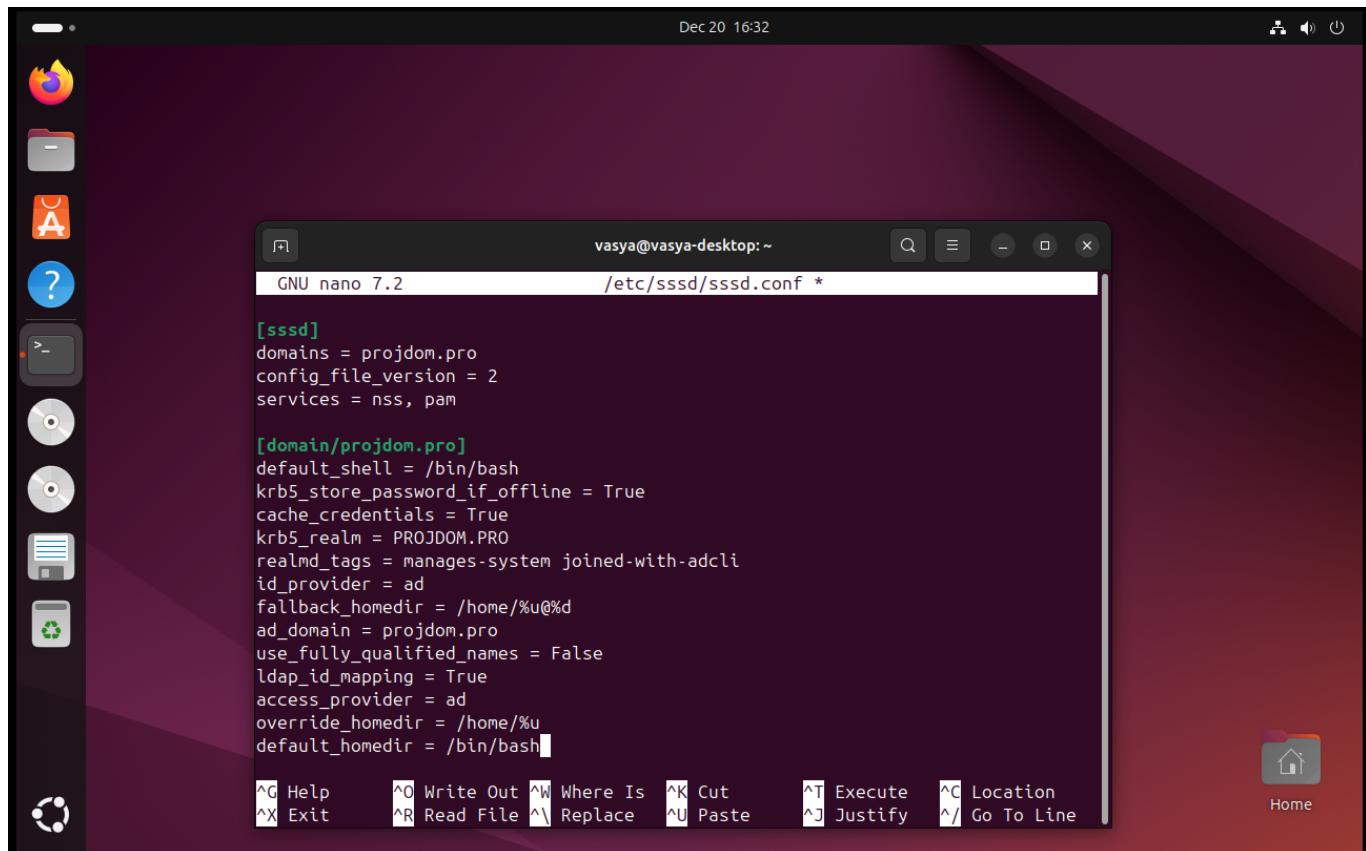
```
vasya@vasya-desktop:~$ sudo apt install oddjob oddjob-mkhomedir
[sudo] password for vasya:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
oddjob is already the newest version (0.34.7-2).
oddjob-mkhomedir is already the newest version (0.34.7-2).
0 upgraded, 0 newly installed, 0 to remove and 131 not upgraded.
vasya@vasya-desktop:~$ sudo systemctl enable oddjobd
sudo systemctl stasudo systemctl start oddjobd
vasya@vasya-desktop:~$ sudo systemctl status oddobj
Unit oddobj.service could not be found.
vasya@vasya-desktop:~$ sudo systemctl status oddobjd
Unit oddobjd.service could not be found.
vasya@vasya-desktop:~$ sudo systemctl status oddjobd
● oddjobd.service - privileged operations for unprivileged applications
  Loaded: loaded (/usr/lib/systemd/system/oddjobd.service; enabled; preset: )
  Active: active (running) since Sat 2025-12-20 16:23:58 MSK; 7min ago
    Main PID: 1242 (oddjobd)
      Tasks: 1 (limit: 4545)
     Memory: 2.2M (peak: 2.5M)
        CPU: 23ms
       CGroup: /system.slice/oddjobd.service
               └─1242 /usr/sbin/oddjobd -n -p /run/oddjobd.pid -t 300

vasya@vasya-desktop:~$
```

Dec 20 16:31

```
Building dependency tree... Done
Reading state information... Done
oddjob is already the newest version (0.34.7-2).
oddjob-mkhomedir is already the newest version (0.34.7-2).
0 upgraded, 0 newly installed, 0 to remove and 131 not upgraded.
vasya@vasya-desktop:~$ sudo systemctl enable oddjobd
sudo systemctl stasudo systemctl start oddjobd
vasya@vasya-desktop:~$ sudo systemctl status oddobj
Unit oddobj.service could not be found.
vasya@vasya-desktop:~$ sudo systemctl status oddobjd
Unit oddobjd.service could not be found.
vasya@vasya-desktop:~$ sudo systemctl status oddjobd
● oddjobd.service - privileged operations for unprivileged applications
  Loaded: loaded (/usr/lib/systemd/system/oddjobd.service; enabled; preset: )
  Active: active (running) since Sat 2025-12-20 16:23:58 MSK; 7min ago
    Main PID: 1242 (oddjobd)
      Tasks: 1 (limit: 4545)
     Memory: 2.2M (peak: 2.5M)
        CPU: 23ms
       CGroup: /system.slice/oddjobd.service
               └─1242 /usr/sbin/oddjobd -n -p /run/oddjobd.pid -t 300

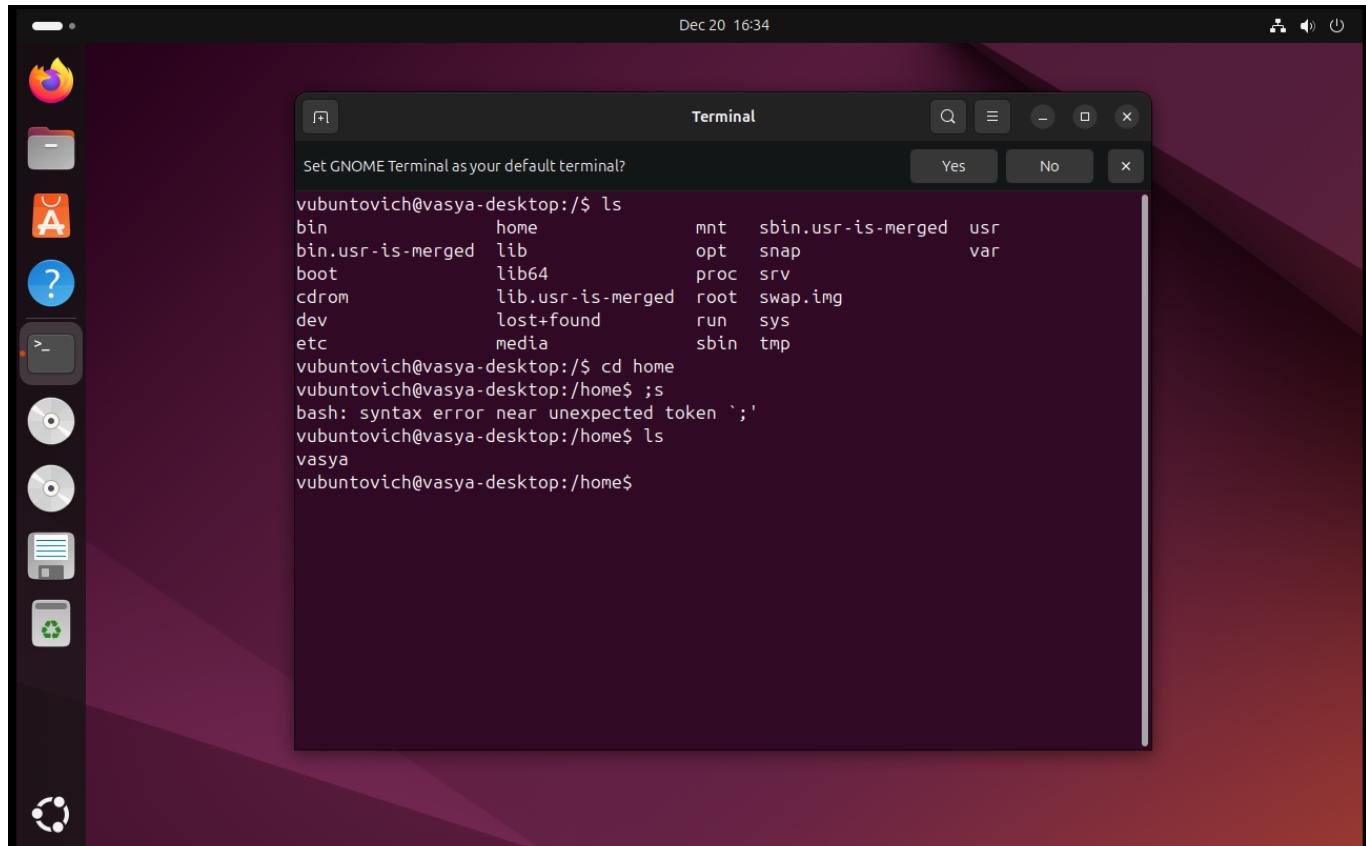
Dec 20 16:23:58 vasya-desktop systemd[1]: Started oddjobd.service - privileged
vasya@vasya-desktop:~$
```



```
[sssd]
domains = projdom.pro
config_file_version = 2
services = nss, pam

[domain/projdom.pro]
default_shell = /bin/bash
krb5_store_password_if_offline = True
cache_credentials = True
krb5_realm = PROJDOM.PRO
realmd_tags = manages-system joined-with-adcli
id_provider = ad
fallback_homedir = /home/%u@%
ad_domain = projdom.pro
use_fullyQualifiedNames = False
ldap_id_mapping = True
access_provider = ad
override_homedir = /home/%u
default_homedir = /bin/bash
```

Идем в доменный аккаунт



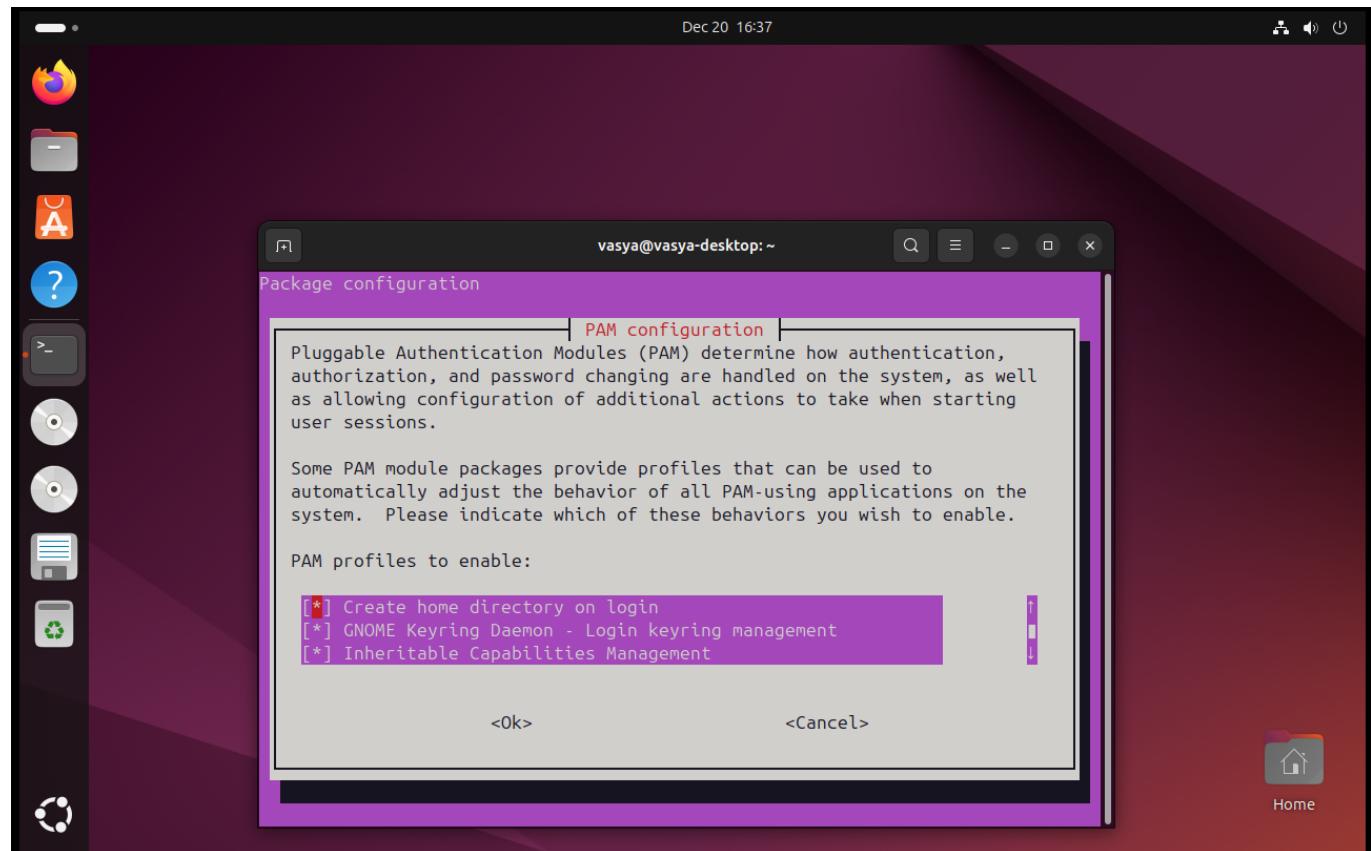
```
Set GNOME Terminal as your default terminal? Yes No x
vubuntovich@vasya-desktop:~$ ls
bin          home          mnt  sbin.usr-is-merged  usr
bin.usr-is-merged lib          opt  snap                  var
boot         lib64         proc  srv
cdrom        lib.usr-is-merged root  swap.img
dev          lost+found    run   sys
etc          media         sbin  tmp
vubuntovich@vasya-desktop:~$ cd home
vubuntovich@vasya-desktop:/home$ ;s
bash: syntax error near unexpected token `;'
vubuntovich@vasya-desktop:/home$ ls
vasya
vubuntovich@vasya-desktop:/home$
```

в home что странно ничего нет про нашего **vubuntovich**

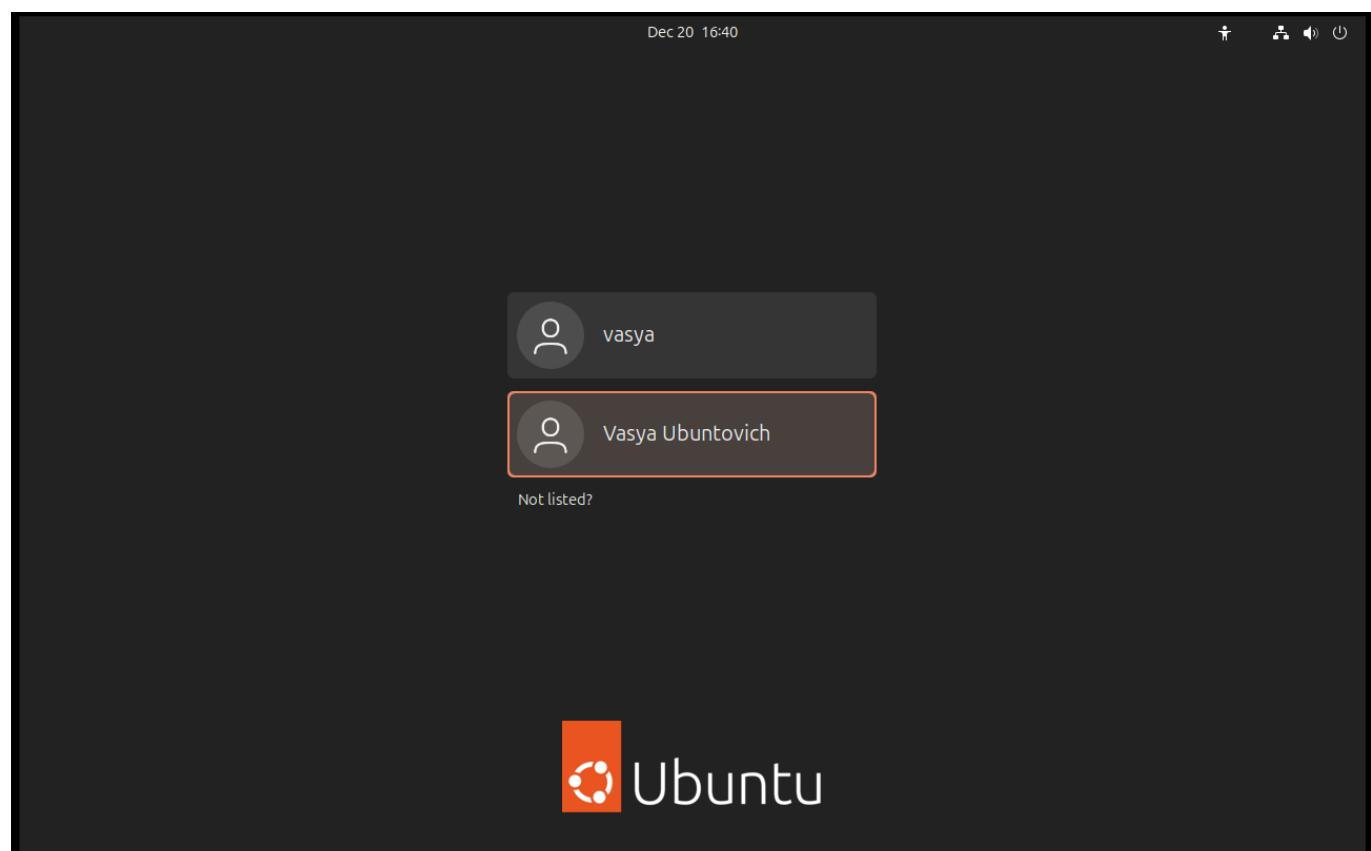
А! Мы забыли включить эту опцию в PAM-модуле:

```
sudo pam-auth-update
```

Листаем и находим **Create home directory on login**

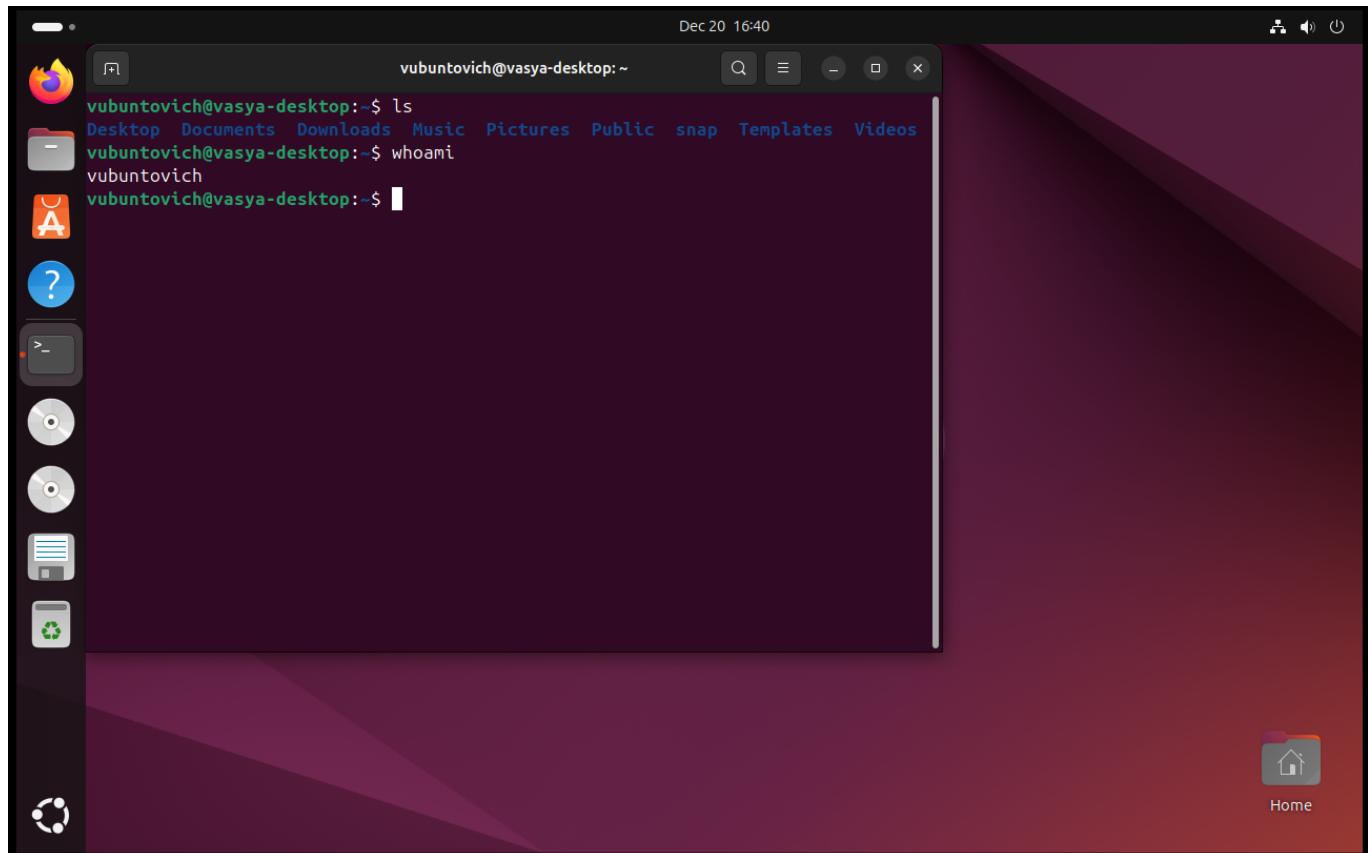


Ребутаем машину и что видим:



На этапе входа в аккаунт домена видим надпись **Creating directory '/home/vubuntovich'**

и все работает! (Да, бесиящая вкладка интро в Ubuntu не уходит, но терпим)



P.S.

На этапе входа в машинку окно пользователя появляется не сразу. Рекомендуется сразу разобраться с **PAM**, **ooddjobd** и затем проделывать вход на AD пользователя