Установка и настройка Active Directory

> Первоначальный источник и опора: статья от testo-lang

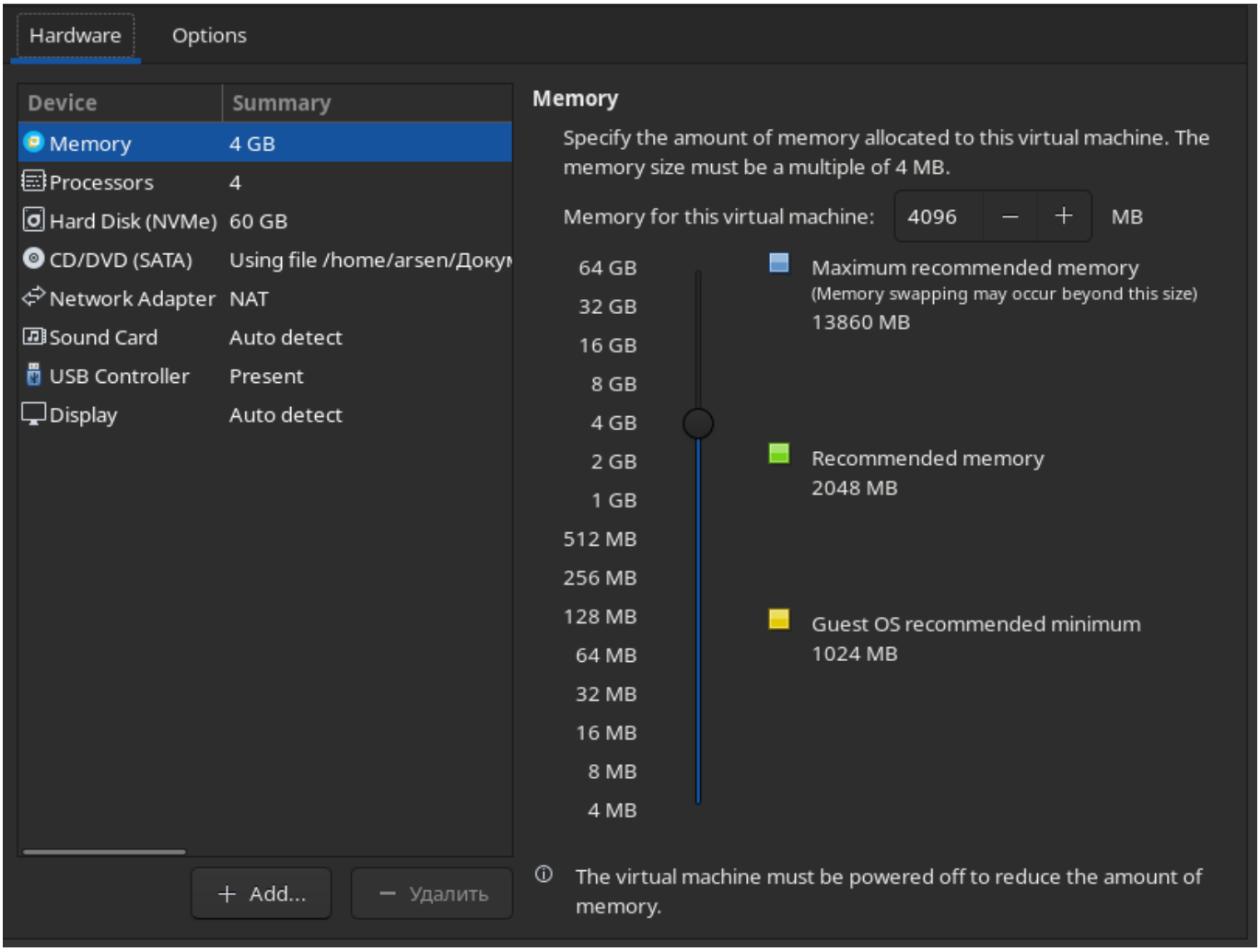
В данном документе будет рассказана пошаговая установка и настройка домена AD состоящего из:

- Microsoft Windows Server 2019 Standart Evaluation: контроллер домена
- Microsoft Windows 10: рабочая станция 1
- Ubuntu 22.04 LTS: рабочая станция 2

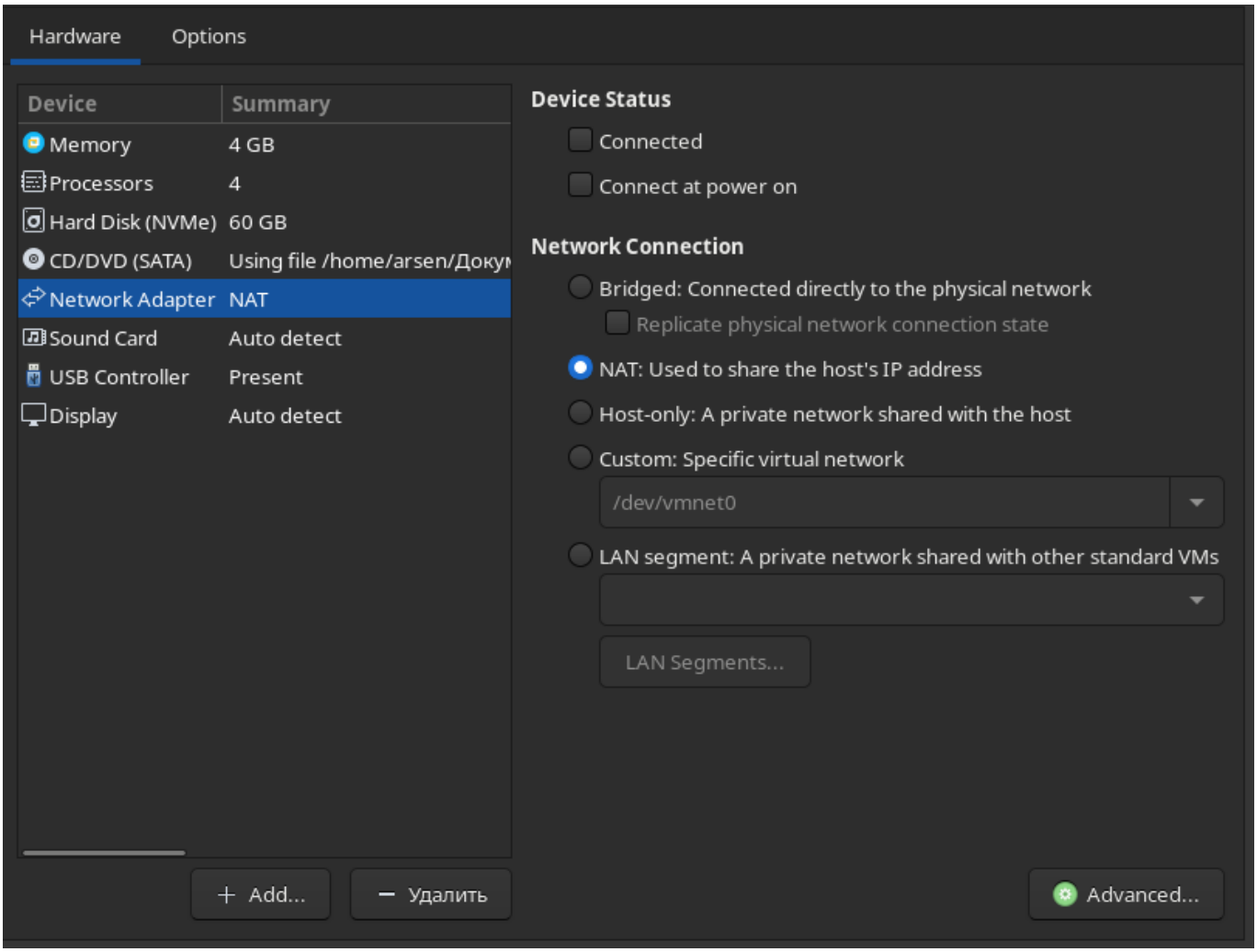
В качетве симуляции вирутальных машин будет использована VMWare Workstation Professional

Установка и настройка контроллера домена

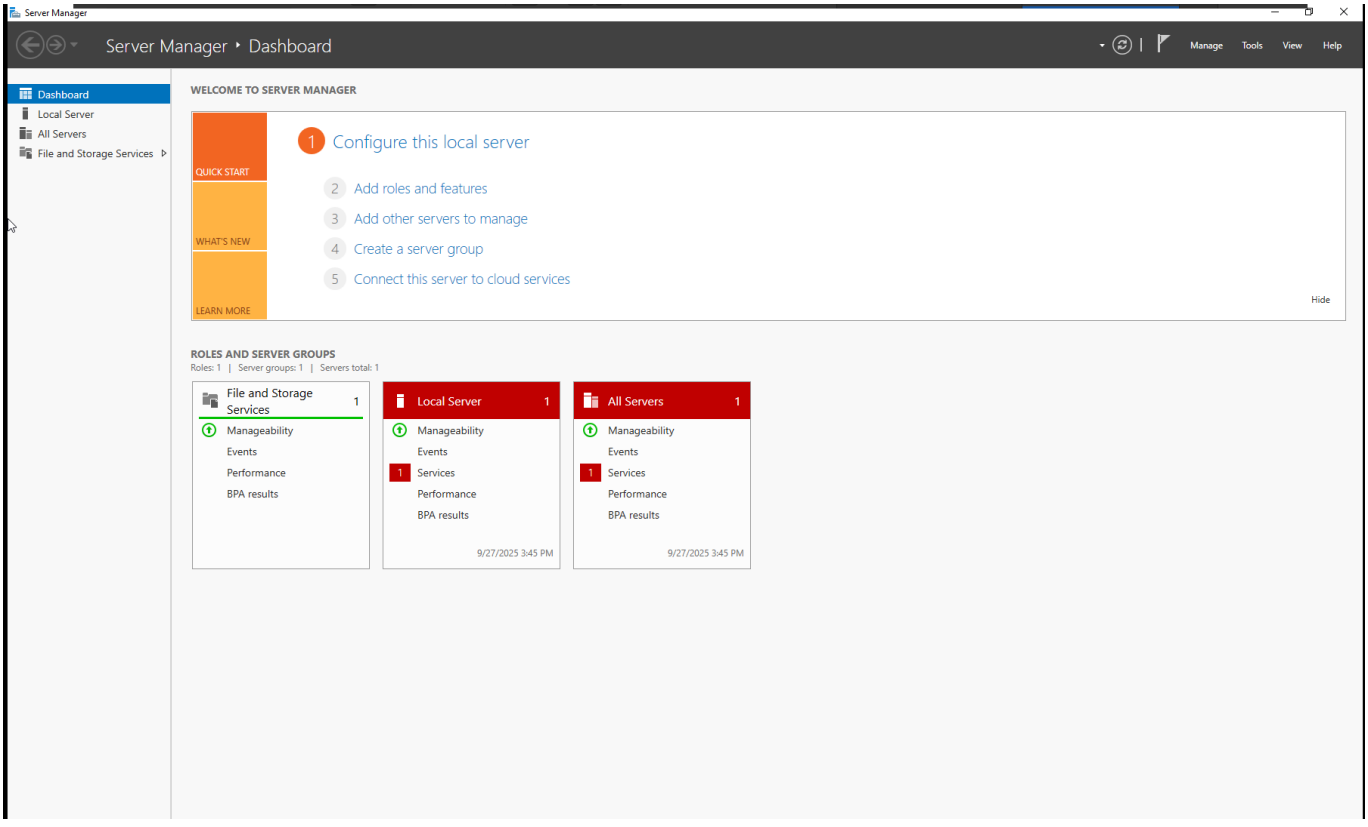
Устанавливаем официальный iso-образ Windows Server 2019 и запускаем виртуальную среду, в нашем случае VMWare. Ниже представлены настройки виртуальной машины:



Важно! Если есть потребность в том, чтобы пропустить сканирование лицензии Microsoft, то стоит отключить доступ в сеть, а после запуска машины уже включить обратно:

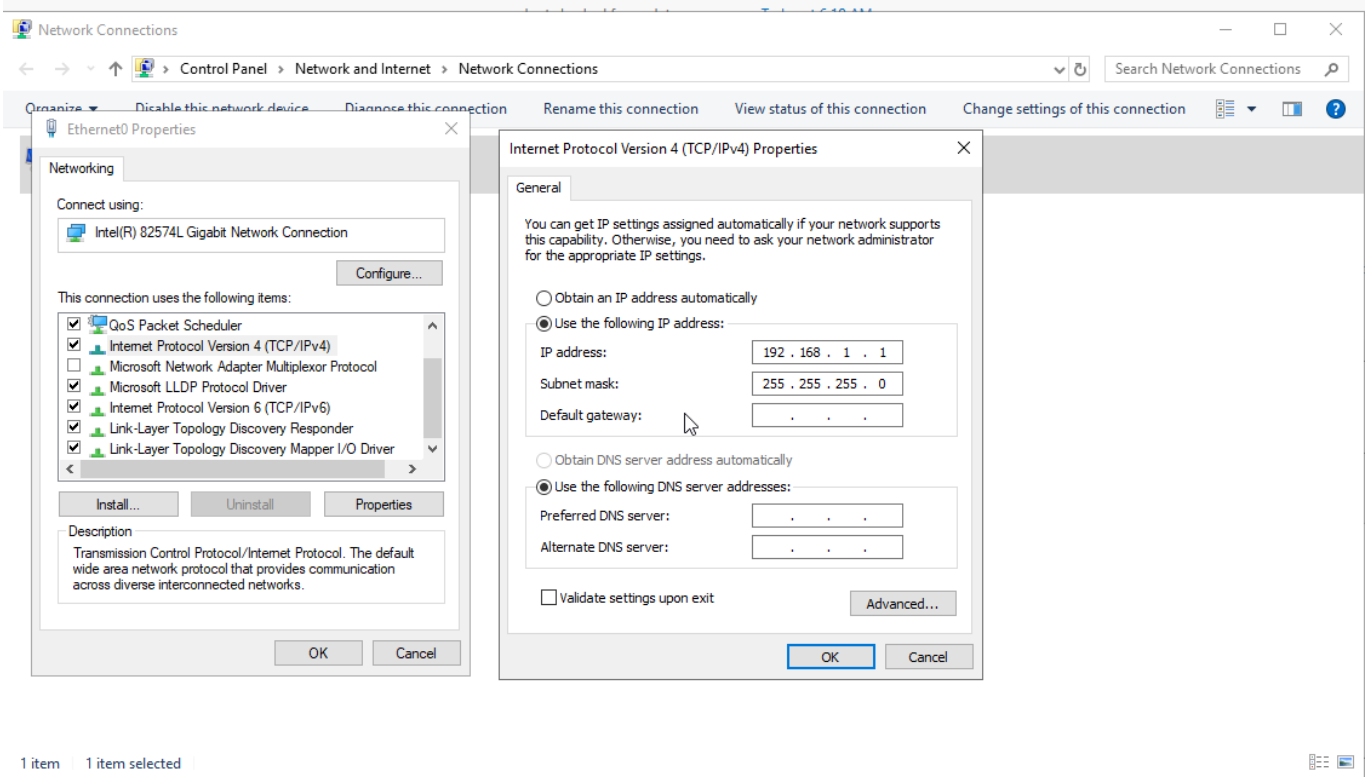


После установки попадаем в панель админа.

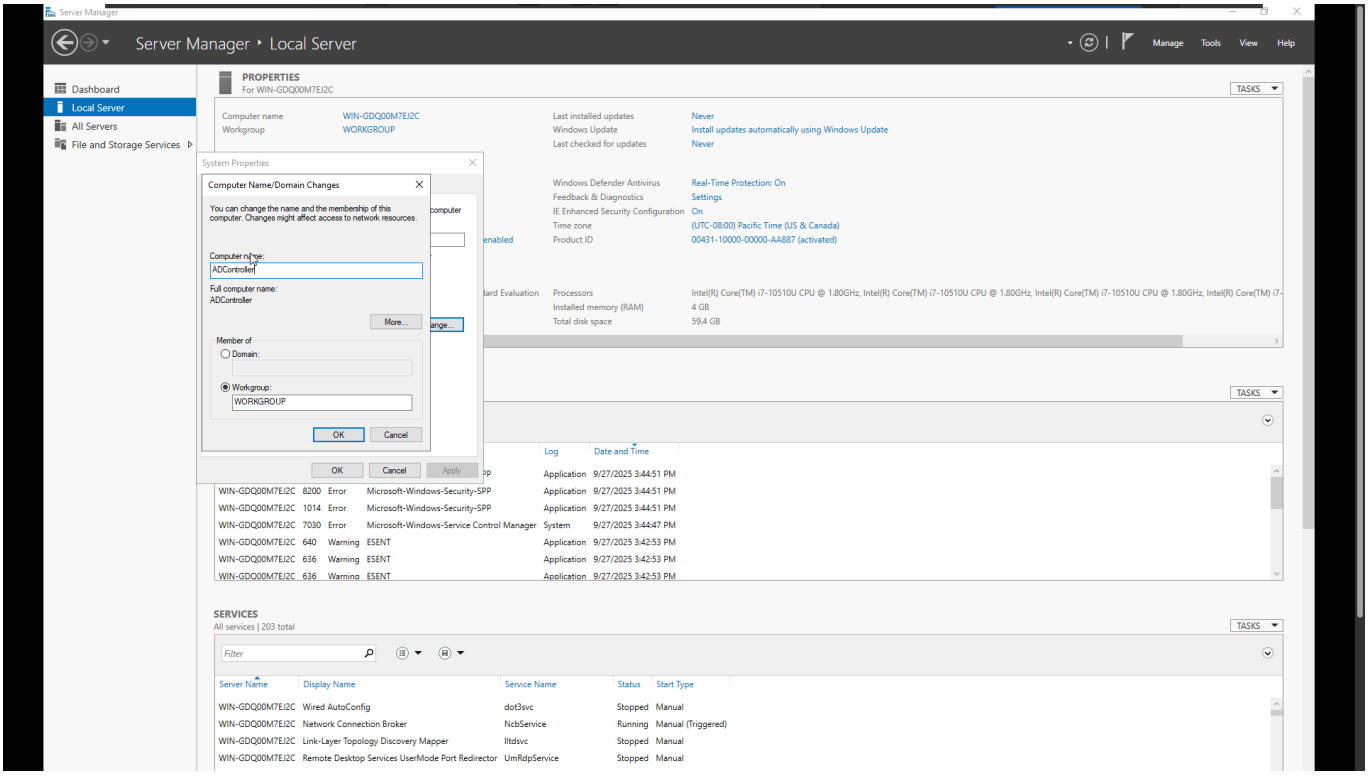


Проводим первоначальную настройку устройства:

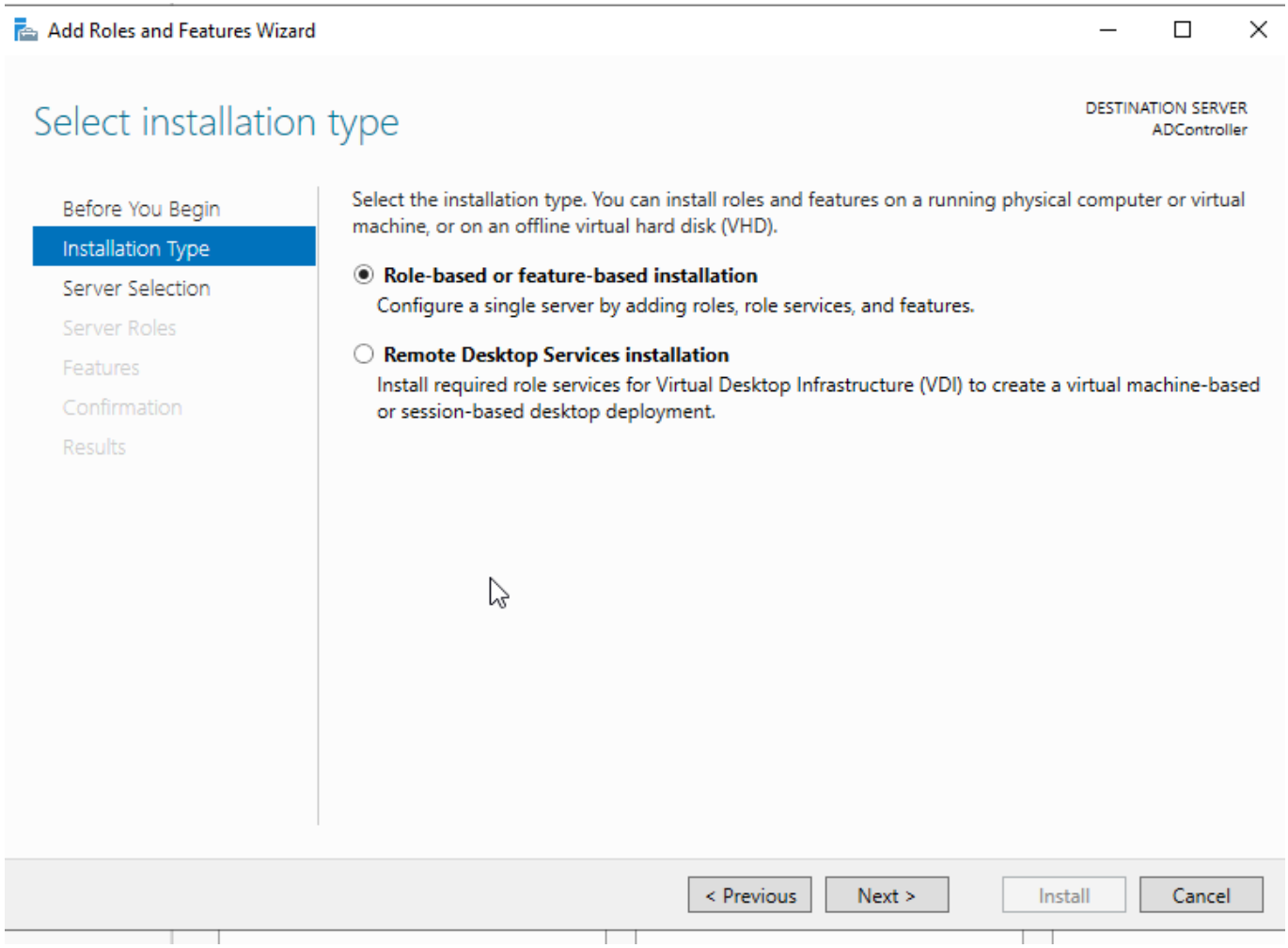
- Настройка IPv4 интерфейса

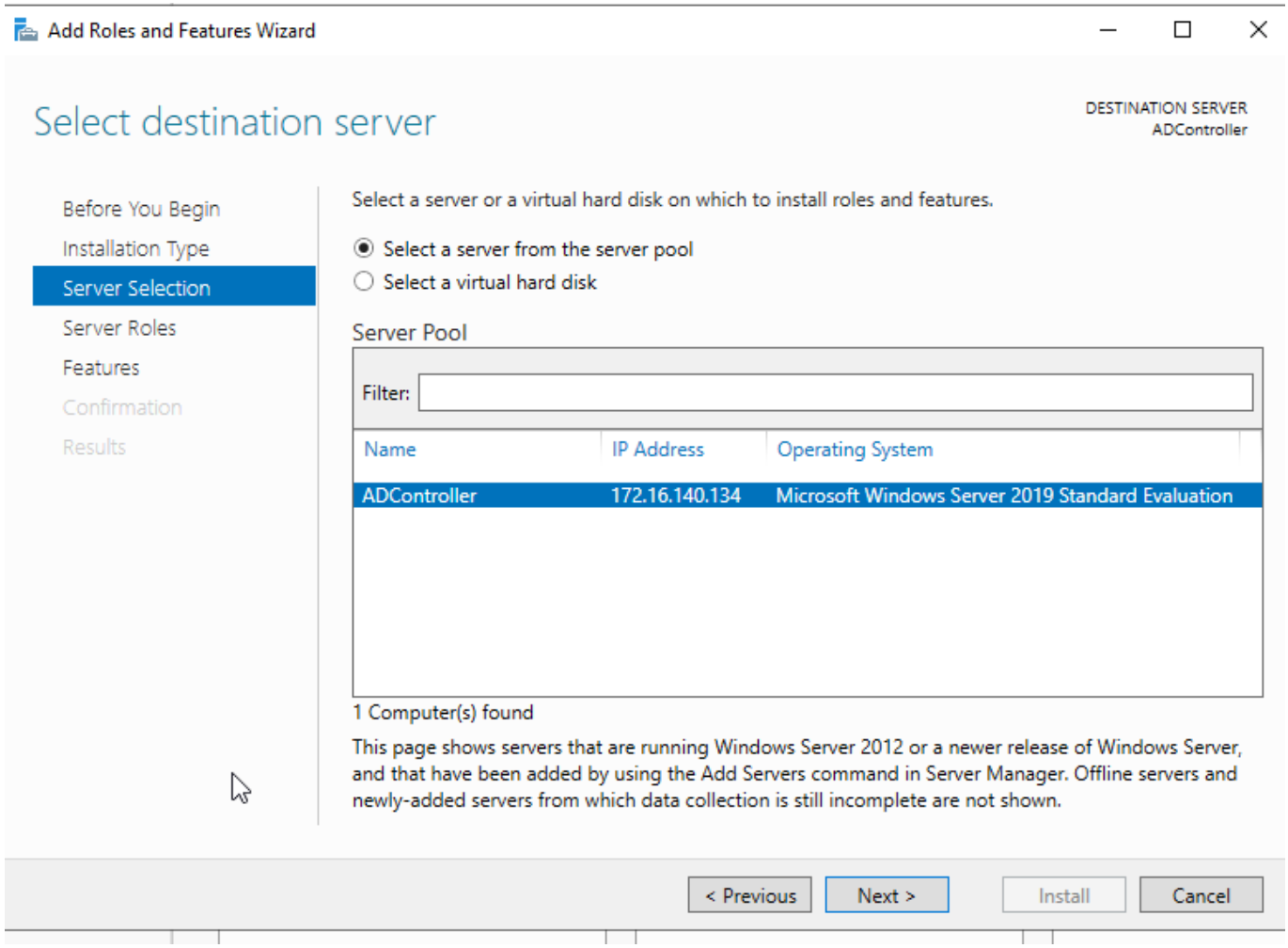


- Смена имени контроллера + последующая перезагрузка



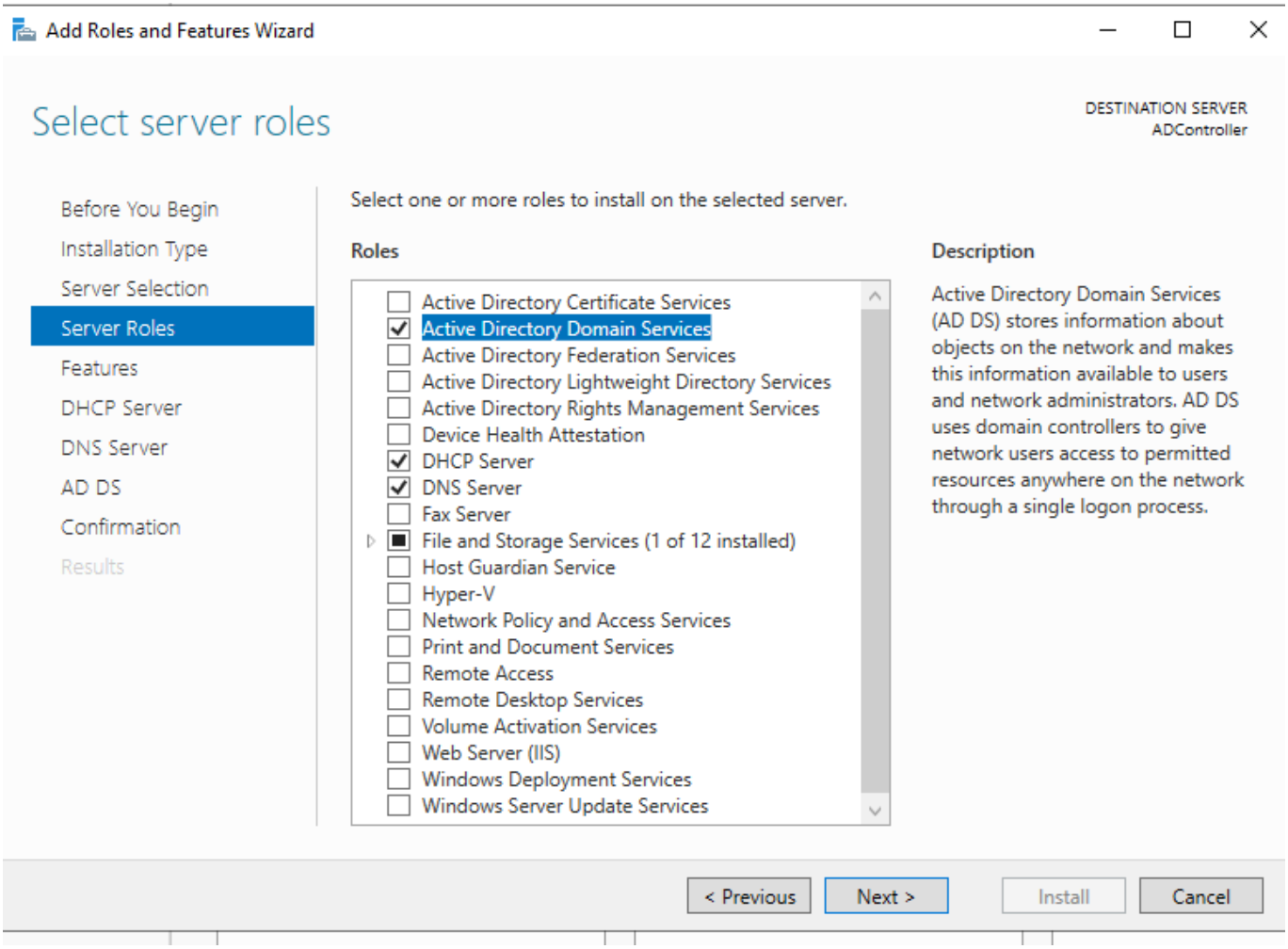
Добавление ролей и компонентов:


Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
ADController
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

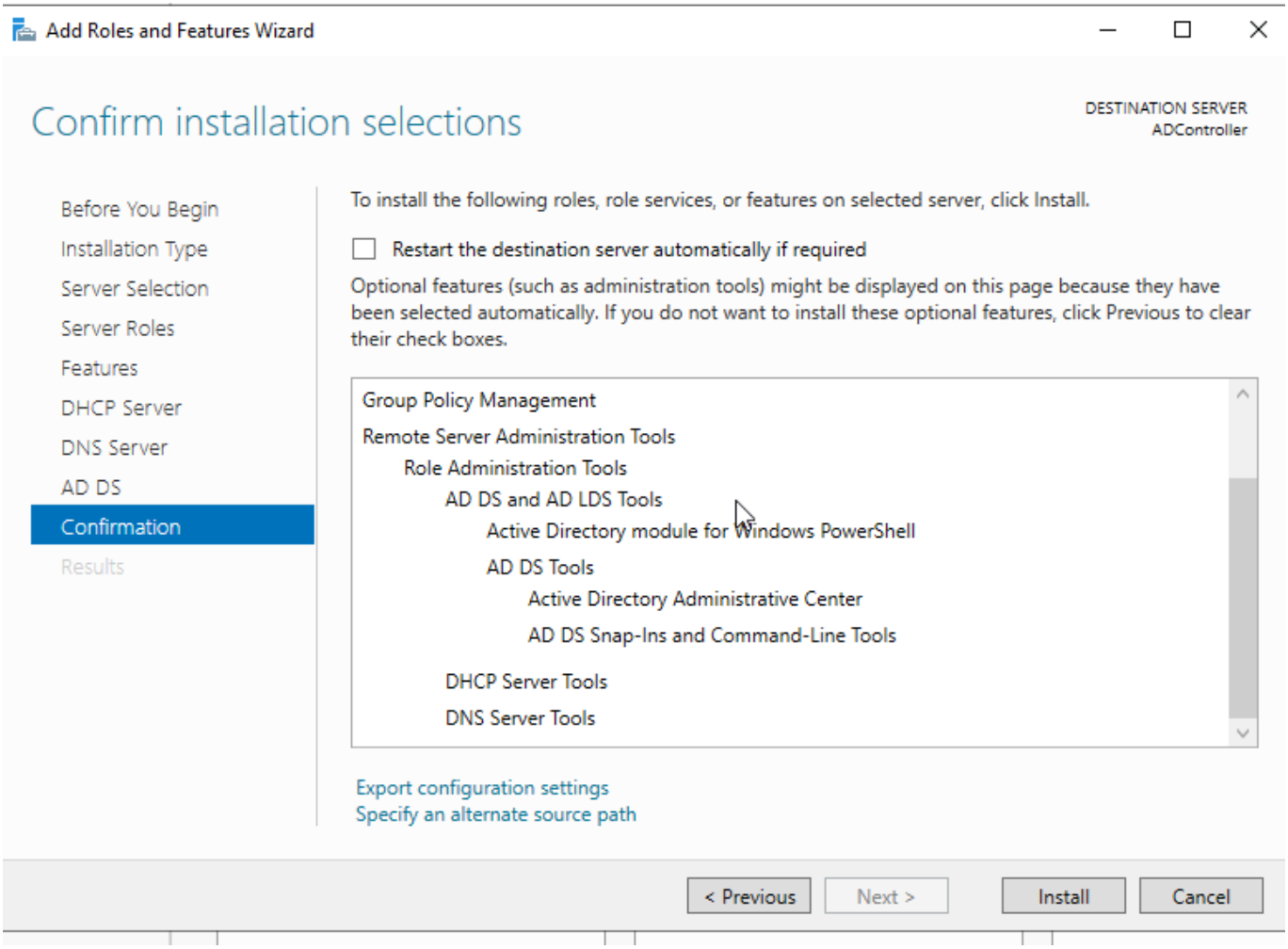

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
ADController
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
ADController
172.16.140.134
Microsoft Windows Server 2019 Standard Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

Затем

- Включаем доменные службы AD
- Ставим DNS-сервер
- Ставим DHCP-сервер

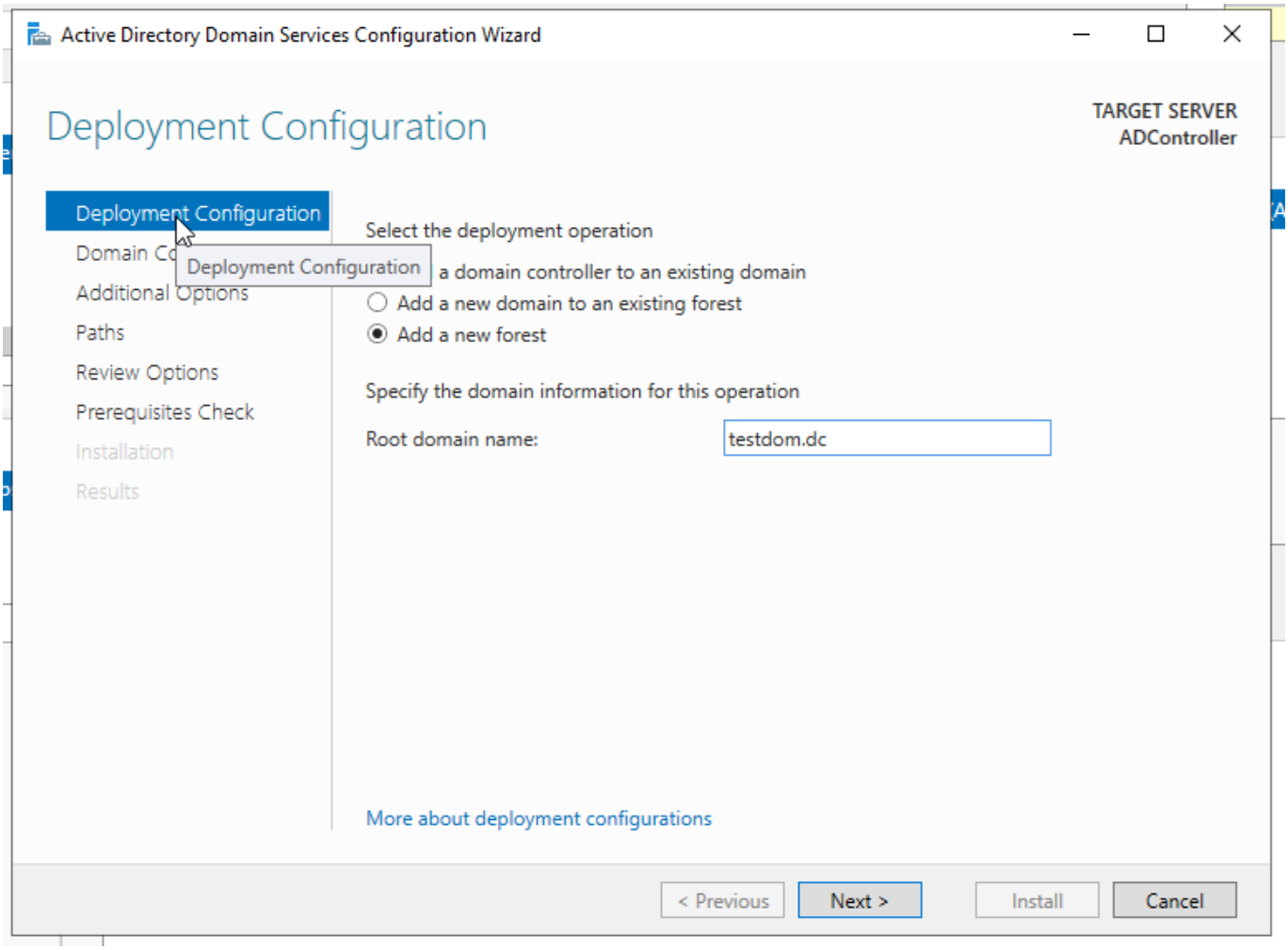


Инсталляция ролей

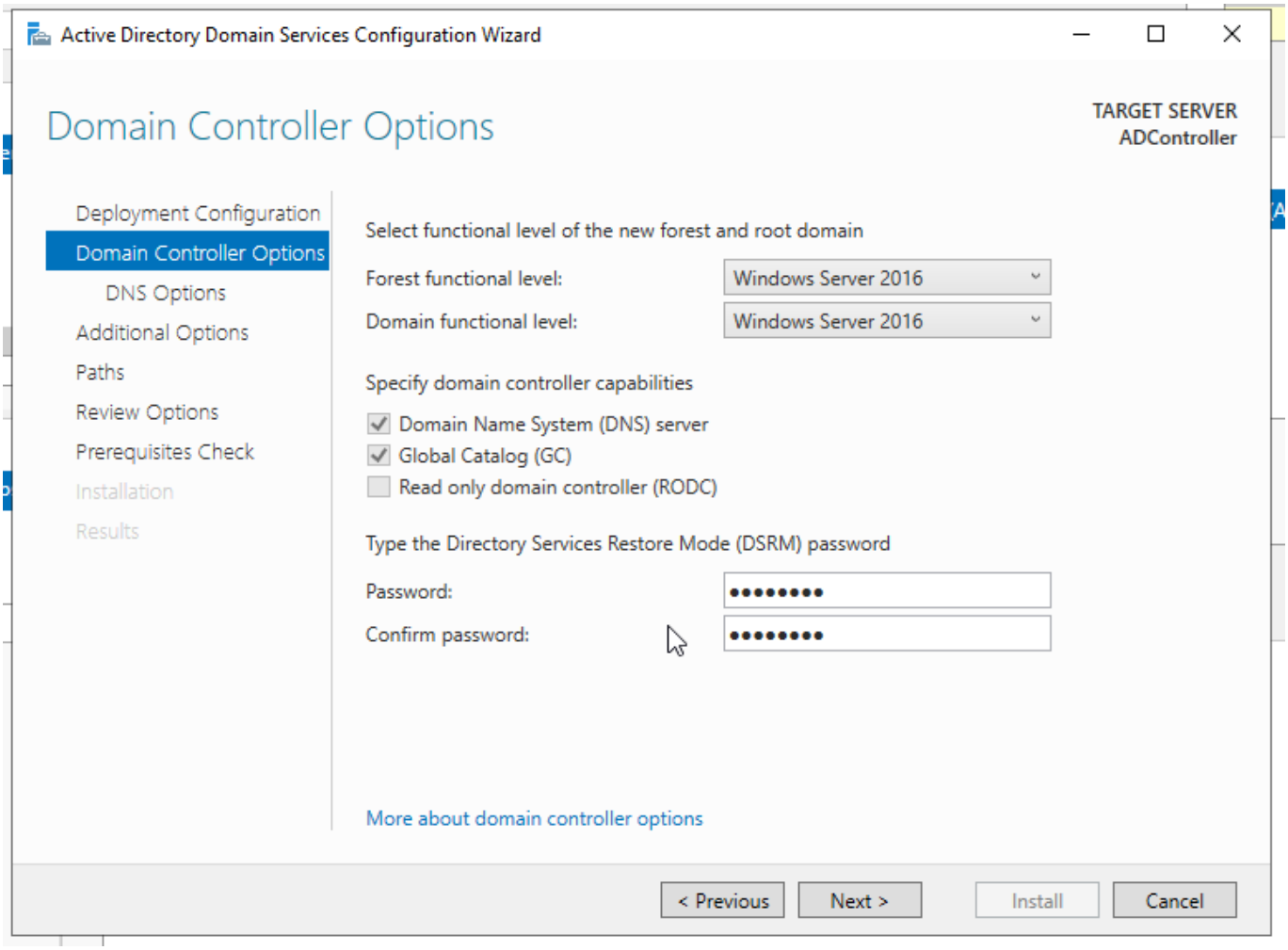


Настойка роли AD

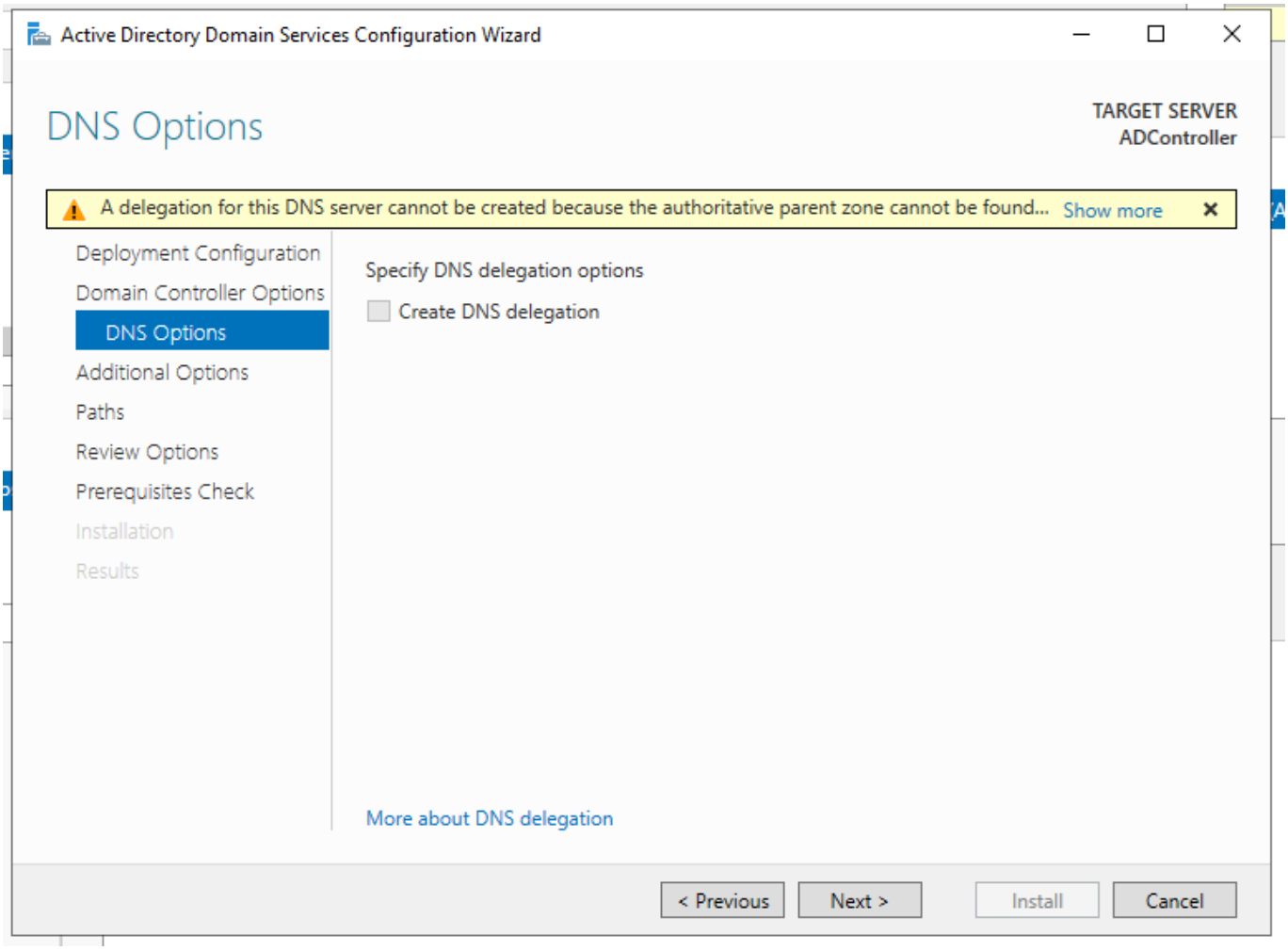
После установки необходимо провести настройку работы AD, так как нам нужно инициализировать корневой элемент леса доменных имен, нужно сначала создать сам лес:



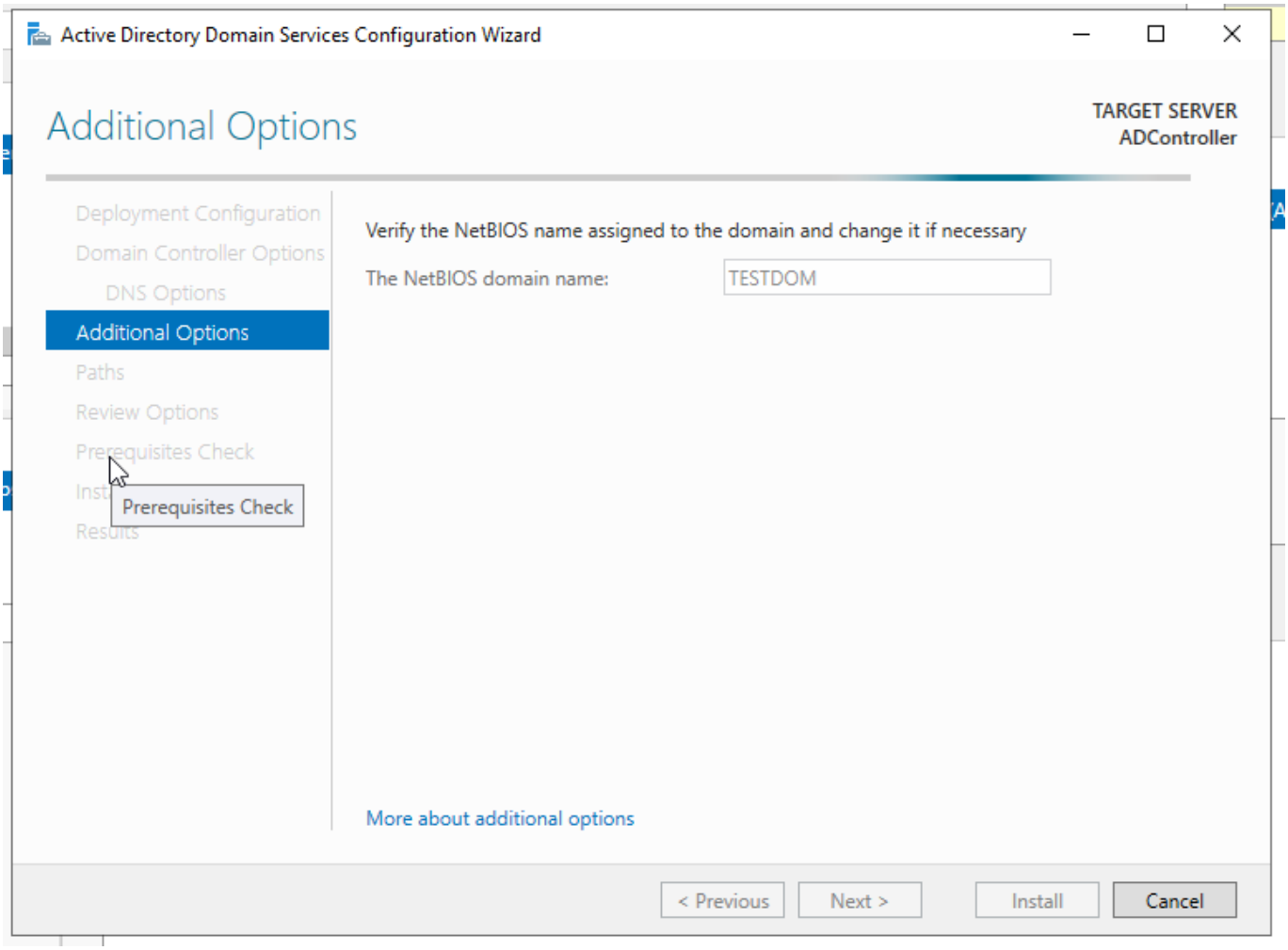
Оставляем настройки по умоляанию.

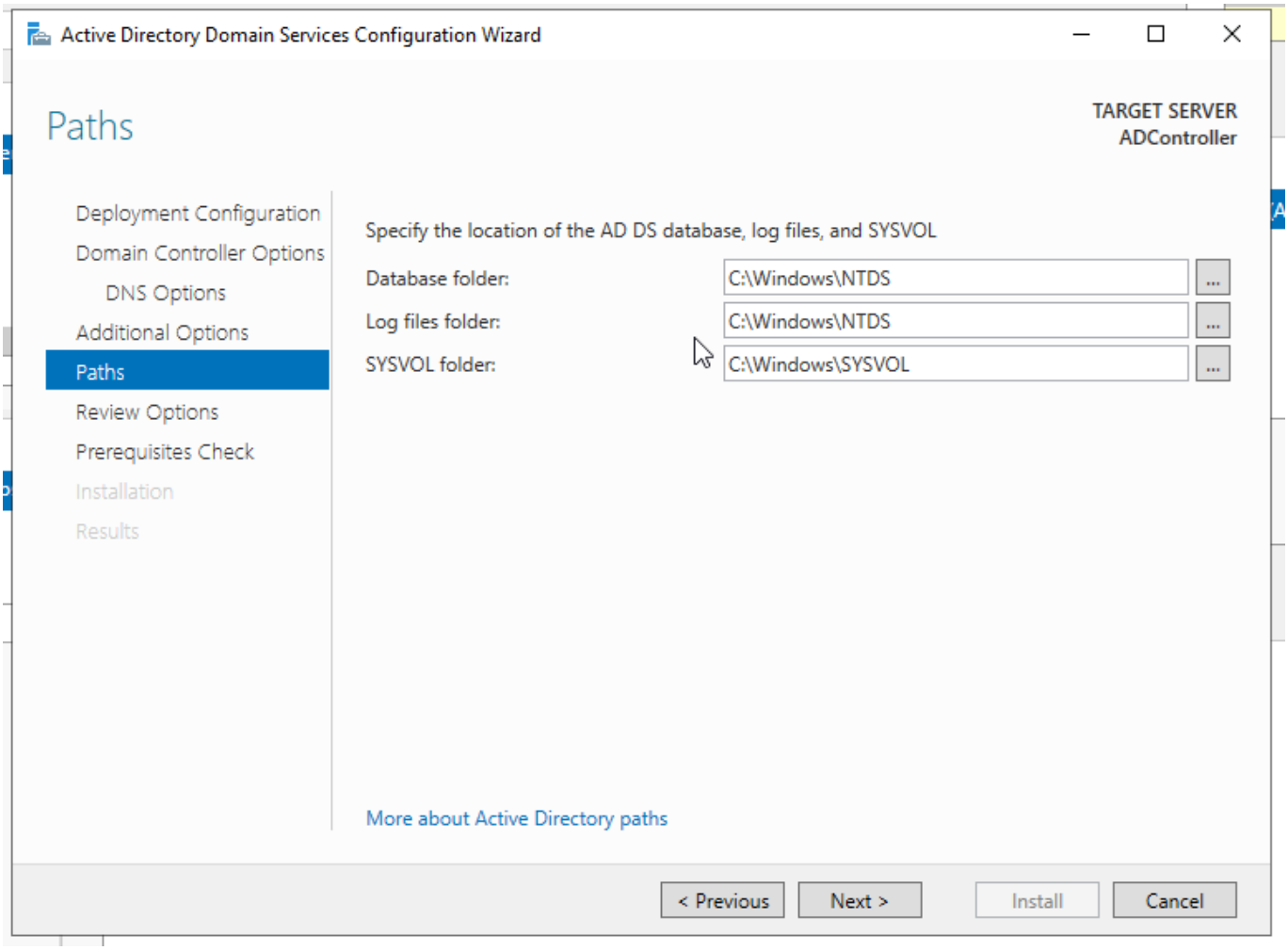


Так как мы имеем только одну машину оснащенную DNS и одно DNS-пространство имен,то нет нужды включать делегирование.

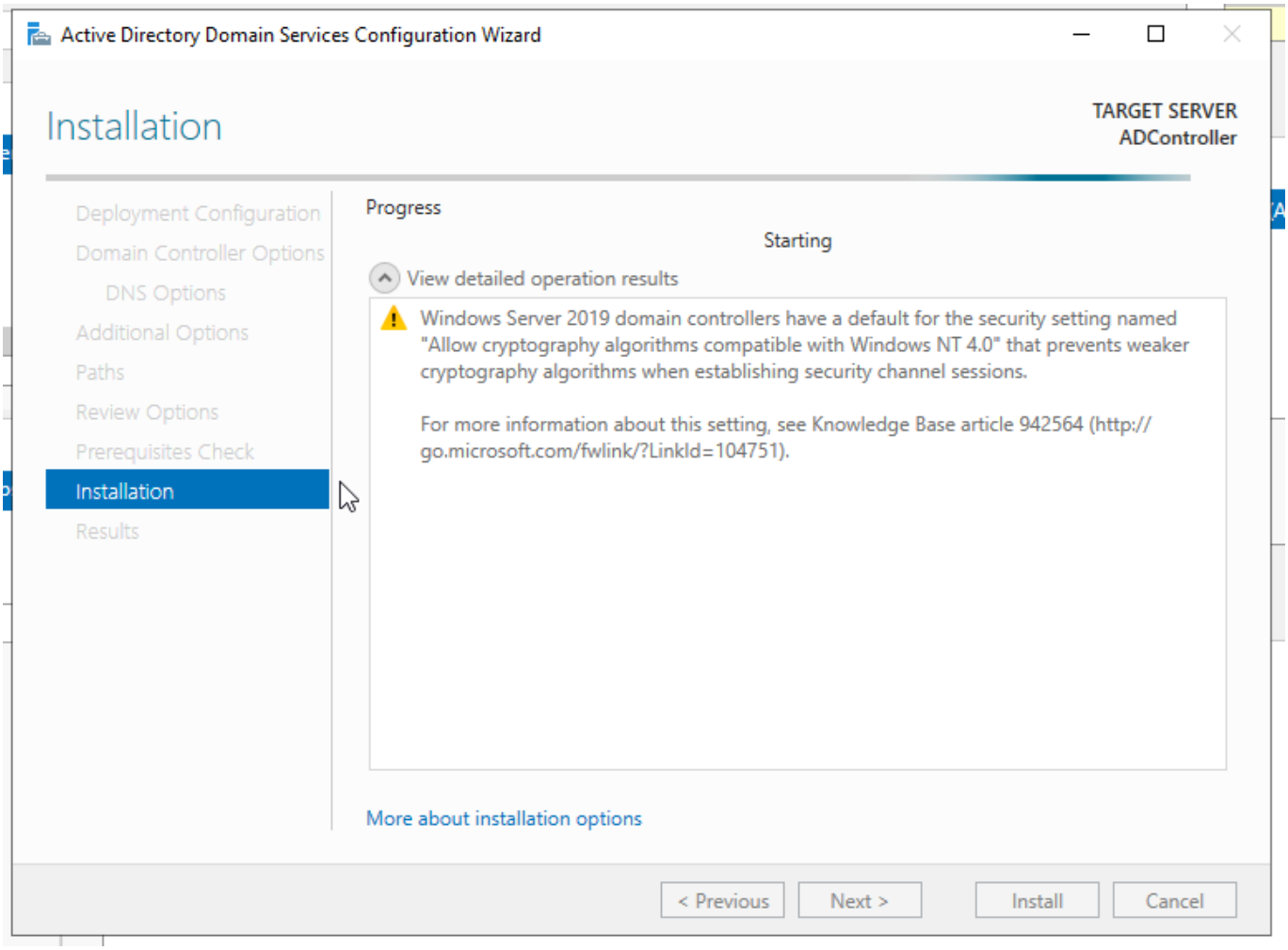


Оставляем сгенерированное NetBIOS имя и автоматически выбранные пути баз данных


Active Directory Domain Services Configuration Wizard
Additional Options
TARGET SERVER
ADController
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Prerequisites Check
Verify the NetBIOS name assigned to the domain and change it if necessary
The NetBIOS domain name:
TESTDOM
More about additional options
< Previous
Next >
Install
Cancel

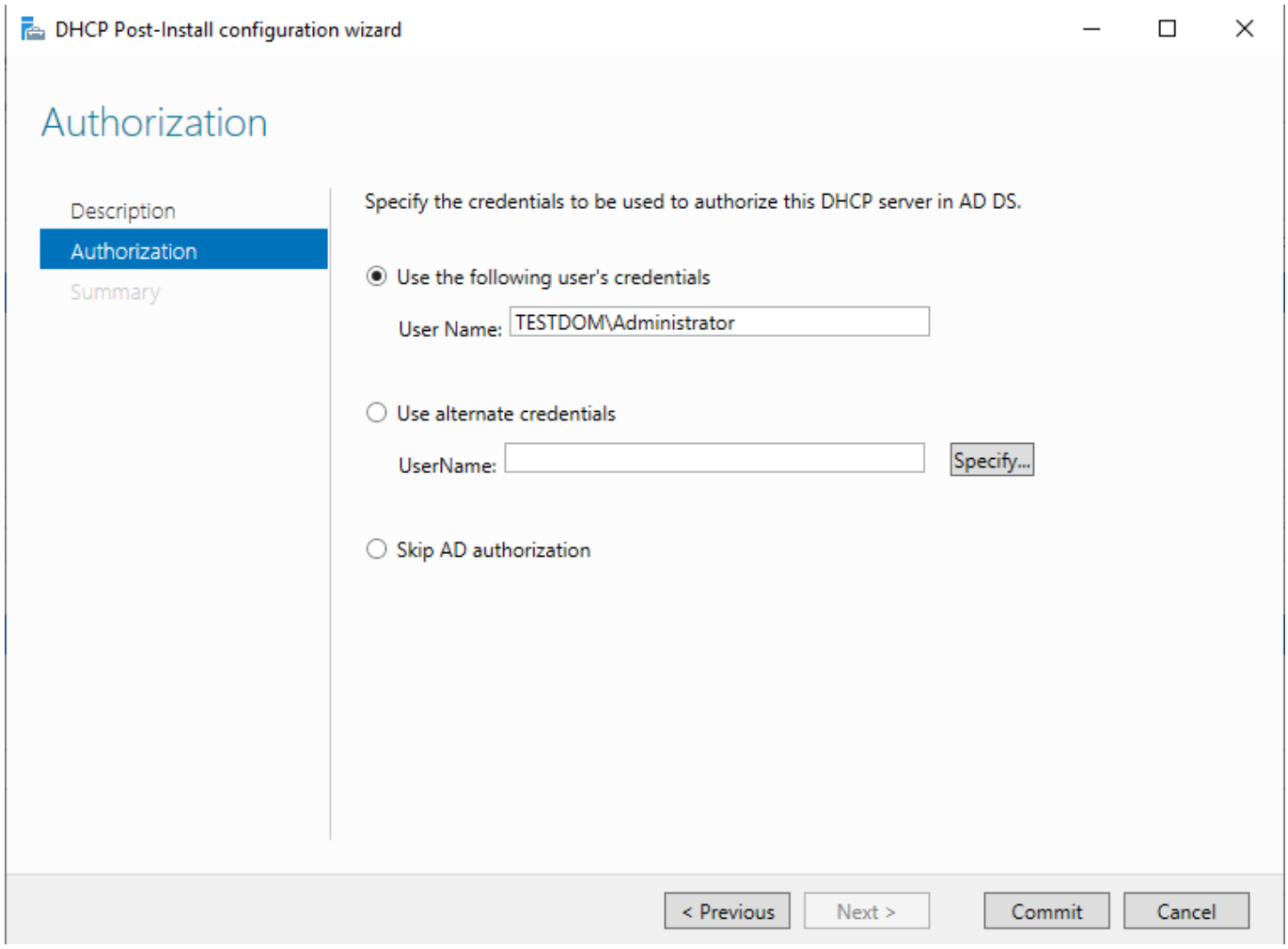

Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
ADController
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
More about Active Directory paths
< Previous
Next >
Install
Cancel

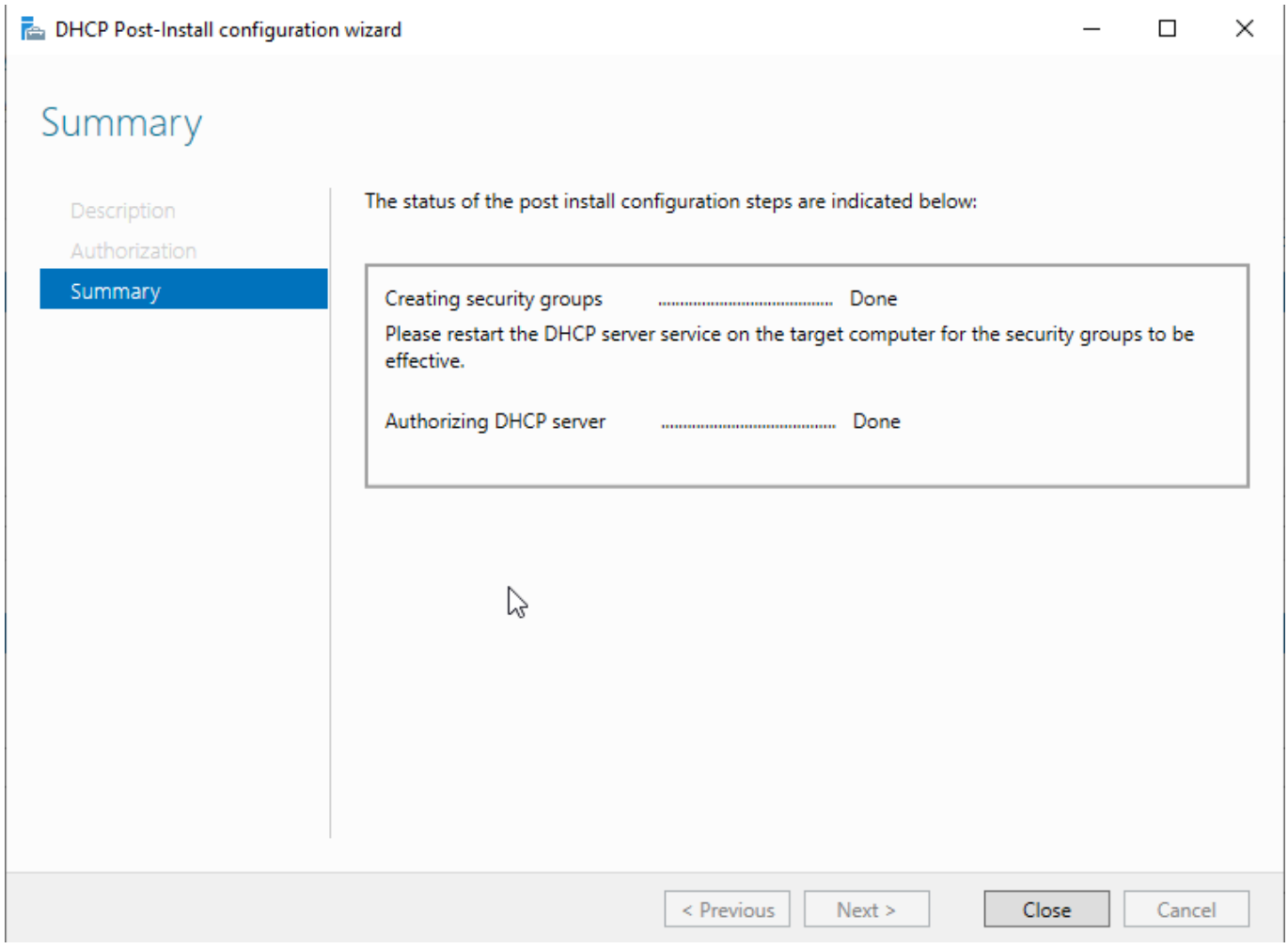
Запускаем установку настроек



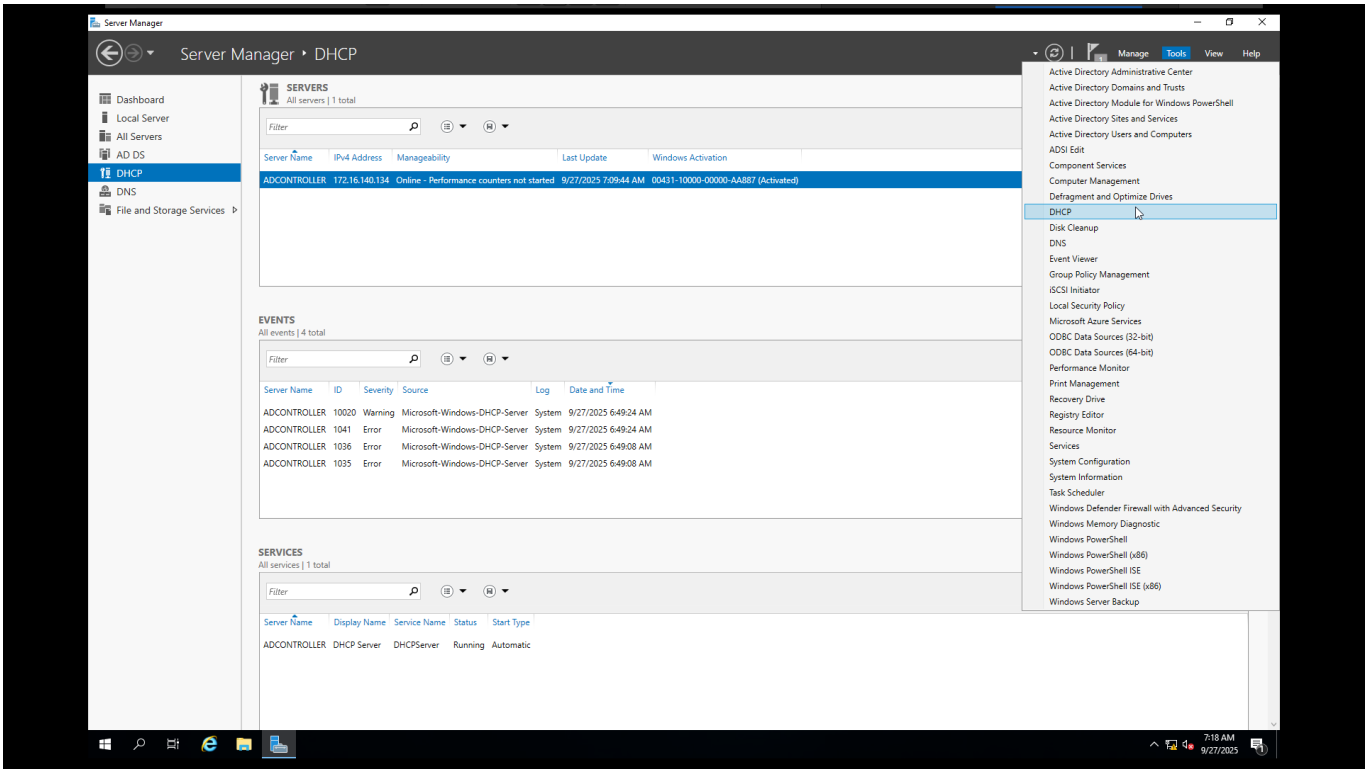
Настройка роли DHCP-сервера

Дабы быстро настроить инфраструктуру, оставим полномочия для регистрации DHCP-сервера на нашем глобальном администраторе (без создания более мелкого).

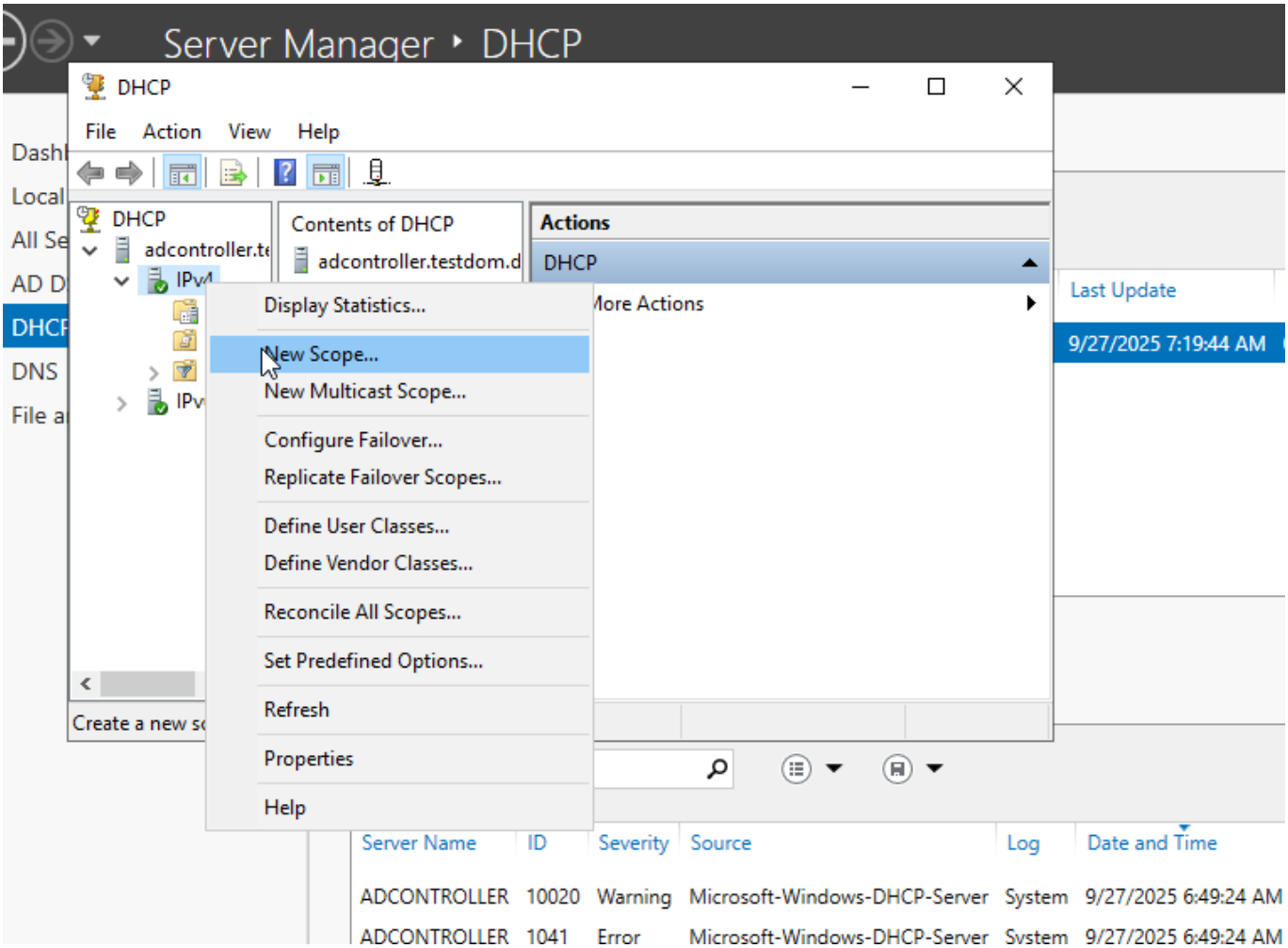

DHCP Post-Install configuration wizard
Authorization
Description
Authorization
Summary
Specify the credentials to be used to authorize this DHCP server in AD DS.
Use the following user's credentials
User Name: TESTDOM\Administrator
Use alternate credentials
UserName:
Specify...
Skip AD authorization
< Previous
Next >
Commit
Cancel

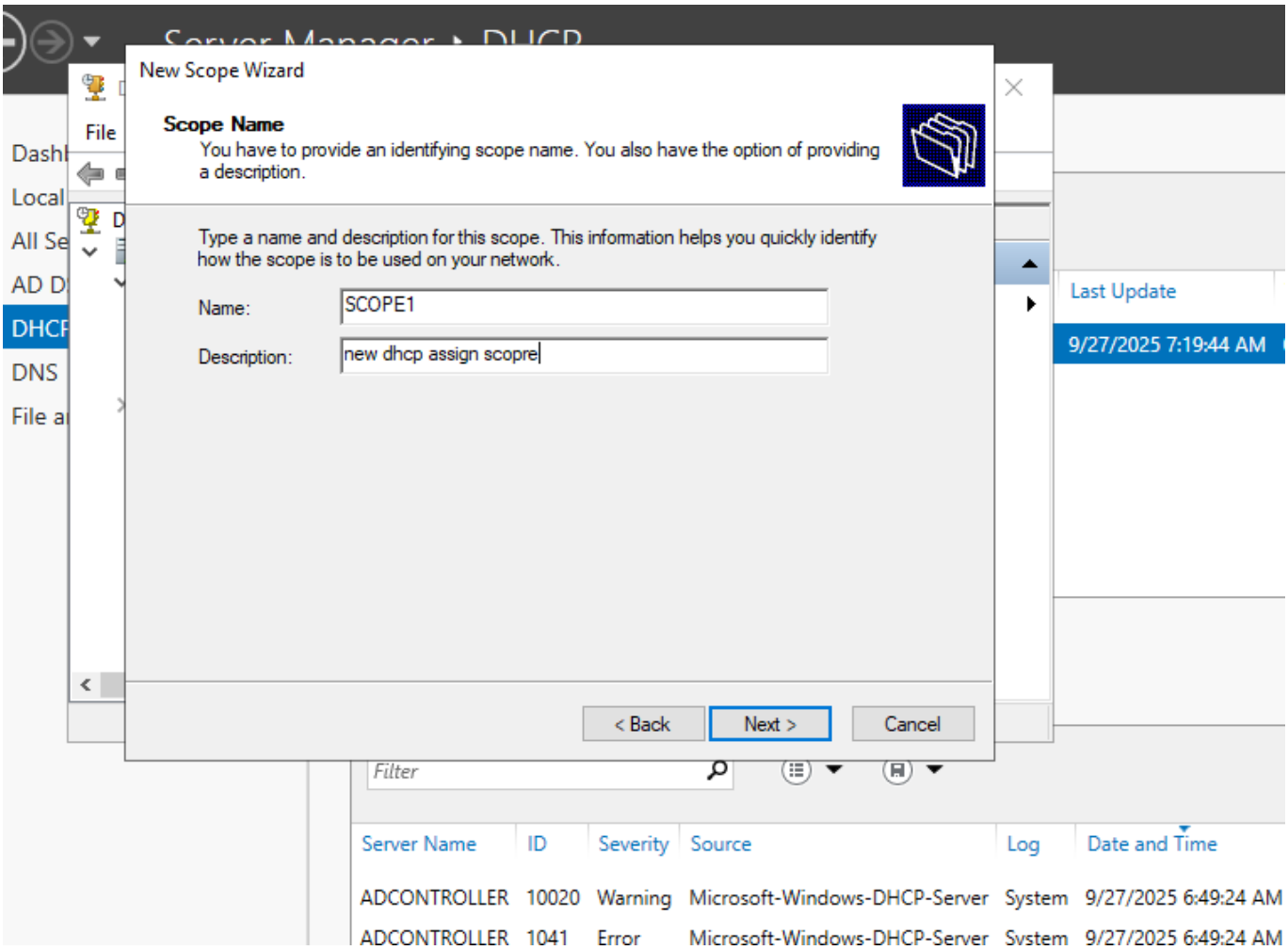

DHCP Post-Install configuration wizard
Summary
Description
Authorization
Summary
The status of the post install configuration steps are indicated below:
Creating security groups ..... Done
Please restart the DHCP server service on the target computer for the security groups to be effective.
Authorizing DHCP server ..... Done
< Previous
Next >
Close
Cancel

Настройка DHCP

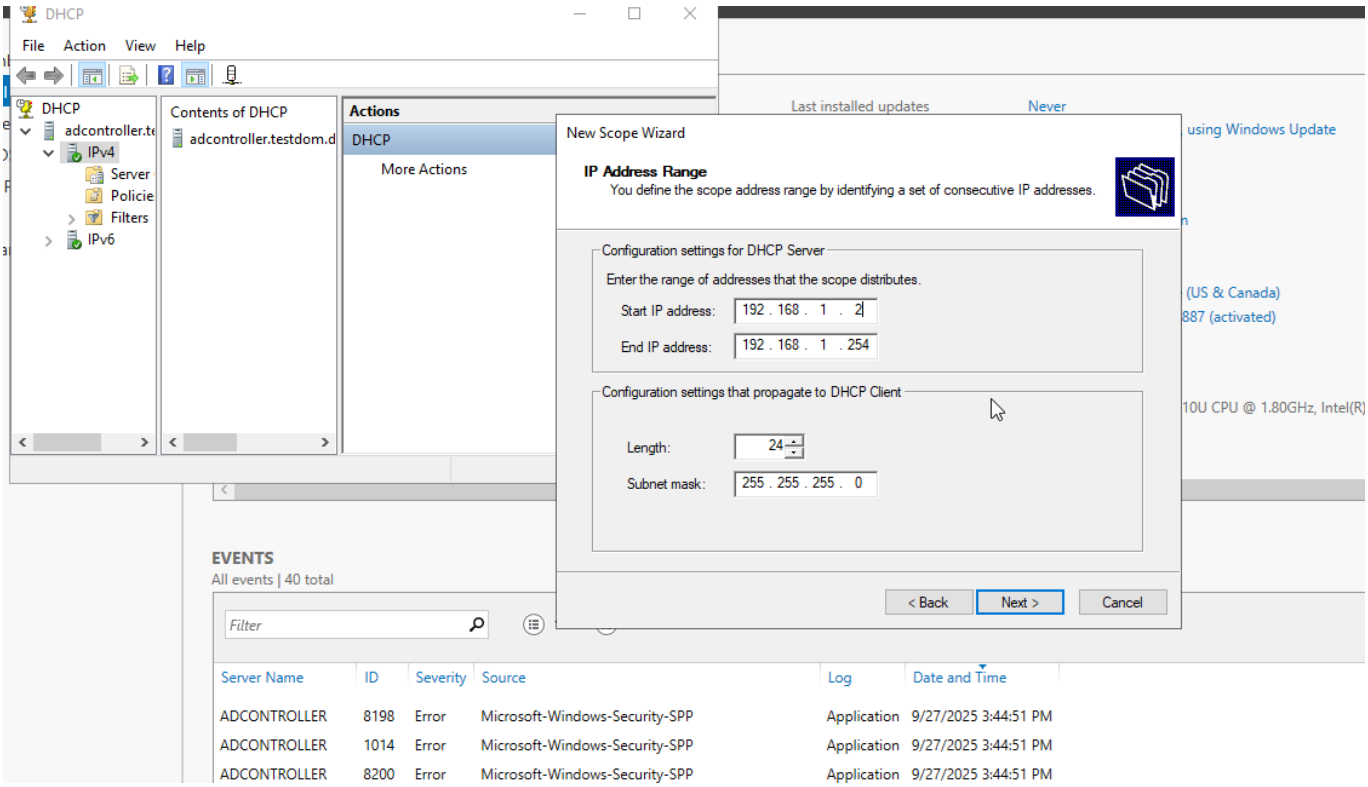


Создание новой области IPv4 адрессов:

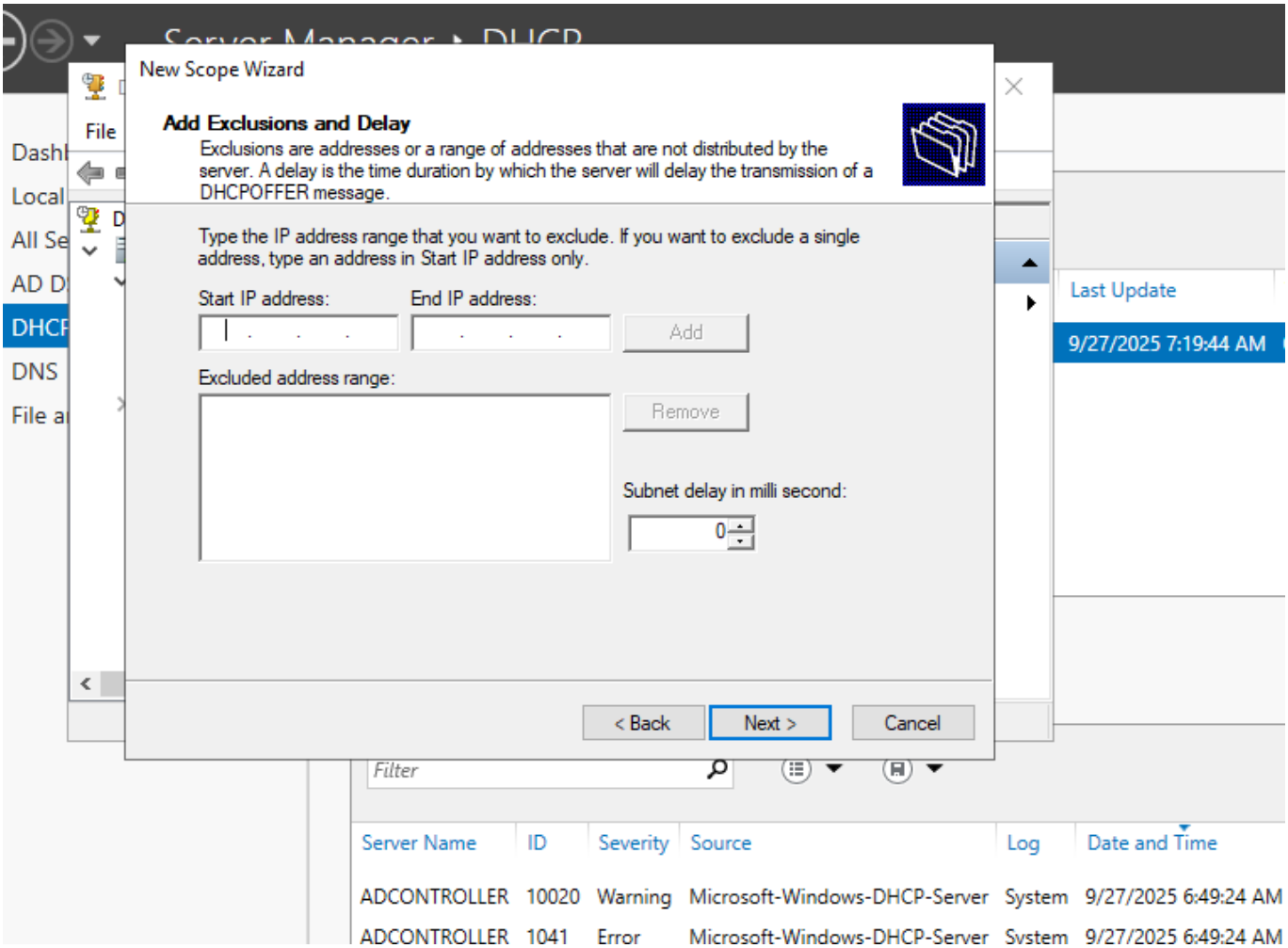




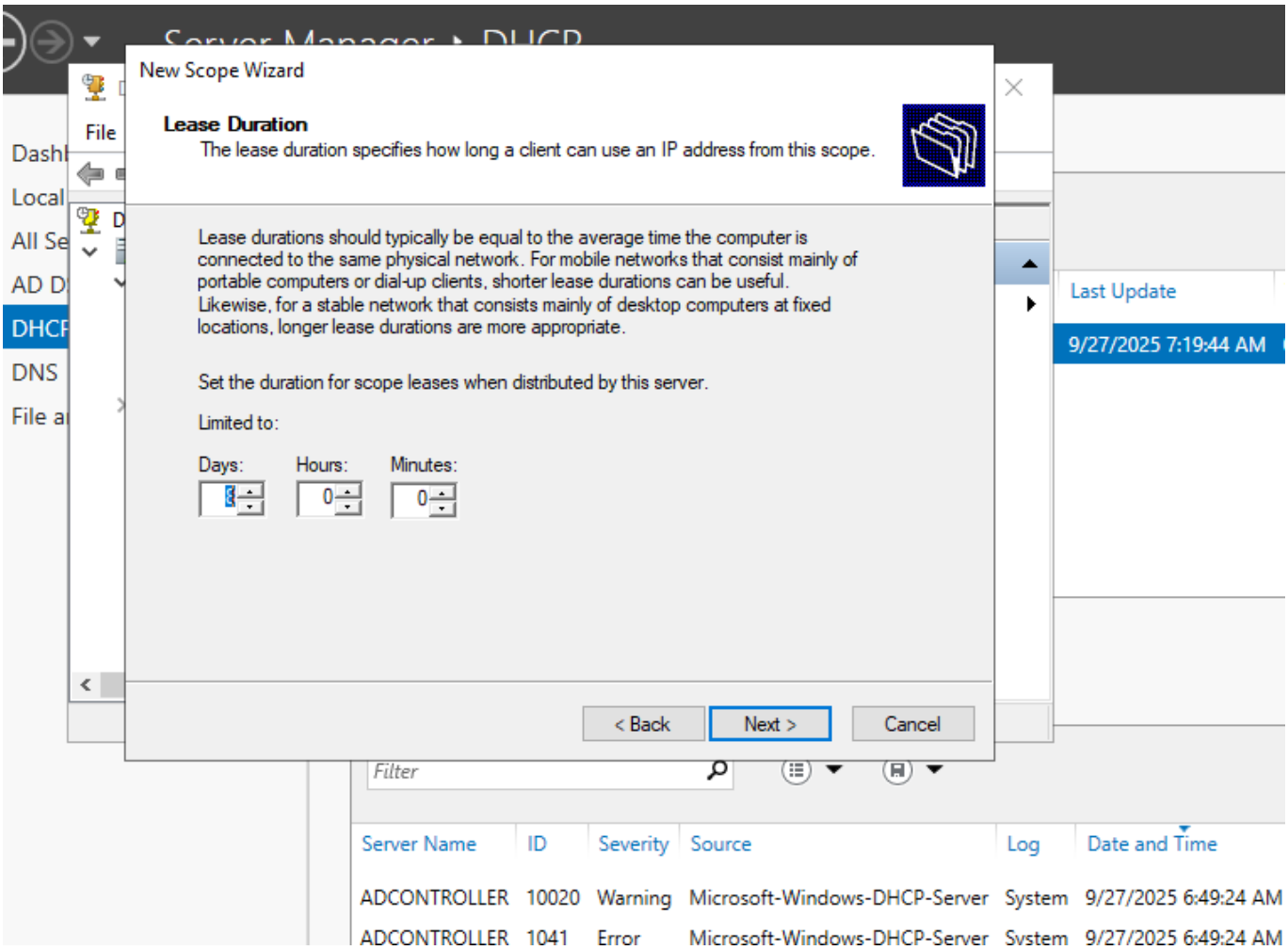
Так как 192.168.1.1 уже зарезервировано за самим контроллерам домена, то адреса с 192.168.1.2 - 192.168.1.254 остаются свободны, их и будем выдавать. Адрес 192.168.1.255 является broadcast адресом и зарезервирован, его выдавать нельзя.



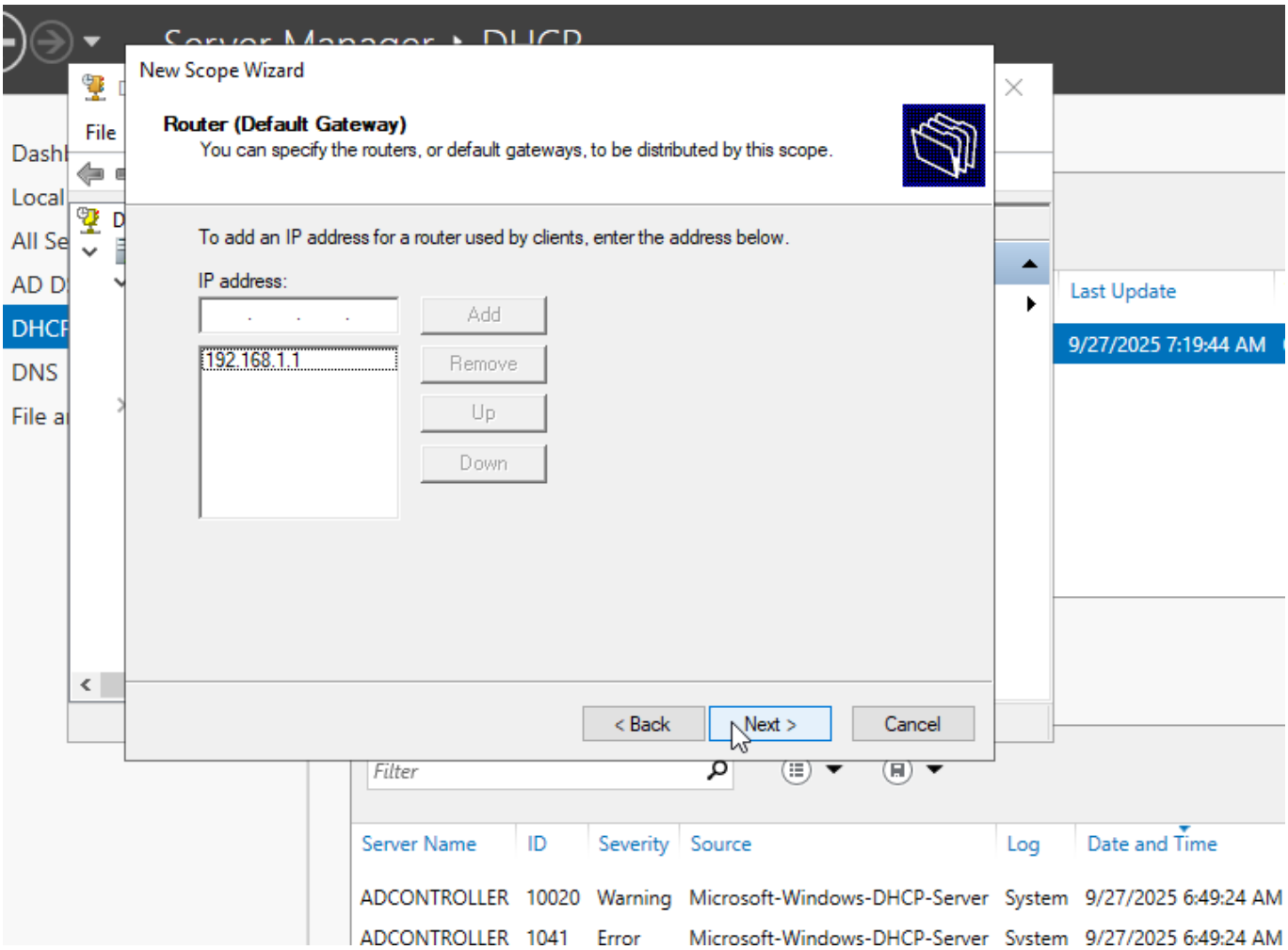
Пропускаем этап с добавлением исключений адрессов так как нет нужды в этом - сеть и так будет самая простая.



Время жизни IP адресов оставляем соответсвующее по умолчанию - 8 дней

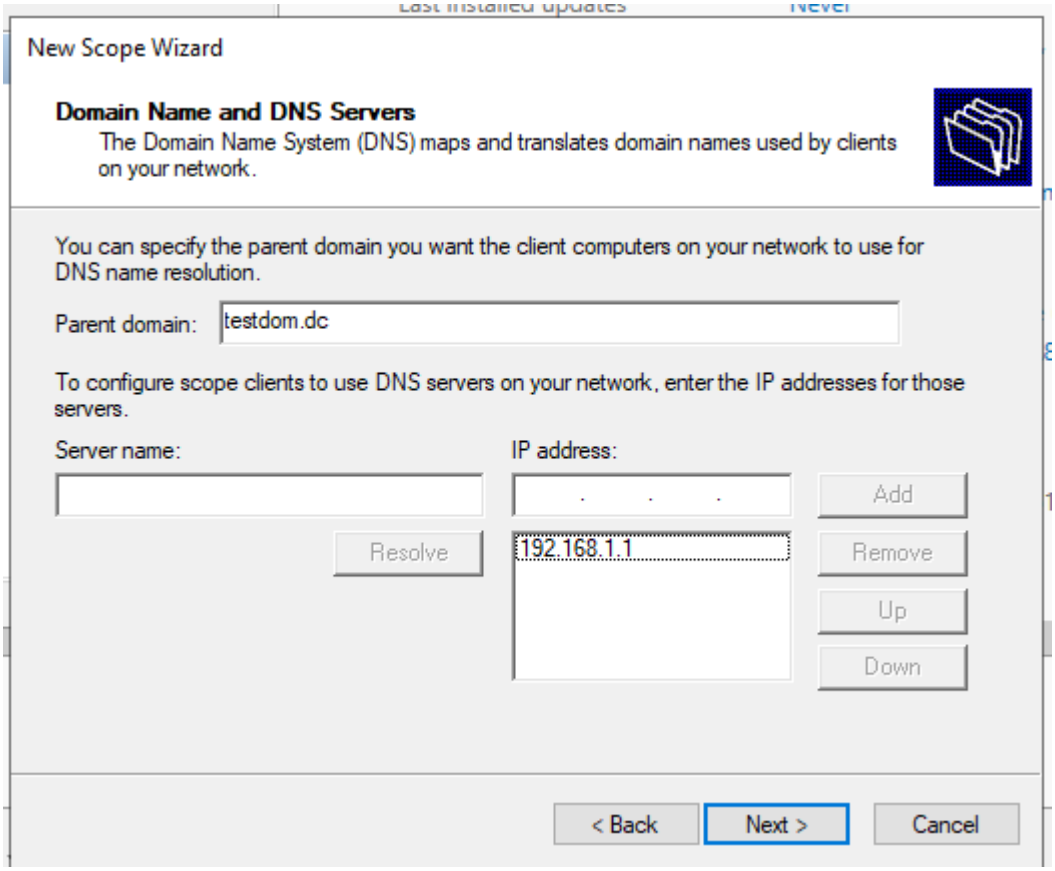


Настроим gateway-шлюз для выхода в сеть по умолчанию через домен-контроллер, то есть 192.168.1.1

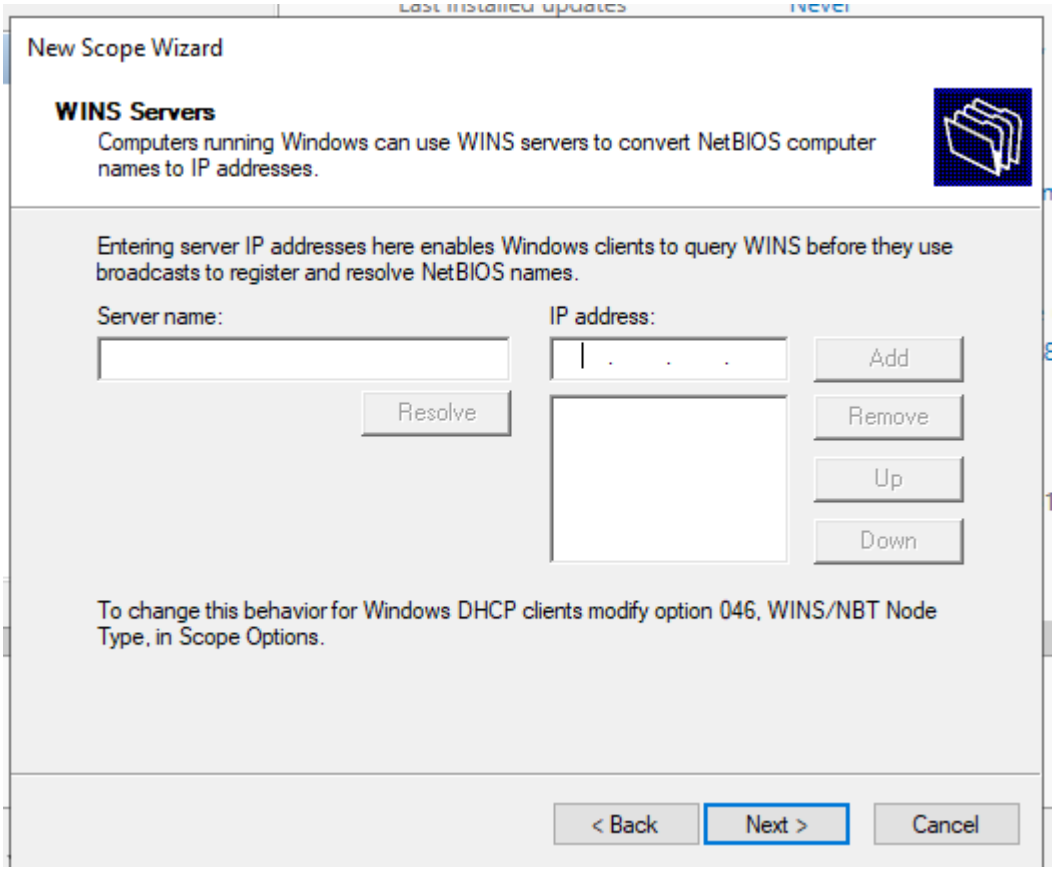


Настройка DNS

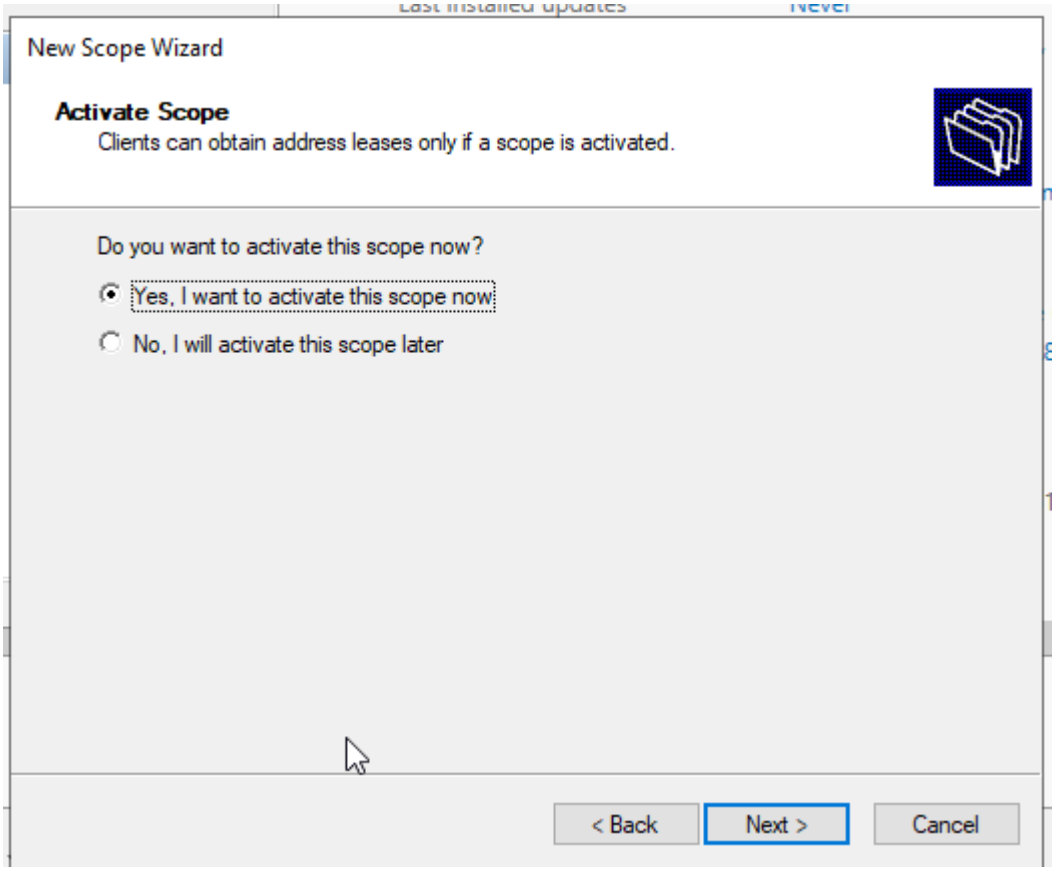
Устонавливаем корневой домен для резолва как называли ранее - `testdom.dc`. Адресс сервера уже должен быть в списке. Если нет - добавим сами:



Так как мы изначально не планировали подключать WINS сервер для резолва NetBIOS имен, то пропускаем шаг с его настройкой:



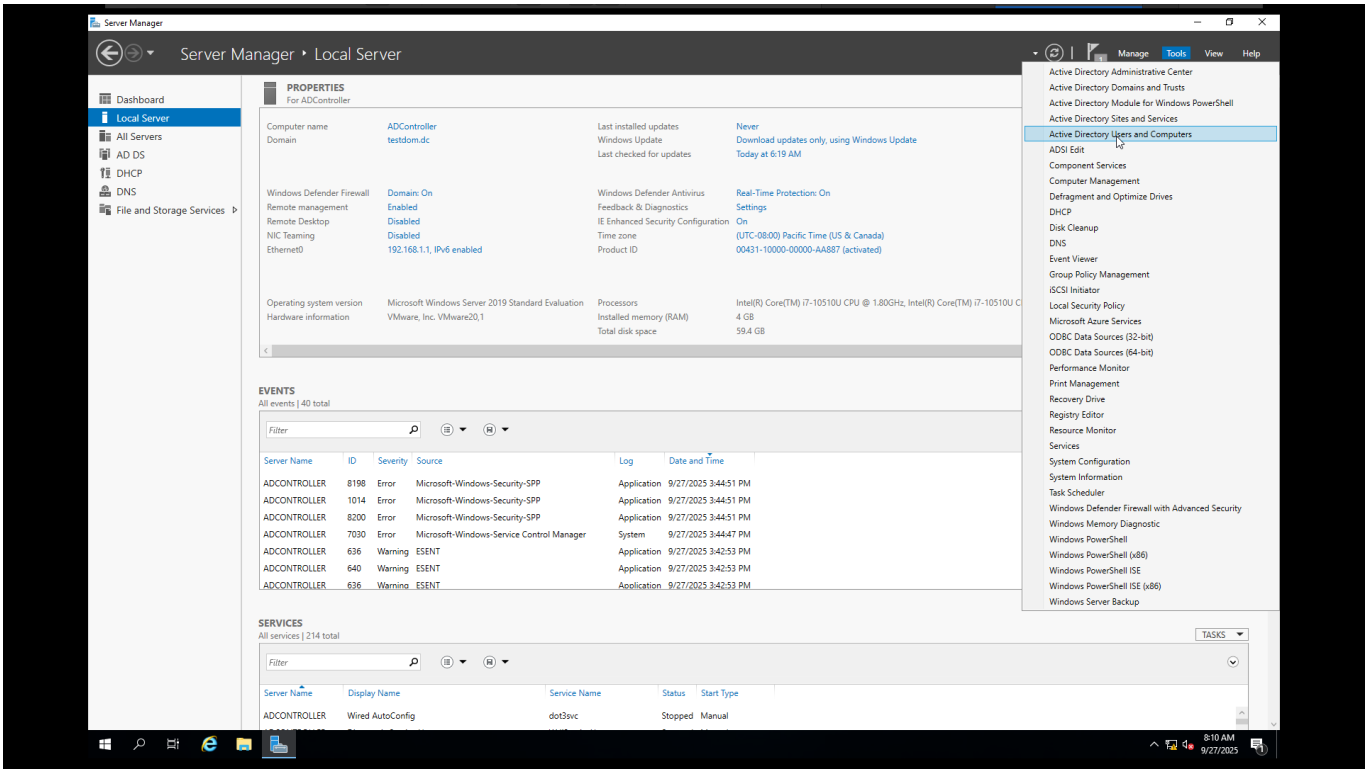
Заканчиваем настройку DHCP активировав область

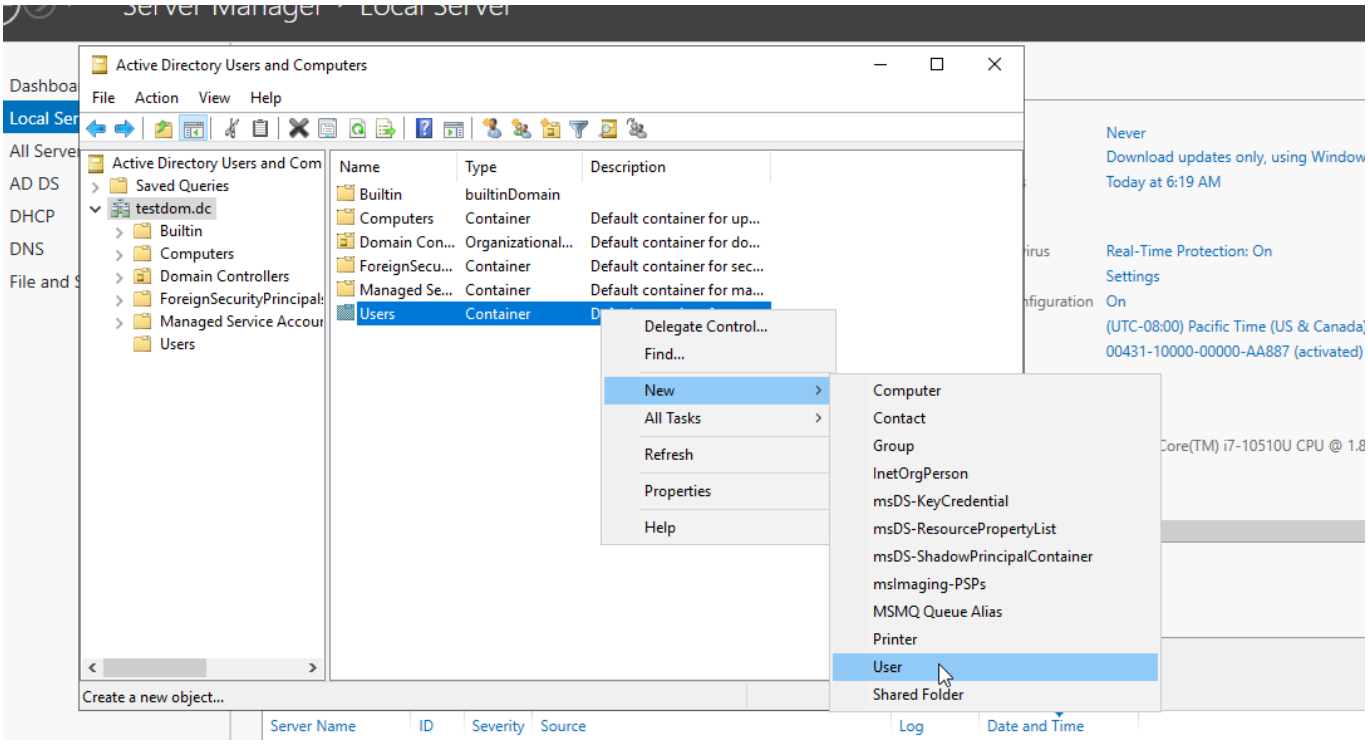


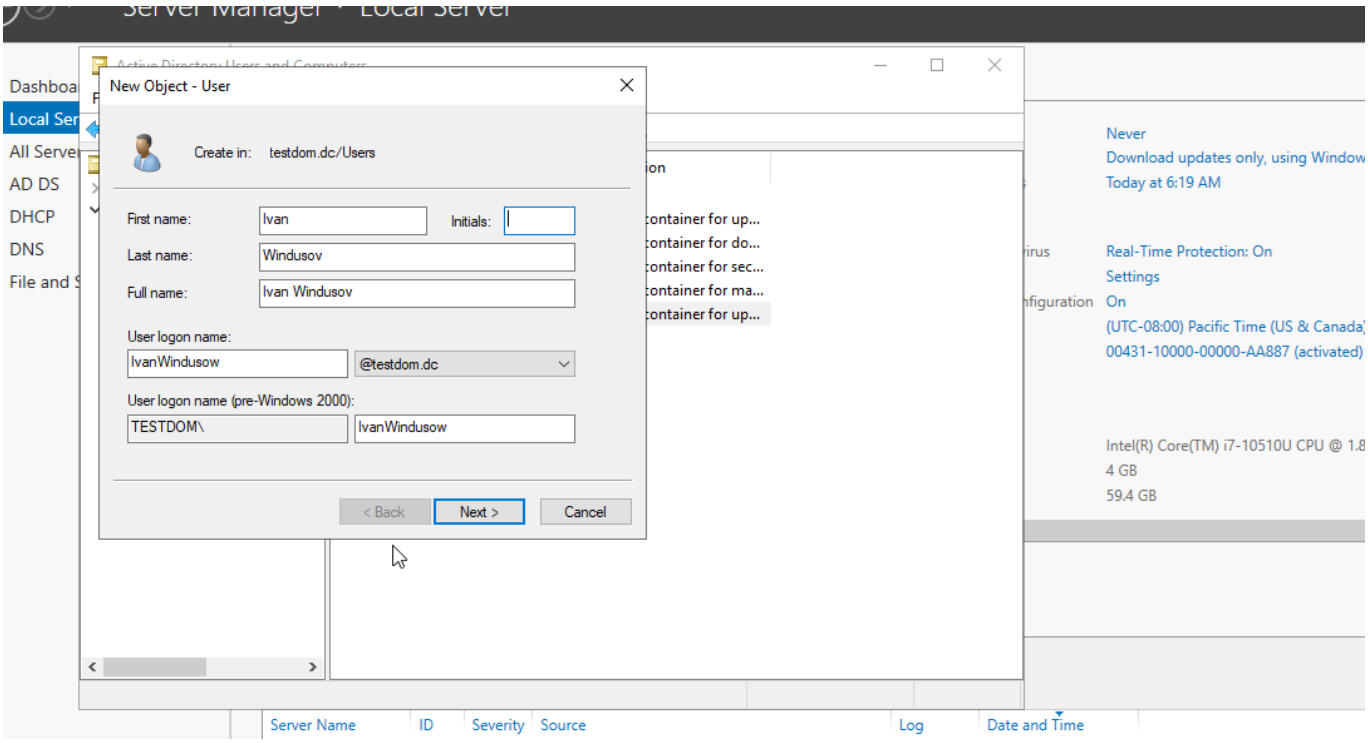
Создание пользователей

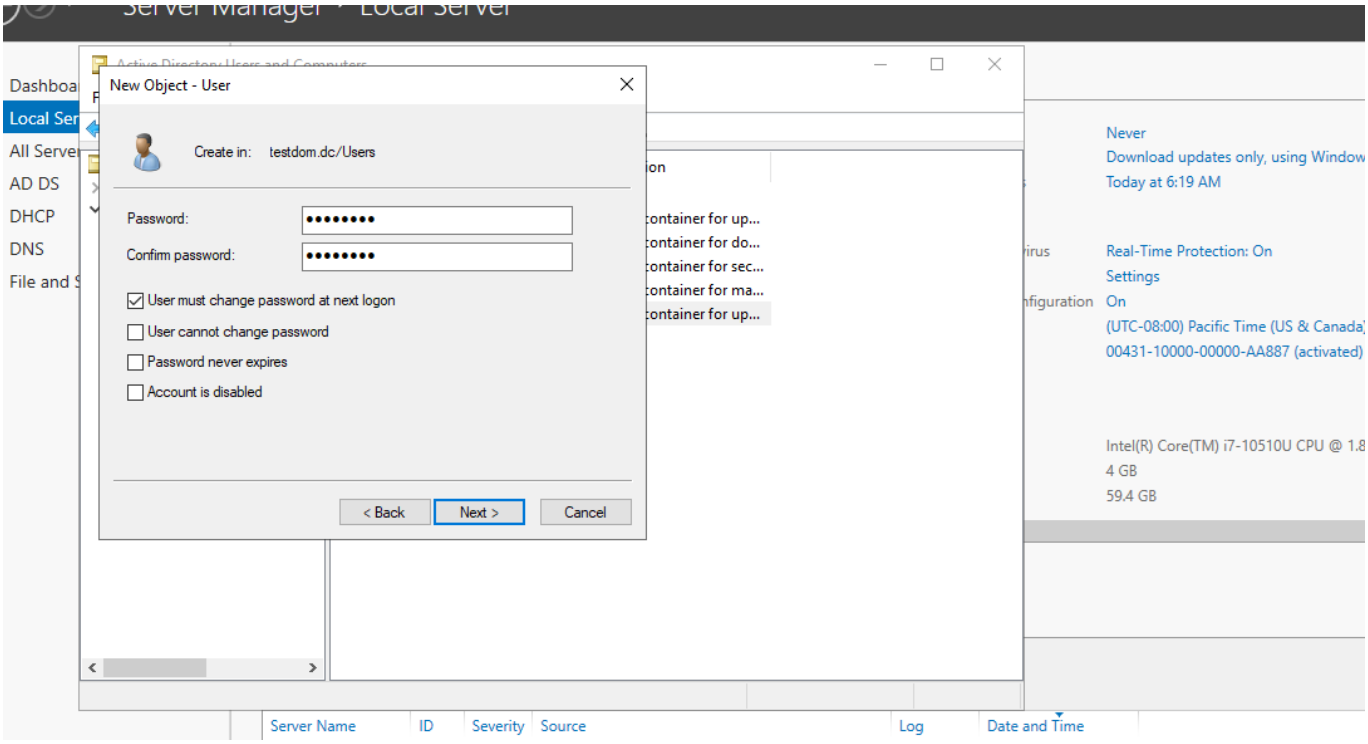
Создаем пользователя AD. Пусть первый будет для рабочей станции Windows, а второй для рабочей станции Linux.

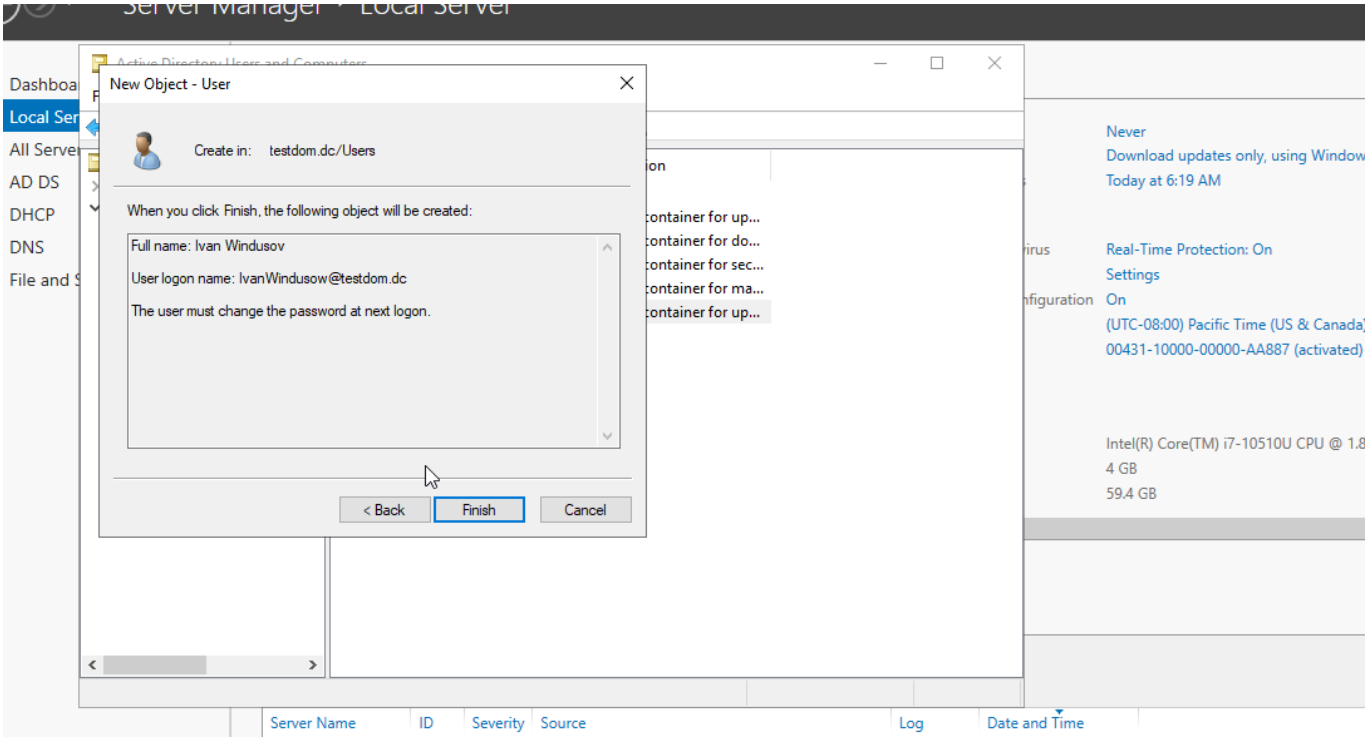
Для Windows пользователя



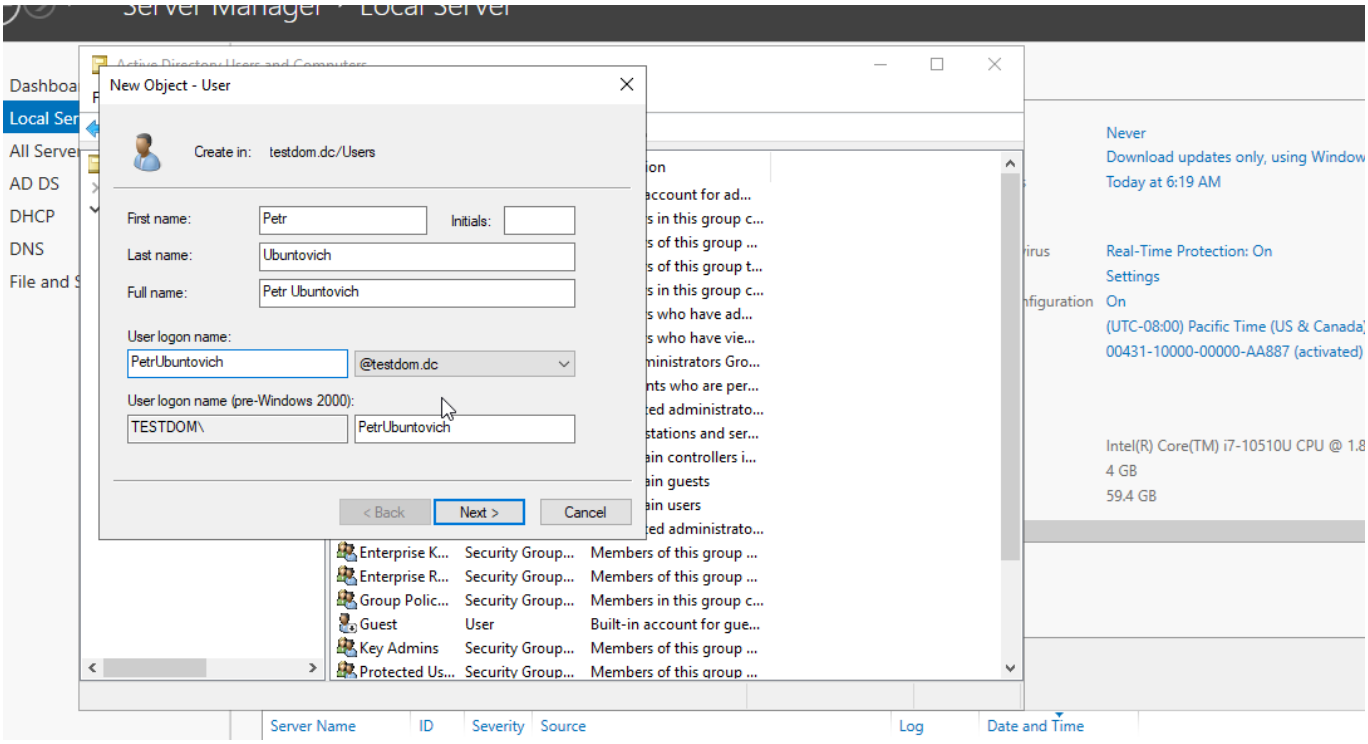

Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
testdom.dc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
Builtin builtinDomain
Computers Container Default container for up...
Domain Con... Organizational... Default container for do...
ForeignSecu... Container Default container for sec...
Managed Se... Container Default container for ma...
Users Container
Delegate Control...
Find...
New
All Tasks
Refresh
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder
Create a new object...
Server Name ID Severity Source Log Date and Time


New Object - User
Create in: testdom.dc/Users
First name: Ivan
Initials:
Last name: Windusov
Full name: Ivan Windusov
User logon name:
IvanWindusow
@testdom.dc
User logon name (pre-Windows 2000):
TESTDOM\
IvanWindusow
< Back
Next >
Cancel
Server Name ID Severity Source Log Date and Time





Для Linux пользователя



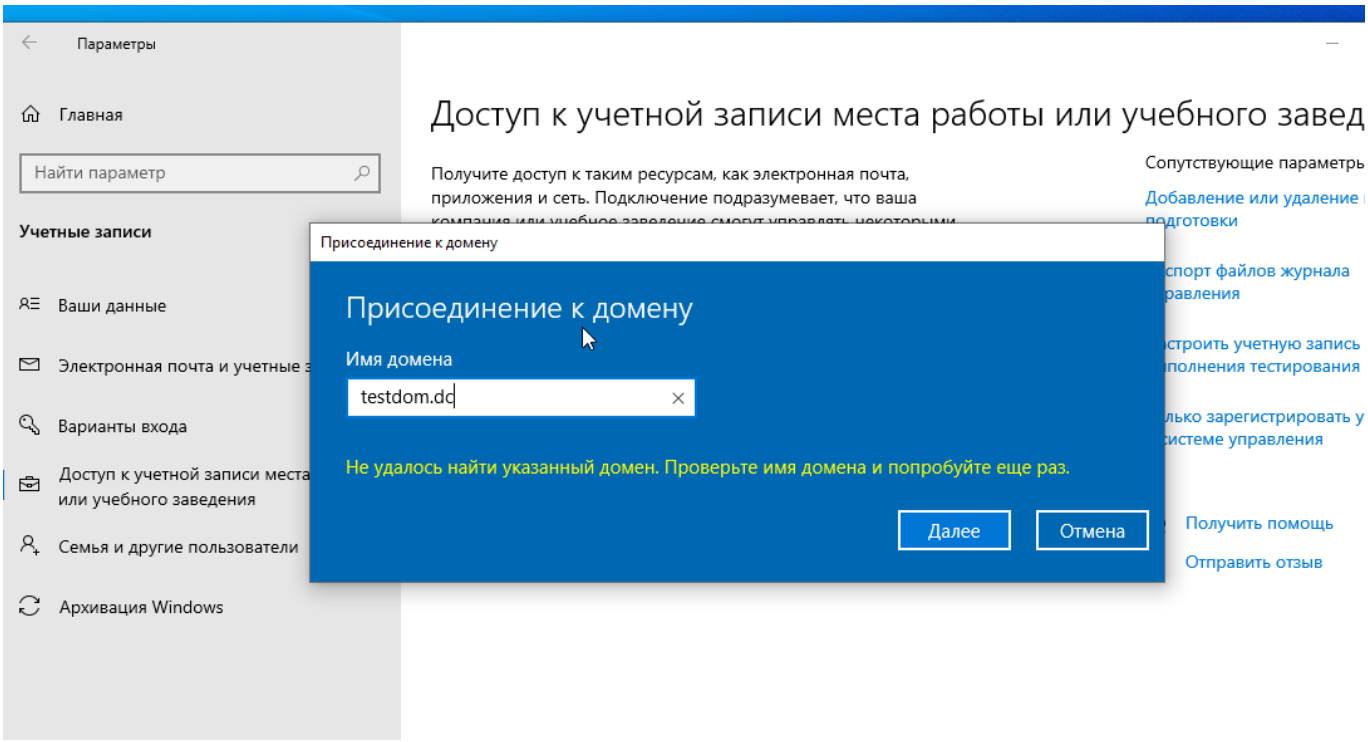
Подключение рабочей станции Windows

Теперь перейдем в ввод домена нового устройства. Устанавливаем операционную систему на новую виртуальную машину. Процедура похожая на установку ВМ для контроллера домена.

Переключаемся на пользователя, затем

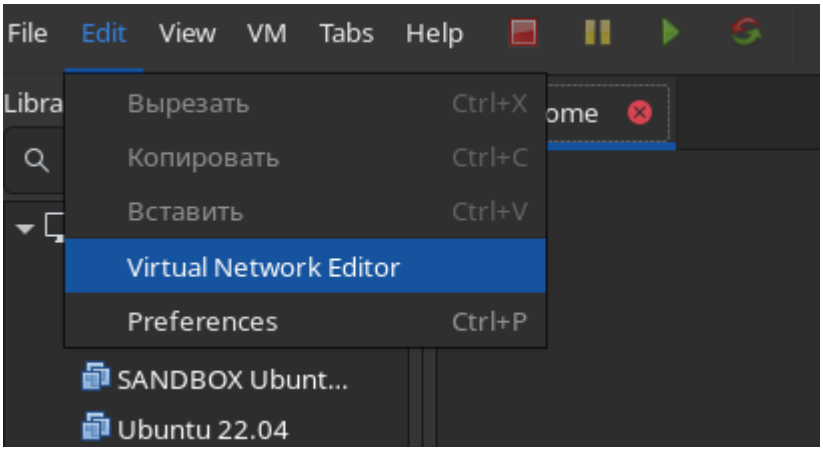
```
Параметры системы -> Учетные записи -> Доступ к учетной записи места работы или учебного заведения -> Подключиться -> Присоединиться к локальному домену AD
```

Вводим наше имя локального домена `testdom.dc`.

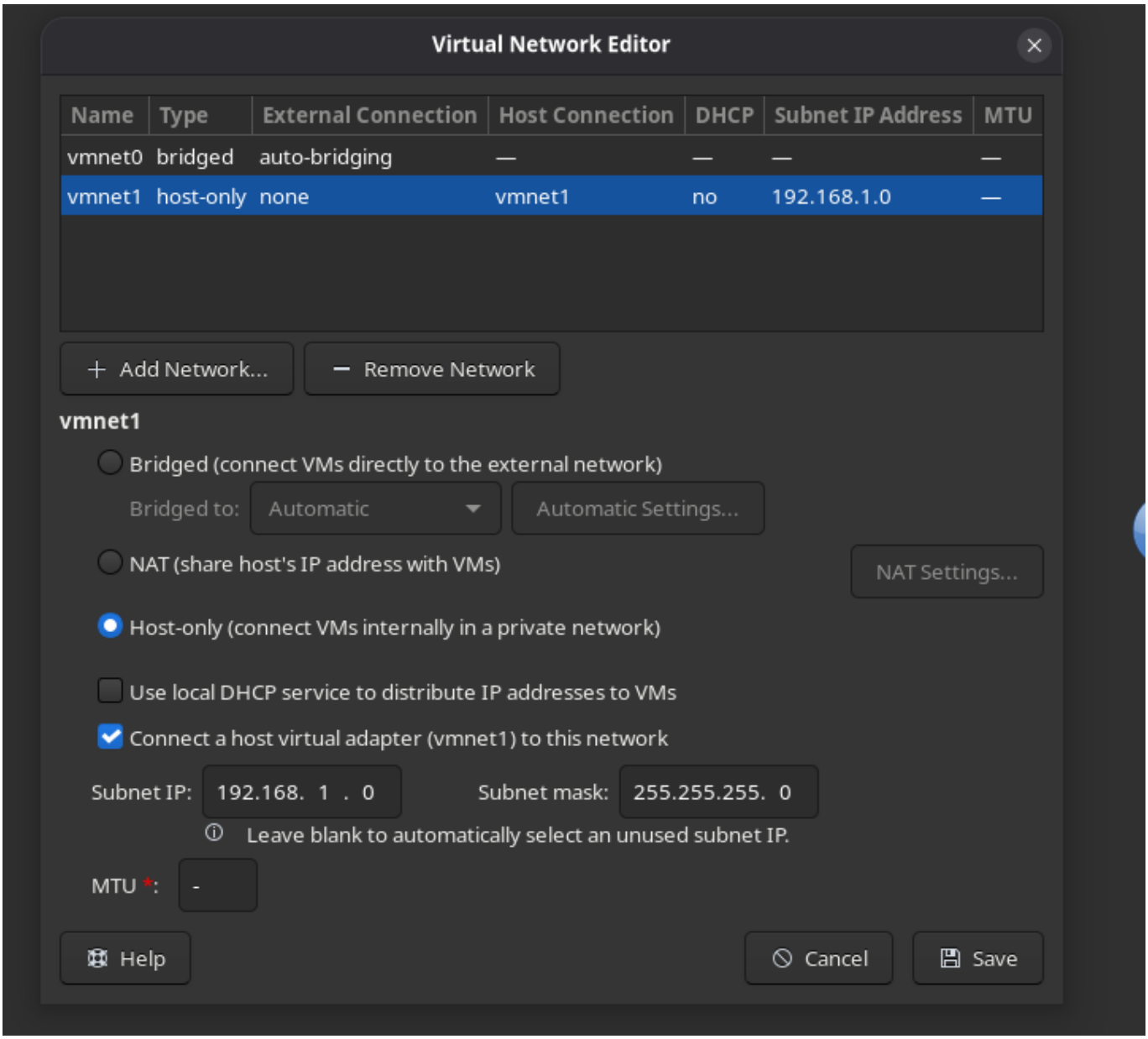


Не выходит. Это из-за того что ВМ не состоит в одной виртуальной сети с контроллером домена. Исправим это.

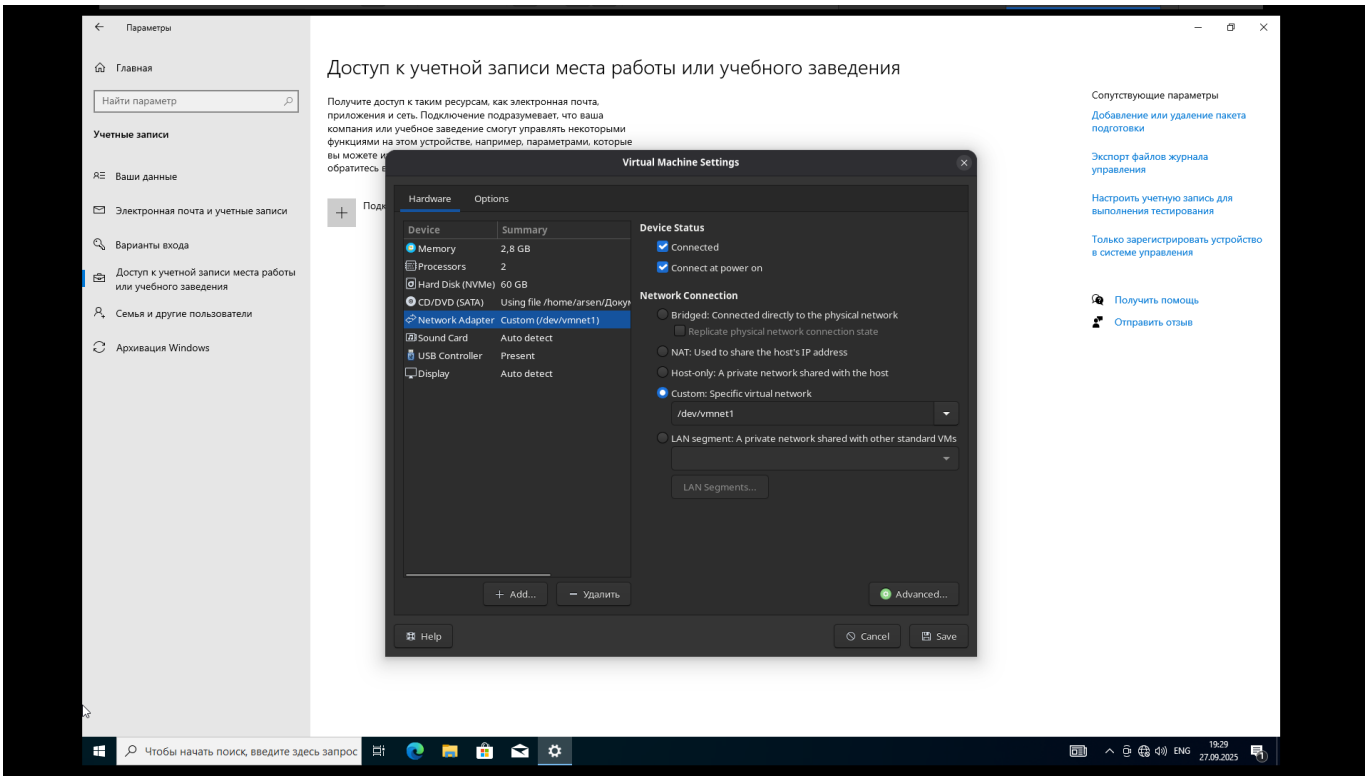
Параметры виртуальной сети



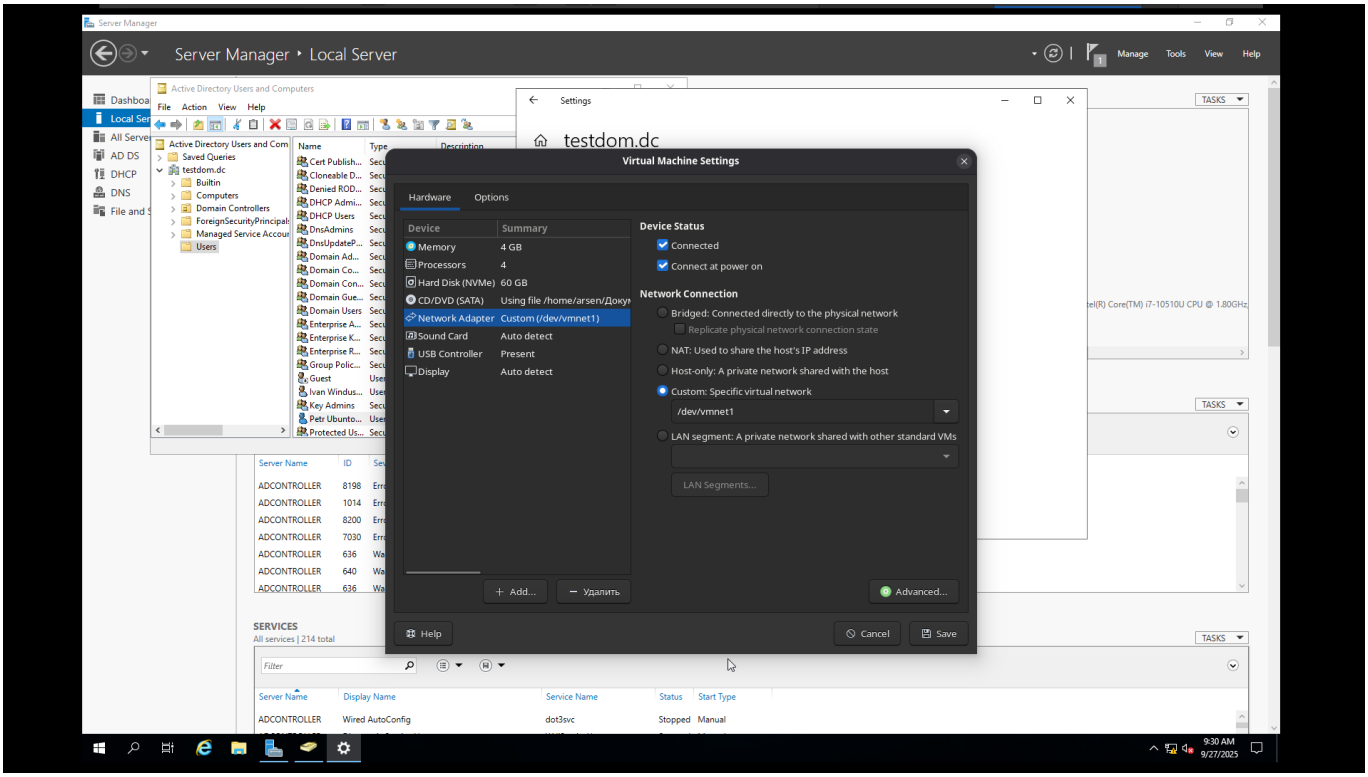
Поставим машины на vmnet1 host-only без DHCP, чтобы было проще и выставим диапазон IP адресов как до этого на контроллере.



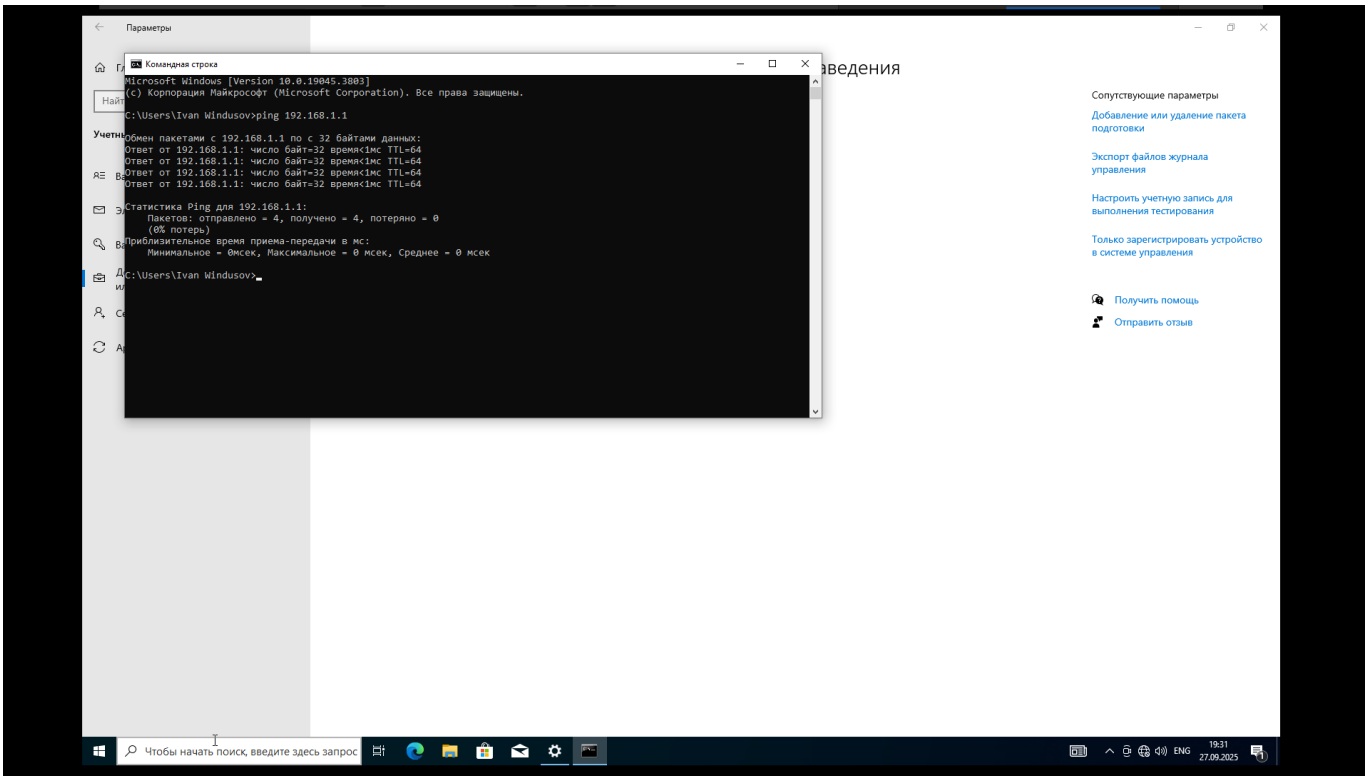
Рабочая станция



Контроллер

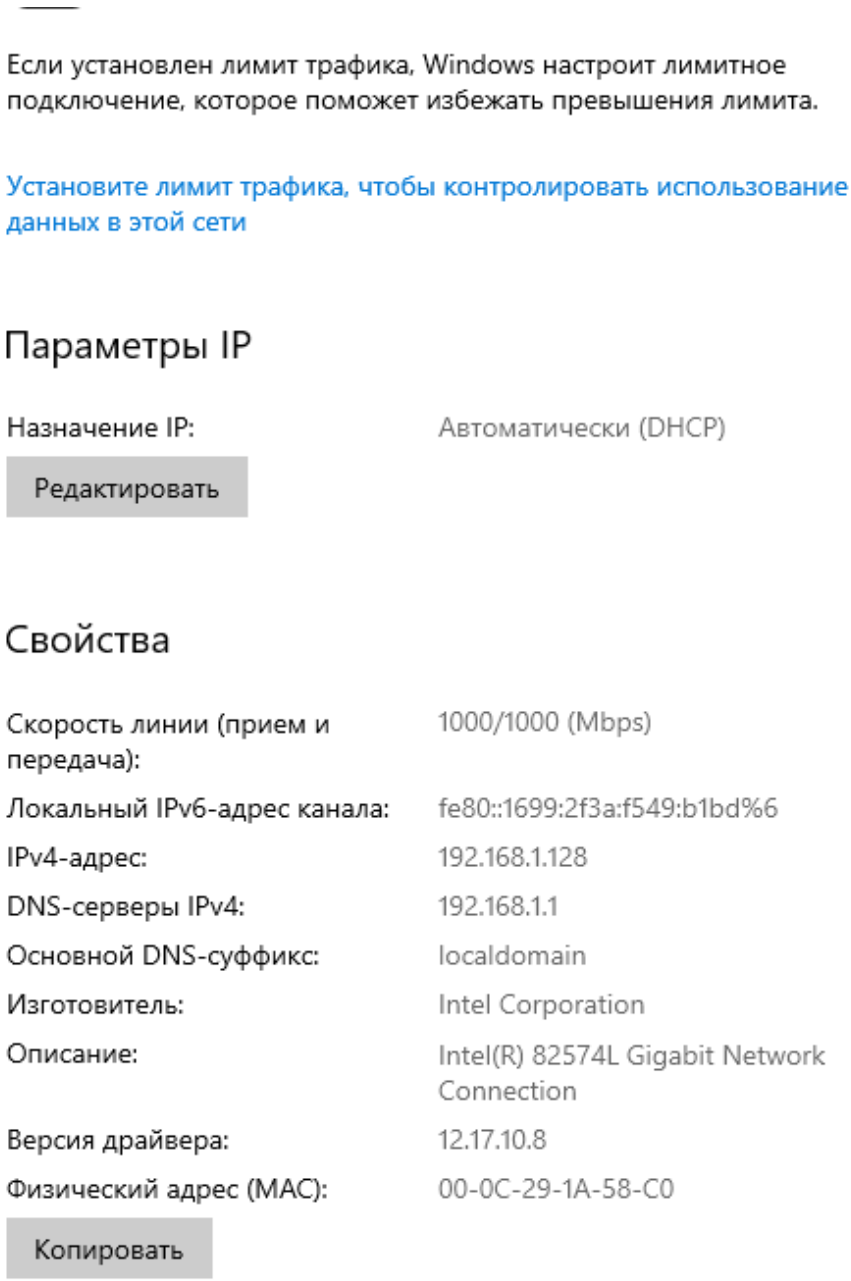


Проверяем со станции на пинг, должны проходить пакеты на 192.168.1.1

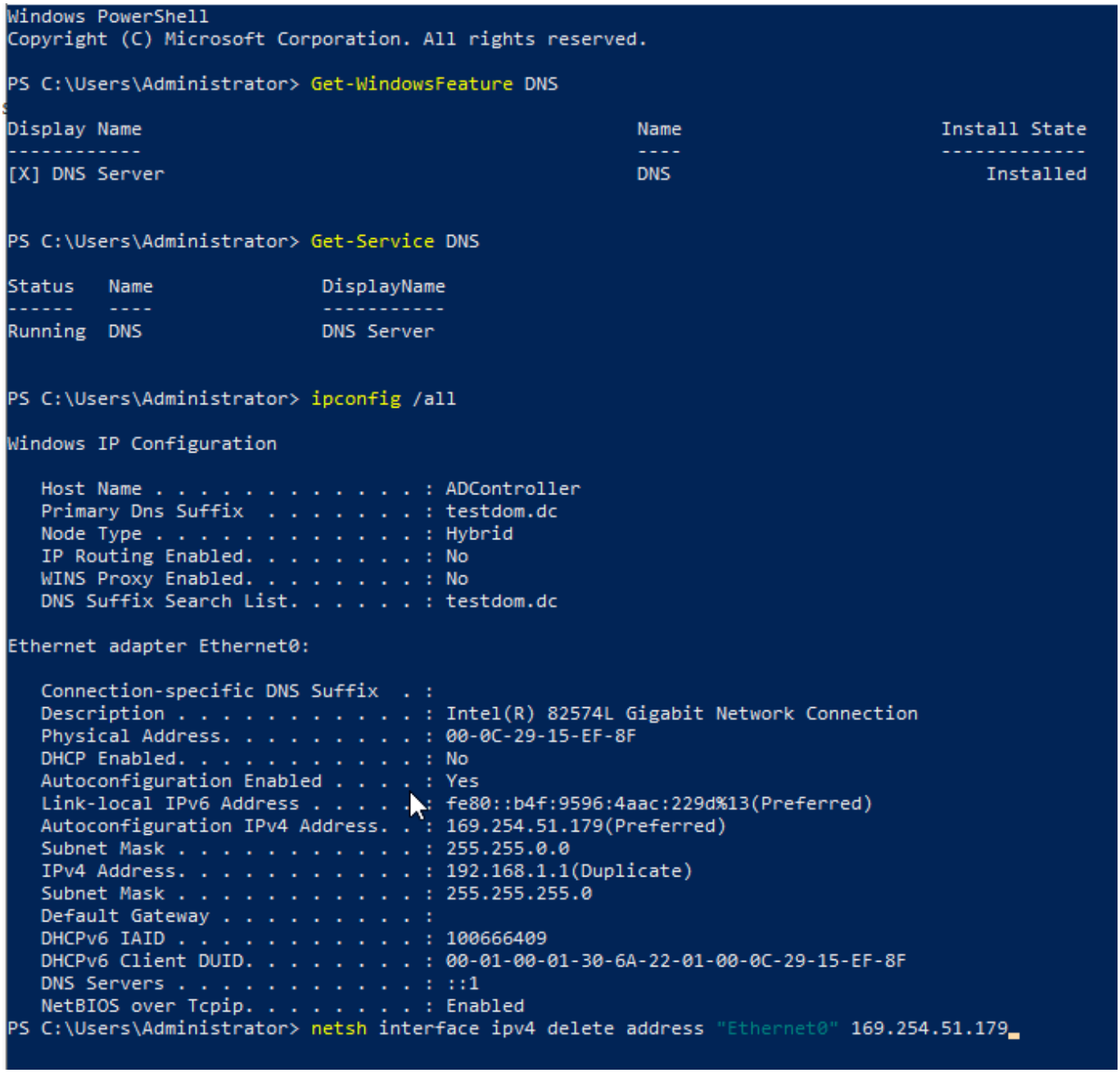


Сеть настроили а домен не виден. Значит надо решить проблему DNS.

Попробовал включить DHCP в сети vmnet1, так же убрал ручную настройку для сетевого интерфейса рабочей станции. Теперь настройки DNS и IP прилетели автоназначением:



Пара запросов в DeepSeek и, кажется, вот в чем проблема: так как я стал настраивать DHCP и DNS до ручного указания IP адресса контроллера, то сработало автоназначение на адресс `169.254.51.179`



а вот команды для диагностики DNS:

```
# Установлена ли роль DNS-сервера
Get-WindowsFeature DNS

# Запущена ли служба DNS
Get-Service DNS

# Проверка настройки DNS на интерфейсе
ipconfig /all
```

Не разобравшись как убрать автоназначенный IP через UI, я использовал команду от того же DeepSeek

```
netsh interface ipv4 delete address "Ethernet0" 169.254.51.179
```

Перезагрузка машинки.

Короче, легче с самого начала все настроить на контроллере нормально.

Spoiler: не получилось. Я проделал все шаги заново, но также столкнулся с проблемой двойной адресации. Нужно отключить автовыданный IP адерсс `169.254.15.*` на клиенте и сервере. Также пересоздал виртуальную сеть, снова без DHCP.

Просто так через граф. интерфейс APIPA адреса не отключаются, поэтому пришлос использовать гайд вот этого замечательного человека.

И все равно фейл.

В общем спустя время разговоров уже с ChatGPT пришел к тому, что во всех тяжких герхах виновать фаерволл на контроллере домена. Пришел к такому выводу набрав

```
Test-NetConnection 192.168.1.1 -Port 53
```

и получив ничего после долгого ожидания. Выключив на сервер фаервол сразу все стало на места: резолвы происходят, подключение к домену идет, тестовое подключение также.

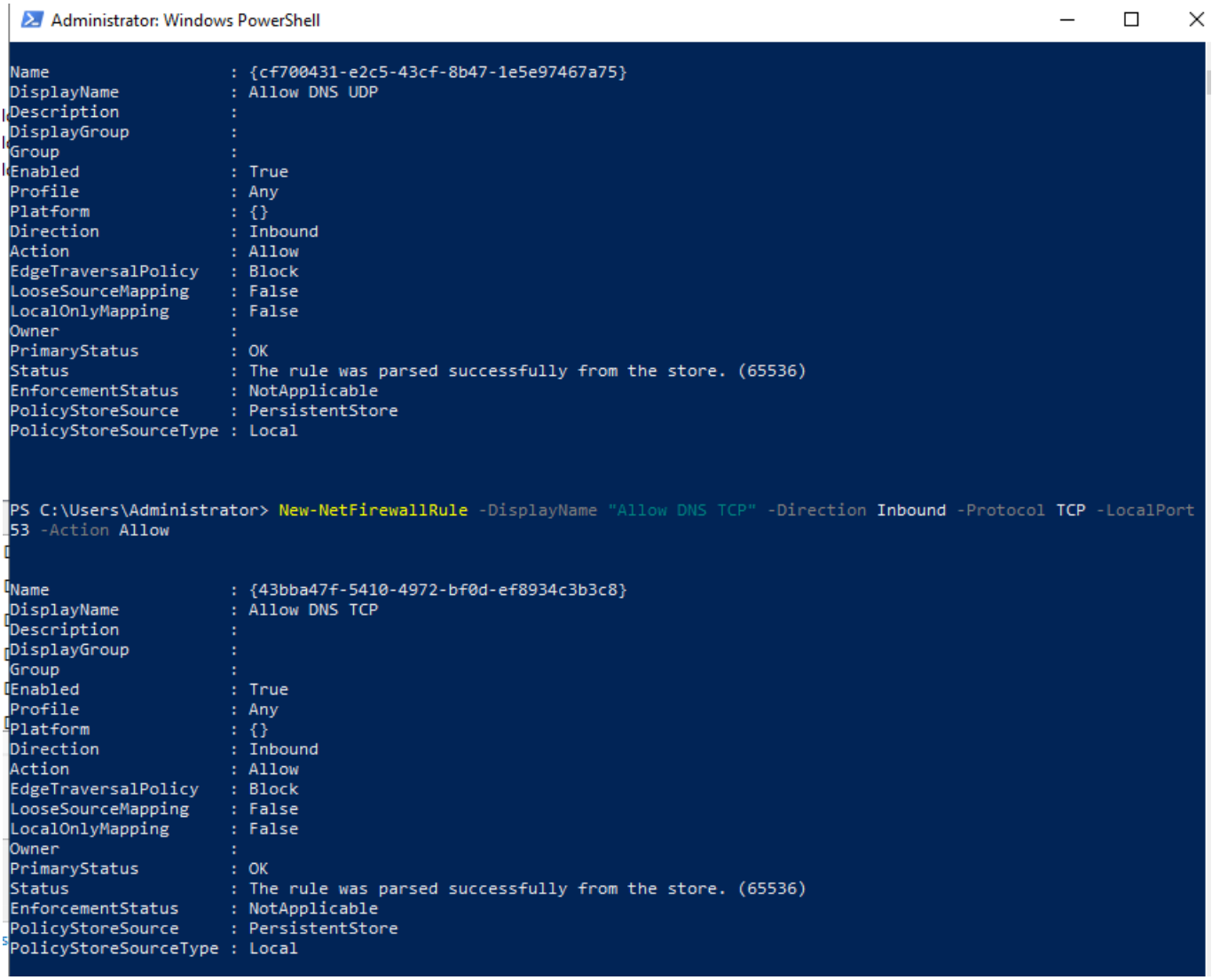
```
netsh advfirewall set allprofiles state off
```

Можно так и оставиьт в общем-то, но попробуем сделать по-умному, ведь открытый фаервол для всего - априори плохо.

от нейросети:

```
# Разрешить DNS (UDP 53)
New-NetFirewallRule -DisplayName "Allow DNS UDP" -Direction Inbound -
Protocol UDP -LocalPort 53 -Action Allow

# Разрешить DNS (TCP 53)
New-NetFirewallRule -DisplayName "Allow DNS TCP" -Direction Inbound -
Protocol TCP -LocalPort 53 -Action Allow
```

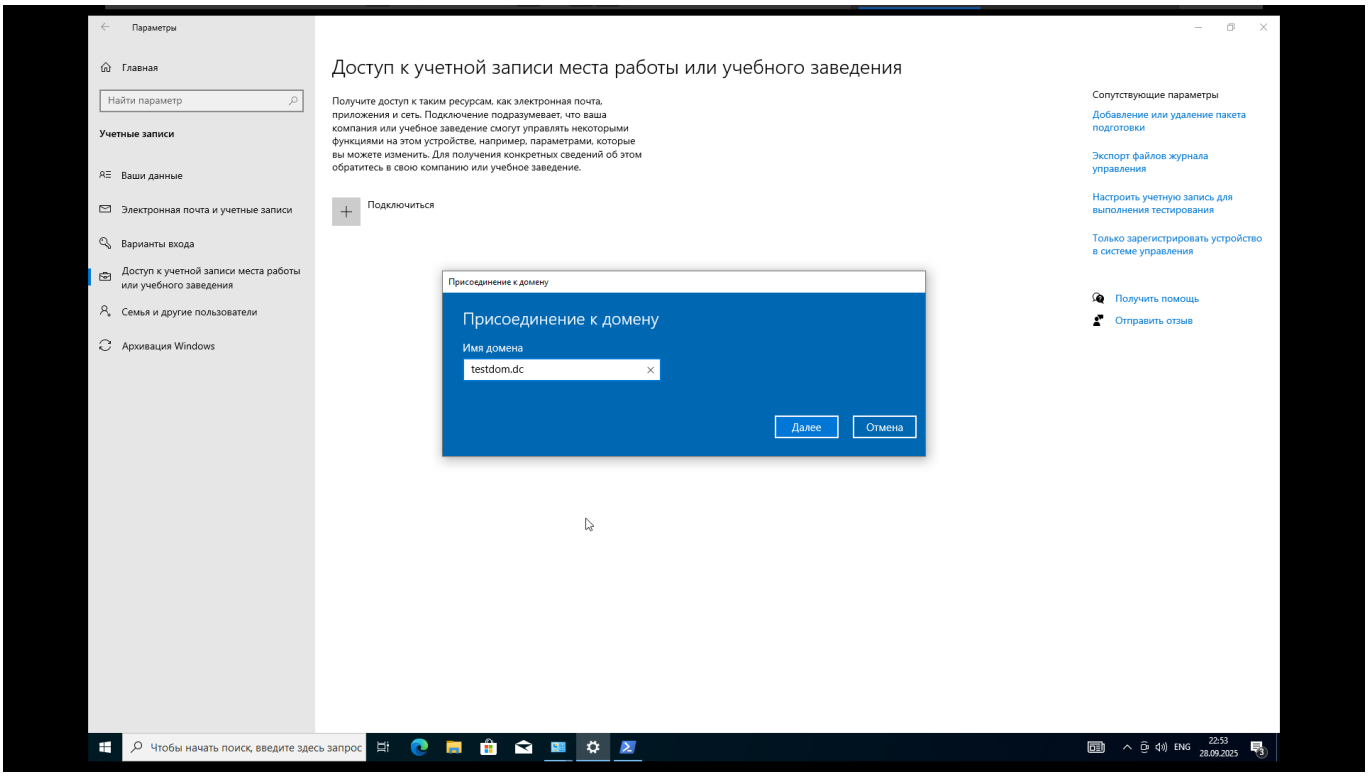


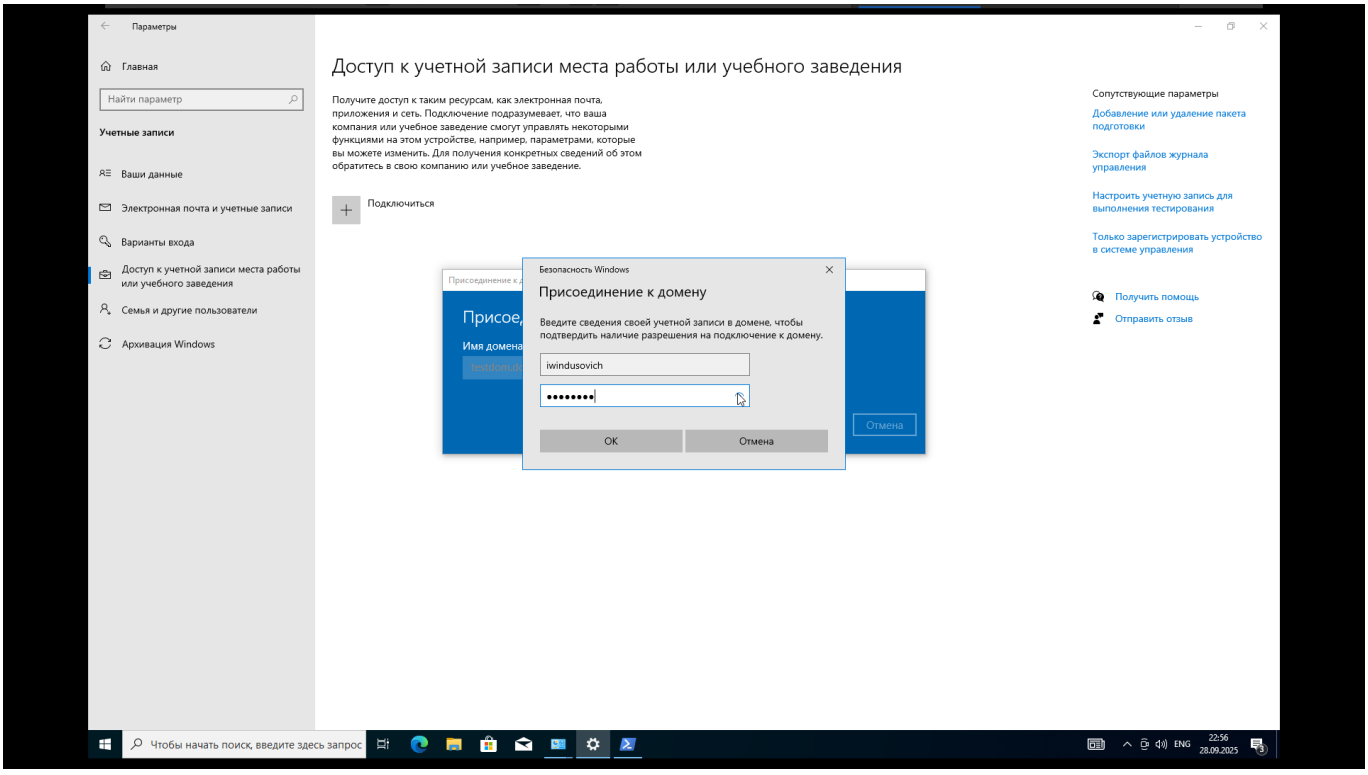
Так, обратно включаем фаерволл и после теста от рабочей станции все также работает.

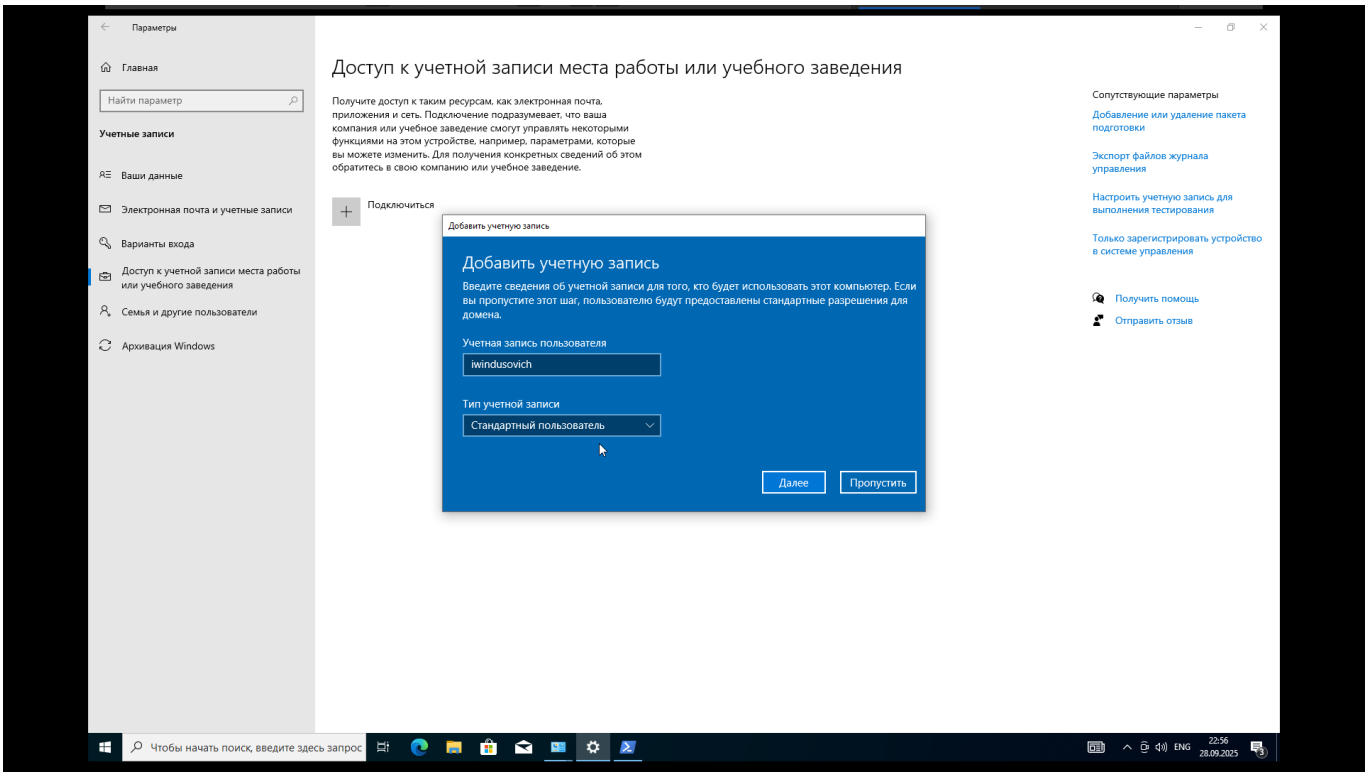
```
netsh advfirewall set allprofiles state on
```

Теперь наконец-то входим в учетку домена для Ивана Виндусовича:

```
Параметры -> Учетные записи -> Доступ к учетной записи места работы или
учебного заведения -> Подключить -> Присоединить это устройство к
локальному домену Active Directory
```

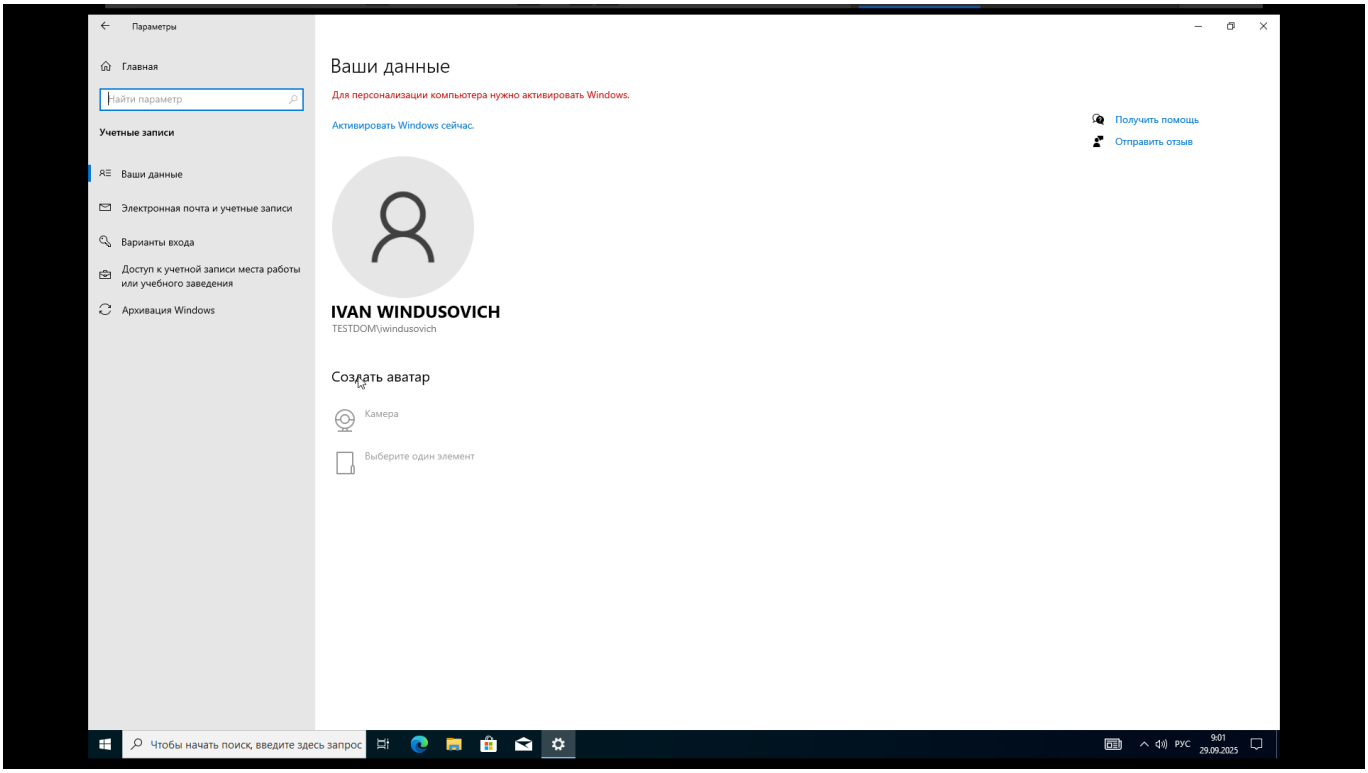

Параметры
Главная
Найти параметр
Учетные записи
Ваши данные
Электронная почта и учетные записи
Варианты входа
Доступ к учетной записи места работы или учебного заведения
Семья и другие пользователи
Архивация Windows
Доступ к учетной записи места работы или учебного заведения
Получите доступ к таким ресурсам, как электронная почта, приложения и сеть. Подключение подразумевает, что ваша компания или учебное заведение смогут управлять некоторыми функциями на этом устройстве, например, параметрами, которые вы можете изменить. Для получения конкретных сведений об этом обратитесь в свою компанию или учебное заведение.
Подключиться
Сопутствующие параметры
Добавление или удаление пакета подготовки
Экспорт файлов журнала управления
Настроить учетную запись для выполнения тестирования
Только зарегистрировать устройство в системе управления
Получить помощь
Отправить отзыв
Присоединение к домену
Присоединение к домену
Имя домена
testdom.dc
Далее
Отмена
Чтобы начать поиск, введите здесь запрос
ENG
22:53
28.09.2025


Параметры
Главная
Найти параметр
Учетные записи
Ваши данные
Электронная почта и учетные записи
Варианты входа
Доступ к учетной записи места работы или учебного заведения
Семья и другие пользователи
Архивация Windows
Доступ к учетной записи места работы или учебного заведения
Получите доступ к таким ресурсам, как электронная почта, приложения и сеть. Подключение подразумевает, что ваша компания или учебное заведение смогут управлять некоторыми функциями на этом устройстве, например, параметрами, которые вы можете изменить. Для получения конкретных сведений об этом обратитесь в свою компанию или учебное заведение.
Подключиться
Сопутствующие параметры
Добавление или удаление пакета подготовки
Экспорт файлов журнала управления
Настроить учетную запись для выполнения тестирования
Только зарегистрировать устройство в системе управления
Получить помощь
Отправить отзыв
Безопасность Windows
Присоединение к домену
Введите сведения своей учетной записи в домене, чтобы подтвердить наличие разрешения на подключение к домену.
iwindusovich
OK
Отмена
Чтобы начать поиск, введите здесь запрос
ENG
22:56
28.09.2025



Затем перезагрузка

При попытке входа в систему после перезагрузки с такими настройками фаерволла войти не получалось, система отвечала что домен не доступен. Ну в общем вырубаем фаерволл.



И вот успешный вход. Первую станцию в AD мы подключили.

Подключение рабочей станции Ubuntu

Для подключения Linux машины нужен интернет для установки дополнительного ПО. Перенастраиваем сеть на NAT и настройки контроллера домена DHCP и сетевого интерфейса.