

**29.01.2024**

## **Курс:**

### **Практическая работа к уроку № Lesson\_3**

--

Настройка Active Directory

## **Задание:**

Перед каждым заданием я рекомендую делать снимки (snapshots) виртуальных машин.

1. Добавьте через Windows Admin Center роль "Доменные службы Active Directory" и компоненту "Telnet"
2. Убедитесь в том, что они появились в "Диспетчере серверов"
3. Сделайте сервер контроллером домена через "Диспетчера серверов".
4. Установите дополнительный контроллер домена на второй машине через "Диспетчера серверов".

## **Команды**

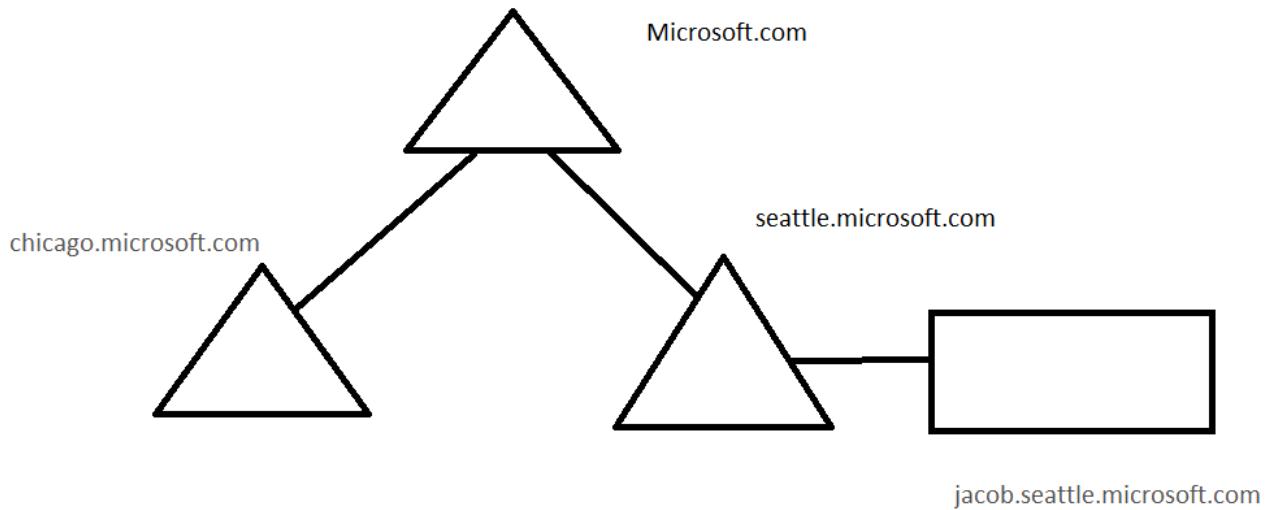
### **Служба Active Directory**

Расширяемая и масштабируемая служба каталогов Active Directory (Активный каталог) позволяет эффективно управлять сетевыми ресурсами. Active Directory - это иерархически организованное хранилище данных об объектах сети, обеспечивающее удобные средства для поиска и использования этих данных. Компьютер, на котором работает Active Directory, называется контроллером домена. С Active Directory связаны практически все административные задачи. Технология Active Directory основана на стандартных Интернет - протоколах и помогает четко определять структуру сети.

### **DNS**

В Active Directory используется доменная система имен. Domain Name System, (DNS) — стандартная служба Интернета, организующая группы компьютеров в домены. Домены DNS имеют иерархическую структуру, которая составляет основу Интернета. Разные уровни этой иерархии идентифицируют компьютеры, домены организаций и домены

верхнего уровня.



Обычные домены, например microsoft.com, называются родительскими (parent domain), поскольку они образуют основу организационной структуры. Родительские домены можно разделить на поддомены разных отделений или удаленных филиалов. Другое название поддомена — дочерний домен (child domain).

Логические структуры Active Directory помогают организовывать объекты каталога и управлять сетевыми учетными записями и общими ресурсами. К логической структуре относятся следующие элементы:

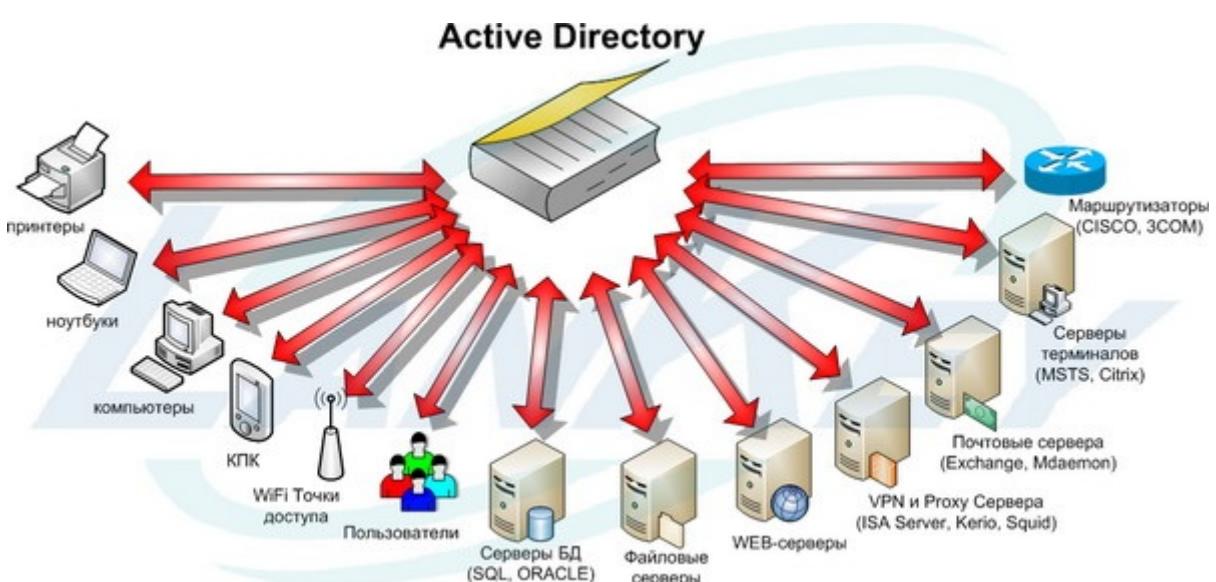
- организационное подразделение (organizational unit) — подгруппа компьютеров, как правило, отражающая структуру компании;
- **домен (domain)** - группа компьютеров, совместно использующих общую БД каталога;
- **дерево доменов (domain tree)** - один или несколько доменов, совместно использующих непрерывное пространство имен;
- **лес доменов (domain forest)** - одно или несколько деревьев, совместно использующих информацию каталога.

Физические элементы помогают планировать реальную структуру сети. На основании физических структур формируются сетевые связи и физические границы сетевых ресурсов. К физической структуре относятся следующие элементы:

- **подсеть (subnet)** - сетевая группа с заданной областью IP- адресов и сетевой маской;
- **сайт (site)** - одна или несколько подсетей. Сайт используется для настройки доступа к каталогу и для репликации.

Организационные подразделения (ОП или **OU**) — это подгруппы в доменах, которые часто отражают функциональную структуру организации. ОП представляют собой своего рода логические контейнеры, в которых размещаются учетные записи, общие ресурсы и другие ОП. Например, можно создать в домене microsoft.com подразделения Resources, IT, Marketing. Потом эту схему можно расширить, чтобы она

содержала дочерние подразделения.

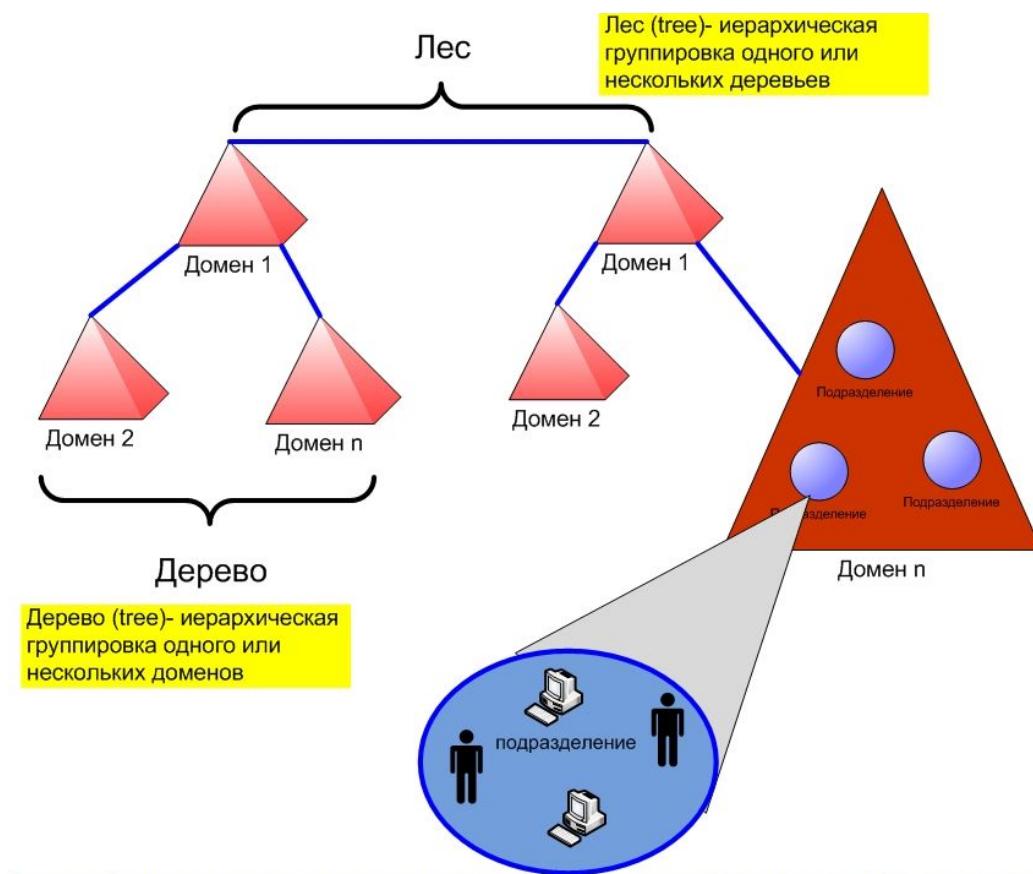


### Леса и деревья

Каждый домен Active Directory обладает DNS-именем типа `microsoft.com`. Домены, совместно использующие данные каталога, образуют **лес (forest)**. Имена доменов леса в иерархии имен DNS бывают несмежными (discontiguous) или смежными

(contiguous).

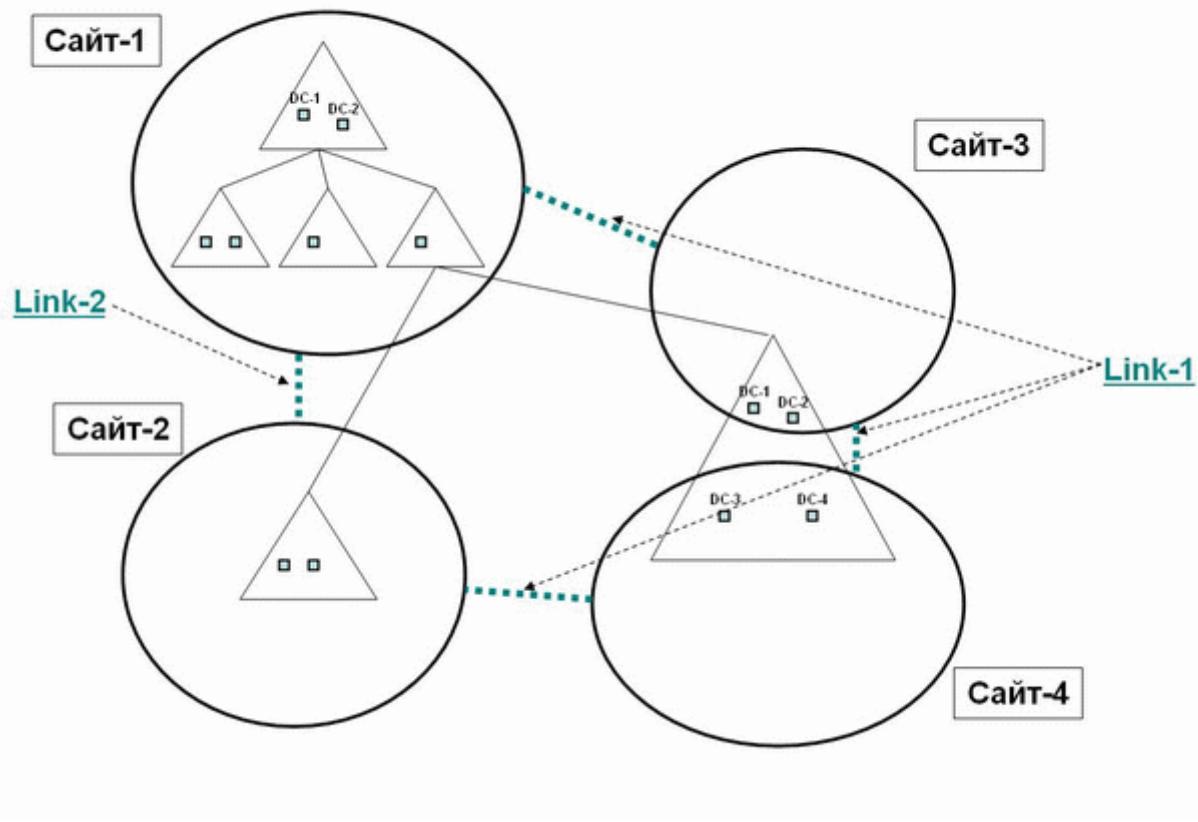
Домены, обладающие смежной структурой имен, называют деревом доменов. Если у доменов леса не смежные DNS-имена, они образуют отдельные деревья доменов в лесу. В лес можно включить одно или несколько деревьев. Для доступа к доменным структурам предназначена консоль Active Directory — домены и доверие (Active Directory Domains and Trusts).



**Сайт** — это группа компьютеров в одной или нескольких IP-подсетях, используемая для планирования физической структуры сети. Планирование сайта происходит независимо от логической структуры домена. Active Directory позволяет создать множество сайтов в одном домене или один сайт, охватывающий множество доменов

(Link).

# Сайты



## Задание\_1:

Добавьте через Windows Admin Center роль "Доменные службы Active Directory" и компоненту "Telnet"

Запускаем в консоле *w2019gui01* (Администратор : password) и смотрим, когда запустится :443

```
192.168.56.16
```

```
netstat -an  
TCP xxx.:443
```

Windows Admin Center | Server Manager

w2019gui01

**Overview**

Computer name: w2019gui01 Domain: WORKGROUP (Workgroup computer) Operating system: Microsoft Windows Server 2019 Standard

Version: 10.0.17763 Installed memory (RAM): 2 GB Disk space (Free / Total): 27.14 GB / 44.4 GB

Processors: Intel(R) Core(TM) i5-5350U CPU @ 1.80GHz Manufacturer: innotek GmbH Logical processors: 2

NIC(s): 3 Up time: 00:00:16:47 Logged in users: 1

Microsoft Defender Antivirus: Real-time protection: On Model: VirtualBox PowerShell Language Mode: Full Language

Azure Backup status: Not protected Azure Arc status: Not installed

CPU Utilization Handles

Tools:

- Azure Backup
- Azure File Sync
- Azure hybrid center
- Azure Kubernetes Service
- Azure Monitor
- Certificates
- Devices
- Events
- Files & file sharing
- Firewall

Installed apps:

Windows Admin Center | Server Manager

w2019gui01

**Roles and features**

+ Install — Uninstall 267 items 2 selected

Name	State	Type
Roles	1 of 91 Installed	
DHCP-сервер	Available	Role
DNS-сервер	Available	Role
Hyper-V	Available	Role
Аттестация работоспособности устройств	Available	Role
> Веб-сервер (IIS)	0 of 43 Installed	Role
✓ Доменные службы Active Directory	Available	Role
Служба опекуна узла	Available	Role
Службы Active Directory облегченного доступа к ка...	Available	Role
> Службы Windows Server Update Services	0 of 3 Installed	Role

**Details - Доменные службы Active Directory (2 Selected)**

Description: Доменные службы Active Directory (AD DS) хранят сведения об объектах сети и делают их доступными ее пользователям и администраторам. С помощью контроллеров домена доменные службы Active Directory предоставляют пользователям доступ к разрешенным ресурсам в сети на основе единого входа в систему.

1

2

3

Windows Admin Center | Server Manager

w2019gui01

**Roles and features**

+ Install — Uninstall 267 items 1 selected

Name	State	Type
System Data Archiver	Installed	Feature
System Insights	Available	Feature
✓ Telnet Client	Available	Feature
TFTP Client	Available	Feature
Windows Defender Antivirus	Installed	Feature
Windows Identity Foundation 3.5	Available	Feature
> Windows PowerShell	2 of 5 Installed	Feature
Windows TIF Filter	Available	Feature
WINS-сервер	Available	Feature
XPS Viewer	Installed	Feature

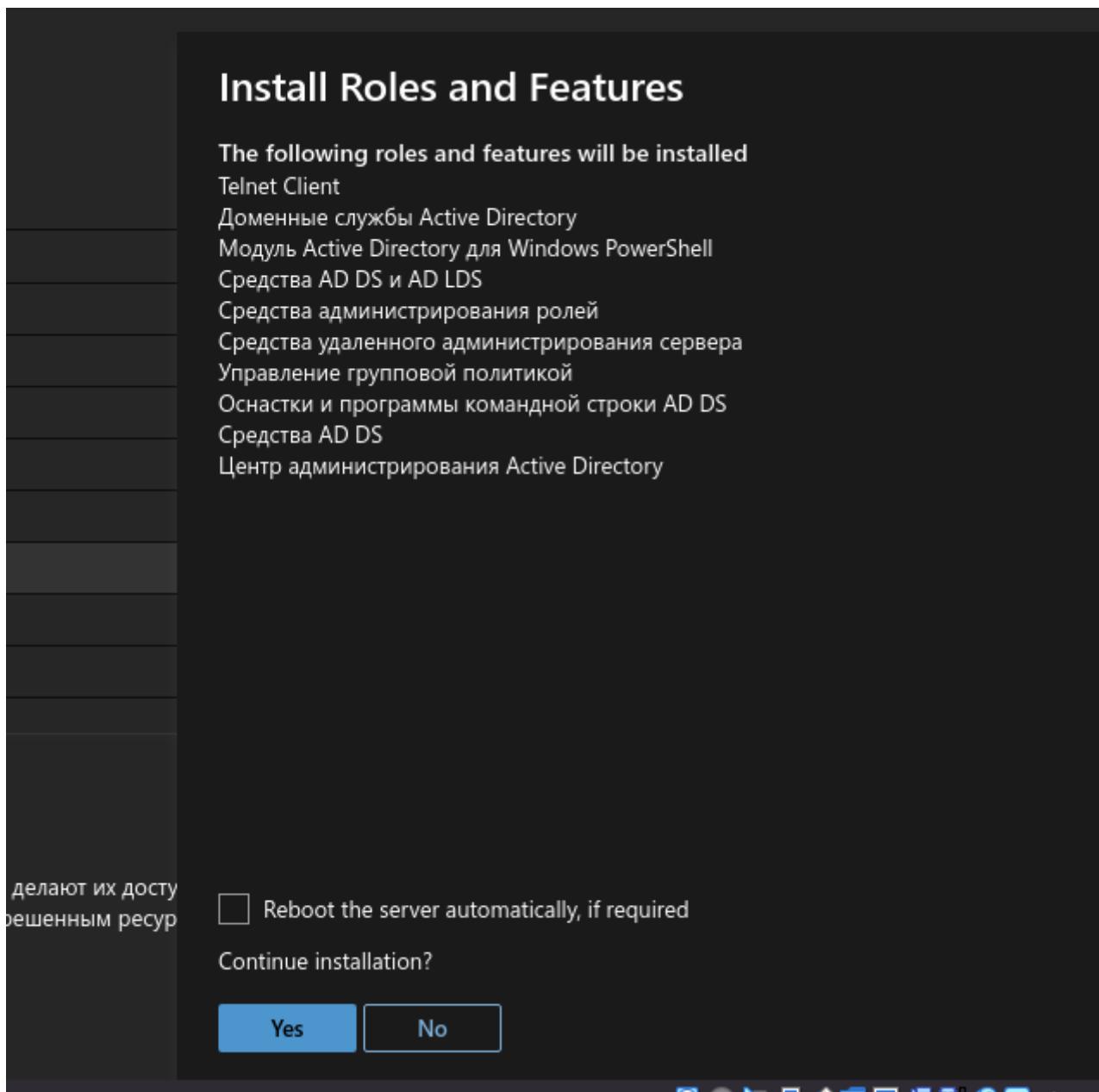
**Details - Telnet Client (1 Selected)**

Description: Telnet Client uses the Telnet protocol to connect to a remote Telnet server and run applications on that server.

1

2

-> Install



Re <https://192.168.56.16/servermanager/connections/server/w2019gui01/tools/rolesfeatures>

Server Manager < Microsoft > Notifications Clear All

Notifications

All More < > 4:54:15 PM

In progress: 92%. Installing Telnet Client, Доменные службы Active Directory  
w2019gui01

Roles and features

Name	State
+ Install — Uninstall	
+ Roles	1 of 91 Installed
DHCP-сервер	Available
DNS-сервер	Available
Hyper-V	Available
Аттестация работоспособности устройств	Available
> Веб-сервер (IIS)	0 of 43 Installed
Доменные службы Active Directory	Available

**View PowerShell scripts for Roles & features**

Got a repetitive task you want to script? Get inspiration from the scripts we use, or press **CTRL + C** to copy a function and make it your own.

[See use rights](#) [Get started with PowerShell](#)

**Script Name**

Get-WACRFRoleAndFeatureDependencies

```
function Get-WACRFRoleAndFeatureDependencies {
<#
.SYNOPSIS
Retrieves all Feature/Role/Role Services, and their dependencies, to be installed on the target server.

.DESCRIPTION
Retrieves all Feature/Role/Role Services, and their dependencies, to be installed on the target server.

```

## Задание\_2:

Убедитесь в том, что они появились в "Диспетчере серверов"

1 Настраить этот локальный сервер

- Добавить роли и компоненты
- Добавить другие серверы для управления
- Создать группу серверов
- Подключить этот сервер к облачным службам

РОЛИ И ГРУППЫ СЕРВЕРОВ

Сервер	Количество
AD DS	1
Файловые службы и службы хранилища	1
Локальный сервер	1
Все серверы	1

2 Добавить роли

Перед началом работы

Этот мастер поможет вам установить роли, службы ролей или компоненты. Определите, что нужно установить, на основании потребностей своей организации, таких как общий доступ к документам или размещение веб-сайта.

Чтобы удалить роли, службы ролей или компоненты: Запустить мастер удаления ролей и компонентов

Прежде чем вы продолжите, убедитесь, что выполнены следующие задачи:

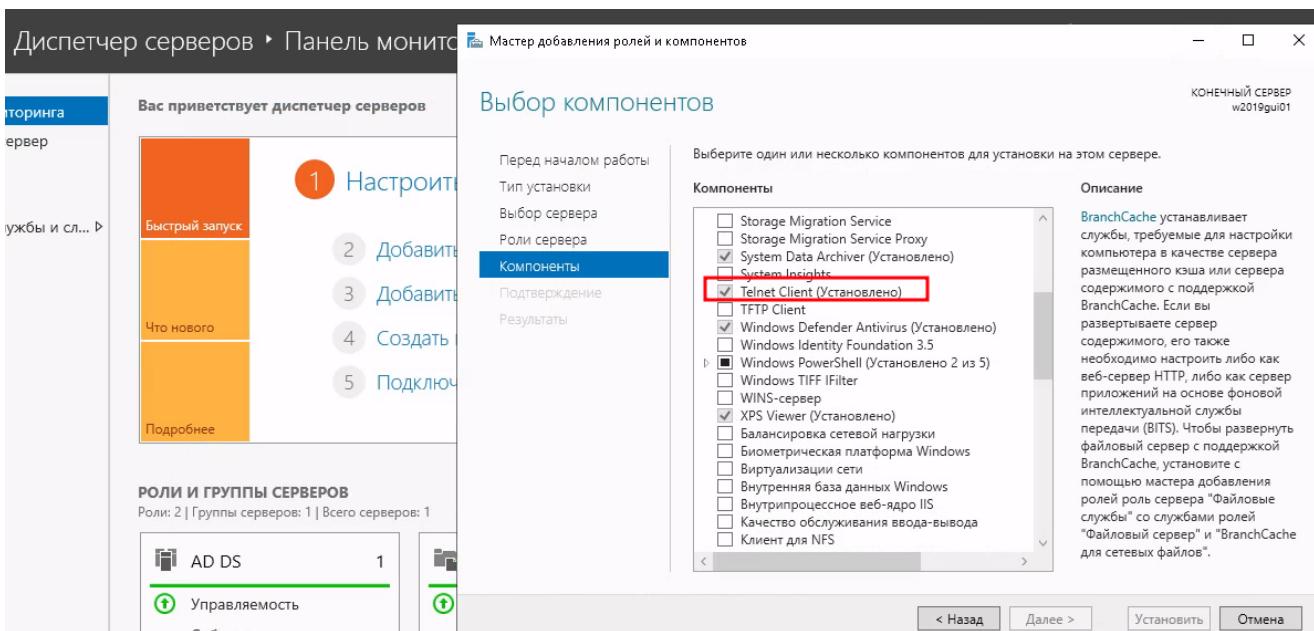
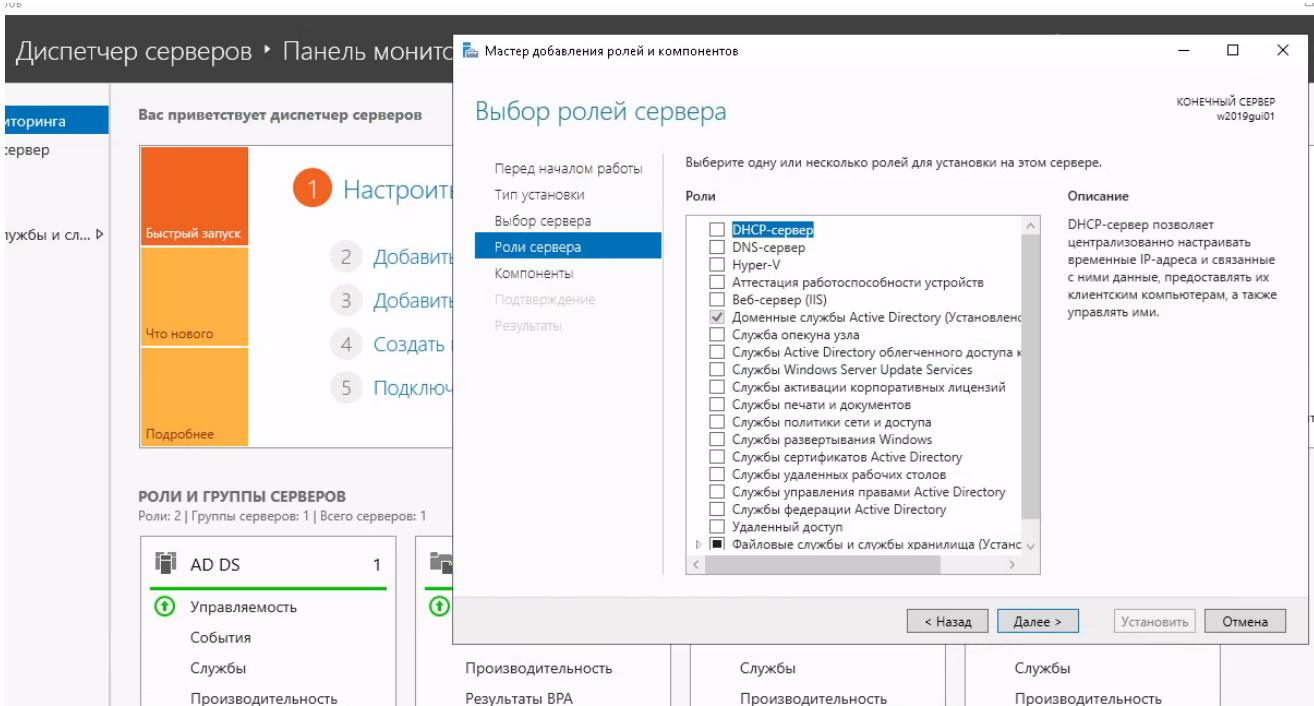
- Учетная запись администратора защищена надежным паролем
- Настроены сетевые параметры, такие как статические IP-адреса
- Установлены новейшие обновления безопасности из Центра обновления Windows

Если вам требуется проверить, выполнены ли какие-либо предшествующие необходимые условия, закройте мастер, выполните необходимые шаги и запустите мастер снова.

Чтобы продолжить, нажмите кнопку "Далее".

Пропускать эту страницу по умолчанию

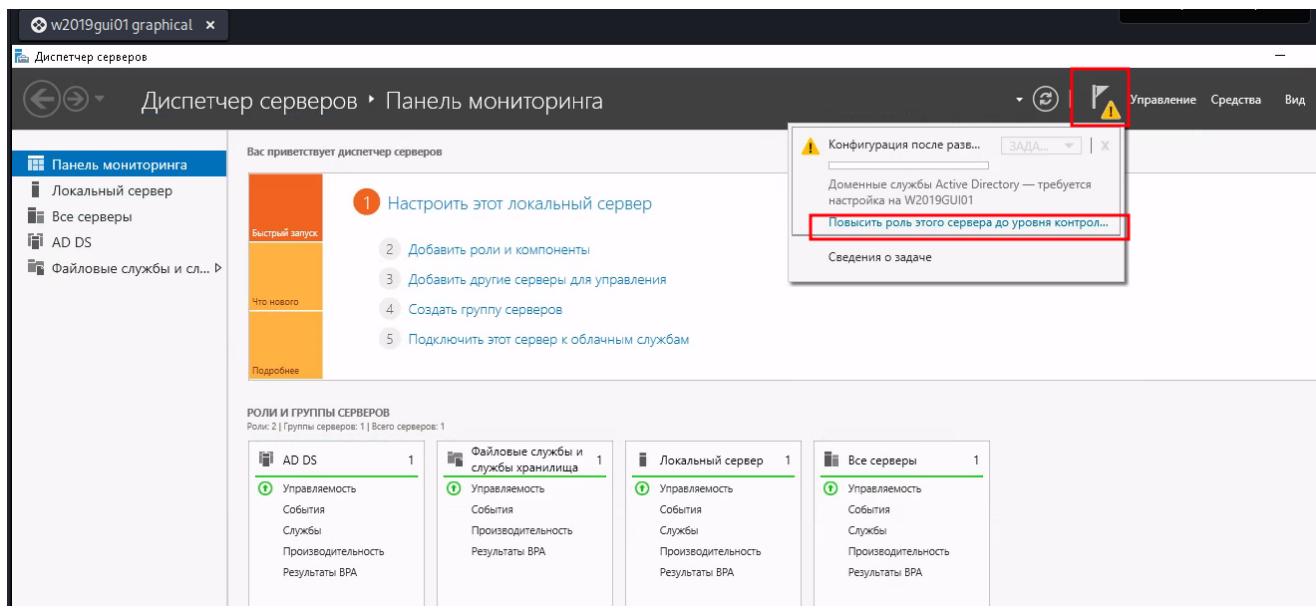
< Назад Далее > Установить Отмена



## Задание\_3:

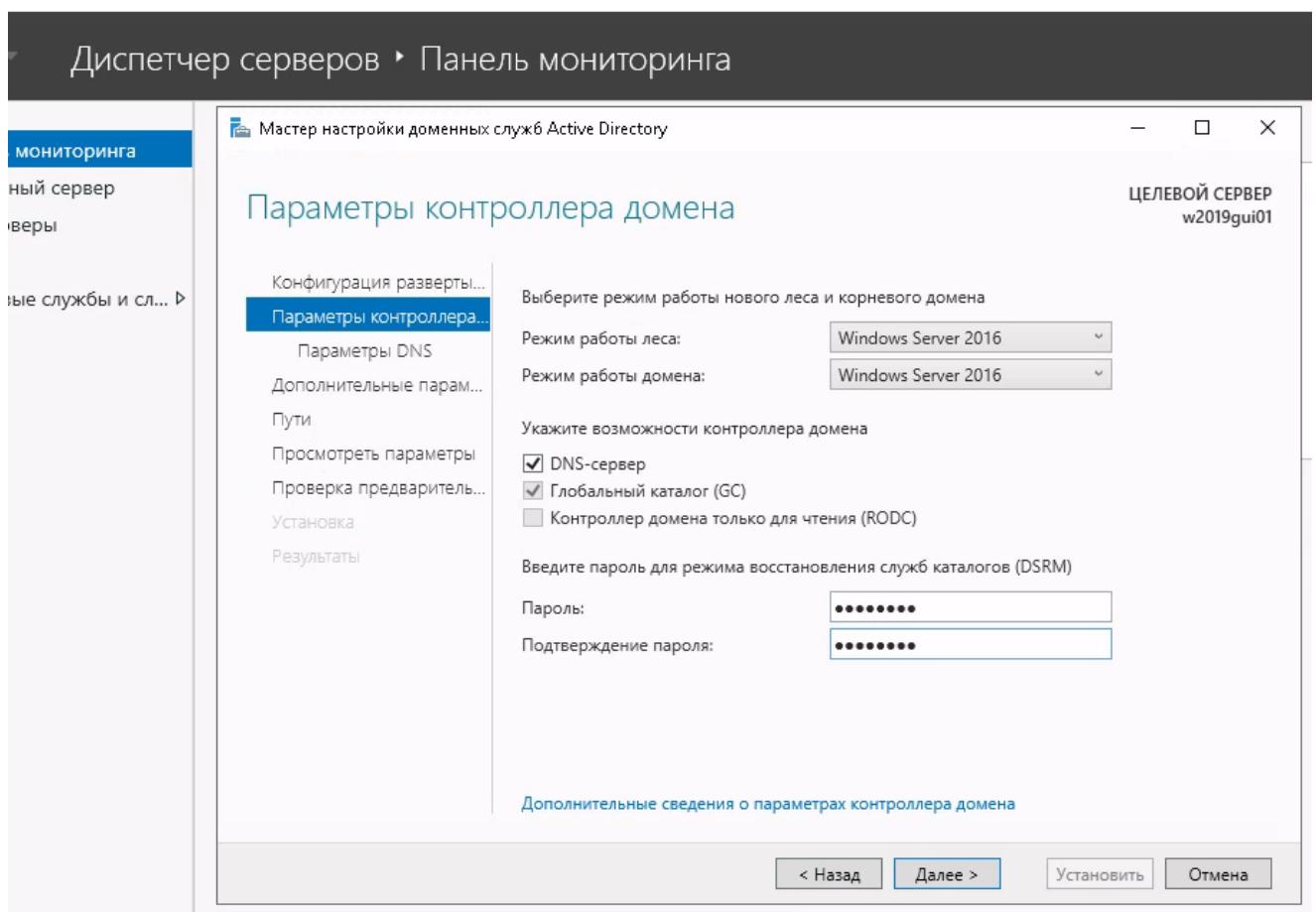
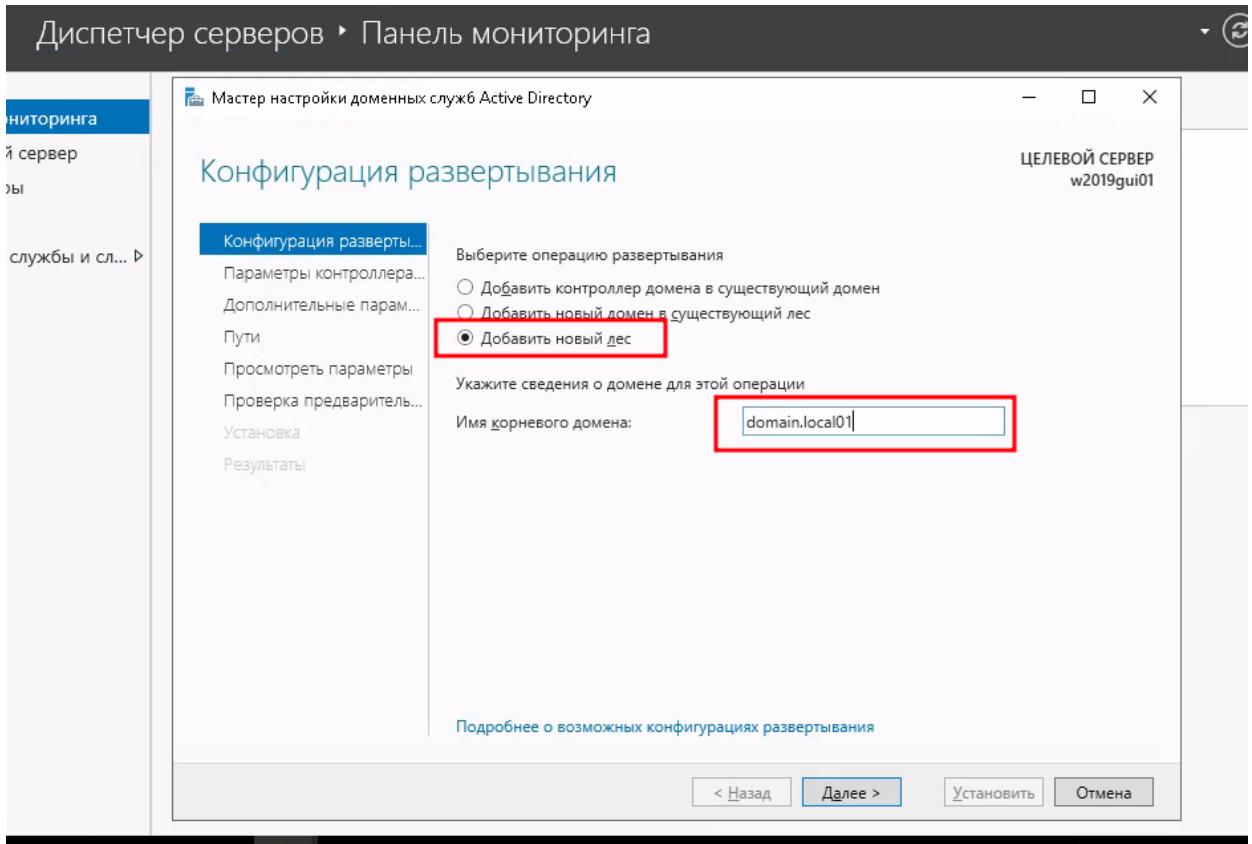
Сделайте сервер контроллером домена через "Диспетчер серверов".

DC1 w2019gui01:



The left screenshot shows the "Сведения о задаче Все серверы" window. It lists a task named "Конфигурация после развертывания..." with status "Запущен..." and message "Доменные службы Active Directory — требуется настройка на W2019GUI01". A red circle labeled "1" highlights the "Уведомление" link next to the message. The right screenshot shows the "Мастер настройки доменных служб Active Directory" window. Under "Конфигурация развертывания", the "Добавить контроллер домена в существующий домен" radio button is selected. A red circle labeled "2" highlights the "Домен:" input field where "W2019GUI01" is entered. Below it, a note says "Для выполнения этой операции введите учетные данные" and "Учетные данные не указаны".

- Добавить новый лес (add forest)



Password: Pass198 (просто Password не пройдет проверку)

## Диспетчер серверов ▶ Панель мониторинга

Мастер настройки доменных служб Active Directory

### Параметры DNS

ЦЕЛЕВОЙ СЕРВЕР  
w2019gui01

**⚠ Делегирование для этого DNS-сервера невозможно создать, поскольку полномочная родительск... Дополнительно**

Конфигурация разверты...  
Параметры контроллера...  
**Параметры DNS**  
Дополнительные параметр...  
Пути  
Просмотреть параметры  
Проверка предваритель...  
Установка  
Результаты

Укажите параметры делегирования DNS  
 Создать делегирование DNS

Дополнительные сведения о делегировании DNS

< Назад Далее > Установить Отмена

## Диспетчер серверов ▶ Панель мониторинга

Мастер настройки доменных служб Active Directory

### Дополнительные параметры

ЦЕЛЕВОЙ СЕРВЕР  
w2019gui01

Конфигурация разверты...  
Параметры контроллера...  
**Параметры DNS**  
**Дополнительные параметр...**  
Пути  
Просмотреть параметры  
Проверка предваритель...  
Установка  
Результаты

Проверьте NetBIOS-имя, присвоенное домену, и при необходимости измените его  
Имя домена NetBIOS:

Подробнее о дополнительных возможностях

< Назад Далее > Установить Отмена

## Диспетчер серверов ▶ Панель мониторинга

Мастер настройки доменных служб Active Directory

### Пути

Укажите расположение базы данных AD DS, файлов журналов и папки SYSVOL

Папка базы данных: C:\Windows\NTDS ...  
Папка файлов журнала: C:\Windows\NTDS ...  
Папка SYSVOL: C:\Windows\SYSVOL ...

Конфигурация разверты...  
Параметры контроллера...  
Параметры DNS  
Дополнительные параметры  
**Пути**  
Просмотреть параметры  
Проверка предваритель...  
Установка  
Результаты

Подробнее о путях Active Directory

< Назад Далее > Установить Отмена

## Диспетчер серверов ▶ Панель мониторинга

Мастер настройки доменных служб Active Directory

### Просмотреть параметры

Просмотрите выбранные параметры:

Сделать данный сервер первым контроллером домена Active Directory в новом лесу.  
Имя нового домена: "domain.local01". Это имя является также именем нового леса.  
NetBIOS-имя домена: DOMAIN  
Режим работы леса: Windows Server 2016  
Режим работы домена: Windows Server 2016  
Дополнительные параметры:  
Глобальный каталог: Да  
DNS-сервер: Да  
Создать DNS-делегирование: Нет

Для автоматизации дополнительных установок эти параметры можно экспортить в сценарий Windows PowerShell

Просмотреть сценарий

Дополнительные сведения о вариантах установки

< Назад Далее > Установить Отмена

[Посмотреть сценарий](#)

```
#  
# Сценарий Windows PowerShell для развертывания AD DS  
#
```

```
Import-Module ADDSDeployment  
Install-ADDSForest  
-CreateDnsDelegation:$false  
-DatabasePath "C:\Windows\NTDS"  
-DomainMode "WinThreshold"  
-DomainName "domain.local01"  
-DomainNetbiosName "DOMAIN"  
-ForestMode "WinThreshold"  
-InstallDns:$true  
-LogPath "C:\Windows\NTDS"  
-NoRebootOnCompletion:$false  
-SysvolPath "C:\Windows\SYSVOL"  
-Force:$true
```

Сделать данный сервер первым контроллером домена Active Directory в новом лесу.

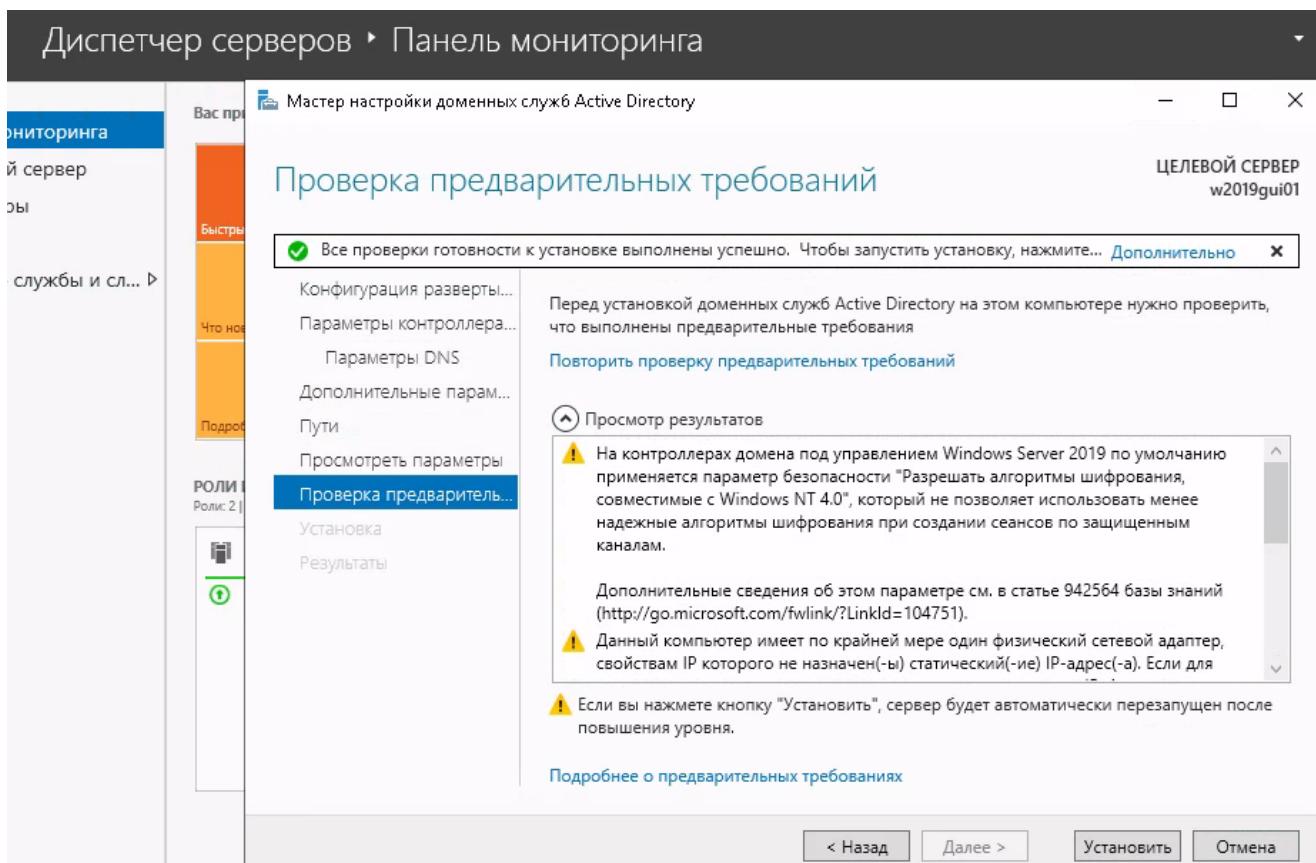
Имя нового домена: "domain.local01". Это имя является также именем нового леса.

NetBIOS-имя домена: DOMAIN

Режим работы леса: Windows Server 2016

Режим работы домена: Windows Server 2016

...



Мастер настройки доменных служб Active Directory

## Установка

Ход выполнения

Запуск

Просмотреть подробные результаты операций

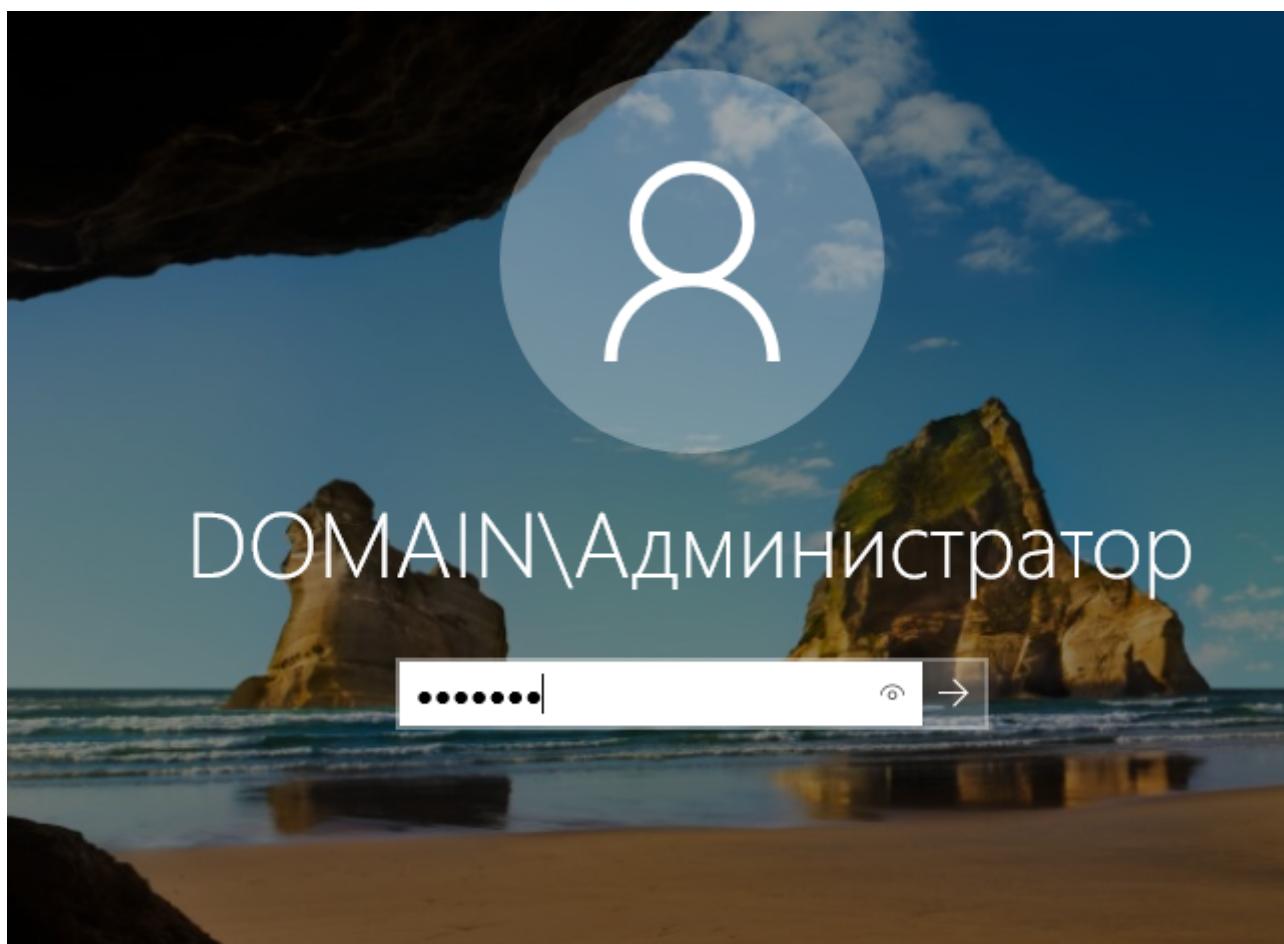
На контроллерах домена под управлением Windows Server 2019 по умолчанию применяется параметр безопасности "Разрешать алгоритмы шифрования, совместимые с Windows NT 4.0", который не позволяет использовать менее надежные алгоритмы шифрования при создании сеансов по защищенным каналам.

Дополнительные сведения об этом параметре см. в статье 942564 базы знаний (<http://go.microsoft.com/fwlink/?LinkId=104751>).

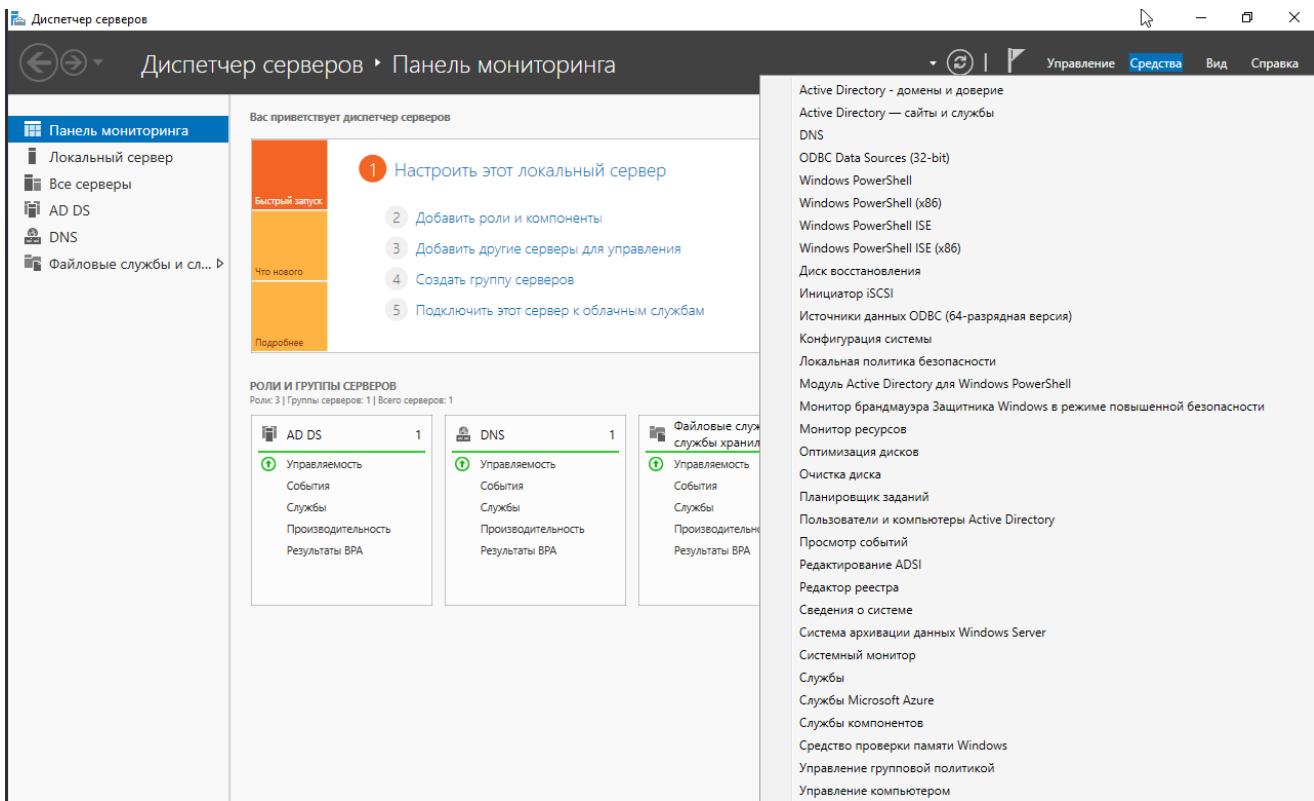
⚠️ Данный компьютер имеет по крайней мере один физический сетевой адаптер, свойствам IP которого не назначен(-ы) статический(-ие) IP-адрес(-а). Если для сетевого адаптера разрешено использование, как протокола IPv4, так и протокола IPv6, то свойствам IPv4 и IPv6 этого физического сетевого адаптера следует, соответственно, назначить статические IP-адреса и в формате IPv4, и в формате IPv6. Для надежной работы системы доменных имен (DNS) такой(-ие) статический(-ие) IP-адрес(-а) следует назначить всем физическим сетевым адаптерам.

Дополнительные сведения о вариантах установки

< Назад | Далее > | Установить | Отмена

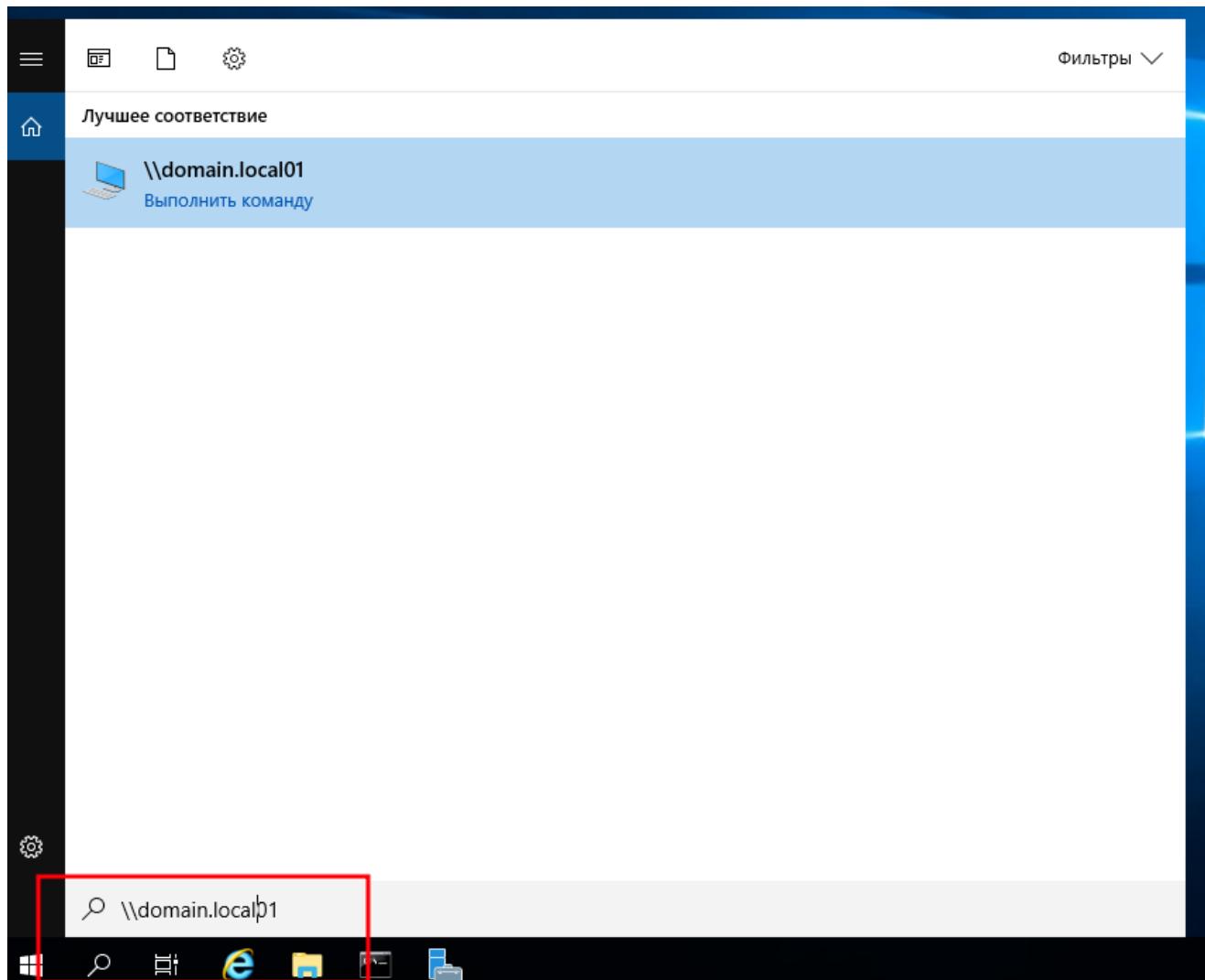


Пароль как у обычного Администратора



## Появились новые службы

The screenshot shows the Windows Event Viewer interface. The left pane shows a tree view of logs: 'Local Computer Log' (selected), 'Application', 'System', 'Security', and 'Event Log'. Under 'Local Computer Log', 'Application' is expanded, showing 'Журналы приложений и служб' (Application and Service Logs) which is highlighted with a red box. This log contains entries for 'Directory Service', 'DNS Server', 'Internet Explorer', 'Microsoft', 'Microsoft-ServerManagementExperience', 'OpenSSH', 'Windows PowerShell', 'Web-сервисы Active Directory', 'Репликация DFS', 'Служба управления ключами', and 'События оборудования'. The right pane shows a table of events with columns: 'Файл' (File), 'Тип' (Type), 'Число событий' (Number of events), and 'Размер' (Size). The table includes rows for 'Directory Service', 'DNS Server', 'Internet Explorer', 'Microsoft', 'Microsoft-ServerManagementExperience', 'OpenSSH', 'Windows PowerShell', 'Web-сервисы Active Directory', 'Репликация DFS', 'Служба управления ключами', and 'События оборудования'. A 'Действия' (Actions) pane on the right lists options like 'Open saved log...', 'Create new...', 'Import...', 'View', 'Update', 'Help', and 'Directory Service' (which is also highlighted with a red box).

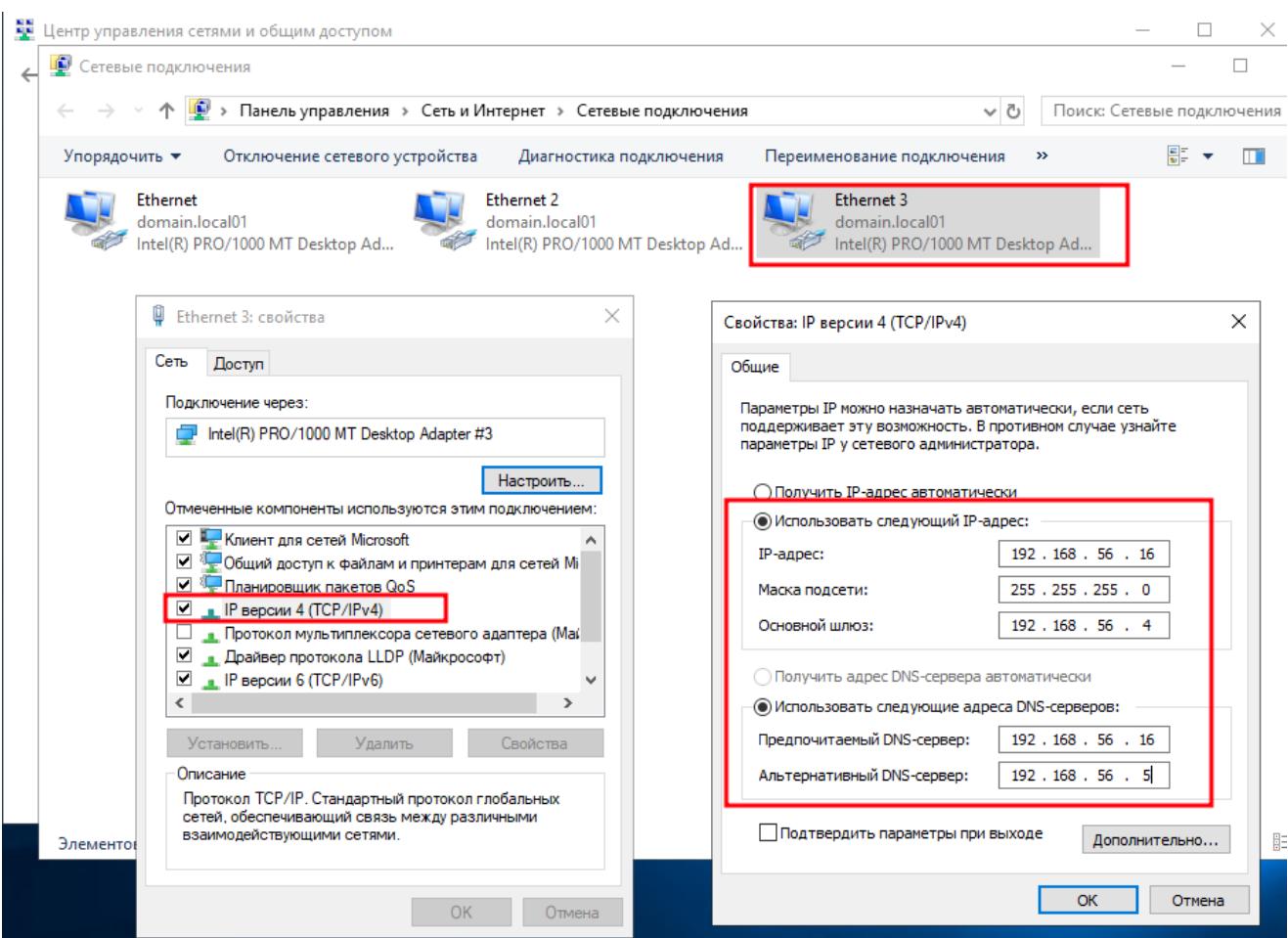
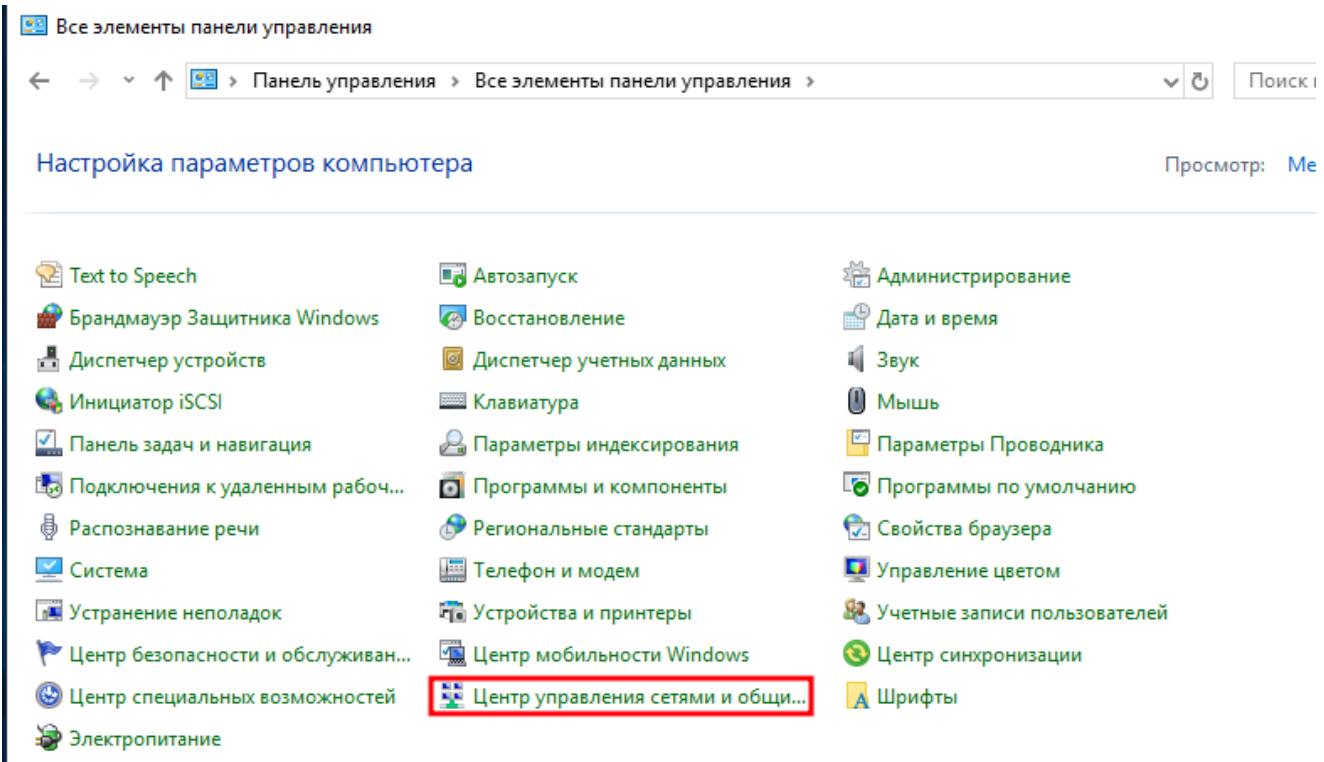


The image contains two side-by-side screenshots of the Windows File Explorer application.

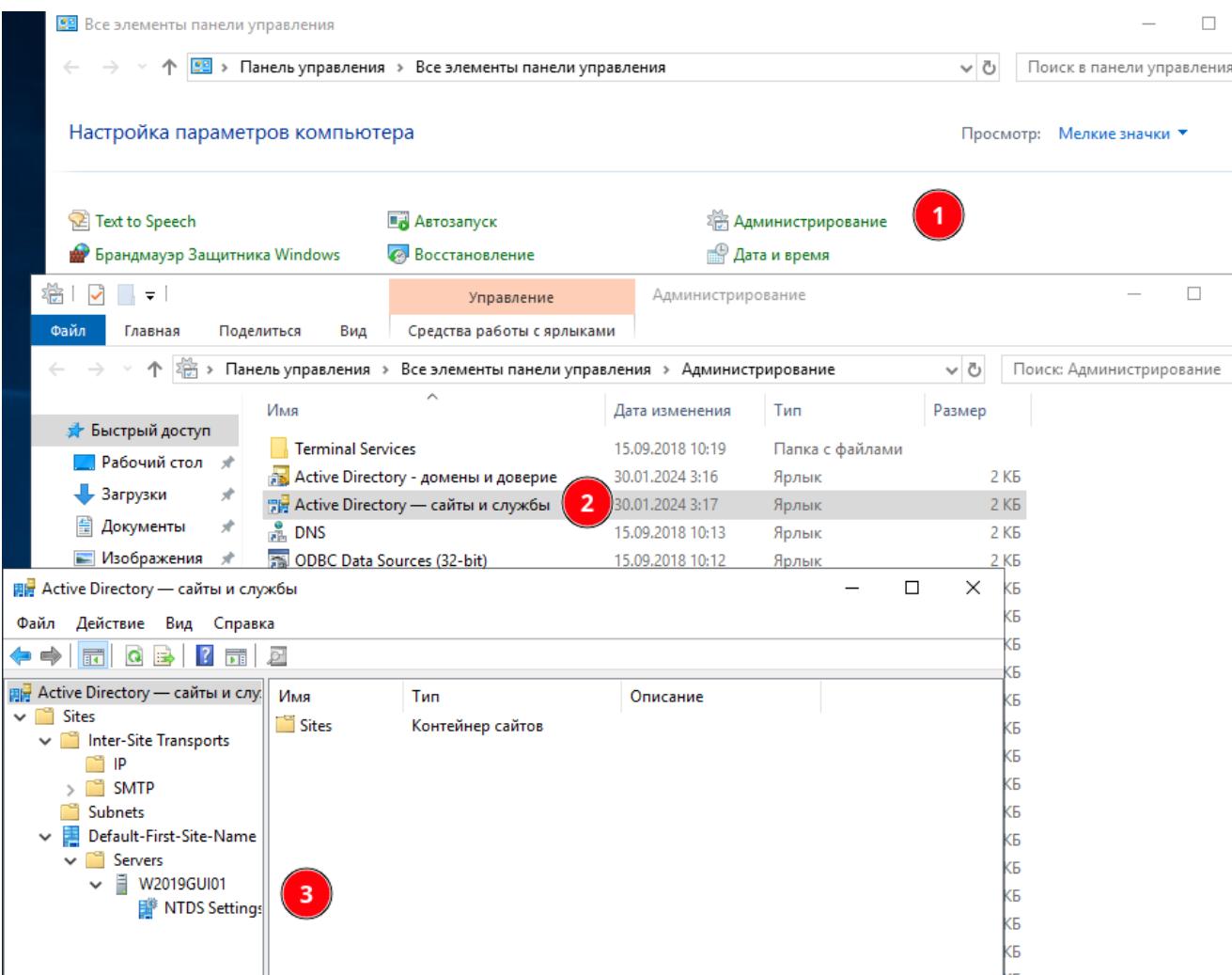
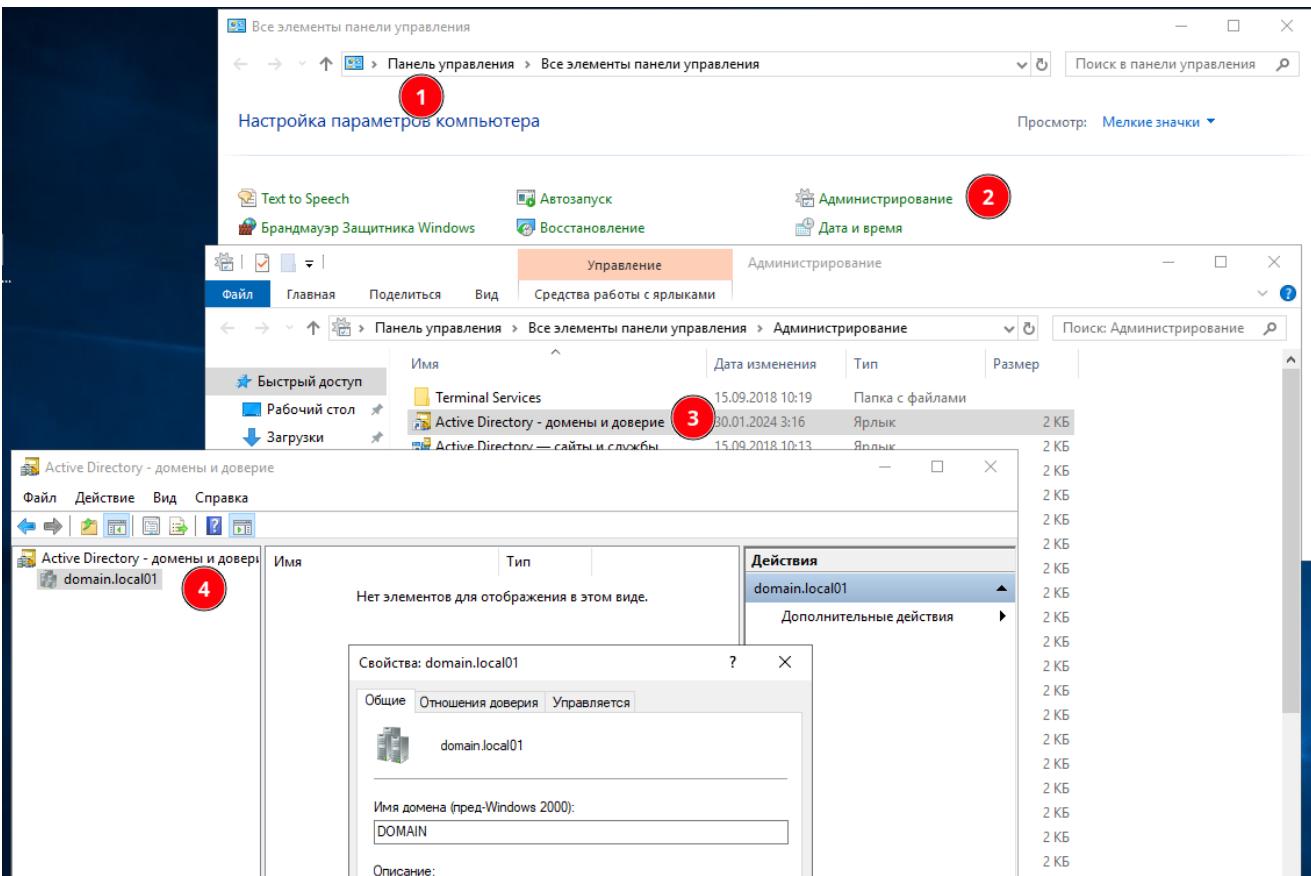
**Top Window:** This window shows a network share 'domain.local01'. The address bar indicates the path is 'Сеть > domain.local01'. The main pane displays two folders: 'NETLOGON' (selected, highlighted in blue) and 'SYSVOL'. The left sidebar shows 'Быстрый доступ', 'Рабочий стол', 'Загрузки', and 'Документы'.

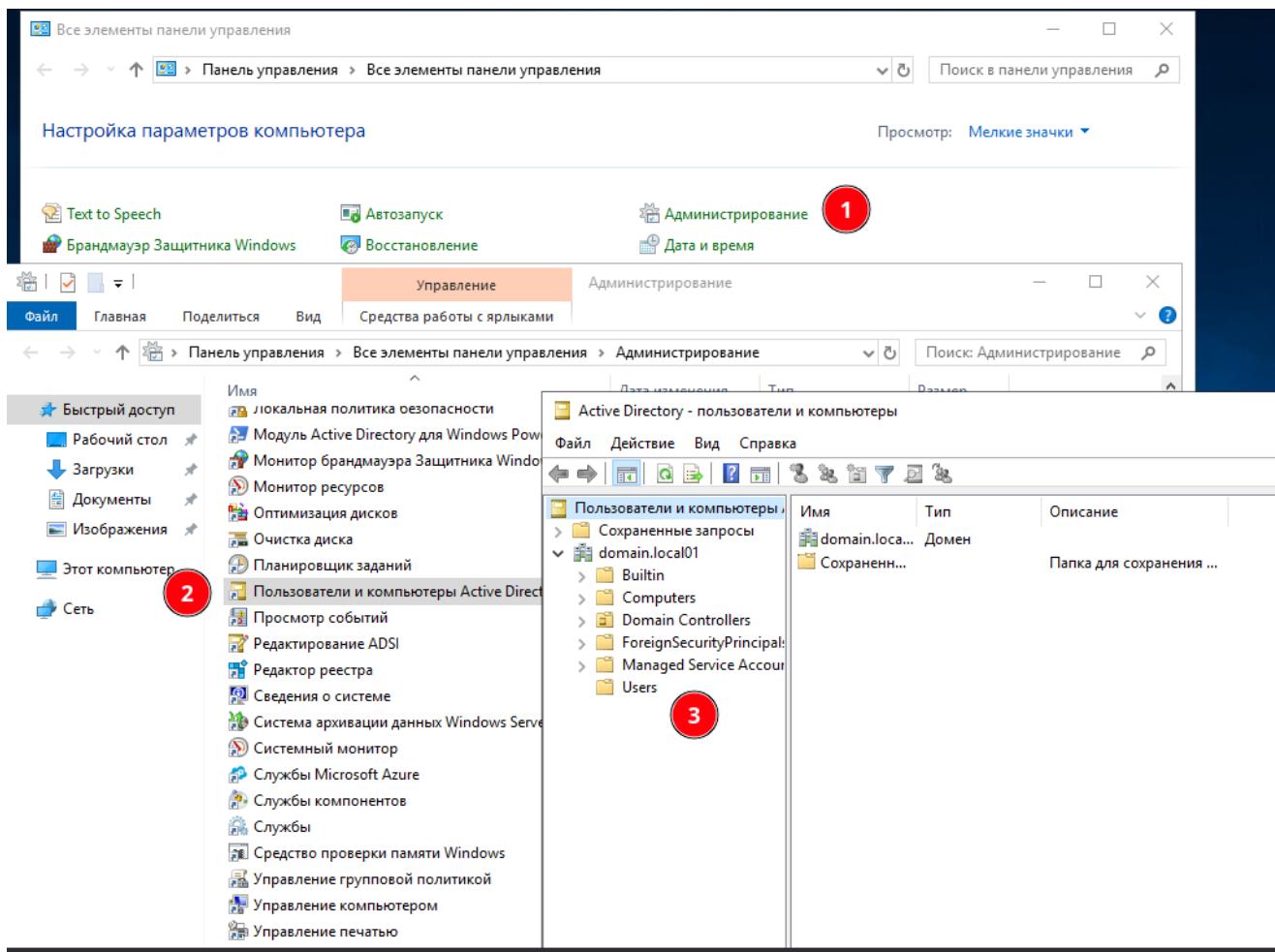
**Bottom Window:** This window shows a folder structure under 'domain.local01 > SYSVOL > domain.local01'. The address bar shows the full path: '<< domain.local01 > SYSVOL > domain.local01 > Policies >'. The 'Policies' folder is selected and highlighted in red. The left sidebar is identical to the top window. The main pane displays a table of files in the 'Policies' folder:

Имя	Дата изменения	Тип	Размер
{6AC1786C-016F-11D2-945F-00C04FB984...}	30.01.2024 2:40	Папка с файлами	
{31B2F340-016D-11D2-945F-00C04FB984...}	30.01.2024 2:40	Папка с файлами	



PC1



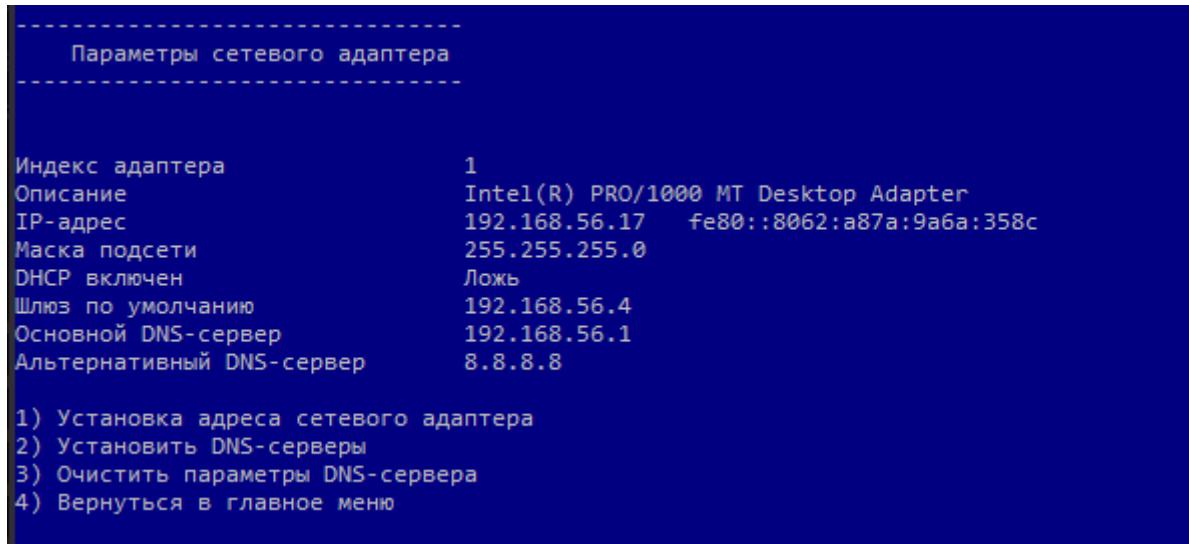


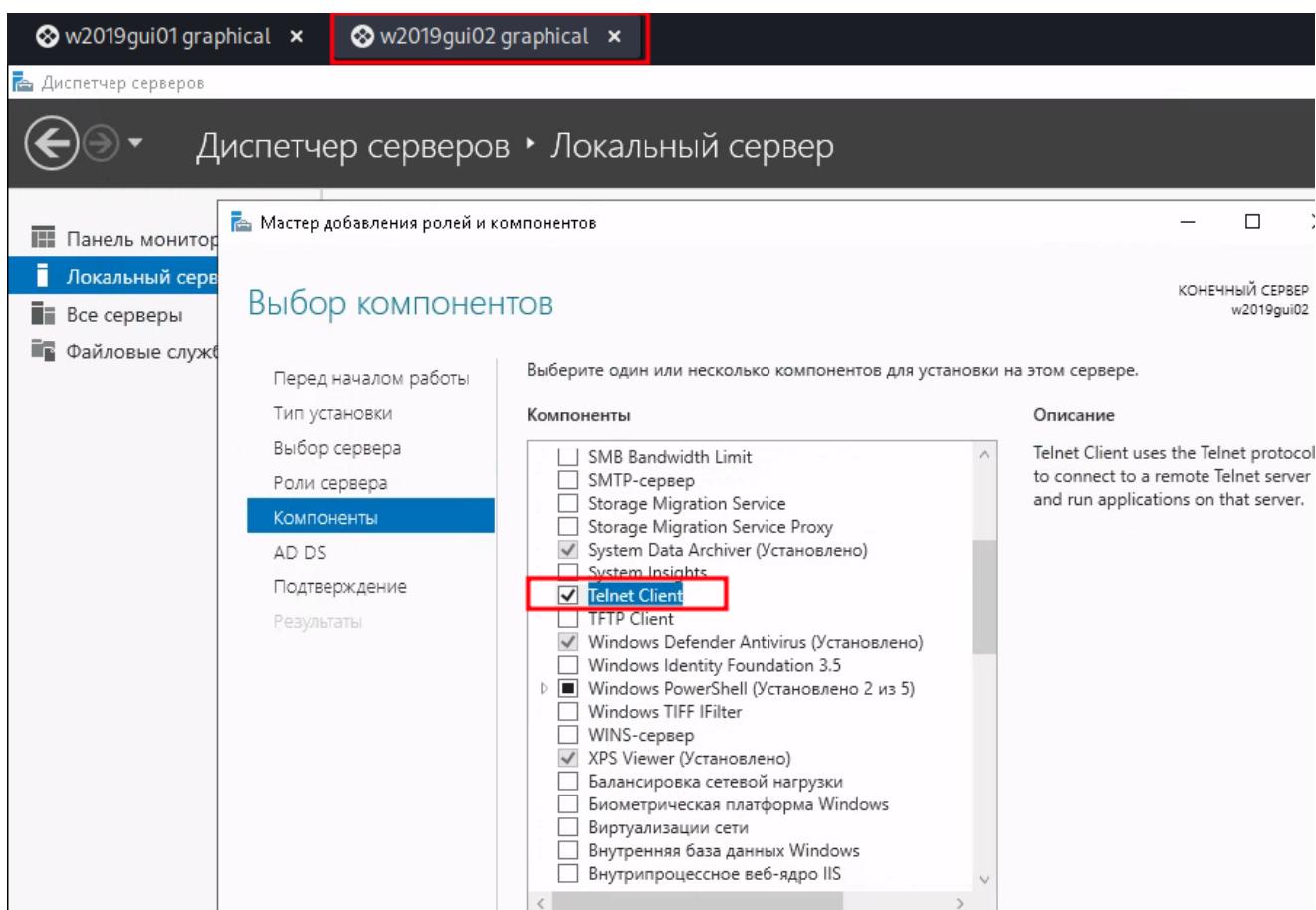
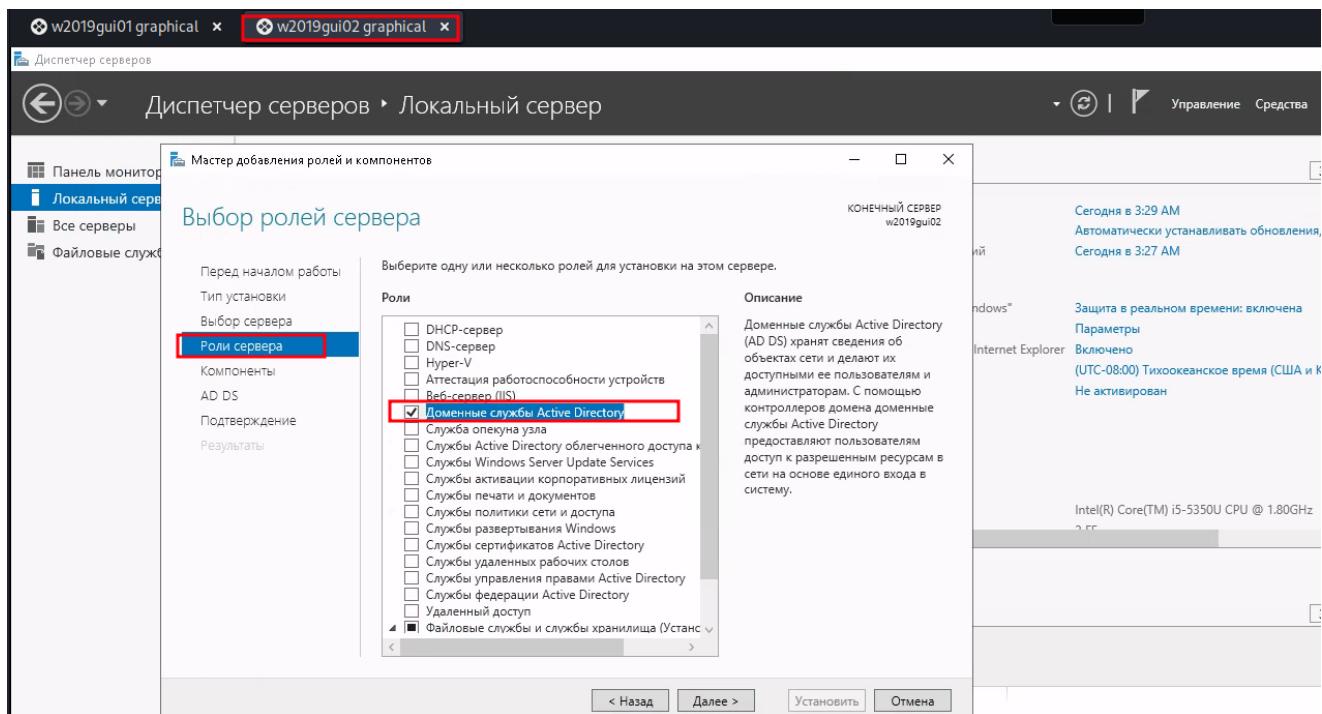
## Задание\_4:

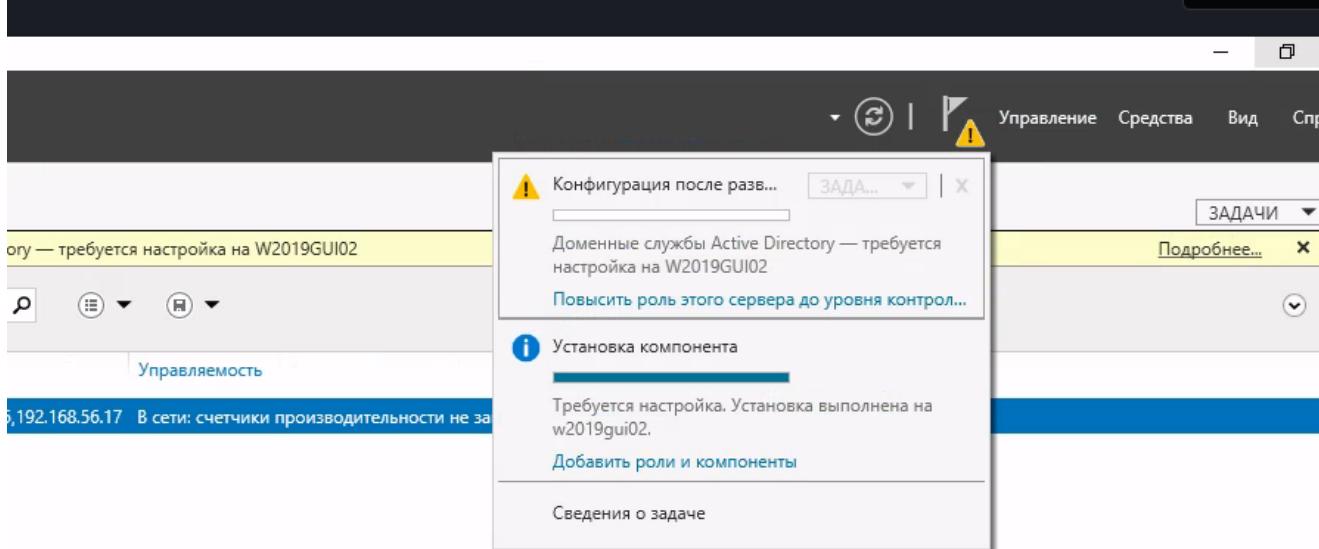
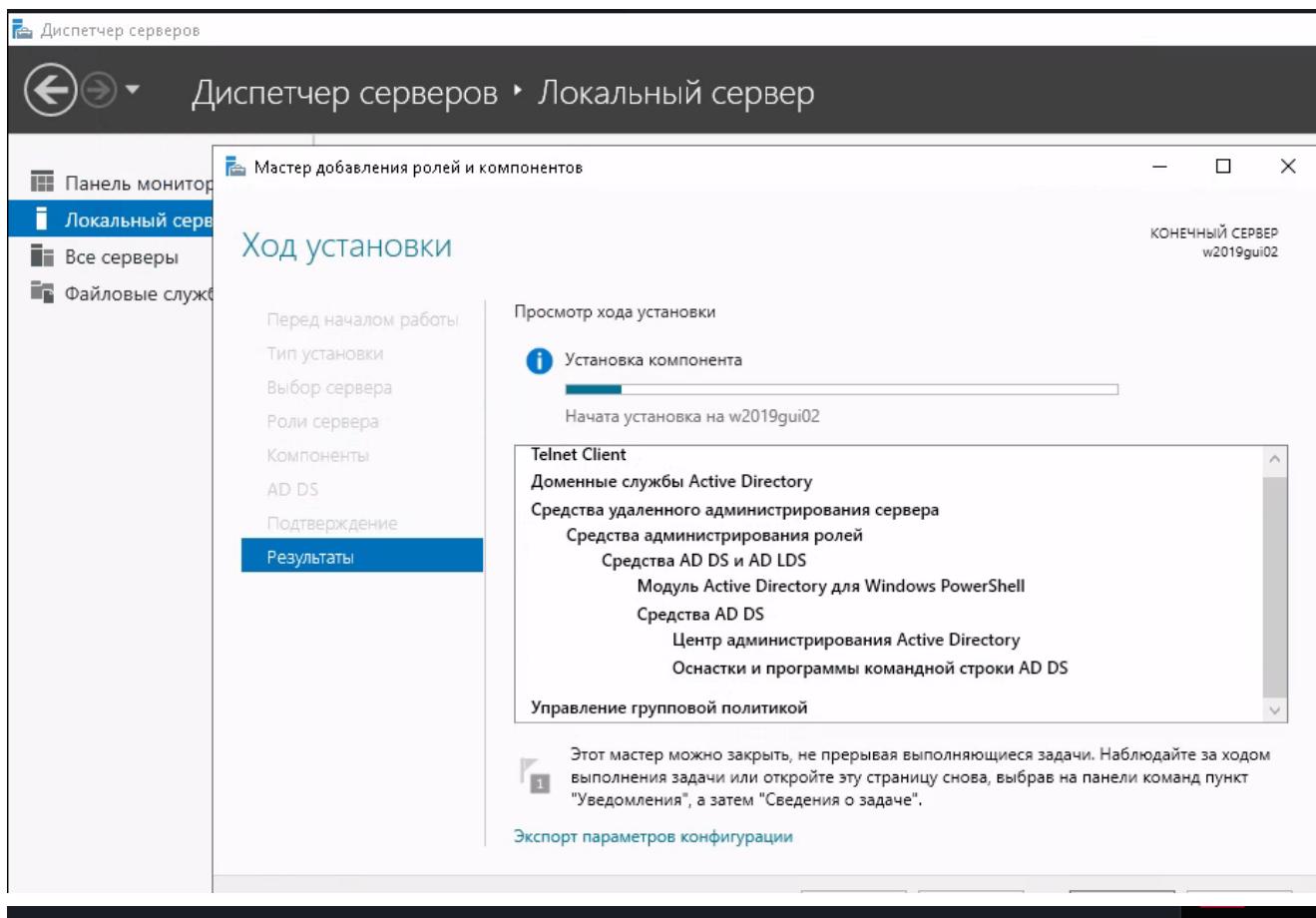
Установите дополнительный контроллер домена на второй машине через "Диспетчер серверов".

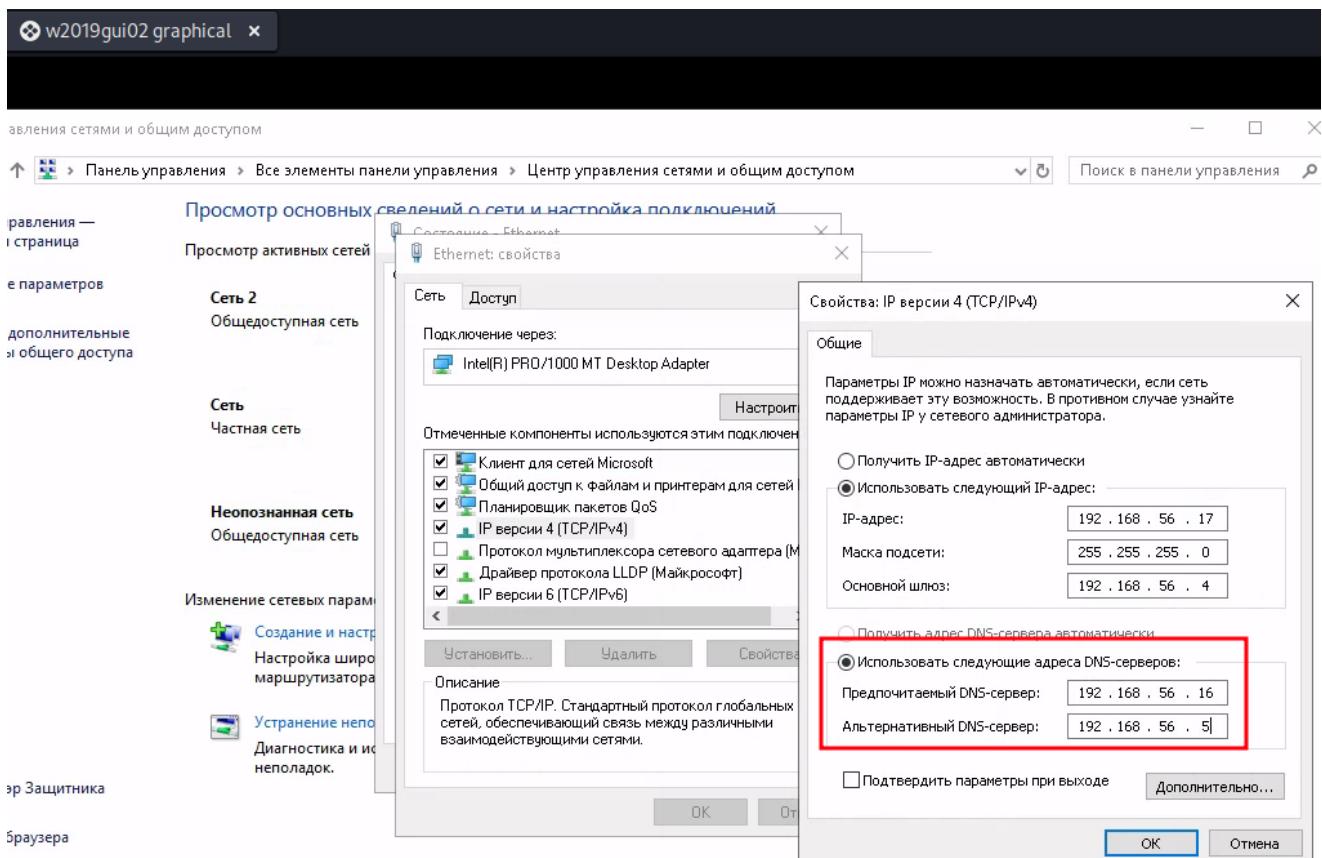
PC2 w2019gui02:

- Устанавливаем роль AD DS









## Из DNS PC1

```
w2019gui02 graphical x
Administrator: Командная строка

C:\Users\Администратор>ping 192.168.56.17

Pinging 192.168.56.17 with 32 bytes of data:
Reply from 192.168.56.17: bytes=32 time<1ms TTL=128
Reply from 192.168.56.17: bytes=32 time<1ms TTL=128
Reply from 192.168.56.17: bytes=32 time<1ms TTL=128

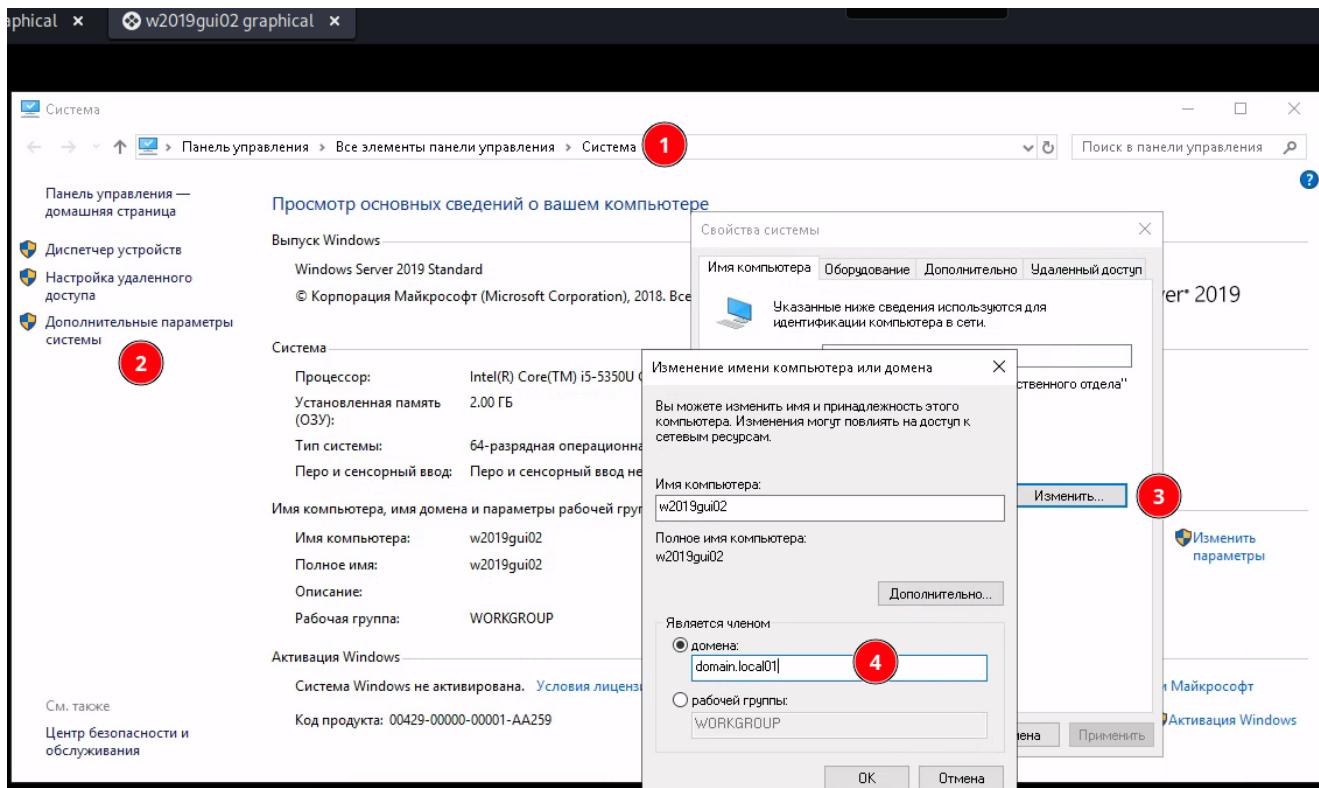
Статистика Ping для 192.168.56.17:
    Пакетов: отправлено = 3, получено = 3, потеряно = 0
        (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
Control-C
^C
C:\Users\Администратор>ping 192.168.56.16

Pinging 192.168.56.16 with 32 bytes of data:
Reply from 192.168.56.16: bytes=32 time<1ms TTL=128
Reply from 192.168.56.16: bytes=32 time<1ms TTL=128
Reply from 192.168.56.16: bytes=32 time<1ms TTL=128

Статистика Ping для 192.168.56.16:
    Пакетов: отправлено = 3, получено = 3, потеряно = 0
        (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек
Control-C
```

```
C:\Users\Администратор>nslookup domain.local01
Server: UnKnown
Address: 192.168.56.16

Name: domain.local01
Addresses: 2a02:3100:71ac:c200:8647:bf7e:91bd:370b
          192.168.56.16
          10.0.3.15
```



domain.local01

метры

Система

Процессор: Intel(R) Core(TM) i5-5350U

Безопасность Windows

## Изменение имени компьютера или домена

Введите имя и пароль учетной записи с правами на присоединение к домену.

domain\Администратор

•••••

OK

Отмена

## Изменение имени компьютера или домена

X



Добро пожаловать в домен domain.local01.

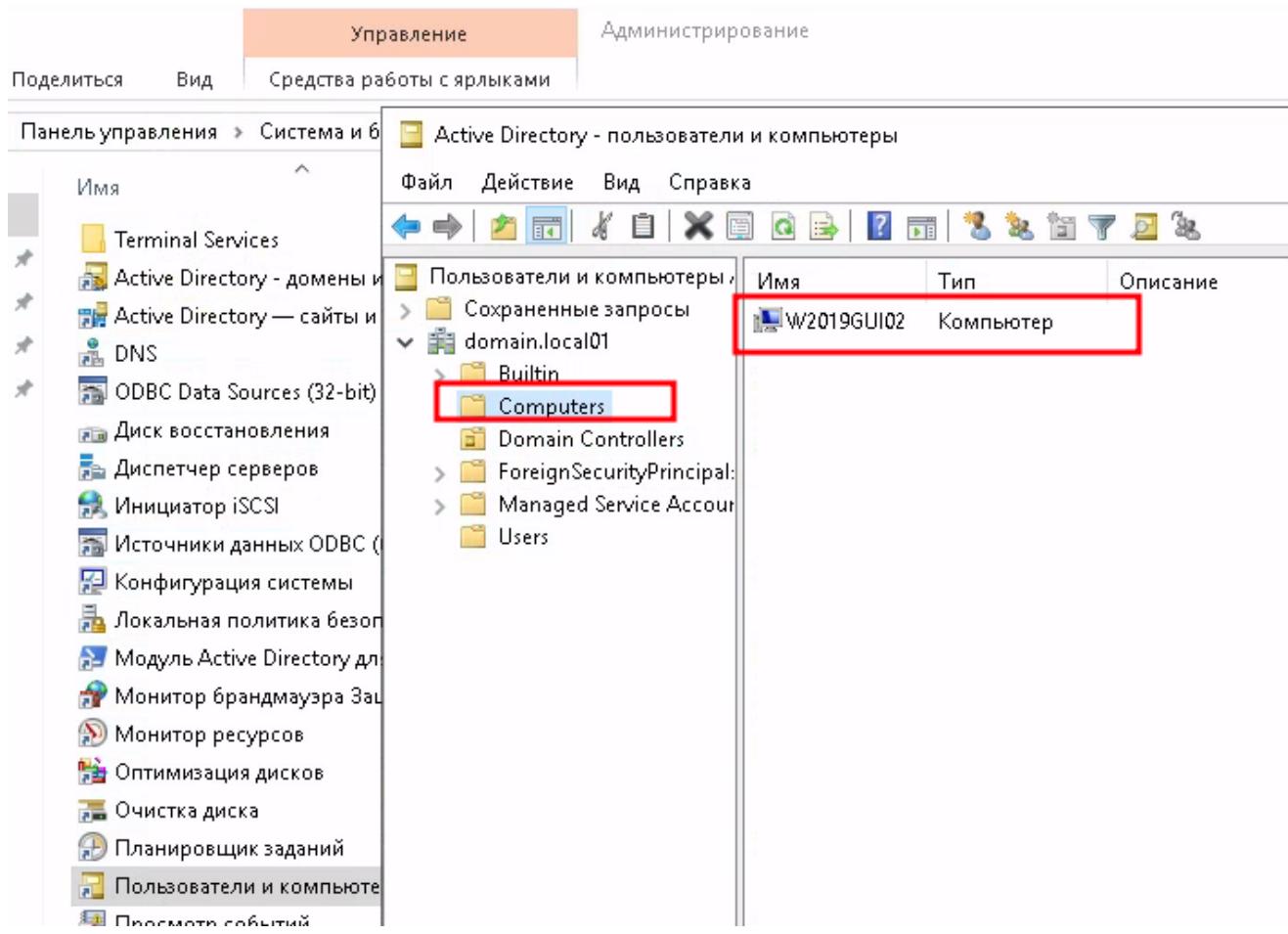
OK

The screenshot shows a Windows Server 2019 desktop environment. The taskbar at the top has two pinned icons: 'w2019gui01 graphical' (selected) and 'w2019gui02 graphical'. The desktop background is black.

The main window is 'Управление' (Management). The left sidebar shows 'Быстрый доступ' (Quick Access) with items like Рабочий стол, Загрузки, Документы, Изображения, System32, Этот компьютер, and Сеть. The right pane shows the 'Система и управление' (System and Management) section. A red box highlights the 'Пользователи и компьютеры' (Users and Computers) link under 'Панель управления' (Control Panel).

A second window titled 'Active Directory - пользователи и компьютеры' (Active Directory - users and computers) is open. It shows a tree view of the domain structure: Пользователи и компьютеры > domain.local01 > Computers. A red box highlights the 'Computers' folder. In the details pane, a table lists objects: Name, Type, Description. One row is selected, showing 'W2019GUI02' as a 'Компьютер' (Computer). Another red box highlights this row.

At the bottom of the screen, status text reads: 'Элементов: 32 Выбран 1 элемент: 1,13 КБ' (Elements: 32 Selected 1 element: 1,13 KB).



## Глоссарий

## Дополнительные материалы

## Используемые источники

Выполнил: AndreiM