

**30.01.2024**

**Курс:**

**Практическая работа к уроку № Lesson\_4**

--

Основные команды PowerShell

**Задание:**

Перед выполнением домашнего задания создайте резервные копии (снапшоты) виртуальных машин с домен контроллерами

1. Запустите утилиты `repadmin /showrepl`
2. Запустите утилиту `dcdiag /test:dns , /test:topology`
3. Узнайте SID пользователя под учетной записью которого вошли в систему
4. Создайте защищенную от удаления ОП (OU)
5. Создайте в ней учетные записи нескольких пользователей, компьютеров, группу
6. Добавьте пользователей в группу
7. Удалите созданную OU
8. Создайте групповую политику (GPO) с блокировкой ссылки "Игры" и подключите к любой OU
9. Удалите созданную GPO
10. Добавьте в качестве сервера пересылки адрес 8.8.8.8
11. Сделайте простой и рекурсивный запросы к ДНС серверу
12. Используя утилиту NTDSUtil и оснастки AD передайте две роли на второй контроллер домена
13. Выключите второй контроллер домена, произведите захват ролей первым контроллером домена, удалите данные о втором контроллере домена из AD

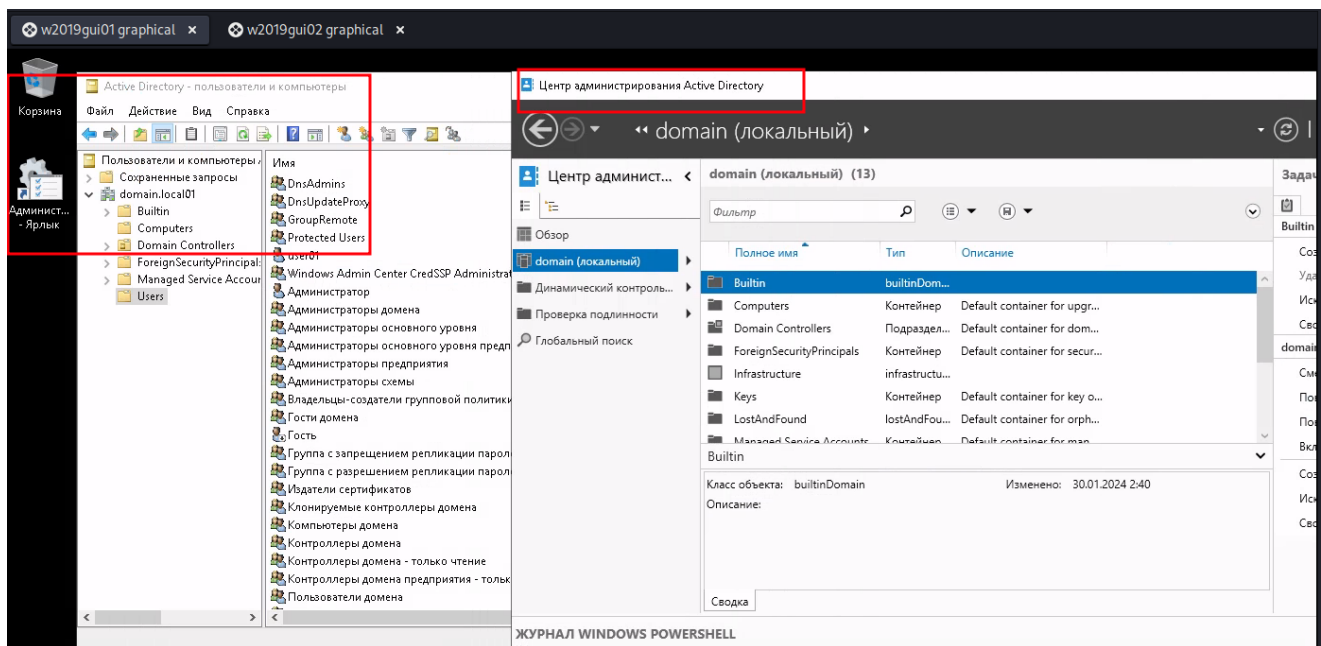
**Команды**

PC1

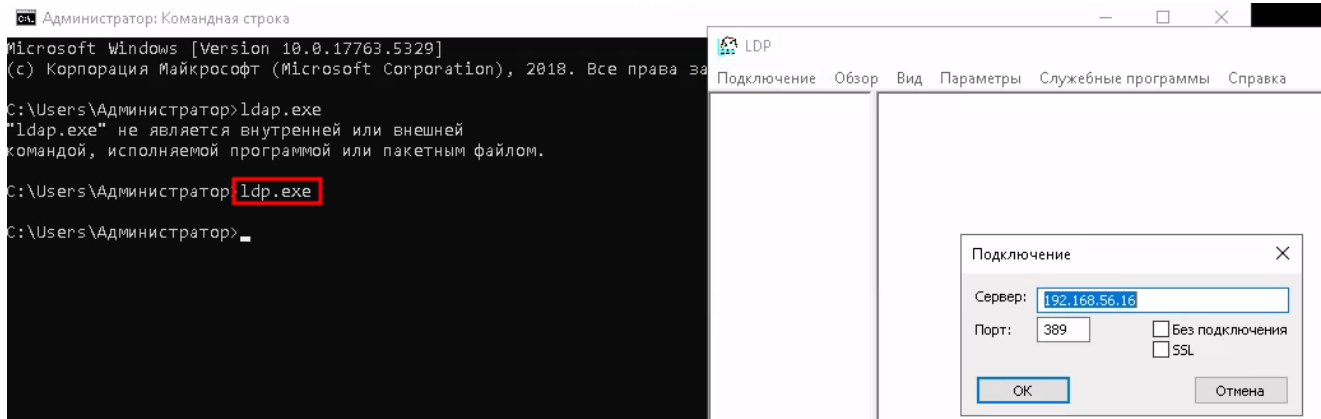
```
Статистика Ping для 192.168.56.16:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0
  (0% потерь)
```

PC2

Статистика Ping для 192.168.56.17:  
Пакетов: отправлено = 3, получено = 3, потеряно = 0



## ldp.exe



```
Id = Idap_open("192.168.56.16", 389);
Established connection to 192.168.56.16.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
configurationNamingContext: CN=Configuration,DC=domain,DC=local01;
currentTime: 30.01.2024 19:34:39 RTZ 2 (зима);
defaultNamingContext: DC=domain,DC=local01;
dnsHostName: w2019gui01.domain.local01;
domainControllerFunctionality: 7 = ( VMN2016 );
domainFunctionality: 7 = ( VMN2016 );
dsServiceName: CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01;
forestFunctionality: 7 = ( VMN2016 );
highestCommittedUSN: 28728;
isGlobalCatalogReady: TRUE;
isSynchronized: TRUE;
IdapServiceName: domain.local01:w2019gui01$@DOMAIN.LOCAL01;
namingContexts (5): DC=domain,DC=local01; CN=Configuration,DC=domain,DC=local01;
CN=Schema,CN=Configuration,DC=domain,DC=local01;
DC=DomainDnsZones,DC=domain,DC=local01; DC=ForestDnsZones,DC=domain,DC=local01;
rootDomainNamingContext: DC=domain,DC=local01;
schemaNamingContext: CN=Schema,CN=Configuration,DC=domain,DC=local01;
serverName: CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01;
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=domain,DC=local01;
supportedCapabilities (6): 1.2.840.113556.1.4.800 = ( ACTIVE_DIRECTORY );
1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 ); 1.2.840.113556.1.4.1791 = (
```

## dsadd

C:\Users\Администратор>dsadd

Описание: параметры этой программы позволяют добавить различные объекты в каталог. Параметры dsadd:

dsadd computer - добавление компьютера в каталог.  
dsadd contact - добавление контакта в каталог.  
dsadd group - добавление группы в каталог.  
dsadd ou - добавление подразделения в каталог.  
dsadd user - добавление пользователя в каталог.  
dsadd quota - добавление квоты в раздел каталога.

Для получения дополнительных сведений по использованию этих параметров введите "dsadd <ObjectType> /?", где <ObjectType> - один из приведенных выше типов. Например, dsadd ou /?.

Примечания.

Перед запятыми, не используемыми для разделения значений в различающихся именах, необходимо поставить символ обратного слэша "\" (например, "CN=Компания\, Inc.,CN=Users,DC=microsoft,DC=com").

Перед символом обратной косой черты, используемым в различающихся именах, необходимо поставить символ обратной косой черты (например, "CN=Sales\\ Latin America,OU=Distribution Lists,DC=microsoft,DC=com").

Дополнительные сведения по программам командной строки службы каталогов:

dsadd /? - сведения по добавлению объектов.  
dsget /? - сведения по отображению объектов.  
dsmod /? - сведения по изменению объектов.  
dsmove /? - сведения по перемещению объектов.  
dsquery /? - сведения по поиску объектов, отвечающих заданным условиям.  
dsrm /? - сведения по удалению объектов.

## ntdsutil

C:\Users\Администратор>ntdsutil

## dcdiag - поиск неисправностей

```
C:\Users\Администратор>dcdiag

Диагностика сервера каталогов

Выполнение начальной настройки:
  Выполняется попытка поиска основного сервера...
  Основной сервер = w2019gui01
  * Определен лес AD.
  Сбор начальных данных завершен.

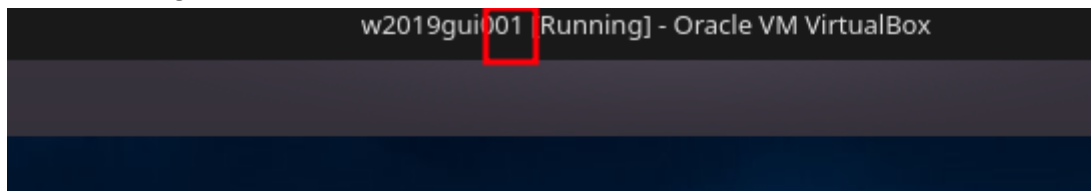
Выполнение обязательных начальных проверок

  Сервер проверки: Default-First-Site-Name\W2019GUI01
  Запуск проверки: Connectivity
  ..... W2019GUI01 - пройдена проверка Connectivity

Выполнение основных проверок

  Сервер проверки: Default-First-Site-Name\W2019GUI01
  Запуск проверки: Advertising
  ..... W2019GUI01 - пройдена проверка Advertising
  Запуск проверки: FrsEvent
  ..... W2019GUI01 - пройдена проверка FrsEvent
  Запуск проверки: DFSREvent
  За последние 24 часа после предоставления SYSVOL в общий доступ зафиксированы предупреждения или сообщения о
  ошибках. Сбои при репликации SYSVOL могут стать причиной проблем групповой политики.
  ..... W2019GUI01 - не пройдена проверка DFSREvent
  Запуск проверки: SysVolCheck
  ..... W2019GUI01 - пройдена проверка SysVolCheck
  Запуск проверки: KccEvent
  ..... W2019GUI01 - пройдена проверка KccEvent
```

## PC1 w2019gui01



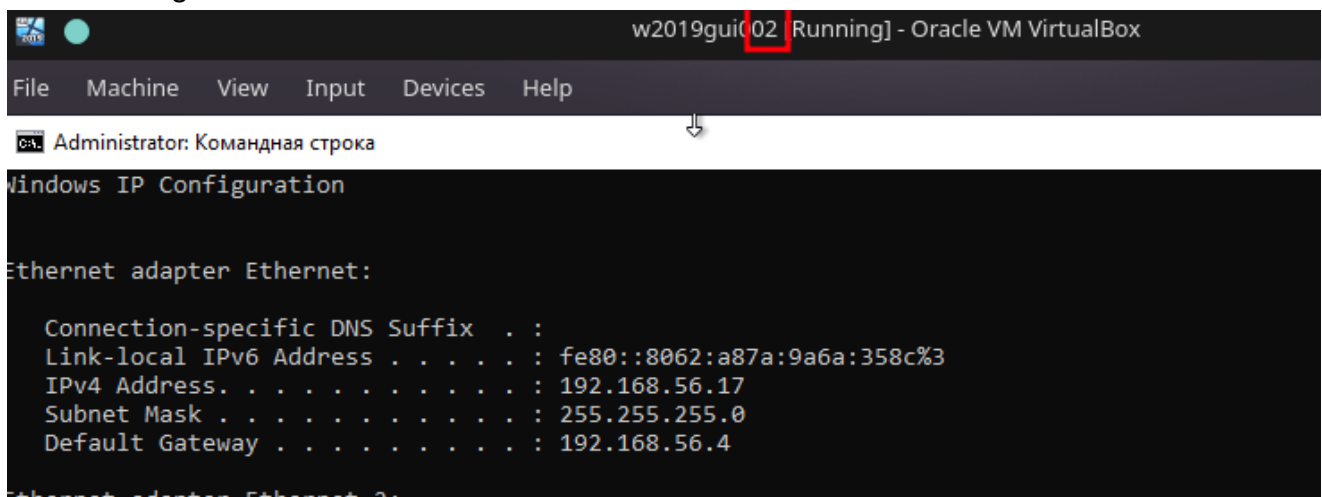
Выбрать Администратор: Командная строка

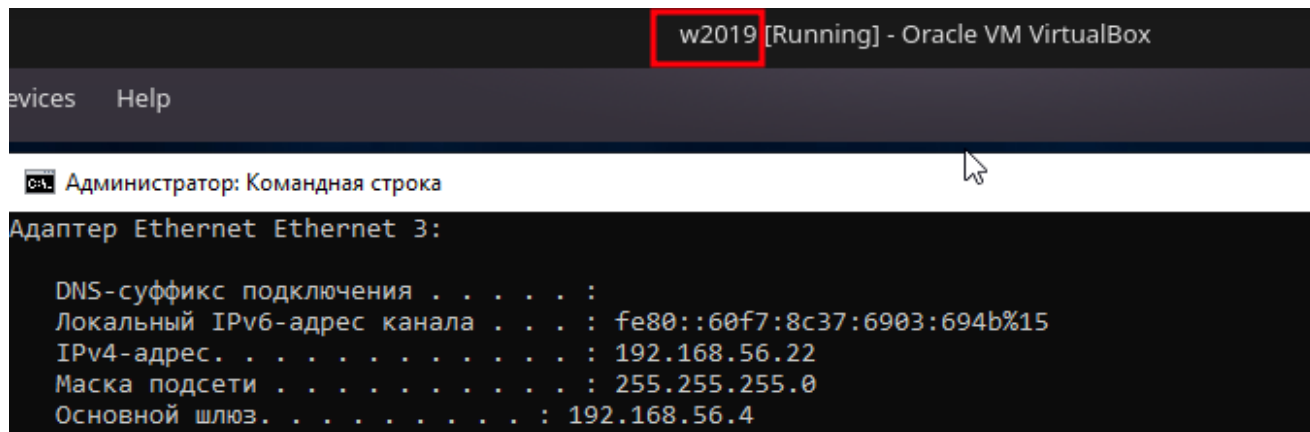
```
Основной шлюз. . . . . : 10.0.3.2

Адаптер Ethernet Ethernet 3:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::d573:b26d:2806:45ad%3
IPv4-адрес. . . . . : 192.168.56.16
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.56.4
```

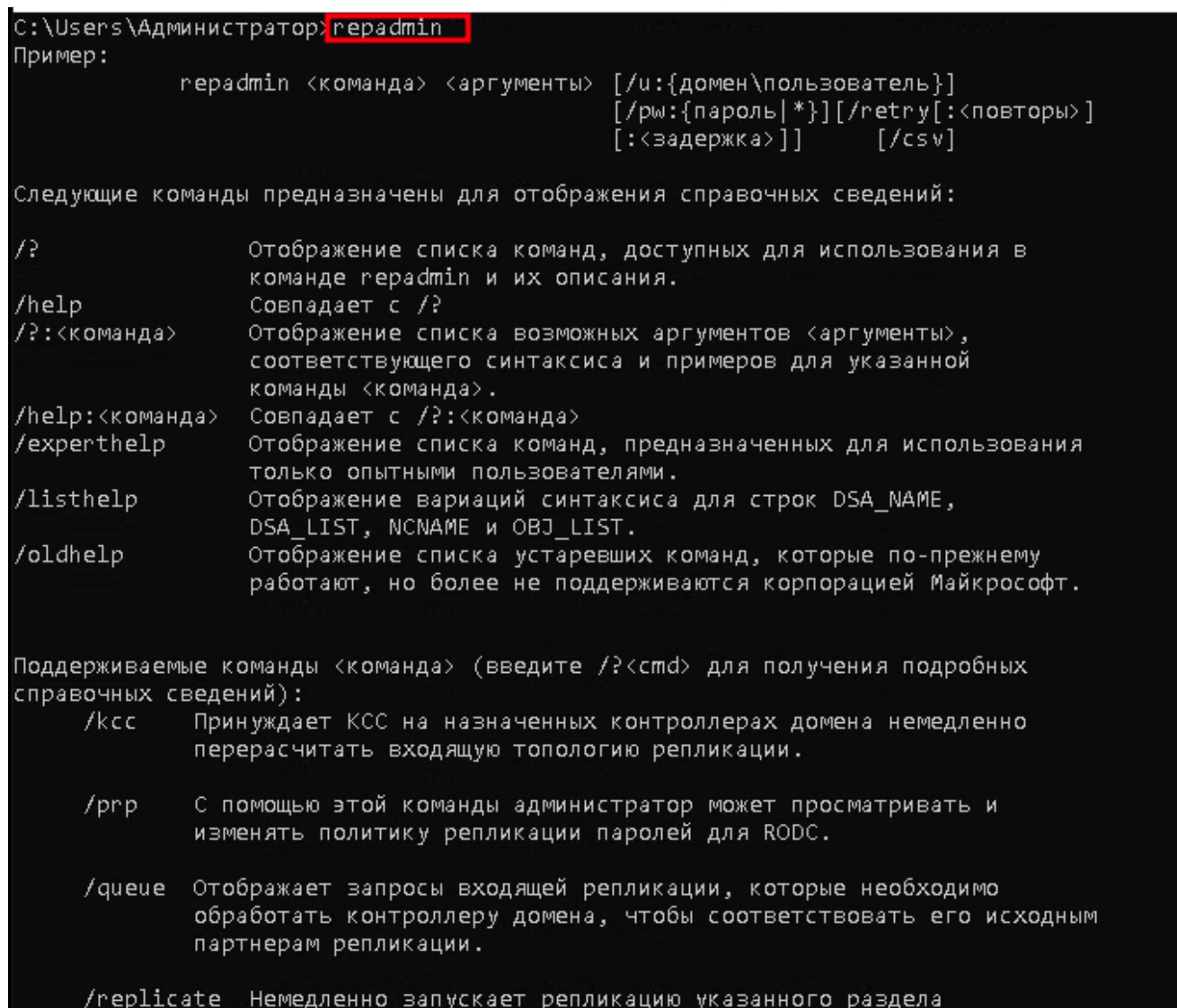
## PC2 w2019gui02





## Задание\_1:

Запустите утилиты repadmin /showrepl



```
C:\Users\Администратор>repadmin /showrepl
```

```
Repadmin: выполнение команды /showrepl контроллере домена localhost с полным доступом  
Default-First-Site-Name\W2019GUI01  
Параметры DSA: IS_GC  
Параметры сайта: (none)  
DSA - GUID объекта: a23e57d9-e9e5-414e-a008-38c0497cffd9  
DSA - код вызова: a23e57d9-e9e5-414e-a008-38c0497cffd9
```

## Задание\_2:

Запустите утилиту dcdiag /test:dns , /test:topology

dcdiag /test:dns

```
C:\Users\Администратор>dcdiag /test:dns
```

Диагностика сервера каталогов

Выполнение начальной настройки:

Выполняется попытка поиска основного сервера...

Основной сервер = w2019gui01

\* Определен лес AD.

Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\W2019GUI01

Запуск проверки: Connectivity

..... W2019GUI01 - пройдена проверка Connectivity

dcdiag /test:topology

```
C:\Users\Администратор>dcdiag /test:topology
```

Диагностика сервера каталогов

Выполнение начальной настройки:

Выполняется попытка поиска основного сервера...

Основной сервер = w2019gui01

\* Определен лес AD.

Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\W2019GUI01

Запуск проверки: Connectivity

..... W2019GUI01 - пройдена проверка Connectivity

Выполнение основных проверок

Сервер проверки: Default-First-Site-Name\W2019GUI01

Запуск проверки: Topology

..... W2019GUI01 - пройдена проверка Topology

Выполнение проверок разделов на: ForestDnsZones

Выполнение проверок разделов на: DomainDnsZones

Выполнение проверок разделов на: Schema

Выполнение проверок разделов на: Configuration

## Задание\_3:

Узнайте SID пользователя под учетной записью которого вошли в систему

- *whoami*

```
C:\Users\Администратор>whoami  
domain\администратор
```

domain\администратор

- *whoami /user (SID) or whoami /all*

```
C:\Users\Администратор>whoami /user
```

Сведения о пользователе

-----

Пользователь	SID
domain\администратор	S-1-5-21-3728292239-2069503345-307188935-500

```
C:\Users\Администратор>_
```

## Задание\_4:

Создайте защищенную от удаления ОП (OU)

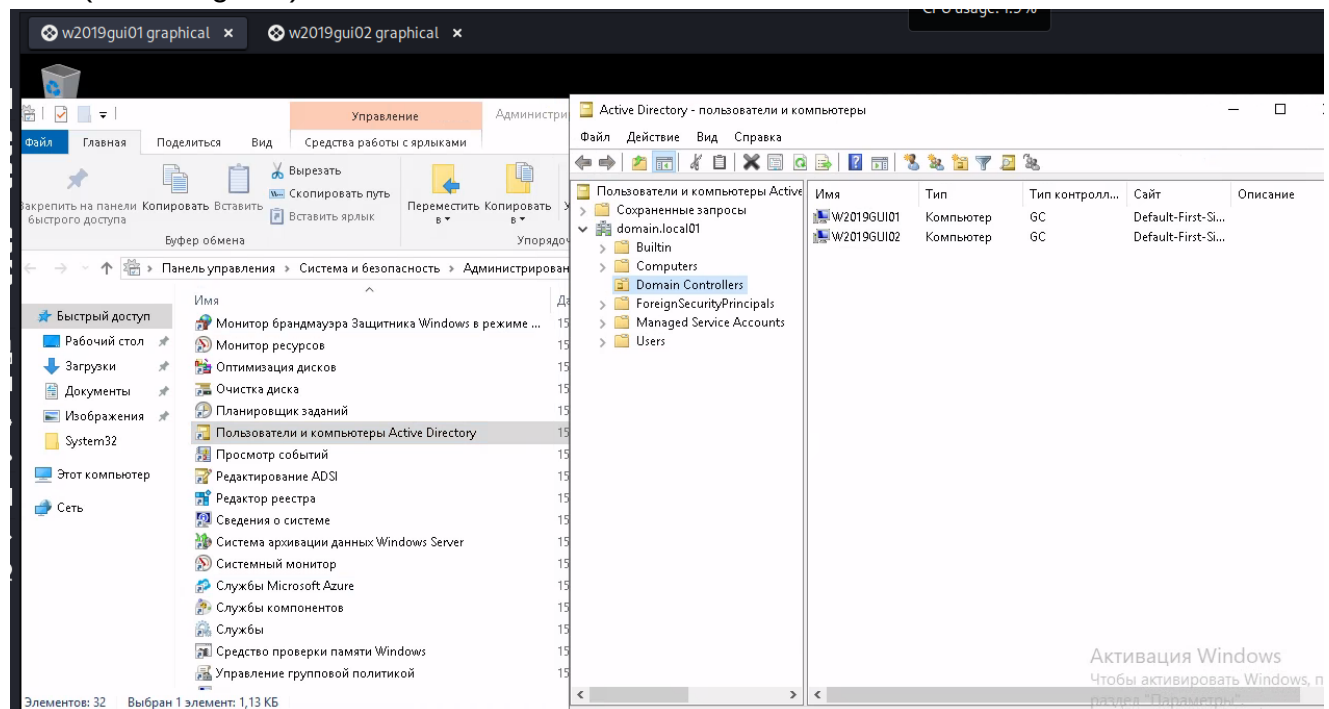
Создайте в ней учетные записи нескольких пользователей, компьютеров, группу



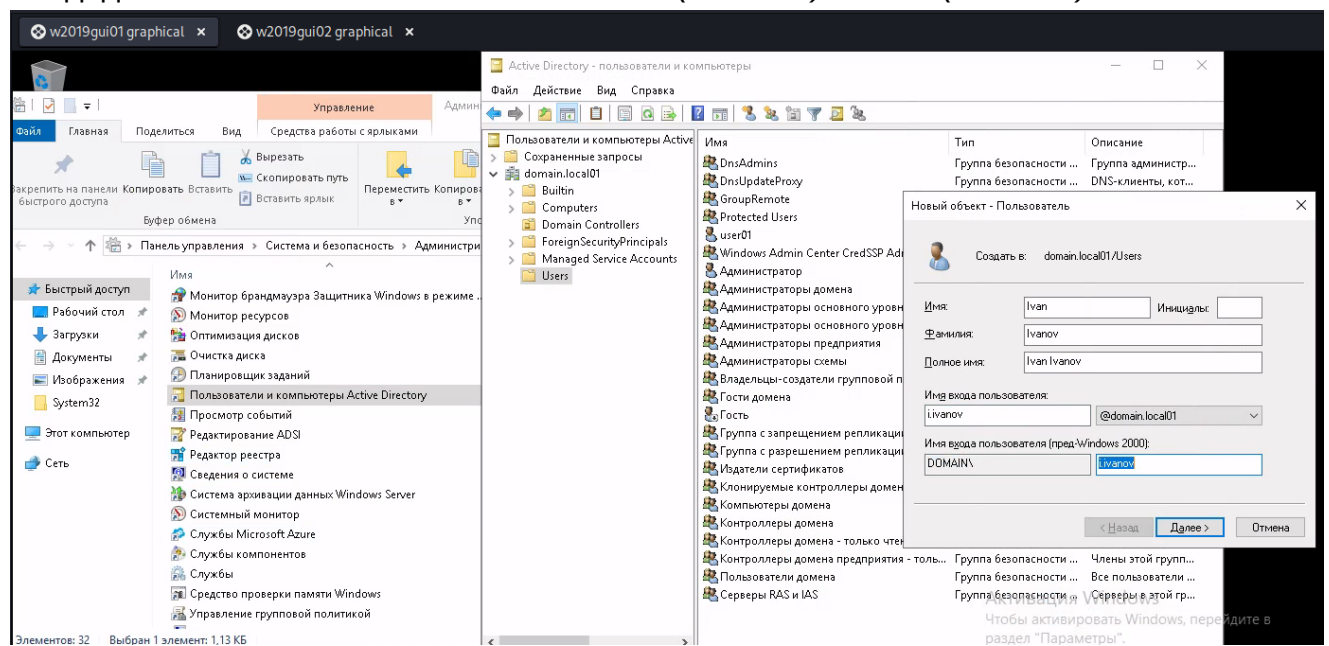
Добавьте пользователей в группу

Удалите созданную OU

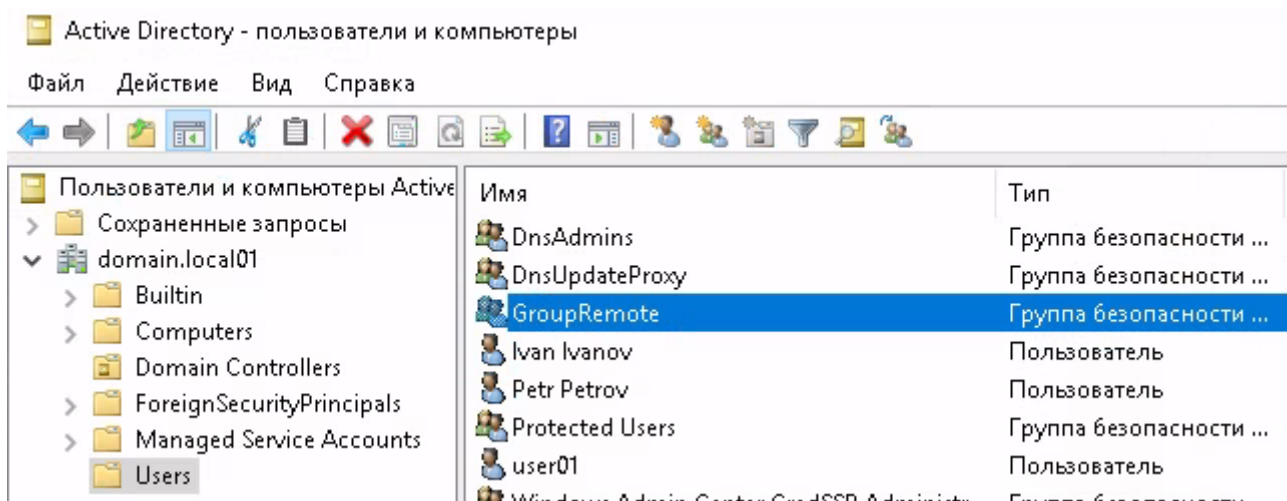
PC1 (win2019gui01)



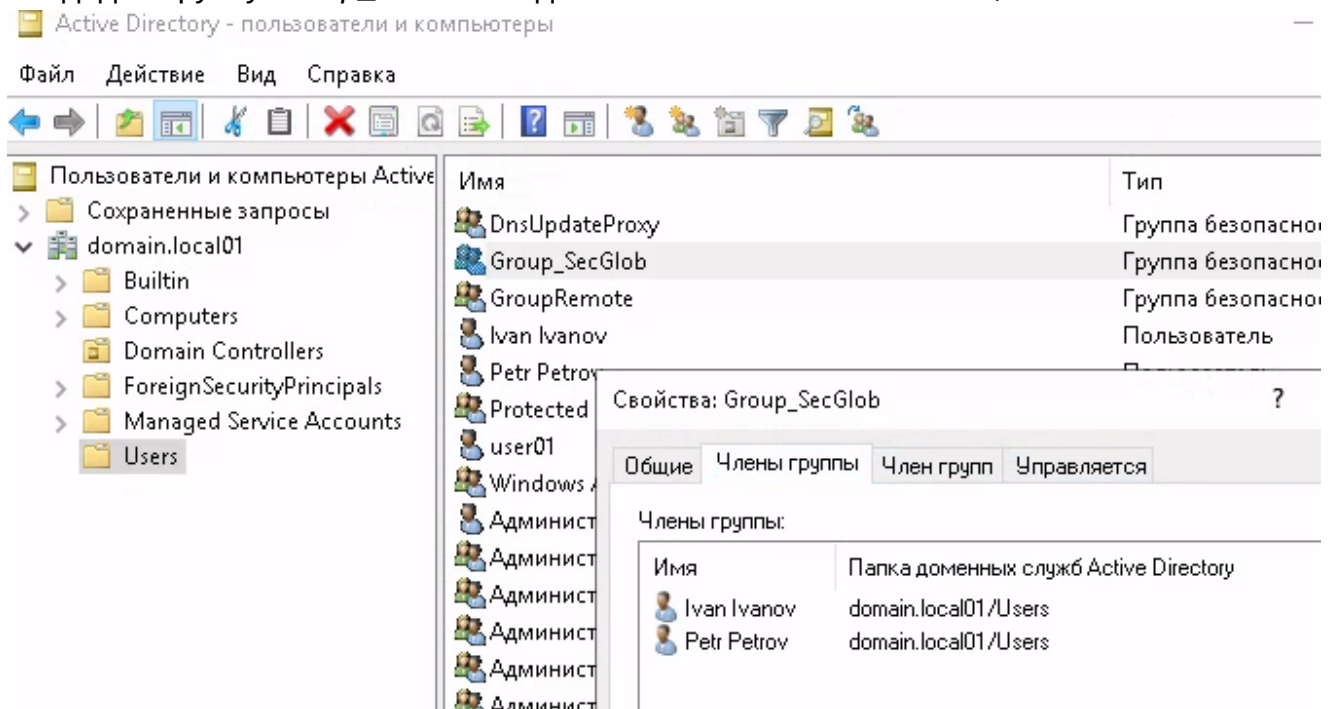
Создадим нескольких пользователей *Ivanov (Pass198)*, *Petrov (Pass198)*





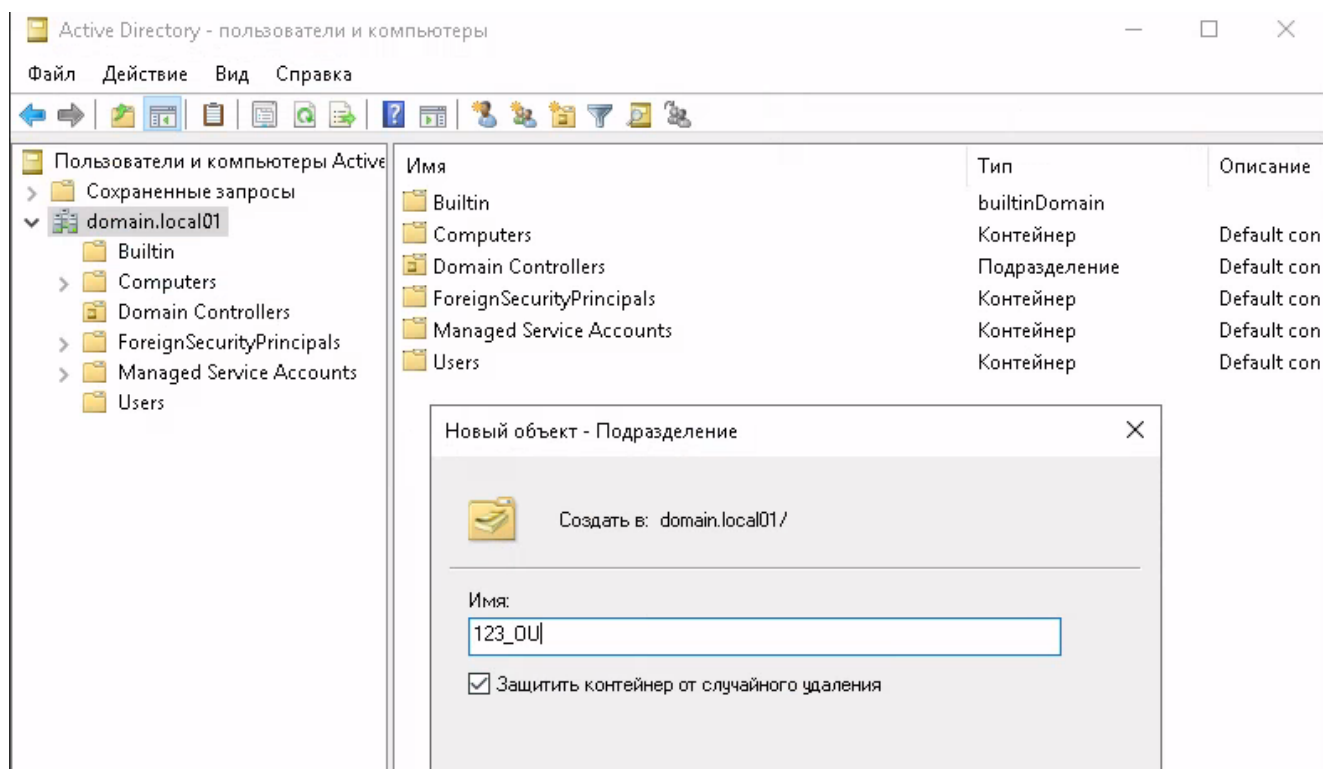


Создадим группу *Group\_SecGlob* и добавим пользователей *Ivanov*, *Petrov*

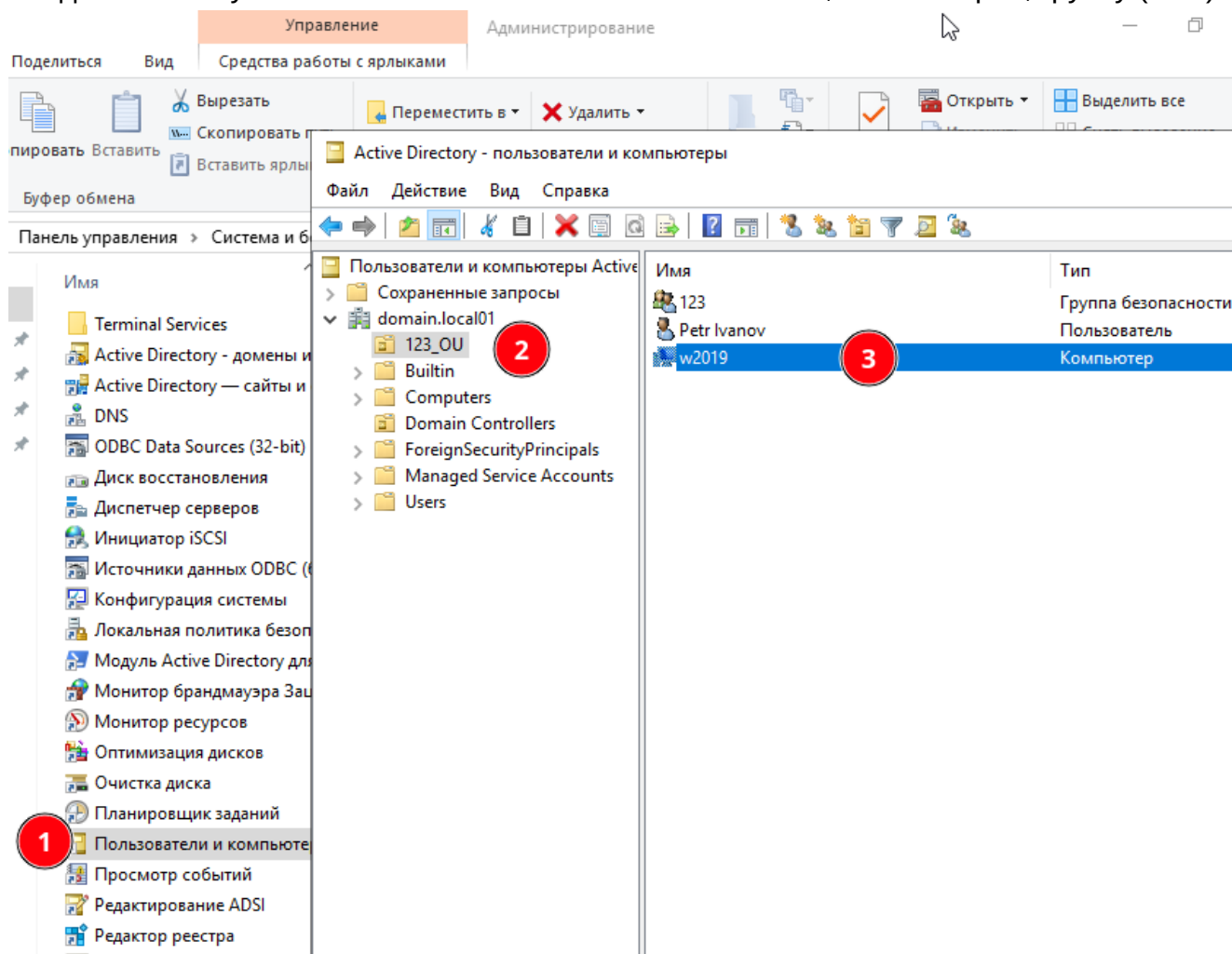


Создайте защищенную от удаления ОП (OU)

Создать подразделение (OU):



Создайте в ней учетные записи нескольких пользователей, компьютеров, группу (PC1):



Добавим новый компьютер PC3 w2019 (Windows 2019) в группу 123\_OU

```
-----
Параметры сетевого адаптера
-----

Индекс адаптера          3
Описание                 Intel(R) PRO/1000 MT Desktop Adapter #3
IP-адрес                 192.168.56.22   fe80::e47a:2003:db54:45ef
Маска подсети            255.255.255.0
DHCP включен             Ложь
Шлюз по умолчанию       192.168.56.4
Основной DNS-сервер      192.168.56.1
Альтернативный DNS-сервер 8.8.8.8

1) Установка адреса сетевого адаптера
2) Установить DNS-серверы
3) Очистить параметры DNS-сервера
4) Вернуться в главное меню
```

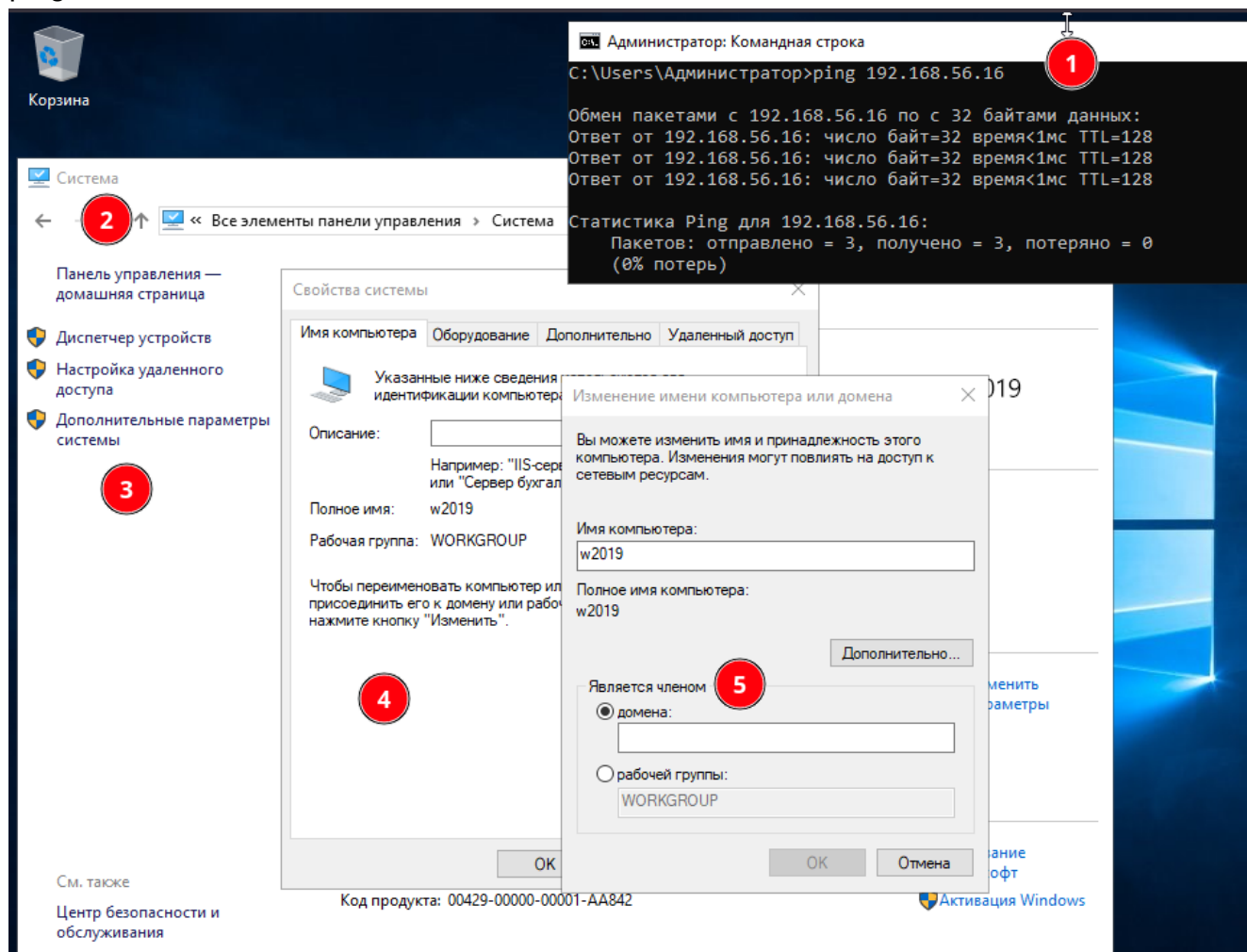
```
Администратор: Командная строка

Microsoft Windows [Version 10.0.17763.5329]
(c) Корпорация Майкрософт (Microsoft Corporation)

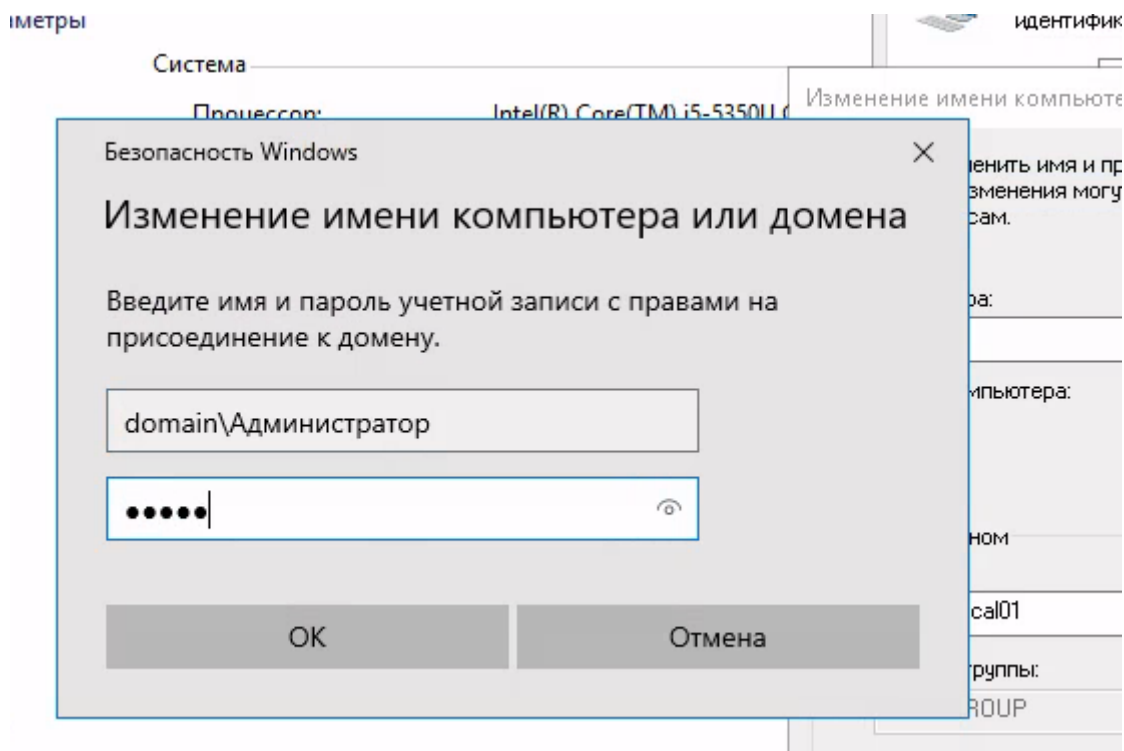
C:\Users\Администратор>whoami
w2019\администратор
```

Добавляем в сеть (PC3):

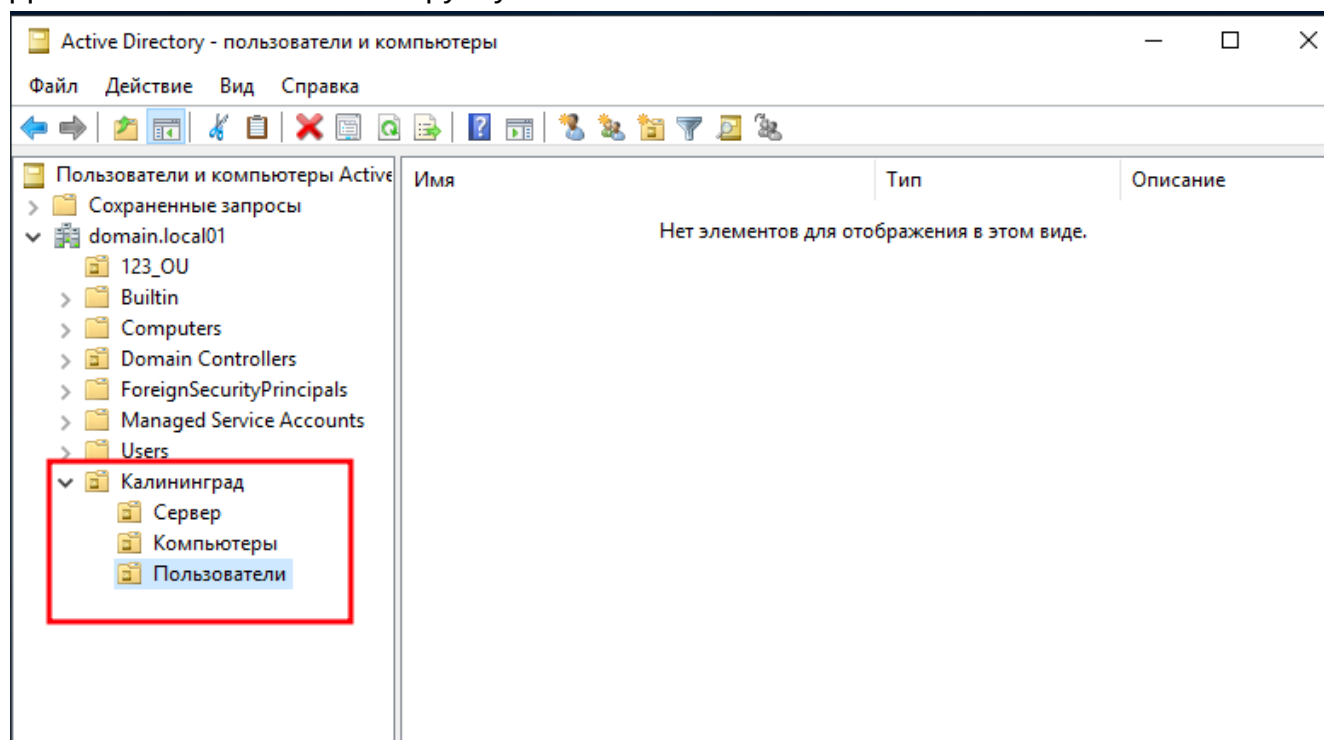
ping PC1



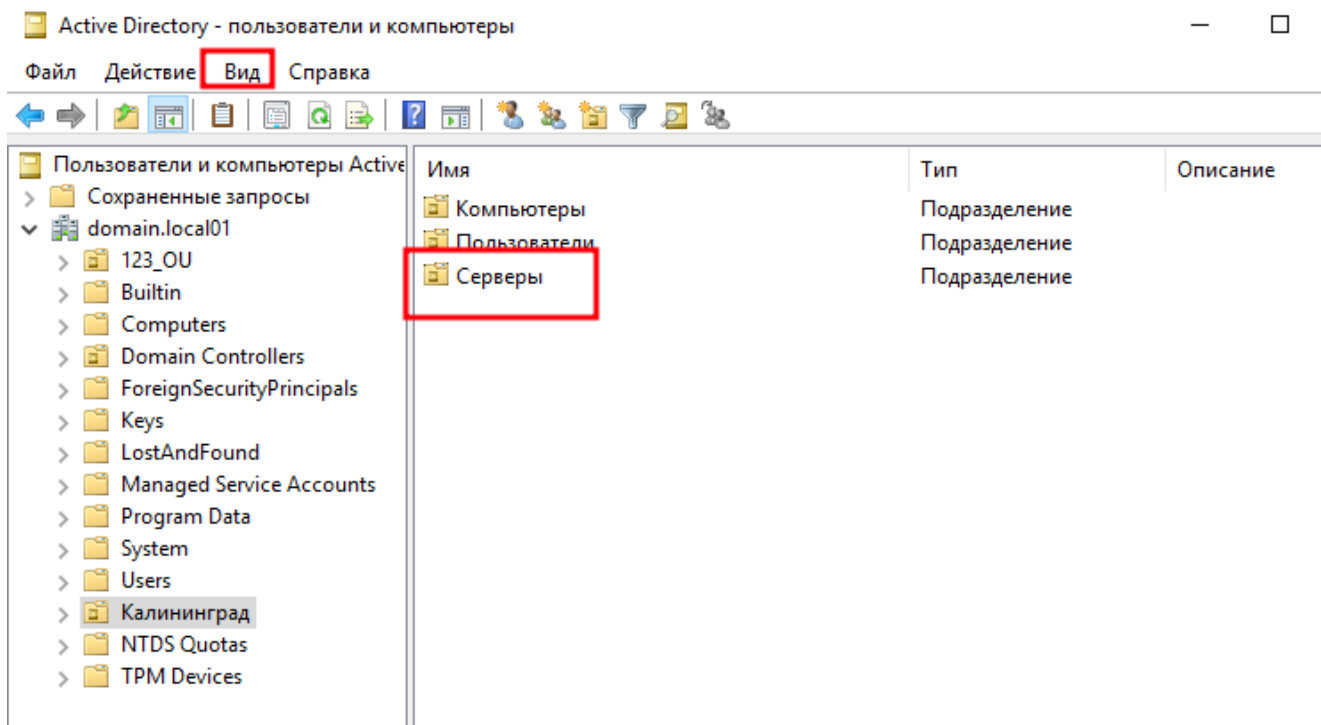
domain.local01



Добавьте пользователей в группу

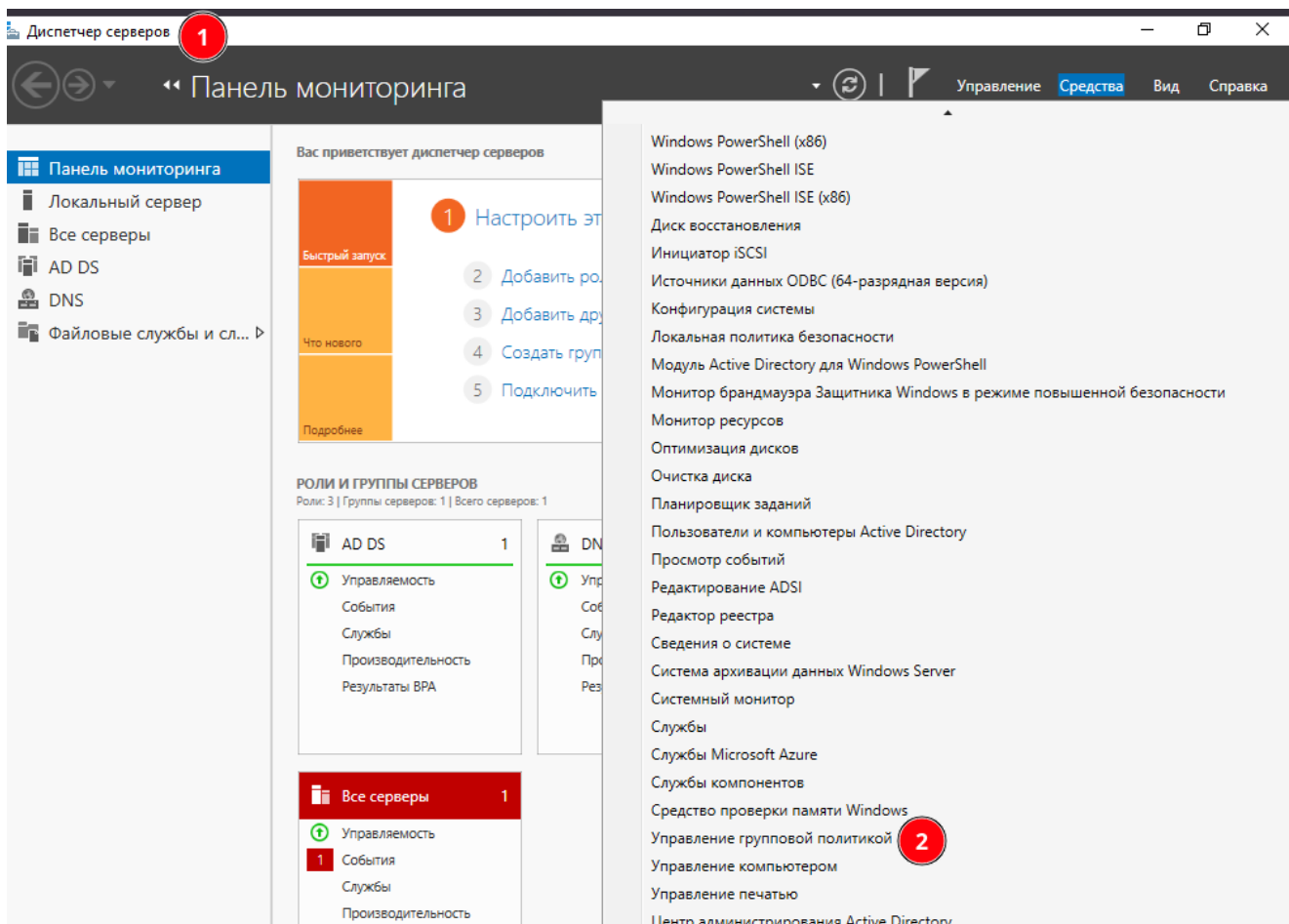


Переименовать ... удалить: Вид - Дополнительные компоненты  
Удалите созданную OU



## Задание\_5:

Создайте групповую политику (GPO) с блокировкой ссылки "Игры" и подключите к любой OU



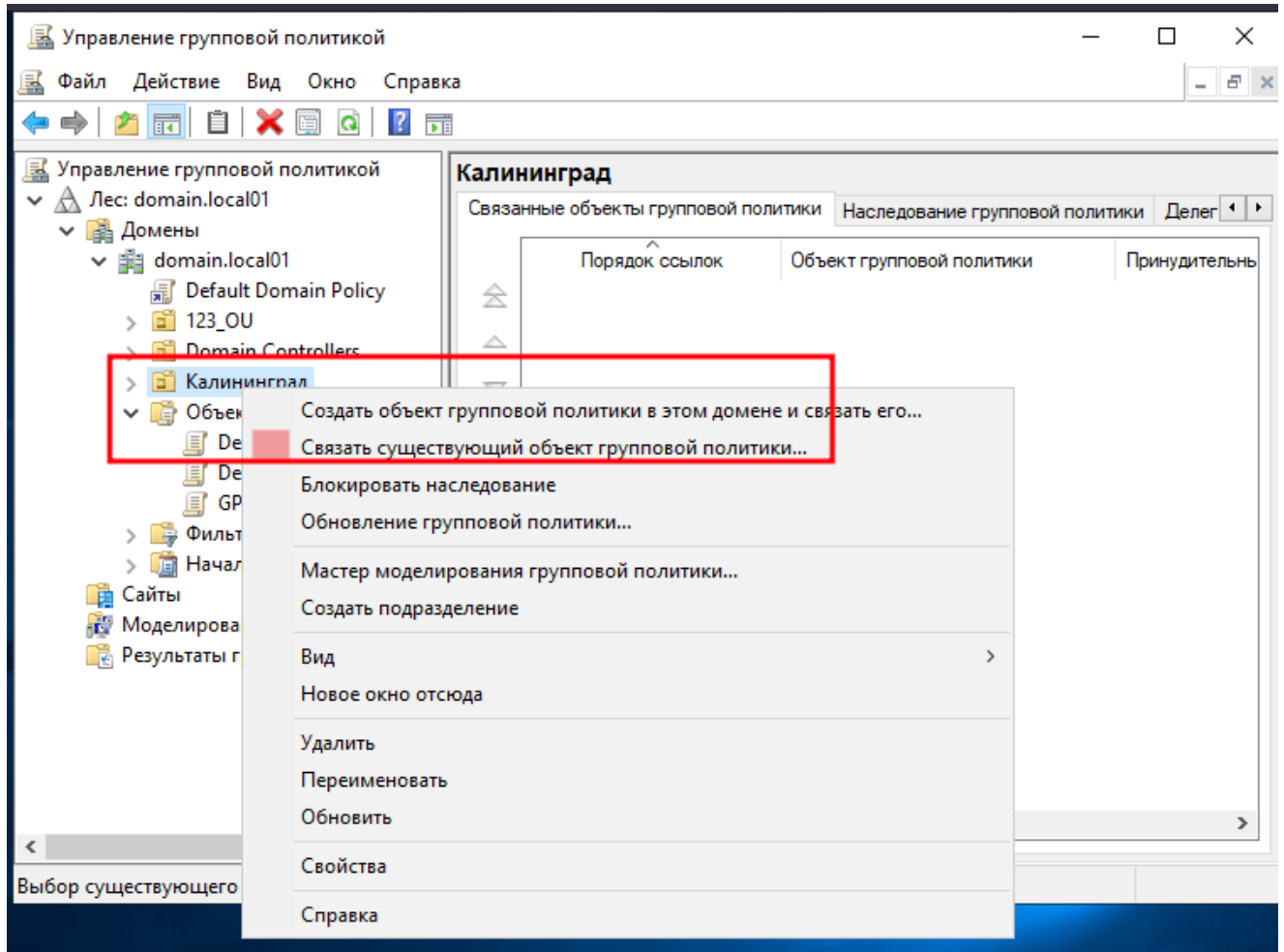
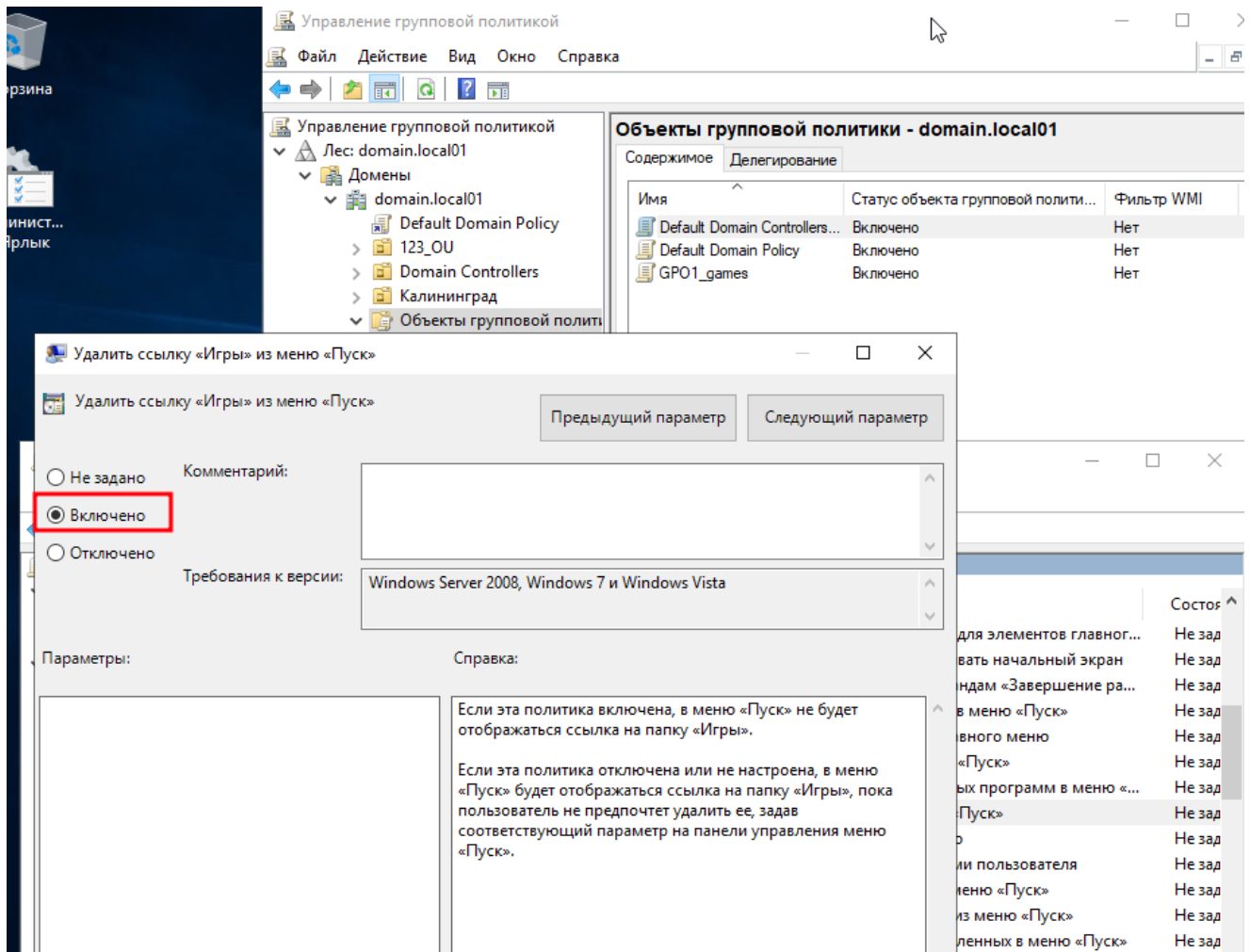


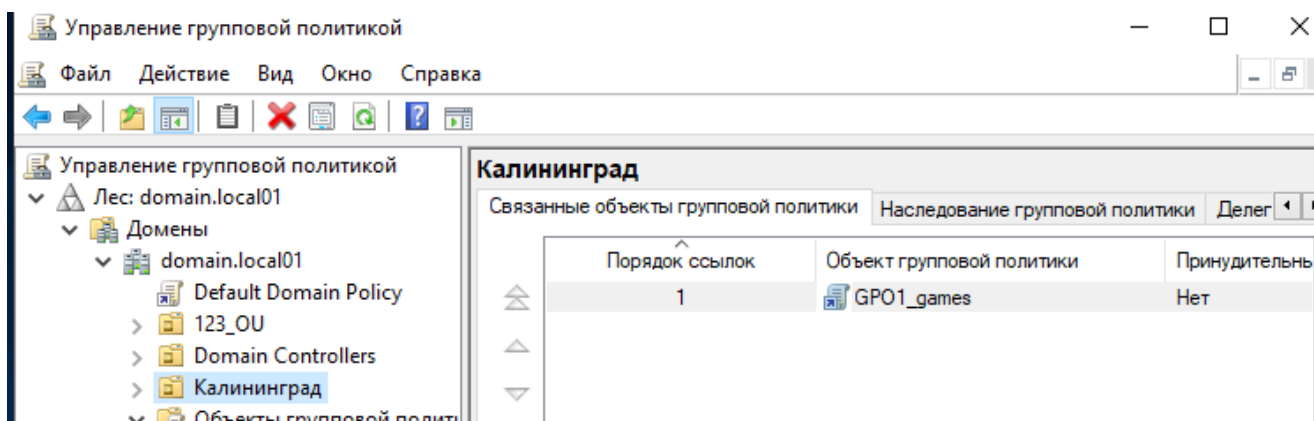
The screenshot displays the Windows 7 desktop environment. The top taskbar shows the Start button, a search bar, and several pinned applications. The desktop background is the standard Windows 7 blue logo wallpaper. Two windows are open:

- Group Policy Management Console (gpmc.msc):** This window is titled "Управление групповой политикой". The left-hand tree view shows the hierarchy: "Лес: domain.local01" > "Домены" > "domain.local01". Under "domain.local01", the "Объекты групповой политики" (Group Policy Objects) folder is selected, highlighted with a red circle labeled "1".
- Group Policy Editor (gpoedit.msc):** This window is titled "Редактор управления групповыми политиками". It shows the "Меню «Пуск» и панель задач" (Start Menu and Taskbar) policy. The "Состояние" (State) column on the right lists various settings. The setting "Удалить ссылку «Игры» из меню «Пуск»" (Remove the Games link from the Start menu) is selected, highlighted with a red circle labeled "4".

Other visible elements include the "Объекты групповой политики - domain.local01" pane in the top right of the GPMC window, which lists several GPOs, including "GPO1\_games" (highlighted with a red circle labeled "2"). The "Изменить" (Change) button is visible below this list. The "Групповые политики" (Group Policies) folder is also visible in the left tree of the GPMC window.



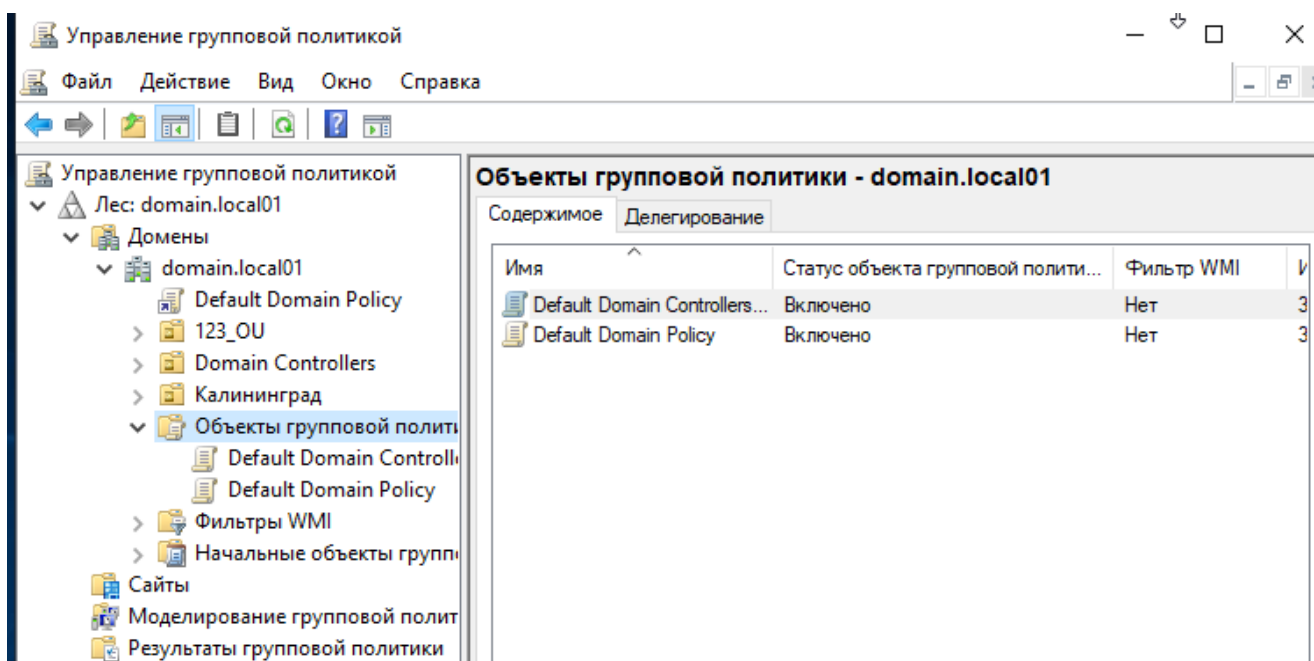




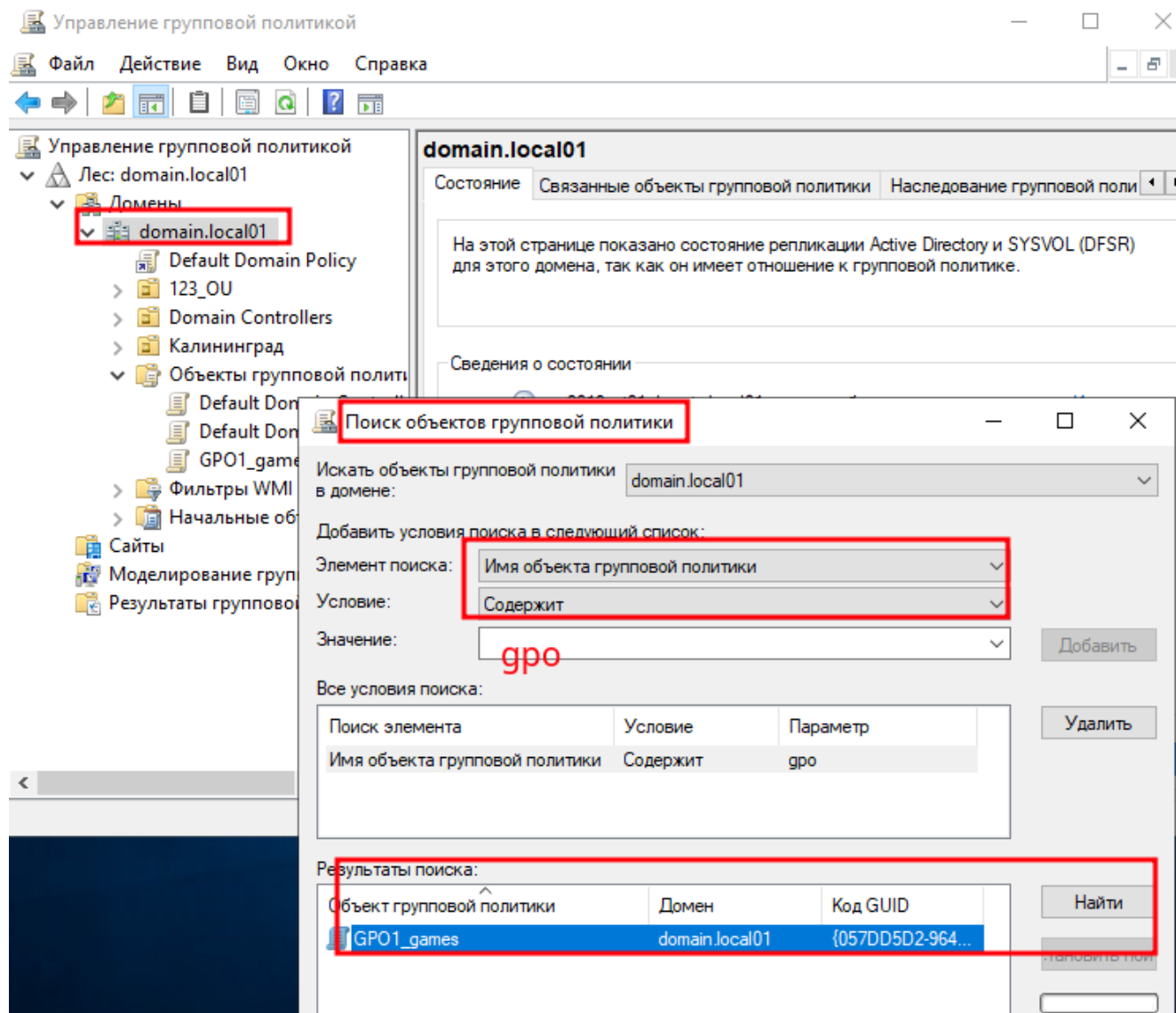
Удалите созданную GPO

**Вид - Дополнительные компоненты**

и удаляем ...

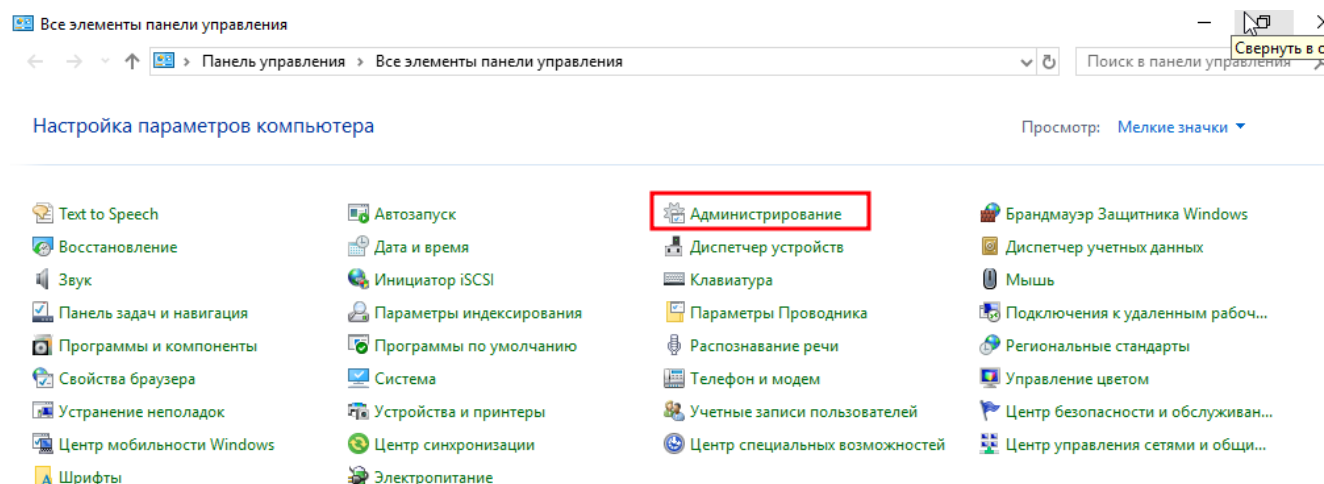


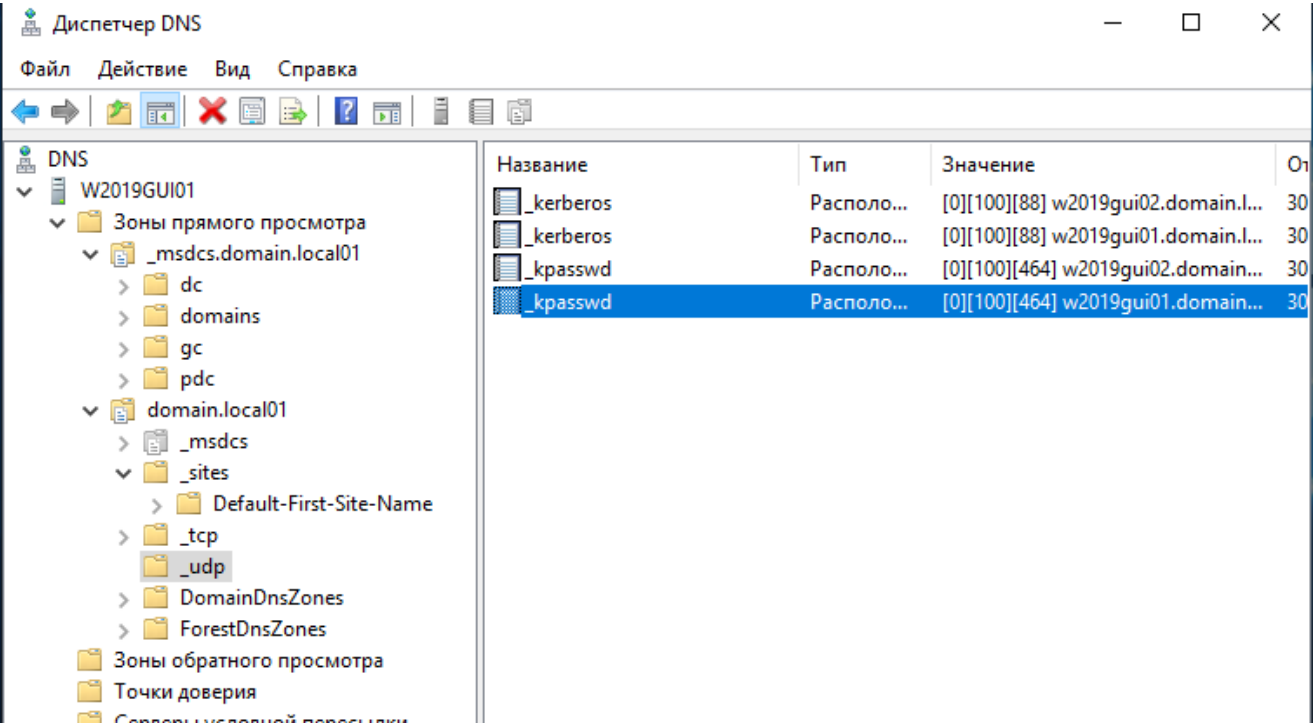
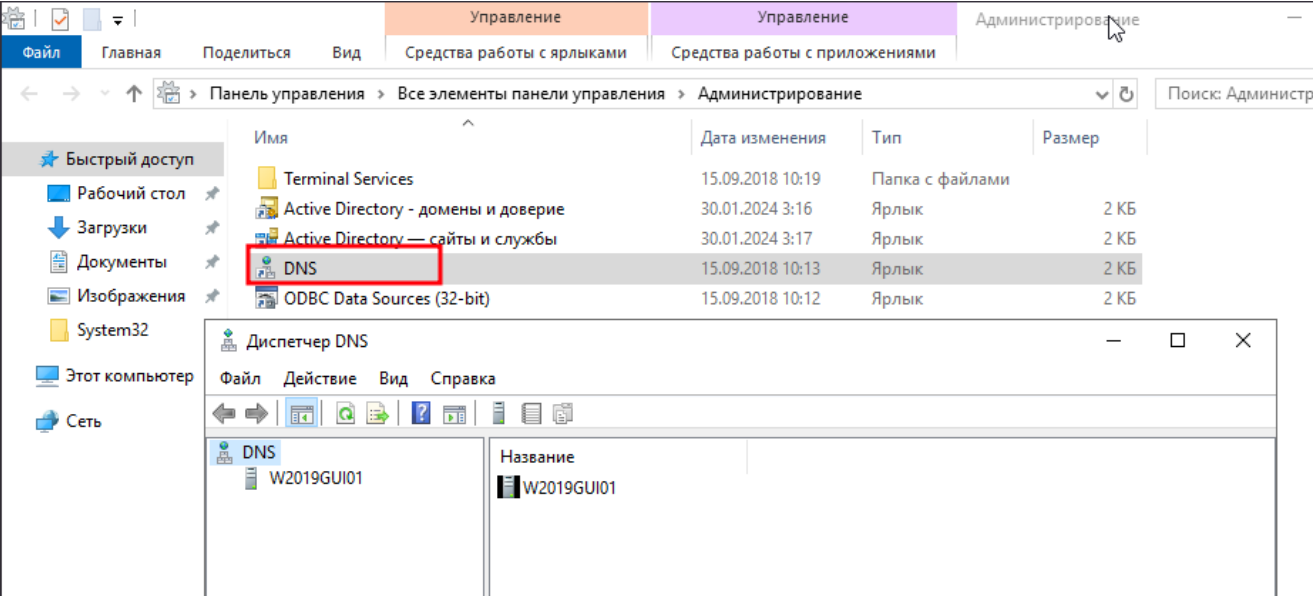
## Дополнительно: поиск GPO



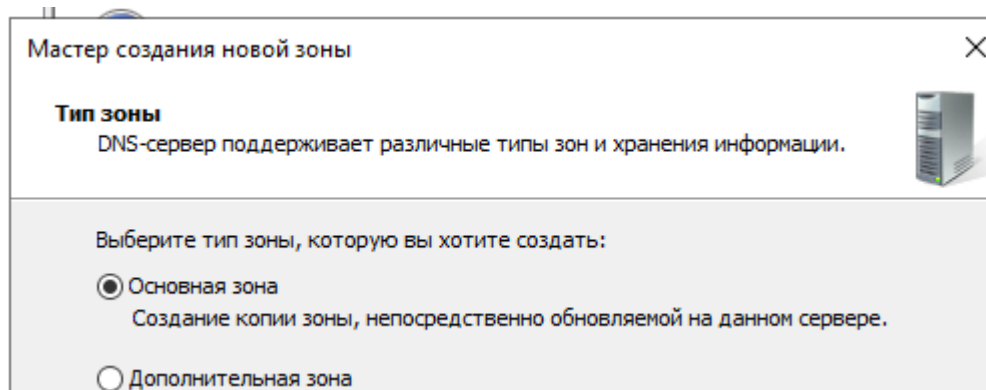
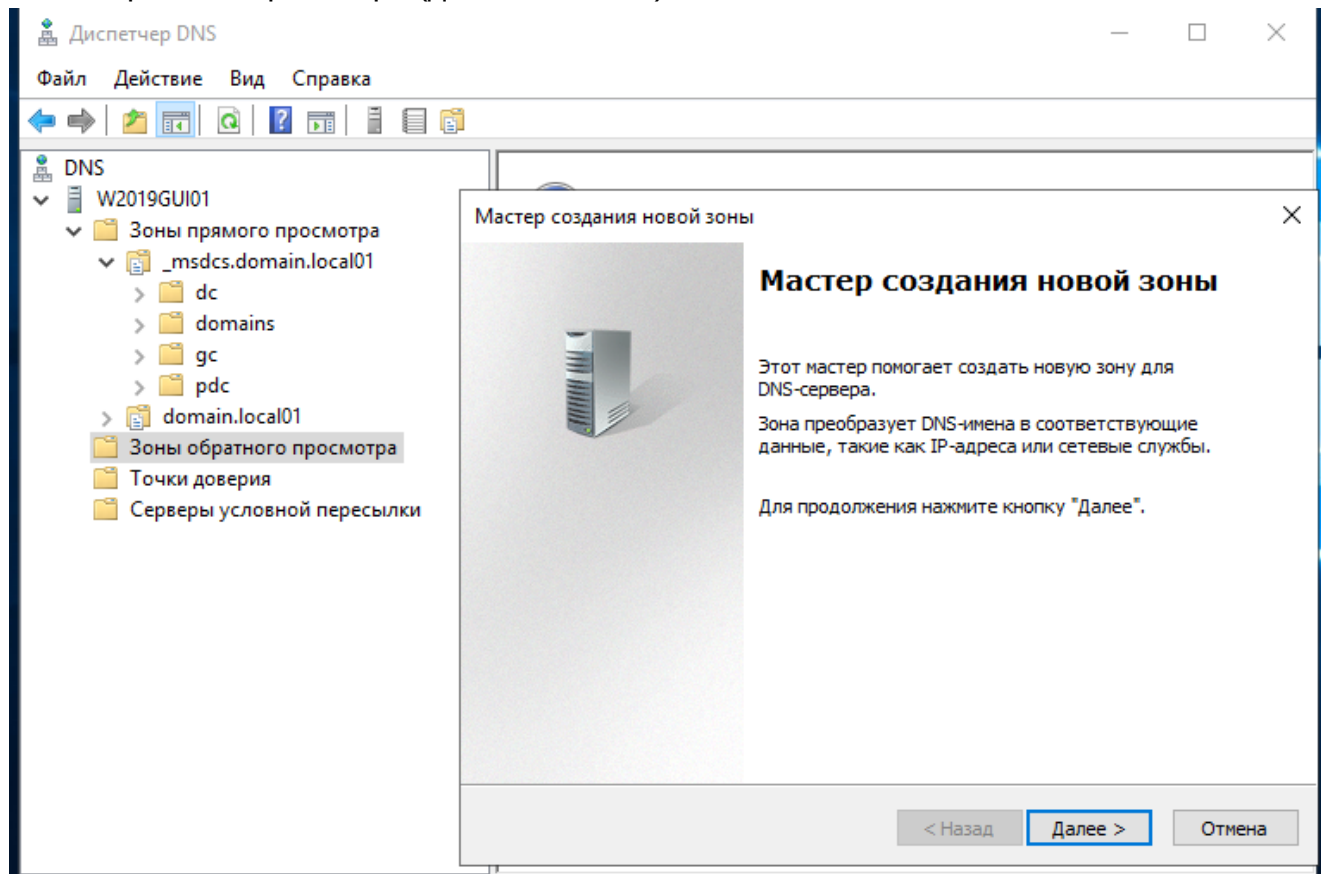
## Задание\_6:

Добавьте в качестве сервера пересылки адрес 8.8.8.8  
Сделайте простой и рекурсивный запросы к DNS серверу





## Зона обратного просмотра (дополнительно)



### Имя зоны обратного просмотра

Зона обратного просмотра преобразует IP-адреса в DNS-имена.



Укажите, хотите ли вы создать зону обратного просмотра для IPv4-адресов или IPv6-адресов.

☒ Зона обратного просмотра IPv4

#### DNS

W2019GUI01

Зоны прямого просмотра

\_msdcs.domain.local01

dc

domains

gc

pdc

domain.local01

Зоны обратного просмотра

Точки доверия

Серверы условной пересылки

### Мастер создания новой зоны

### Имя зоны обратного просмотра

Зона обратного просмотра преобразует IP-адреса в DNS-имена.



Можно задать зону обратного просмотра, указав идентификатор сети или имя этой зоны.

☒ Идентификатор сети:

192 .168 .56 .

Идентификатор сети - это часть IP-адресов, которые принадлежат данной зоне. Введите идентификатор сети в обычном (не в обратном) порядке.

При явном использовании нуля в идентификаторе сети он появится в имени зоны. Например, идентификатор сети '10' будет соответствовать зоне '10.in-addr.arpa', а идентификатор сети '10.0' будет соответствовать зоне '0.10.in-addr.arpa'.

☐ Имя зоны обратного просмотра:

56.168.192.in-addr.arpa

#### Диспетчер DNS

Файл Действие Вид Справка



#### DNS

W2019GUI01

Зоны прямого просмотра

\_msdcs.domain.local01

dc

domains

gc

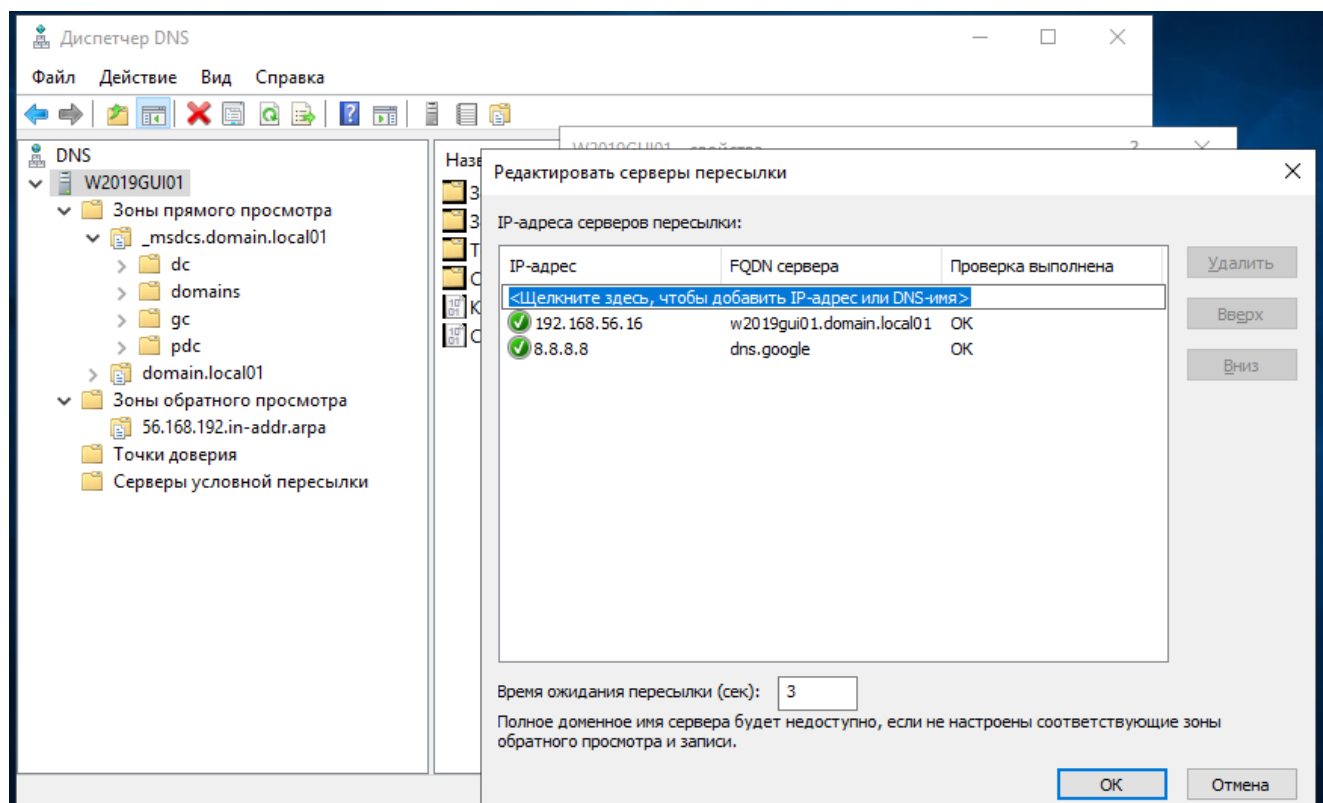
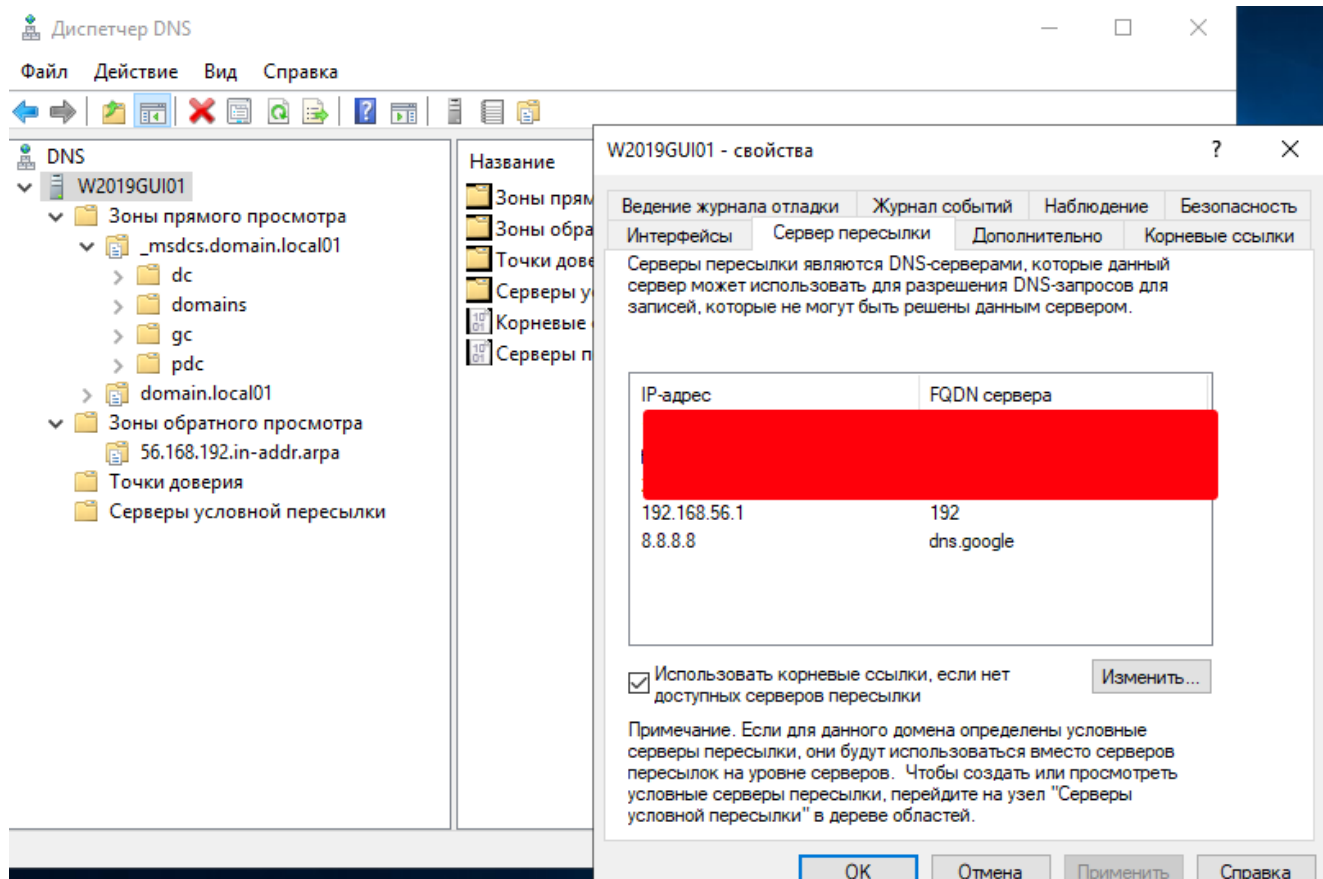
pdc

domain.local01

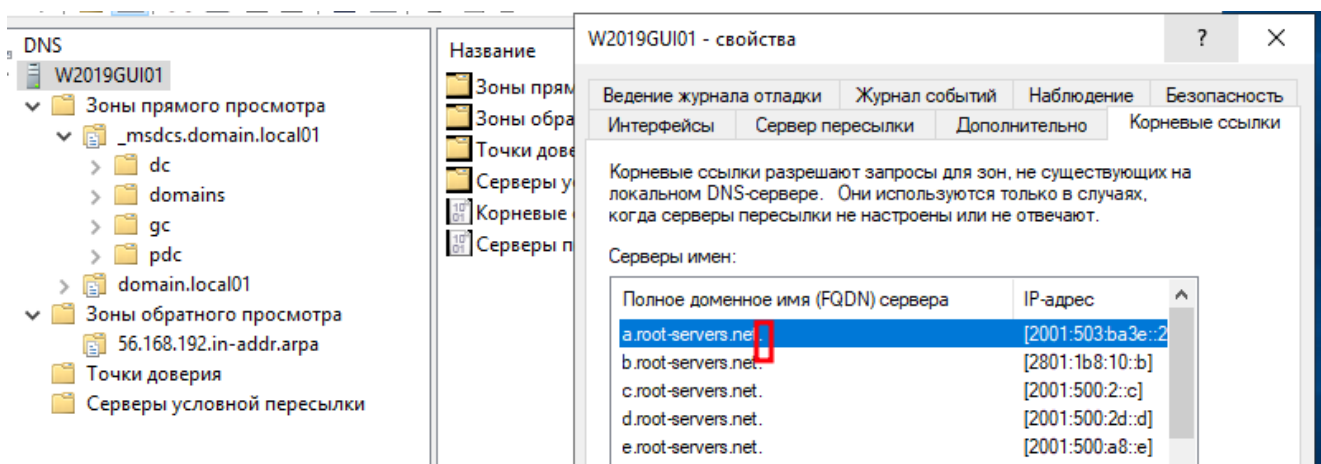
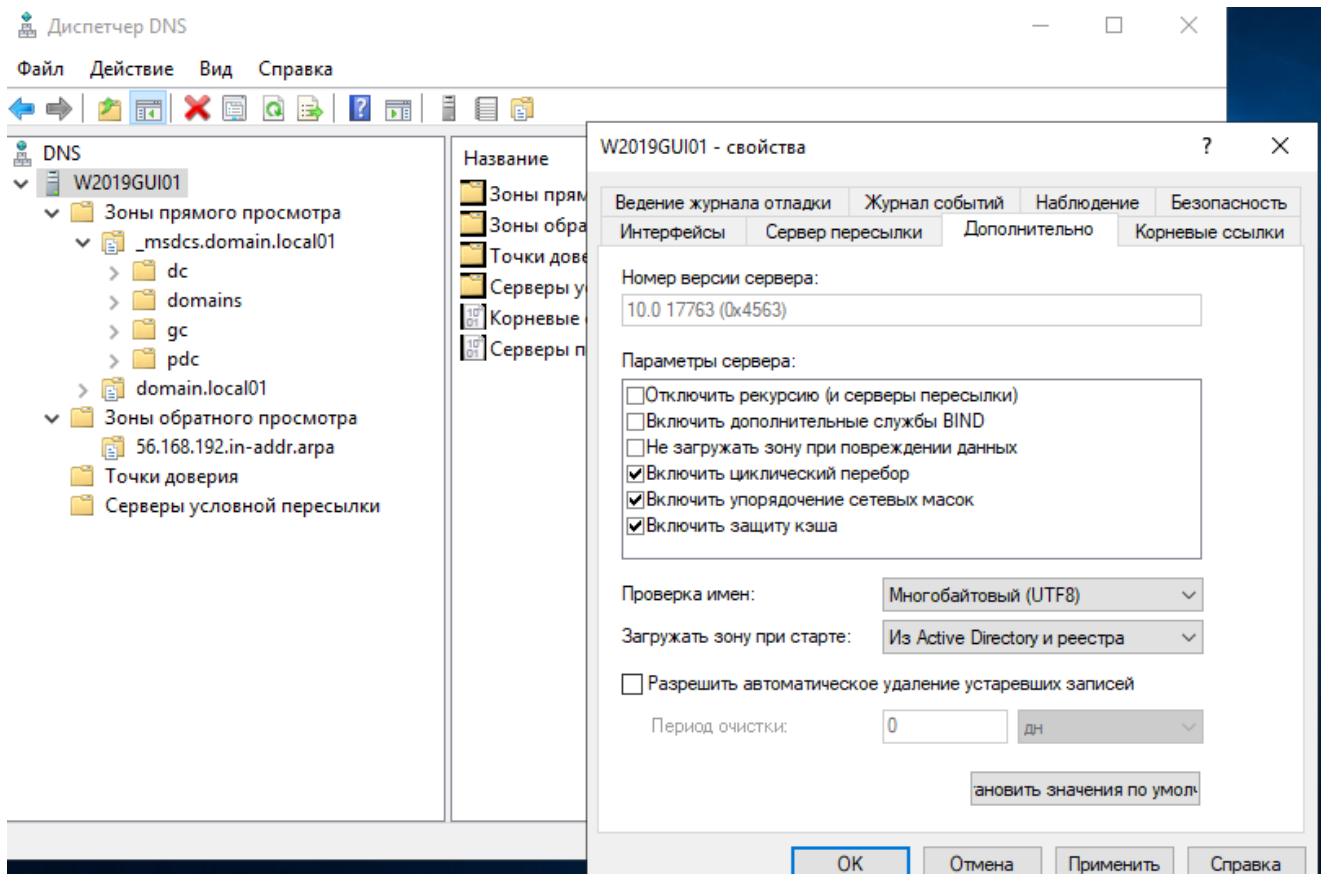
Зоны обратного просмотра

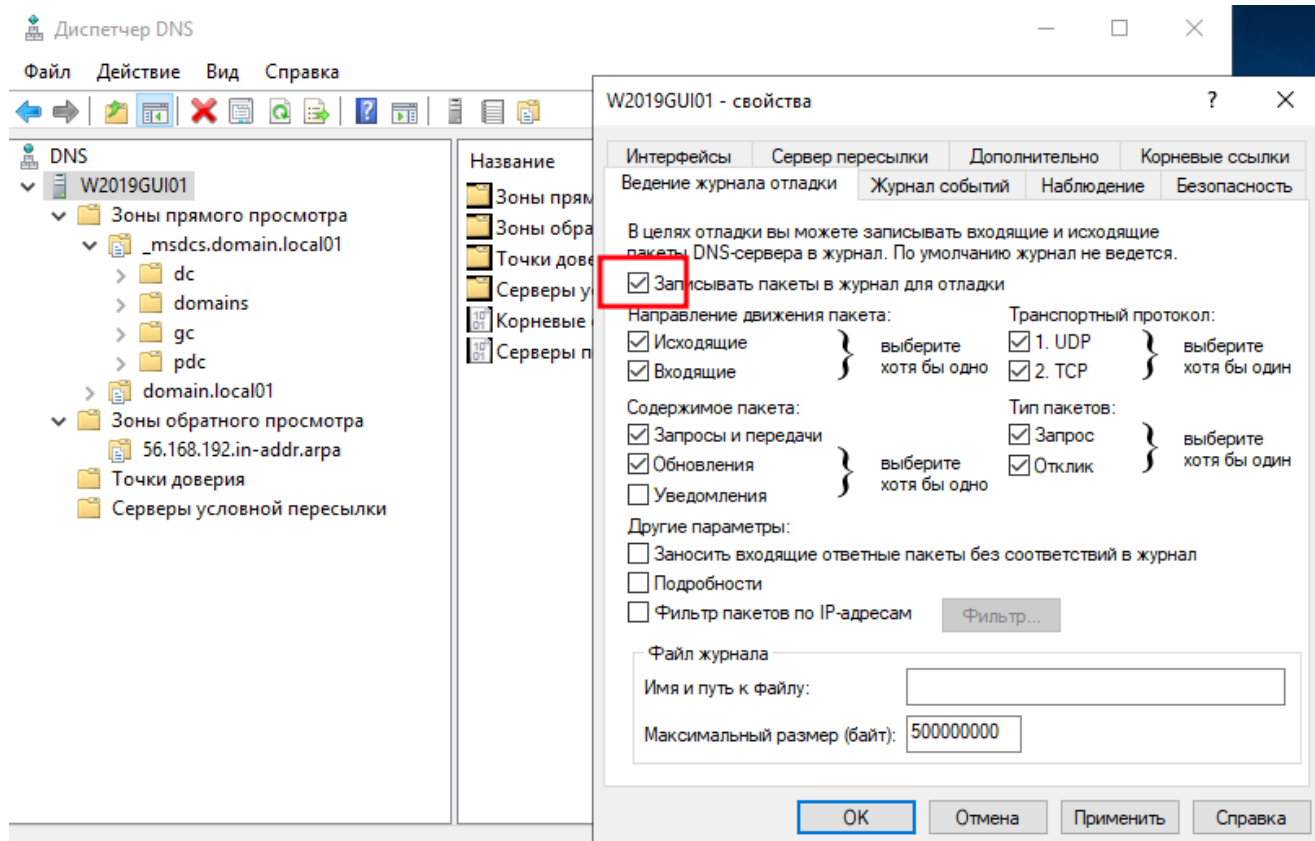
Название	Тип	Состояние	Со
56.168.192.in-addr.arpa	Интегрированная в Active Di...	Выполняется	Не

## Сервер пересылки адрес 8.8.8.8

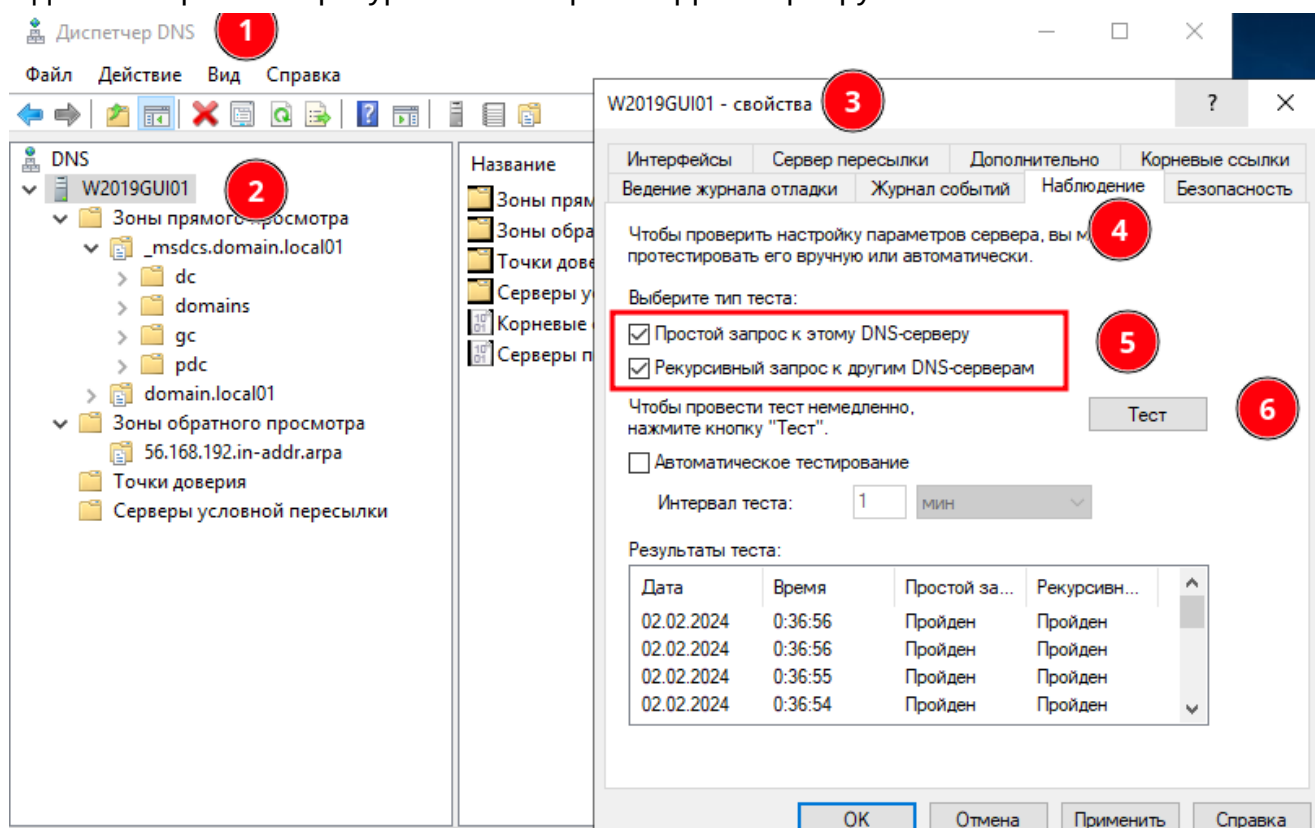


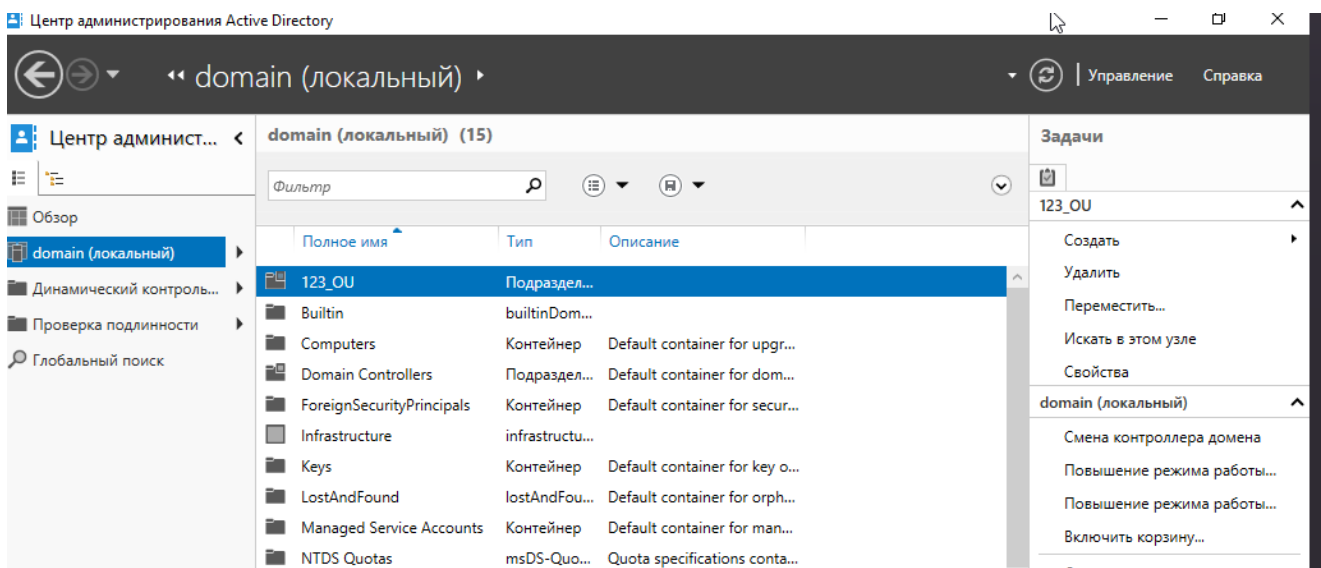
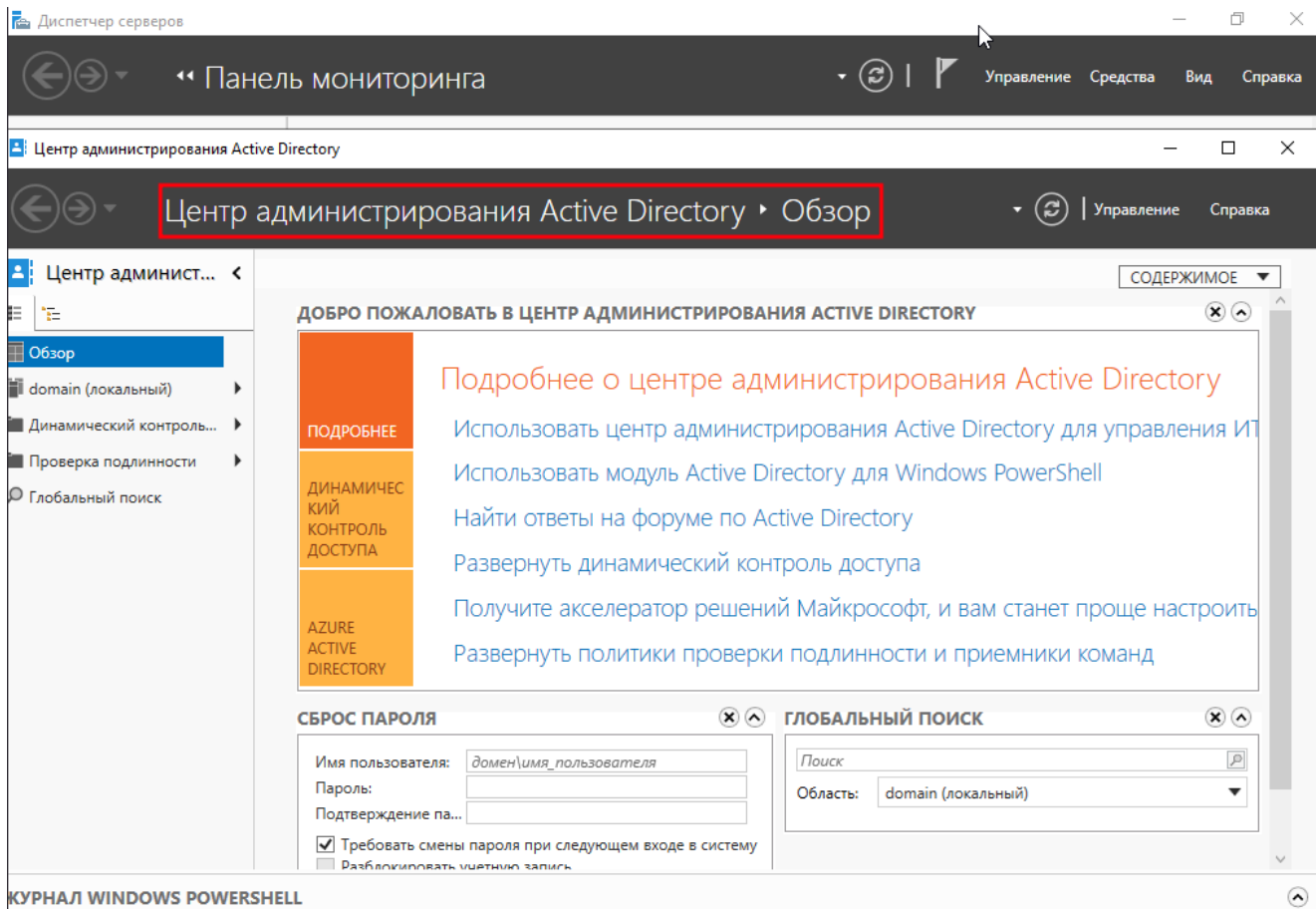


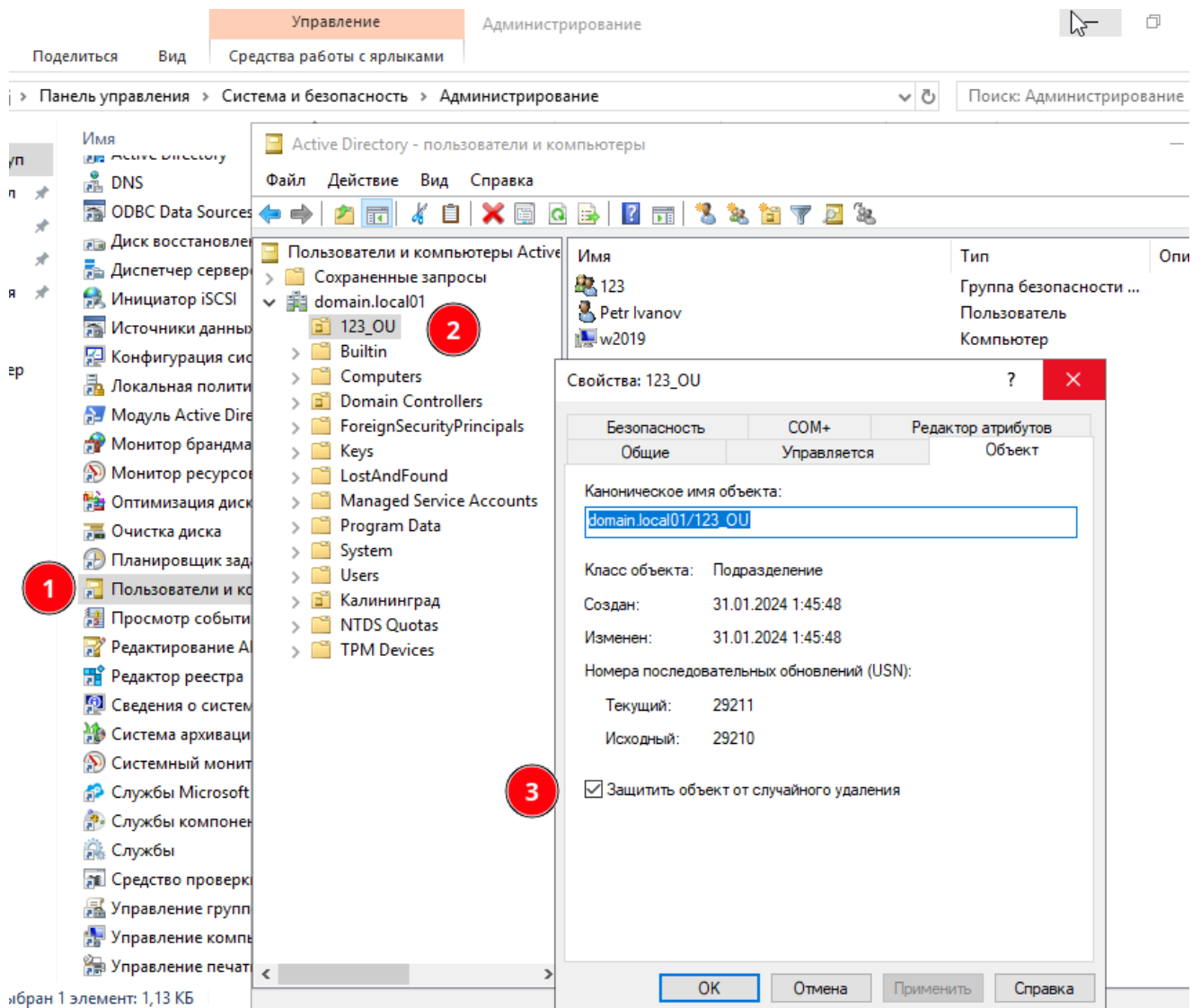




Сделайте простой и рекурсивный запросы к ДНС серверу

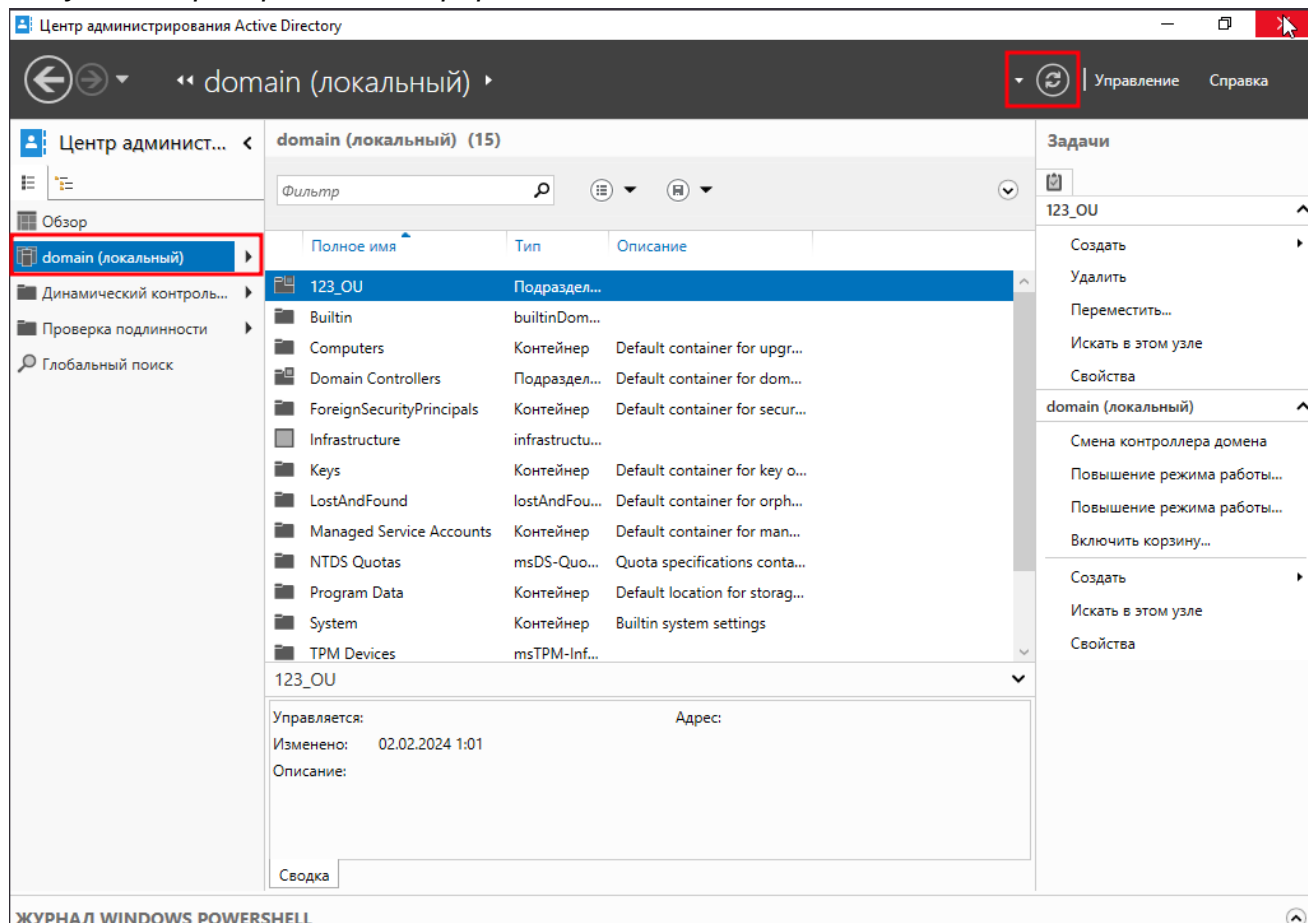




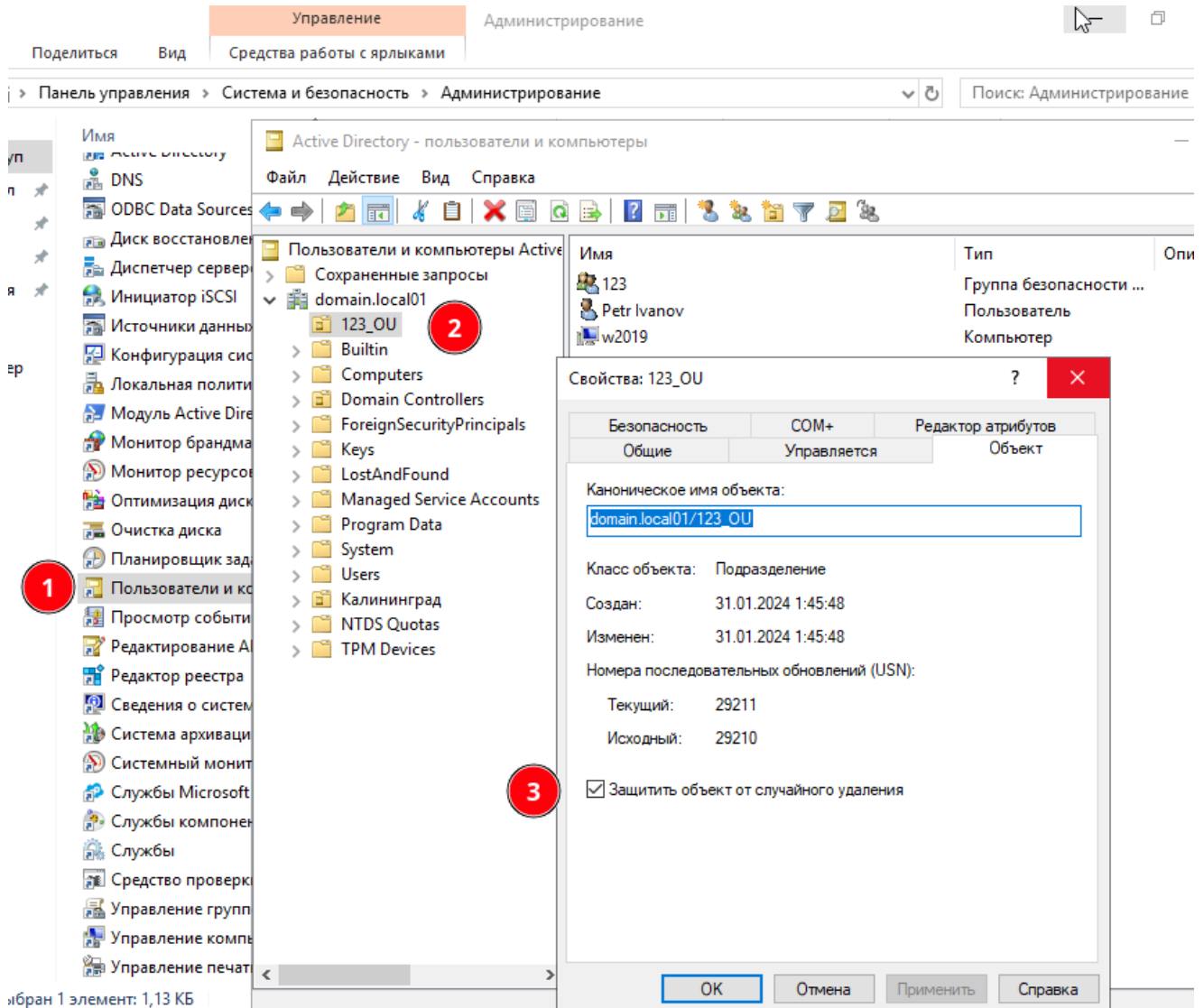


Удаляем УЕшку 123\_OU и далее пробуем ее восстановить

## Запускаем Центр администрирования



## Удаляем УЕшку



Ищем в разделе *Deleted Objects* в *Центре администрирования (domain)* ...

## Задание\_7:

Использую утилиту NTDSUtil и оснастки AD передайте две роли на второй контроллер домена

Владельцы fsmo

```
C:\Users\Администратор>netdom query fsmo
Хозяин схемы w2019gui01.domain.local01
Хозяин именования доменов w2019gui01.domain.local01
PDC w2019gui01.domain.local01
Диспетчер пула RID w2019gui01.domain.local01
Хозяин инфраструктуры w2019gui01.domain.local01
Команда выполнена успешно.
```

ntdsutil

```
C:\Users\Администратор>ntdsutil
ntdsutil: ?

? - Вывод этой справочной информации
Activate Instance %s - Устанавливает "NTDS" или определенный экземпляр AD LDS
                        в качестве активного экземпляра.
Authoritative restore - Принудительно восстановить базу данных DIT
Change Service Account %s1 %s2 - Измените учетную запись службы AD DS/LDS на
                                имя пользователя %s1 и пароль %s2.
                                Используйте "NULL" для пустого пароля или "*" для
                                ввода пароля с консоли.
Configurable Settings - Управление настраиваемыми параметрами
DS Behavior - Просмотр и изменение режима работы AD DS/LDS
Files - Управление файлами DS/LDS-базы данных AD
Group Membership Evaluation - Оцените идентификаторы безопасности в токене для
```

```
ntdsutil: roles
fsmo maintenance: con
server connections: con to ser w2019gui01
Привязка к w2019gui01 ...
Подключен к w2019gui01 с помощью учетных данных локального пользователя.
server connections: q
fsmo maintenance: ?

? - Вывод этой справочной информации
Connections - Подключение к определенному DC/LDS-экземпляру AD
Help - Вывод этой справочной информации
Quit - Возврат к предыдущему меню
Seize infrastructure master - Переписать роль инфраструктуры на подключенном сервере
Seize naming master - Переписать роль хозяина именования на подключенном сервере
Seize PDC - Переписать роль PDC на подключенном сервере
Seize RID master - Переписать роль RID на подключенном сервере
Seize schema master - Переписать роль схемы на подключенном сервере
Select operation target - Выбор сайтов, серверов, доменов, ролей, контекстов именования
Transfer infrastructure master - Сделать подключенный сервер хозяином инфраструктуры
Transfer naming master - Сделать подключенный сервер хозяином именования
Transfer PDC - Сделать подключенный сервер PDC
Transfer RID master - Сделать подключенный сервер хозяином RID
Transfer schema master - Сделать подключенный сервер хозяином схемы

fsmo maintenance: _
```

## Задание\_8:

Выключите второй контроллер домена, произведите захват ролей первым контроллером домена, удалите данные о втором контроллере домена из AD

```
con to serv win2019gui02
q
?
fsmo maintenance: Transfer infrastructure master

DISCONNECT the Server2 gui02 (shutdown) ...

ntdsutil
roles
con
con to ser pc1
q
```



(CMD 2 перехват) netdom query fsmo  
Seize PDC

```
fsmo maintenance: SEIZE PDC
Попытка безопасной передачи PDC FSMO перед захватом.
Ошибка ldap_modify_sW, код ошибки 0xc(12 (Недоступное критическое расширение).
Расширенное сообщение об ошибке LDAP 000020AE: SvcErr: DSID-03210857, problem 5010 (UNAVAIL_EXTENSION), data 8610

Возвращенная ошибка Win32 0x20ae(Атрибут владельца роли не может быть прочитан.)
)
В зависимости от кода ошибки это может быть
ошибка подключения, LDAP или передачи роли.
Не удалось передать PDC FSMO, выполняется захват...
Серверу "w2019gui01" известно о 5 ролях
Схема - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
Хозяин именования - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
PDC - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
RID - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
Инфраструктура - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
fsmo maintenance: SEIZE RID MASTER
Попытка безопасной передачи RID FSMO перед захватом.
Ошибка ldap_modify_sW, код ошибки 0xc(12 (Недоступное критическое расширение).
Расширенное сообщение об ошибке LDAP 000020AE: SvcErr: DSID-032112BA, problem 5010 (UNAVAIL_EXTENSION), data 8610

Возвращенная ошибка Win32 0x20ae(Атрибут владельца роли не может быть прочитан.)
)
В зависимости от кода ошибки это может быть
ошибка подключения, LDAP или передачи роли.
Не удалось передать RID FSMO, выполняется захват...
Поиск наивысшего пула RID в домене
Серверу "w2019gui01" известно о 5 ролях
Схема - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
Хозяин именования - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
PDC - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
RID - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
Инфраструктура - CN=NTDS Settings,CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
fsmo maintenance: SEIZE RID MASTER
```

## Удаление

Active Directory - пользователи и компьютеры

Файл Действие Вид Справка

Пользователи и компьютеры Active Directory

- Сохраненные запросы
- domain.local01
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Keys
  - LostAndFound
  - Managed Service Accounts
  - Program Data
  - System
  - Users
  - Калининград
  - NTDS Quotas
  - TPM Devices

Имя	Тип	Тип контролл...	Сайт	Описание
W2019GUI01	Компьютер	GC	Default-First-Si...	
W2019GUI02	Компьютер	GC	Default-First-Si...	

## Или Metadata cleanup (Ntdsutil)

```
C:\Users\Администратор>ntdsutil
ntdsutil: Metadata cleanup
metadata cleanup: connections
server connections: con to ser w2019gui01
Привязка к w2019gui01 ...
Подключен к w2019gui01 с помощью учетных данных локального пользователя.
server connections: q
metadata cleanup: sel op tar
select operation target: list domain
Найдено доменов: 1
0 - DC=domain,DC=local01
select operation target: sel dom 0
Нет текущего сайта
Домен - DC=domain,DC=local01
Нет текущего сервера
Нет текущего контекста именования
select operation target:
```

Администратор: Командная строка

Microsoft Windows [Version 10.0.17763.5329]  
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

```
C:\Users\Администратор>netdom query fsmo
Хозяин схемы                w2019gui01.domain.local01
Хозяин именования доменов   w2019gui01.domain.local01
PDC                         w2019gui01.domain.local01
Диспетчер пула RID          w2019gui01.domain.local01
Хозяин инфраструктуры      w2019gui01.domain.local01
Команда выполнена успешно.
```

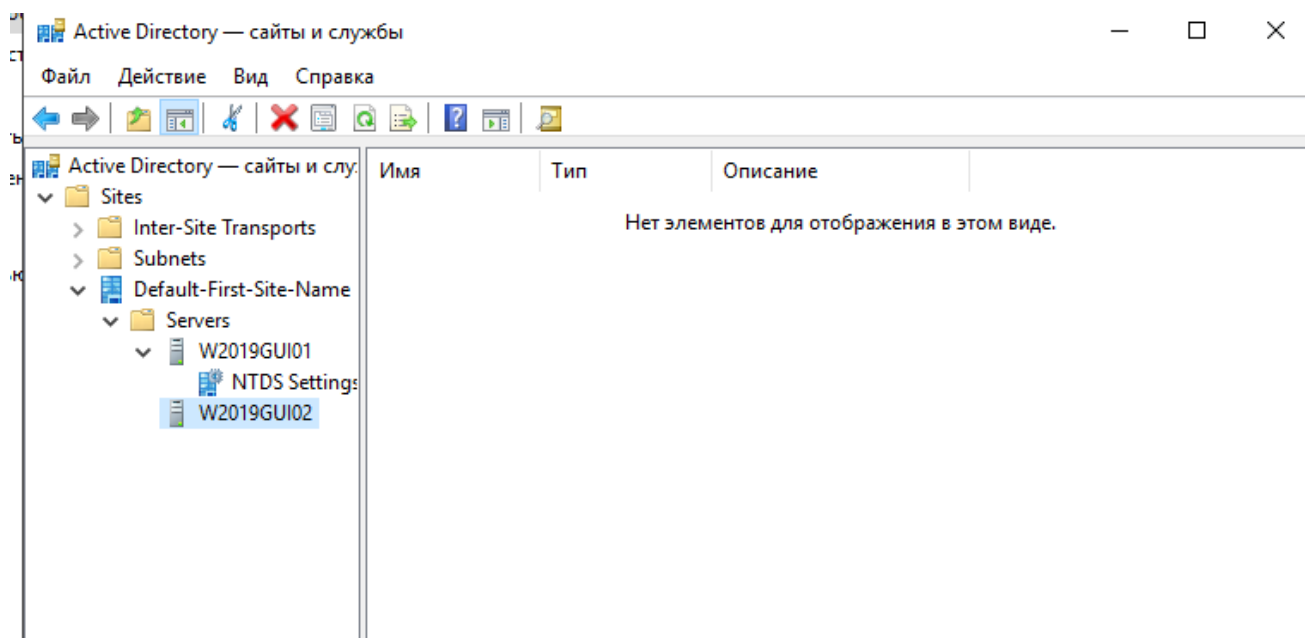
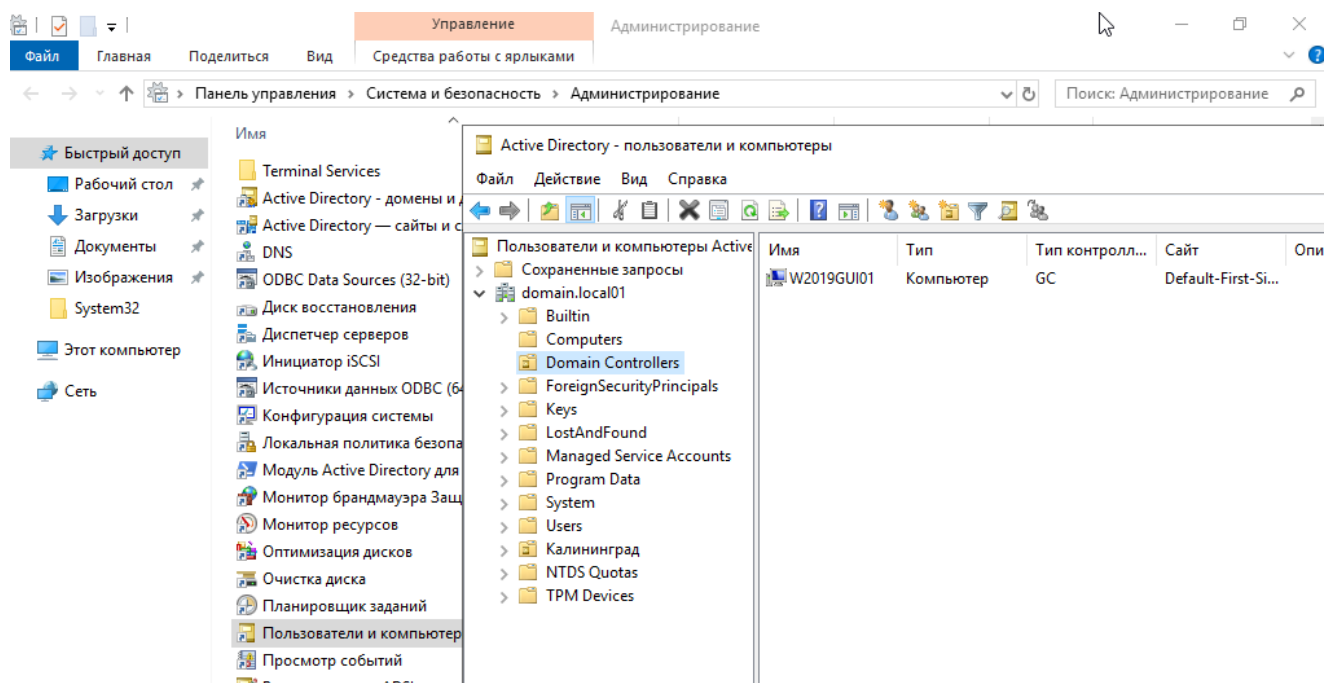
```
select operation target: list site
Найдено сайтов: 1
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
select operation target: sel si 0
Сайт - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
Домен - DC=domain,DC=local01
Нет текущего сервера
Нет текущего контекста именования
select operation target: _
```

```
select operation target: list servers in site
Найдено серверов: 2
0 - CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
1 - CN=W2019GUI02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
select operation target:
```

## Удаляем сервер 1

```
0 - CN=W2019GUI01,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
1 - CN=W2019GUI02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
select operation target: sel ser 1
Сайт - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
Домен - DC=domain,DC=local01
Сервер - CN=W2019GUI02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
        Объект DSA - CN=NTDS Settings,CN=W2019GUI02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01
        Имя DNS-узла - w2019gui02.domain.local01
        Объект-компьютер - CN=W2019GUI02,OU=Domain Controllers,DC=domain,DC=local01
Нет текущего контекста именования
select operation target:
```

```
Нет текущего контекста именования
select operation target: q
metadata cleanup: rem sel ser
Передача или захват ролей FSMO от выбранного сервера.
Удаление метаданных FRS для выбранного сервера.
Поиск членов FRS в "CN=W2019GUI02,OU=Domain Controllers,DC=domain,DC=local01".
Удаление поддерева в "CN=W2019GUI02,OU=Domain Controllers,DC=domain,DC=local01".
Ошибка при попытке удалить параметры FRS на CN=W2019GUI02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01: "Элемент не найден.";
очистка метаданных продолжается.
"CN=W2019GUI02,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local01" удалена с сервера "w2019gui01"
metadata cleanup:
```



Удаляем вручную

Active Directory - пользователи и компьютеры  
Domain Controllers - w2019gui02 (удалить)

Управление Управление Администрирование

Главная Поделиться Вид Средства работы с ярлыками Средства работы с приложениями

Панель управления > Система и безопасность > Администрирование

Поиск: Админи

Имя	Дата изменения	Тип	Размер
Terminal Services	15.09.2018 10:19	Папка с файлами	
Active Directory - домены и доверие	30.01.2024 3:16	Ярлык	2 КБ
Active Directory — сайты и службы	30.01.2024 3:17	Ярлык	2 КБ
DNS	15.09.2018 10:13	Папка с файлами	2 КБ

Диспетчер DNS

Файл Действие Вид Справка

Название Тип Значение Отметка времени

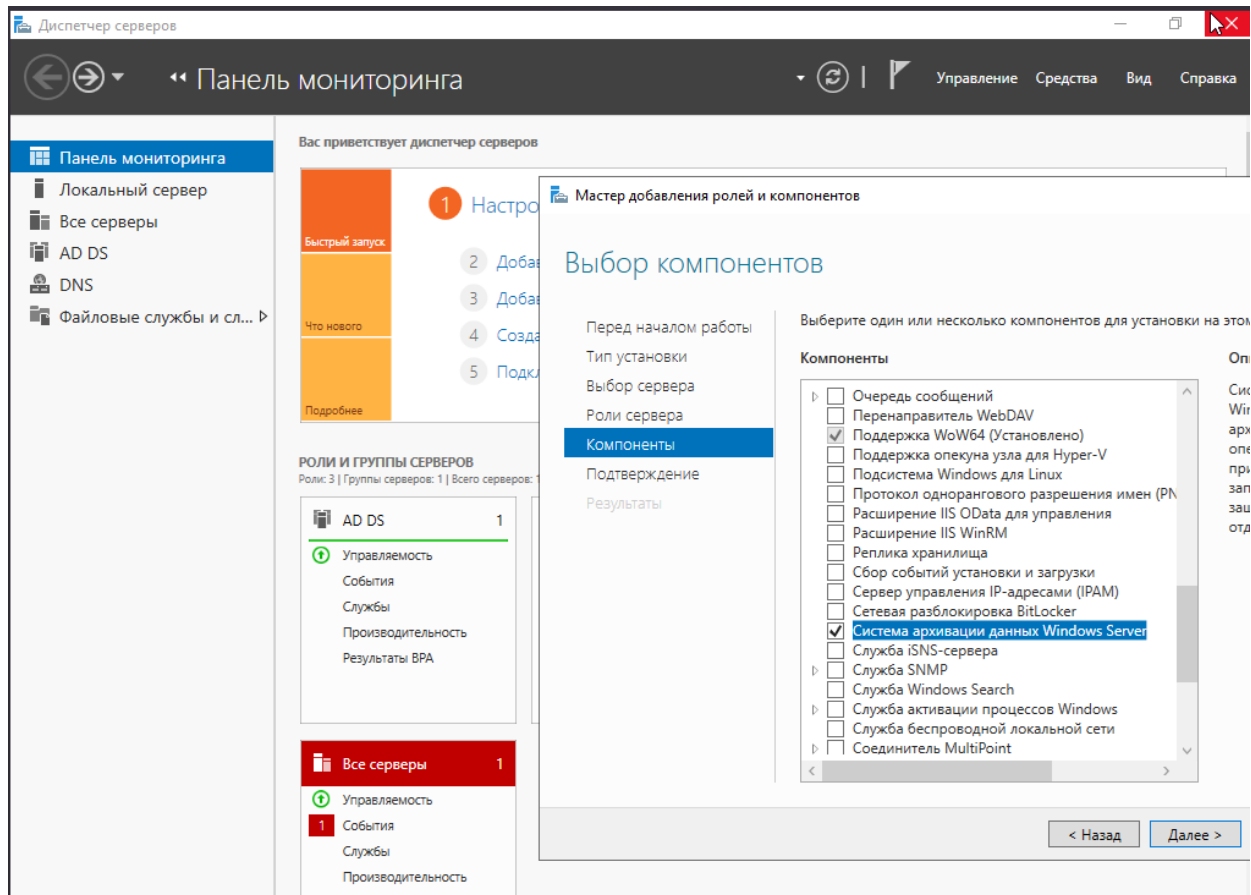
Название	Тип	Значение	Отметка времени
_ldap	Располо...	[0][100][389] w2019gui02.domain...	30.01.2024 23:00
_ldap	Располо...	[0][100][389] w2019gui01.domain...	30.01.2024 2:00

ДНС

- W2019GUI01
  - Зоны прямого просмотра
    - \_msdcs.domain.local01
      - domain.local01
        - \_msdcs
          - \_sites
            - Default-First-Site-Name
              - \_tcp
              - \_tcp
              - \_udp
              - DomainDnsZones
                - \_sites
                  - Default-First-Site-Name
                    - \_tcp
                    - ForestDnsZones
                      - \_sites
                        - \_tcp
- Зоны обратного просмотра
  - 56.168.192.in-addr.arpa
  - Серверы условной пересылки

Дополнительно (восстановление):

- Система архивных данных (компоненты)



- Webadmin ...

## Дополнительно:

### Восстановление контроллера домена AD из system state бэкапа

Чтобы приступить к восстановлению, вам нужно установить на новом сервере ту же версию Windows Server, которая была установлена на неисправном DC. В чистой ОС на новом сервере нужно установить роль **AD DS** (не настраивая ее) и компонент **Windows Server Backup**.



Для восстановления Active Directory вам нужно загрузить сервер в режиме восстановления служб каталогов **DSRM** (Directory Services Restore Mode). Для этого запустите **msconfig** и на вкладке **Boot** выберите Safe Boot -> **Active Directory repair**.



Перезагрузите сервер. Он должен загрузиться в режиме DSRM. Запустите Windows Server Backup (wbadmin) и в правом меню выберите **Recover**.



В мастере восстановления выберите, что резервная копия хранится в другом месте (A backup stored on another location).



Заметем выберите диск, на котором находится резервная копия старого контроллера AD, или укажите UNC путь к ней.

Чтобы WSB увидел бэкап на диске, нужно поместить каталог WindowsImageBackup с резервной копией в корень диска. Можете проверить наличие резервных копий на диске с помощью команды:

```
wbadmin get versions -backupTarget:D:
```

Выберите дату, на которую нужно восстановить резервную копию.



Укажите, что вы восстанавливаете состояние System State.



Выберите для восстановления «Исходное размещение» (Original location) и обязательно установите галочку «**Выполнить заслуживающее доверия восстановление файлов Active Directory**» (Perform an authoritative restore of Active Directory files).



Система покажет предупреждение, что эта резервная копия другого сервера



Согласитесь с еще одним предупреждением:



После этого запустится процесс восстановления контроллера домена AD на новом сервере. По завершении сервер потребует перезагрузку (имя нового сервера будет изменено на имя DC из бэкапа).



Загрузите сервер в обычном режиме (отключите загрузку в DSRM режиме)

Авторизуйтесь на сервере под учетной записью с правами администратора домена.

При первом запуске консоли ADUC я получил ошибку:

Active Directory Domain Services

Naming information cannot be located for the following reason:

The server is not operational.



При этом на сервере нет сетевых папок SYSVOL and NETLOGON. Чтобы исправить ошибку:

1. Запустите regedit.exe;

2. Перейдите в

ветку `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters`

3. Измените значение параметра SysvolReady с 0 на 1;

4. Потом перезапустите службу NetLogon: `net stop netlogon & net start netlogon`

## Восстановление отдельных объектов в AD

### Включаем Active Directory Recycle Bin в домене

Из консоли Active Directory Administrative Center. Для этого в консоли нужно выбрать ваш домен и в правой панели найти и нажать кнопку «**Enable Recycle Bin**».


Если обновить консоль, то вы увидите, что в дереве AD появился новый контейнер OU с названием **Deleted object**



### Восстановление удаленных объектов Active Directory из корзины

Удалим несколько пользователей домена из AD, а затем попробуем их восстановить. Выделим несколько пользователей в тестовой OU и удалим их.



Затем в консоли ADAC перейдем в созданную ранее OU Deleted Objects и в ней должны оказаться все удаленный нами пользователи. Выделим все объекты, которые нужно восстановить и в правой панели нажмем кнопку **Restore**. Если нужно восстановить объекты в OU, отличную от той, из которой были они удалены, воспользуемся кнопкой **Restore To**.

После чего можно удостовериться, что все удаленные объекты появятся в исходном контейнере.

Если вам нужно восстановить отдельные объекты в AD, но время захоронения уже просрочено, или ActiveDirectory RecycleBin не включена, вы можете восстановить отдельные объекты AD в режиме авторитативного восстановления.

Вкратце процедура выглядит следующим образом:

1. Загрузите DC в DSRM режиме;
2. Выведите список доступных резервных копий: `wbadmin get versions`
3. Запустите восстановление выбранной резервной копии: `wbadmin start systemstaterecovery -version:[your_version]`
4. Подтвердите восстановление DC (в не полномочном режиме);
5. После перезагрузки запустите: `ntdsutil`
6. `activate instance ntds`
7. `authoritative restore`

Укажите полный путь к объекту, который нужно восстановить. Можно восстановить OU целиком:

```
restore subtree "OU=Users,DC=winitpro,DC=ru"
```

Или один объект:



```
restore object "cn=Test,OU=Users,DC=winitpro,DC=ru"
```



Данная команда запретит репликацию указанных объектов (путей) с других контроллеров домена и увеличит USN объекта на 100000.

Выйдите из ntdsutil: quit

### **Передача/захват ролей FSMO на другой контроллер домена Active Directory**

Рассмотрим, как определить контроллеры домена с ролями FSMO в Active Directory, способы передачи одной или нескольких FSMO ролей другому контроллеру домена (дополнительному), а также способ принудительного захвата FSMO ролей в случае выхода из строя контроллера домена, которой является владельцем роли.

Всего в домене Active Directory может быть **пять** ролей FSMO.

#### **Две уникальные роли для леса AD:**

1. **Хозяин схемы (Schema master)** – отвечает за внесение изменение в схему Active Directory;
2. **Хозяин именования домена (Domain naming master)** – обеспечивает уникальность имен для всех создаваемых доменов и разделов приложений в лесу AD;

И **три** роли для каждого **домена** :

1. **Эмулятор PDC (PDC emulator)** – является основным обозревателем в сети Windows (Domain Master Browser – нужен для нормального отображения компьютеров в сетевом окружении); отслеживает блокировки пользователей при неправильно введенном пароле, является главным NTP сервером в домене, используется для совместимости с клиентами Windows 2000/NT, используется корневыми серверами DFS для обновления информации о пространстве имён;
2. **Хозяин инфраструктуры (Infrastructure Master)** — отвечает за обновление в междоменных объектных ссылок;
3. **Хозяин RID (RID Master)** — сервер раздает другим контроллерам домена идентификаторы RID (пачками по 500 штук) для создания уникальных идентификаторов объектов — SID.

#### **Просмотр владельцев FSMO ролей в домене**

Чтобы найти всех владельцев FSMO ролей в домене AD, выполните команду:

```
netdom query fsmo
```

В этом примере видно, что все FSMO роли расположены на контроллере домена DC01. При развертывании нового леса AD (домена), все FSMO роли помещаются на первый DC. Любой контроллер домена кроме RODC может быть хозяином любой

FSMO роли. Соответственно, администратора домена может передать любую FSMO роль на любой другой контроллер домен.

Есть два способа передачи FSMO ролей:

**добровольный** (Transfer, когда оба DC доступны)

**принудительный** (Seize, когда DC с ролью FSMO недоступен/вышел из строя)

### Передача FSMO ролей из графических оснасток Active Directory

Для переноса FSMO ролей можно использовать стандартные графические оснастки Active Directory. Операцию переноса желательно выполнять на DC с FSMO ролью.

Если же консоль сервера не доступна, необходимо выполнить команду **Change Domain Controller** и выбрать контроллер домена в mmc-оснастке.



Передача ролей RID Master, PDC Emulator и Infrastructure Master

Для передачи ролей уровня домена (RID, PDC, Infrastructure Master) используется стандартная консоль Active Directory Users and Computers (DSA.msc)

1. Откройте консоль Active Directory Users and Computers;
2. Щелкните правой кнопкой мыши по имени вашего домена и выберите пункт **Operations Master**;
3. Перед вами появится окно с тремя вкладками (RID, PDC, Infrastructure), на каждой из которых можно передать соответствующую роль, указав нового владельца FSMO роли и нажав кнопку **Change**.

Передача роли Schema Master

Для переноса FSMO уровня леса Schema Master используется оснастка Active Directory Schema.

1. Перед запуском оснастки нужно зарегистрировать библиотеку schmmgmt.dll, выполнив в командной строке команду: `regsvr32 schmmgmt.dll`
2. Откройте консоль MMC, набрав **MMC** в командной строке;3. В меню выберите пункт **File -> Add/Remove snap-in** и добавьте консоль **Active Directory Schema**;
4. Щелкните правой кнопкой по корню консоли (Active Directory Schema) и выберите пункт **Operations Master**;
3. Введите имя контроллера, которому передается роль хозяина схемы, нажмите кнопку **Change** и ОК. Если кнопка недоступна, проверьте что ваша учетная запись входит в группу Schema admins.

Передача FSMO роли Domain naming master

1. Для передачи FSMO роли хозяина именования домена, откройте консоль управления доменами и доверием **Active Directory Domains and Trusts**;
2. Щелкните правой кнопкой по имени вашего домена и выберите опцию **Operations Master**;

3. Нажмите кнопку **Change**, укажите имя контроллера домена и нажмите OK. 

## Передача FSMO ролей из командной строки с помощью утилиты ntdsutil


**Внимание:** Использовать утилиту ntdsutil необходимо с осторожностью, четко понимая, что вы делаете, иначе можно просто сломать ваш домен Active Directory!

1. На контроллере домена откройте командную строку и введите команду: `ntdsutil`
2. Наберите команду: `roles`
3. Затем: `connections`
4. Затем нужно подключиться к DC, **на который** вы хотите передать роль. Для этого наберите: `connect to server <servername>`
5. Введите q и нажмите Enter.
6. Для передачи FSMO роли используется команда:

`transfer <role>`, где `<role>` это роль которую вы хотите передать.

Например: `transfer schema master`, `transfer RID` и т.д.



7. Подтвердите перенос FSMO роли; 
8. После переноса ролей нажмите q и Enter, чтобы завершить работу с ntdsutil.exe;
9. Перезагрузите контроллер домена.

## Принудительный захват FSMO ролей Active Directory

Если DC с одной из FSMO ролей вышел из строя (и его не возможно восстановить), или недоступен длительное время, вы можете принудительно перехватить у него любую из FSMO ролей. Но при этом крайне важно убедиться, что сервер, у которого забрали FSMO роль **никогда** не должен появиться в сети, если вы не хотите новых проблем с AD (даже если вы позднее восстановите DC из резервной копии). Если вы захотите вернуть потерянный сервер в домен, единственный правильный способ – удаление его из AD, чистая переустановка Windows, установка роли ADDS и повышение сервера до контроллера домена.

Вы можете принудительно захватить FSMO роли с помощью утилиты NTDSUtil. Также вы можете перенести роли FSMO с помощью утилиты ntdsutil. Процедура захвата роли через ntdsutil похожа на обычную передачу.

Используйте следующие команды:

Вводим `ntdsutil`, попадем в исполняемую среду.

Набираем команду: `roles`

Затем: `connections`

В server connections пишем: `connect to server <имя сервера>`

Вводим: q нажимаем Enter

Пишем в fsmo maintenance: `seize <role>`, где `<role>` это роль которую вы хотите захватить, например: `seize RID master`.

## Теперь, когда все роли захвачены или переданы, то можно производить удаление всех старых данных.

Если у вас уровень леса и домена Windows Server 2008 R2 и выше, то самый простой способ это удалить, объект компьютера из контейнера Domain Controllers, все старые метаданные будут удалены автоматически и вам не придется делать описанные ниже манипуляции.

Но рассмотрим ручной способ, для более глубоко понимания, что именно происходит и откуда удаляются данные о недоступном контроллере домена.



Удаляем контроллер с помощью NTDSutil

Откройте командную строку от имени администратора.

Пишем команду ntdsutil

Далее нам необходимо зайти в режим metadata cleanup

Теперь вам необходимо подключиться к работающему контроллеру домена, пишем connections

Далее вводим connect to server и имя сервера, видим успешное подключение

Выходим из данного меню, введите q и нажмите enter.

Далее введите select operation target

Посмотрим список доменов командой List domain

Выберем нужный домен, select domain

Теперь поищем какие сайты у нас есть, делается это командой list sites

Выбираем нужный select site и номер

Посмотрим список серверов в сайте, list servers in site, выбираем нужный select server и номер

Выходим из режима select operation target, введите q

Команда на удаление remove selected server



У вас появится предупреждение, что "Вы действительно хотите удалить объект сервера, имя сервера. Это не последний сервер домена. Сервер должен постоянно работать автономно и не возвращаться в сеть обслуживания. При возвращении сервера в сеть обслуживания, объект сервера будет восстановлен."



После удаления контроллера необходимо проверить следующие оснастки:

1. сайты Active Directory, открываем данную оснастку



Все теперь можно удалять, когда все связи устранены.



2. удаление записей в зоне DNS, вот пример записи "Сервер имен (NS)",



так же проверим папки:

\_msdcs

\_sites

\_tcp

\_udp



## Глоссарий

## Дополнительные материалы

## Используемые источники

Выполнил: **AndreiM**