

## Выполнил студент группы 2345 Романенко Кирилл

### 1. Запустите утилиты repadmin /showrepl

Ввёл команду

repadmin /showrepl

```
Repadmin: выполнение команды /showrepl контроллере домена localhost с полным доступом
Default-First-Site-Name\WIN-SERVER1
Параметры DSA: IS_GC
Параметры сайта: (none)
DSA - GUID объекта: dceab910-5249-4bc7-9da0-26f40952cca3
DSA - код вызова: dceab910-5249-4bc7-9da0-26f40952cca3

==== ВХОДЯЩИЕ СОСЕДИ =====
DC=domain,DC=local
  Default-First-Site-Name\WIN-SERVER2 через RPC
  DSA - GUID объекта: feb10b4e-668e-48a8-898f-6f16bb4b5697
  Последняя попытка @ 2022-09-20 15:37:15 успешна.
CN=Configuration,DC=domain,DC=local
  Default-First-Site-Name\WIN-SERVER2 через RPC
  DSA - GUID объекта: feb10b4e-668e-48a8-898f-6f16bb4b5697
  Последняя попытка @ 2022-09-20 15:36:44 успешна.
CN=Schema,CN=Configuration,DC=domain,DC=local
  Default-First-Site-Name\WIN-SERVER2 через RPC
  DSA - GUID объекта: feb10b4e-668e-48a8-898f-6f16bb4b5697
  Последняя попытка @ 2022-09-20 15:36:18 успешна.
DC=DomainDnsZones,DC=domain,DC=local
  Default-First-Site-Name\WIN-SERVER2 через RPC
  DSA - GUID объекта: feb10b4e-668e-48a8-898f-6f16bb4b5697
  Последняя попытка @ 2022-09-20 15:40:56 успешна.
DC=ForestDnsZones,DC=domain,DC=local
  Default-First-Site-Name\WIN-SERVER2 через RPC
  DSA - GUID объекта: feb10b4e-668e-48a8-898f-6f16bb4b5697
  Последняя попытка @ 2022-09-20 15:40:53 успешна.
```

### 2. Запустите утилиту dcdiag /test:dns , /test:topology

Ввёл команду

dcdiag /test:dns

```
Диагностика сервера каталогов

Выполнение начальной настройки:
  Выполняется попытка поиска основного сервера...
  Основной сервер = WIN-Server1
  * Определен лес AD.
  Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

  Сервер проверки: Default-First-Site-Name\WIN-SERVER1
  Запуск проверки: Connectivity
  ..... WIN-SERVER1 - пройдена проверка Connectivity

Выполнение основных проверок

  Сервер проверки: Default-First-Site-Name\WIN-SERVER1

  Запуск проверки: DNS

  Проверки DNS выполняются без зависания. Подождите несколько минут...
  ..... WIN-SERVER1 - пройдена проверка DNS

Выполнение проверок разделов на: ForestDnsZones
Выполнение проверок разделов на: DomainDnsZones
Выполнение проверок разделов на: Schema
Выполнение проверок разделов на: Configuration
Выполнение проверок разделов на: domain

Выполнение проверок предприятия на: domain.local
  Запуск проверки: DNS
  ..... domain.local - пройдена проверка DNS
```

Ввёл команду

dcdiag /test:topology

```
Диагностика сервера каталогов

Выполнение начальной настройки:
  Выполняется попытка поиска основного сервера...
  Основной сервер = WIN-Server1
  * Определен лес AD.
  Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

  Сервер проверки: Default-First-Site-Name\WIN-SERVER1
  Запуск проверки: Connectivity
  ..... WIN-SERVER1 - пройдена проверка Connectivity

Выполнение основных проверок

  Сервер проверки: Default-First-Site-Name\WIN-SERVER1
  Запуск проверки: Topology
  ..... WIN-SERVER1 - пройдена проверка Topology

Выполнение проверок разделов на: ForestDnsZones
Выполнение проверок разделов на: DomainDnsZones
Выполнение проверок разделов на: Schema
Выполнение проверок разделов на: Configuration
Выполнение проверок разделов на: domain
Выполнение проверок предприятия на: domain.local
```

3. Узнайте SID пользователя под учетной записью которого вошли в систему

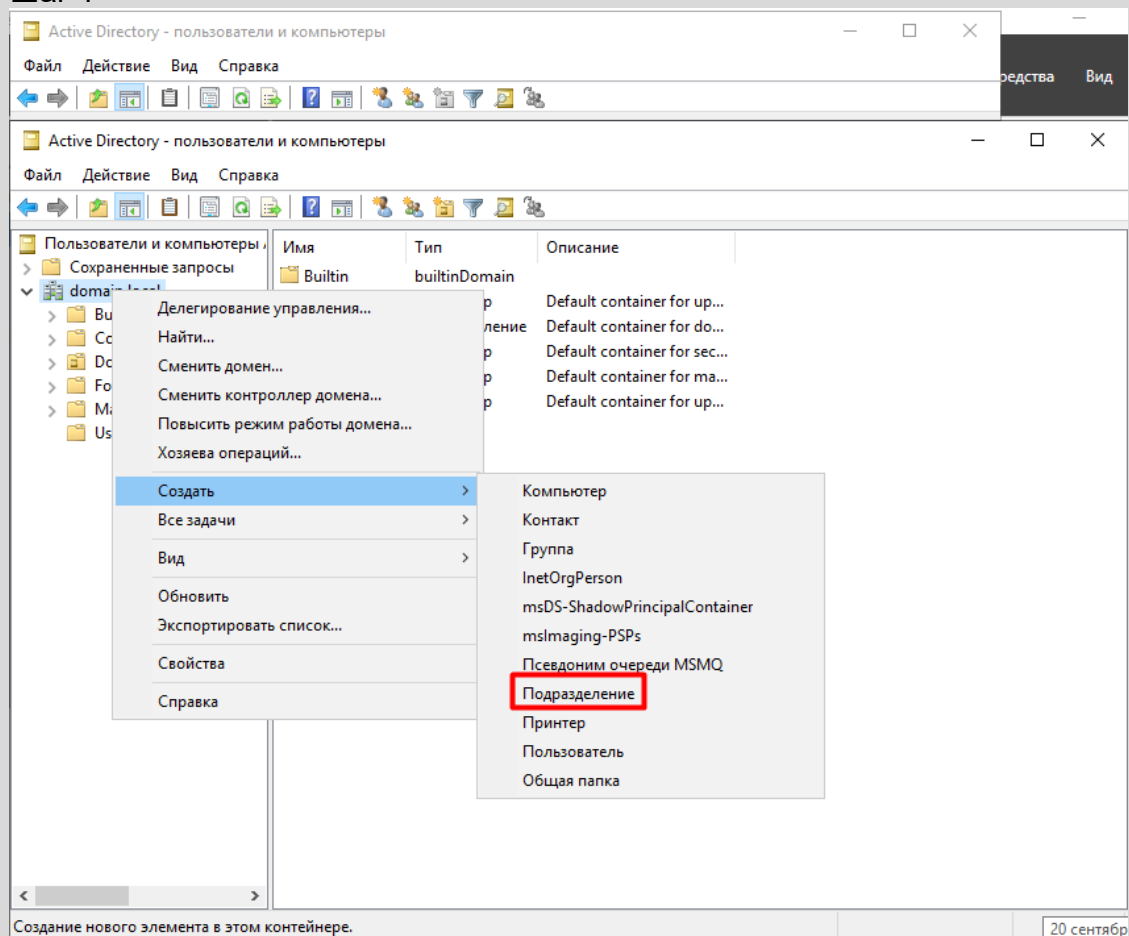
Ввел команду whoami /user

```
Сведения о пользователе
-----

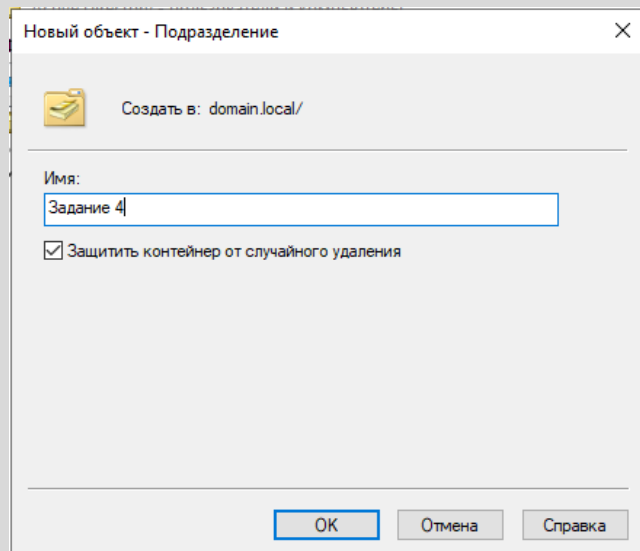
Пользователь          SID
=====
domain\администратор S-1-5-21-3361738476-3567923889-2254631205-500
```

#### 4. Создайте защищенную от удаления ОП (OU)

##### Шаг 1



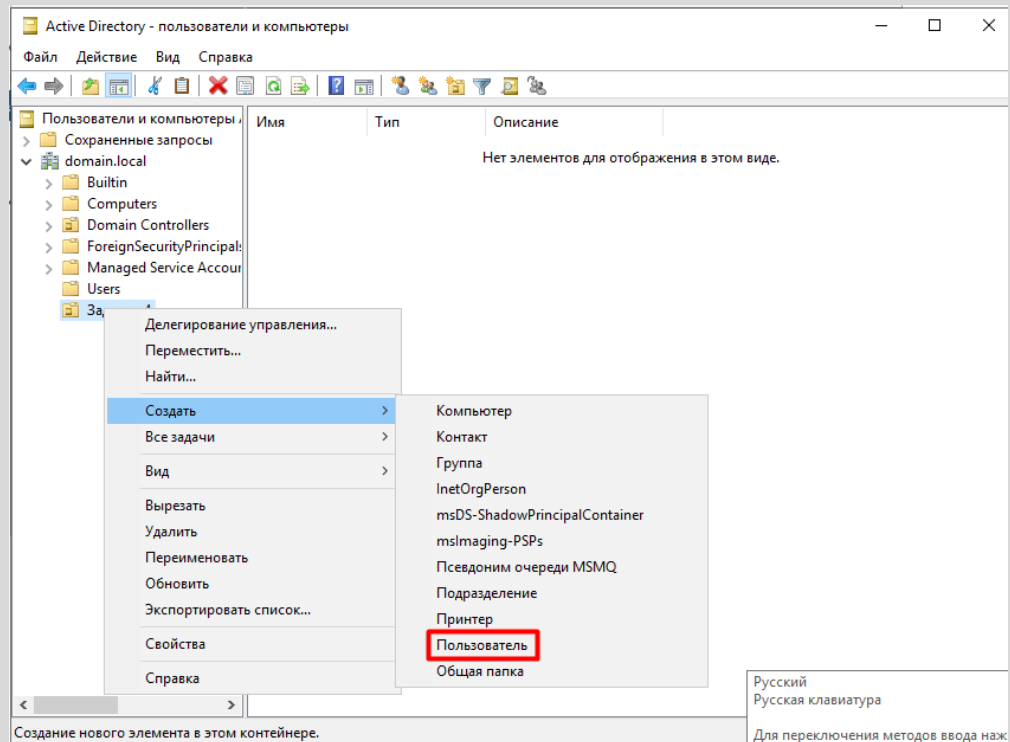
##### Шаг 2



5. Создайте в ней учетные записи нескольких пользователей, компьютеров, группу

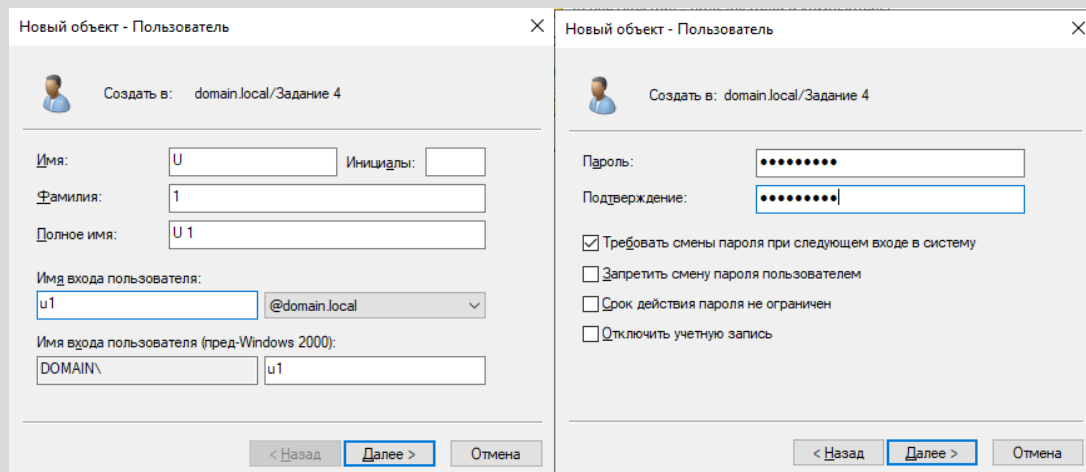
## Создал пользователей

### Шаг 1



### Шаг 2

### Создал пользователя u1



Новый объект - Пользователь

Создать в: domain.local/Задание 4

После нажатия на кнопку "Готово" будет создан следующий объект:

Полное имя: U 1  
Имя входа пользователя: u1@domain.local  
Требовать смены пароля при следующем входе в систему.

< Назад Готово Отмена

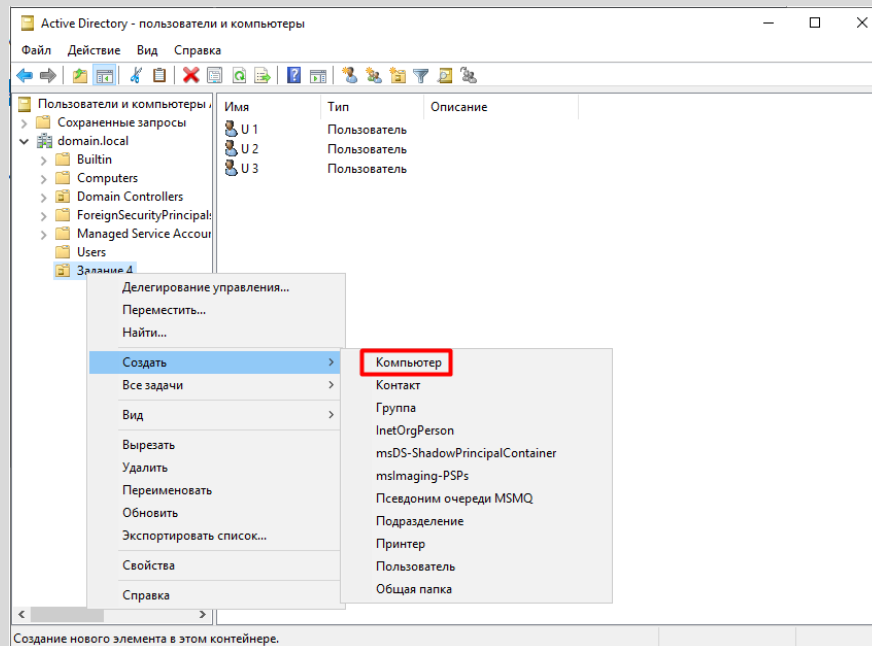
### Шаг 3

По аналогии Шаг 2 создал пользователей u2 и u3

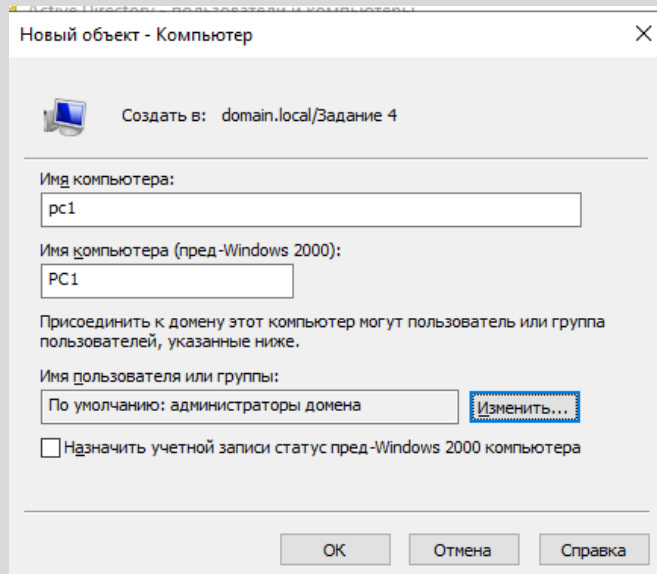
Active Directory - пользователи и компьютеры			
Файл Действие Вид Справка			
<b>Пользователи и компьютеры</b>			
Сохраненные запросы			
domain.local			
Built-in			
Computers			
Domain Controllers			
ForeignSecurityPrincipal:			
Managed Service Account			
Users			
Задание 4			
Имя	Тип	Описание	
U 1	Пользователь		
U 2	Пользователь		
U 3	Пользователь		

# Создал компьютеры

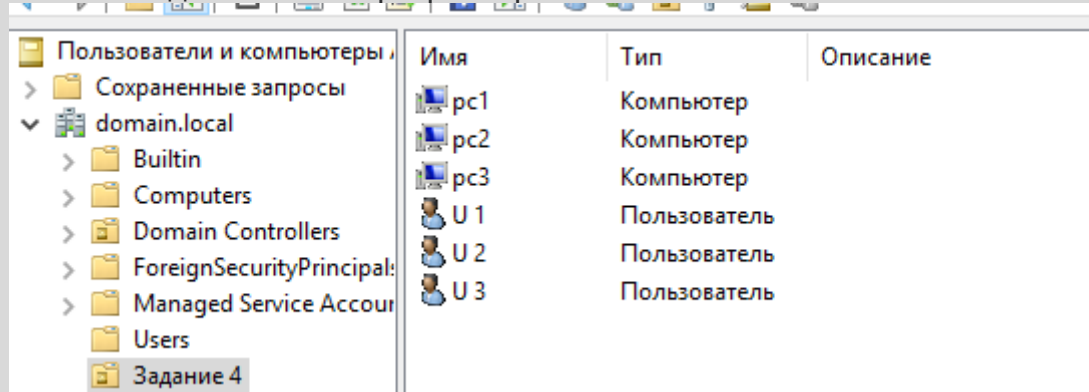
## Шаг 1



## Шаг 2

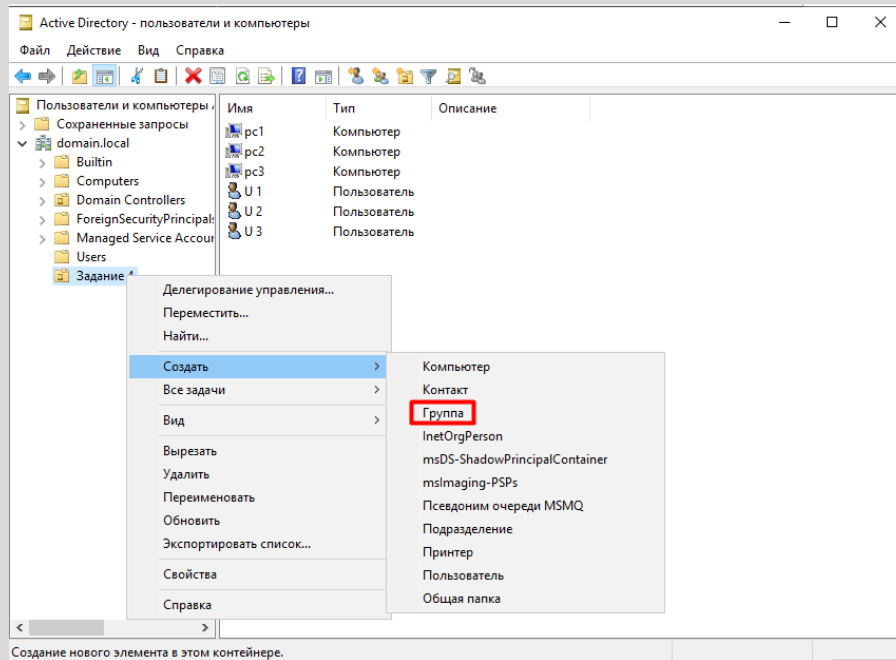


## Шаг 3. Создал компьютеры pc2 и pc3

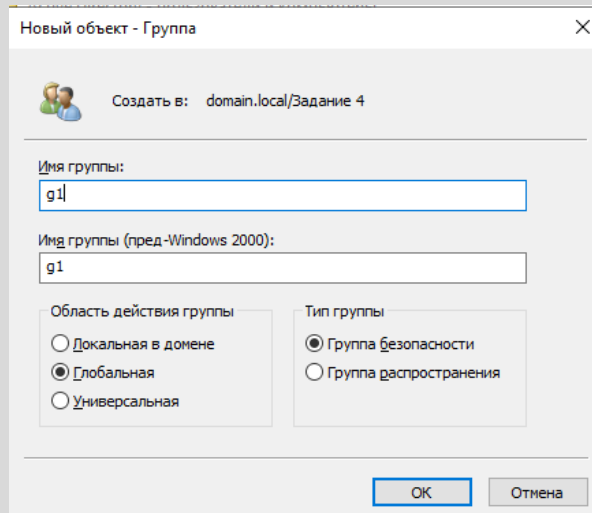


# Создал группу

## Шаг 1

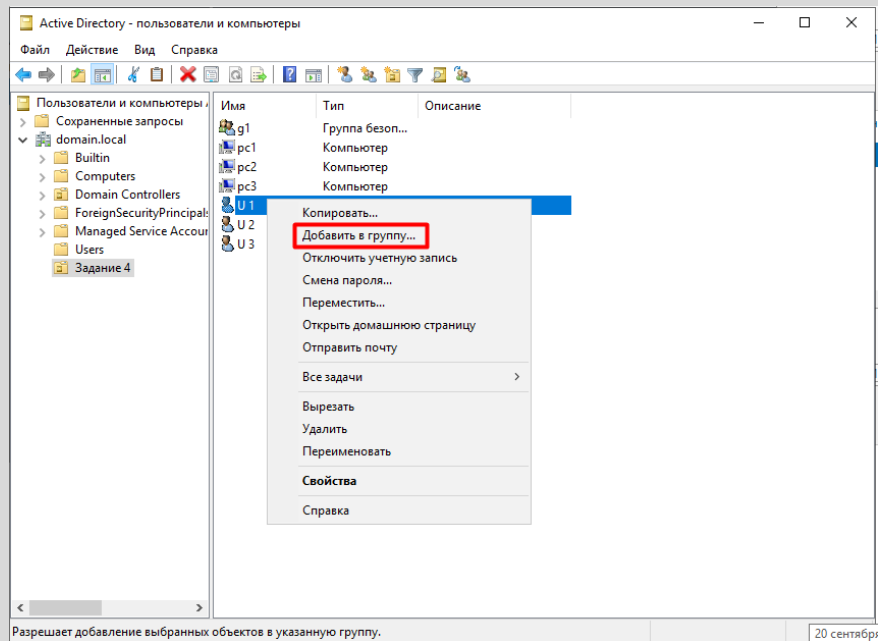


## Шаг 2

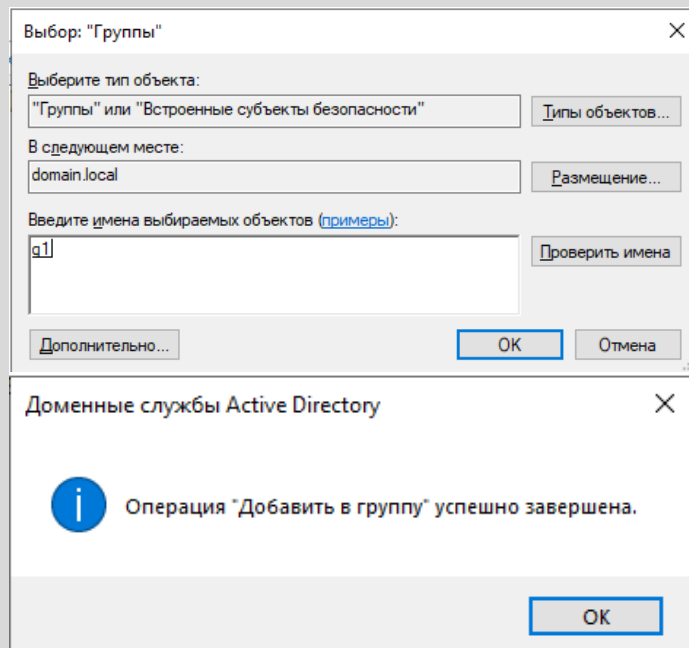


## 6. Добавьте пользователей в группу

### Шаг 1

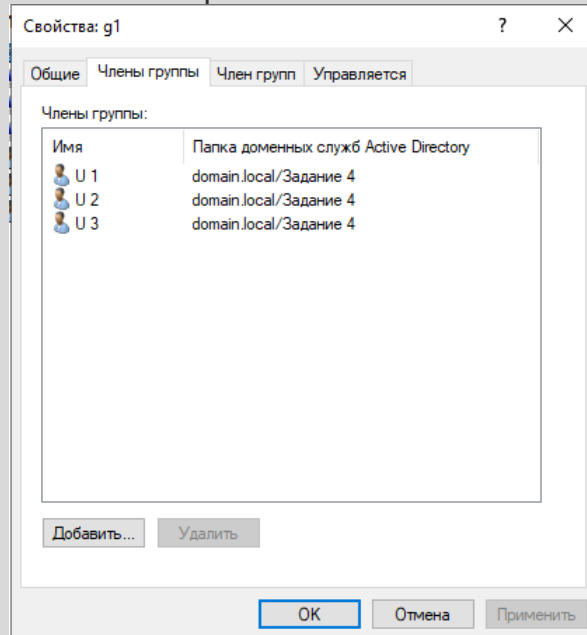


### Шаг 2



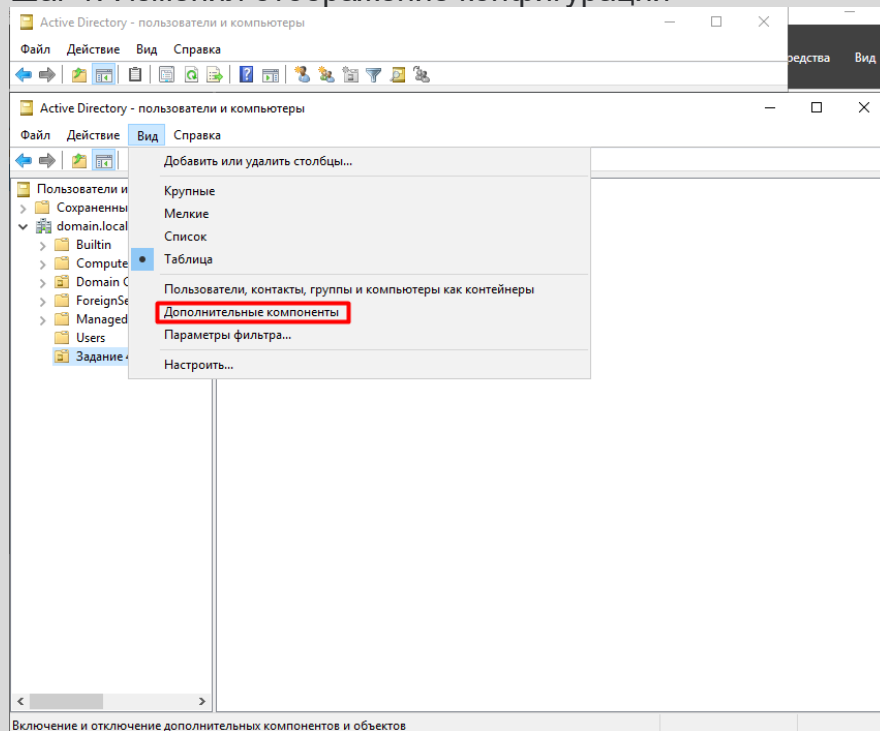


### Шаг 3. Повторил с пользователями u2 и u3

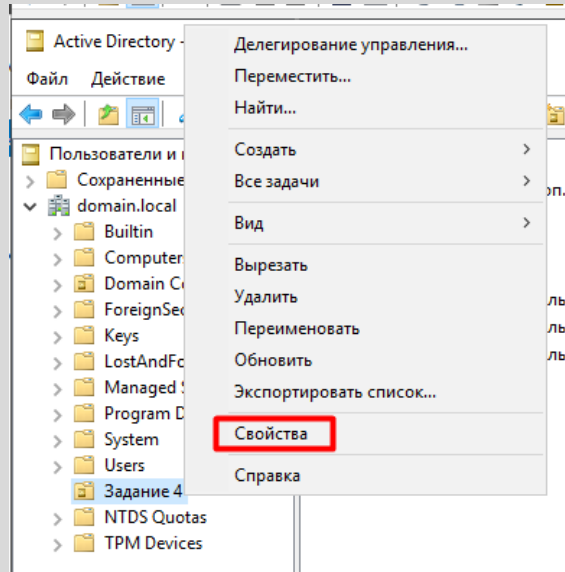


### 7. Удалите созданную OU

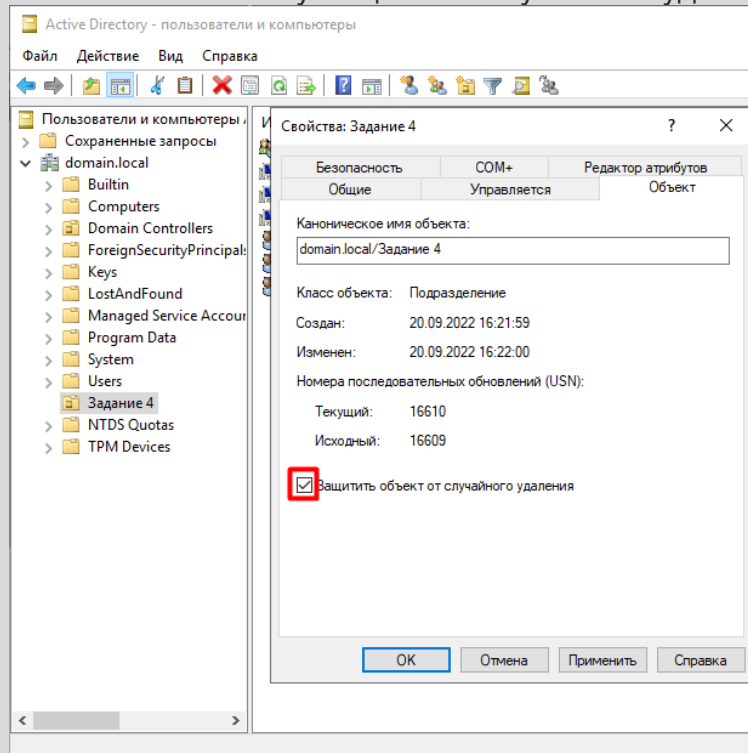
### Шаг 1. Изменил отображение конфигурации

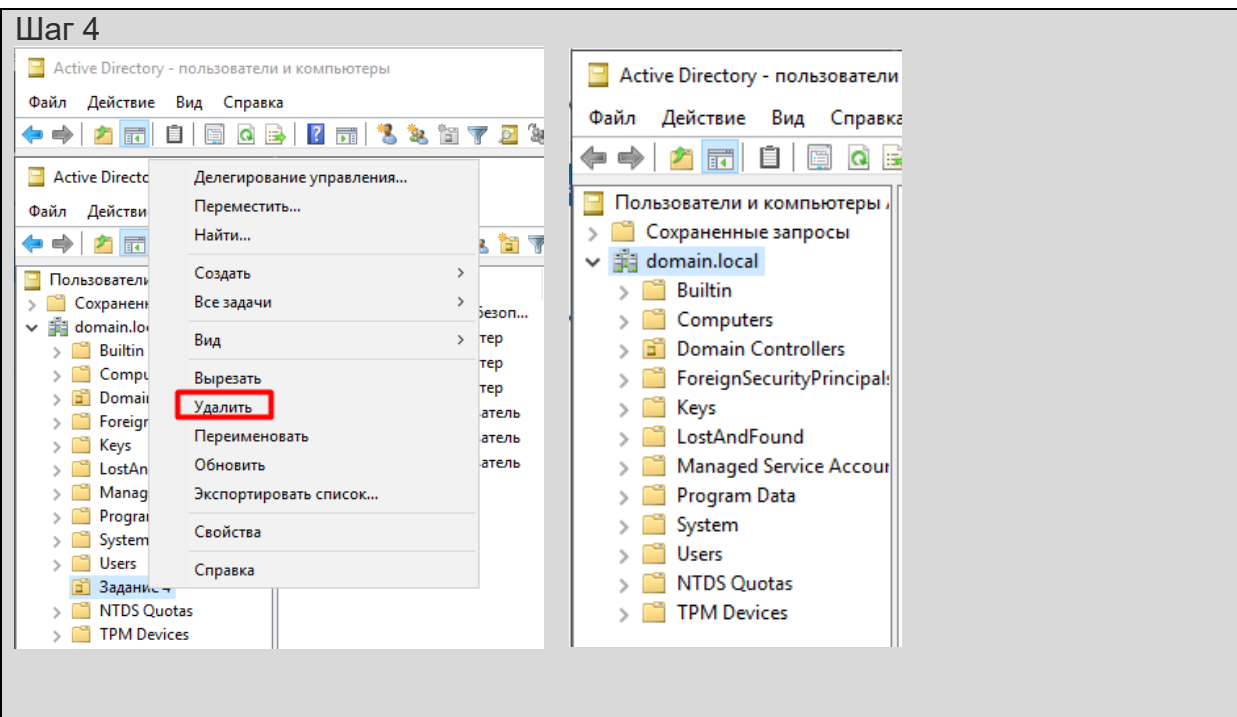


## Шаг 2

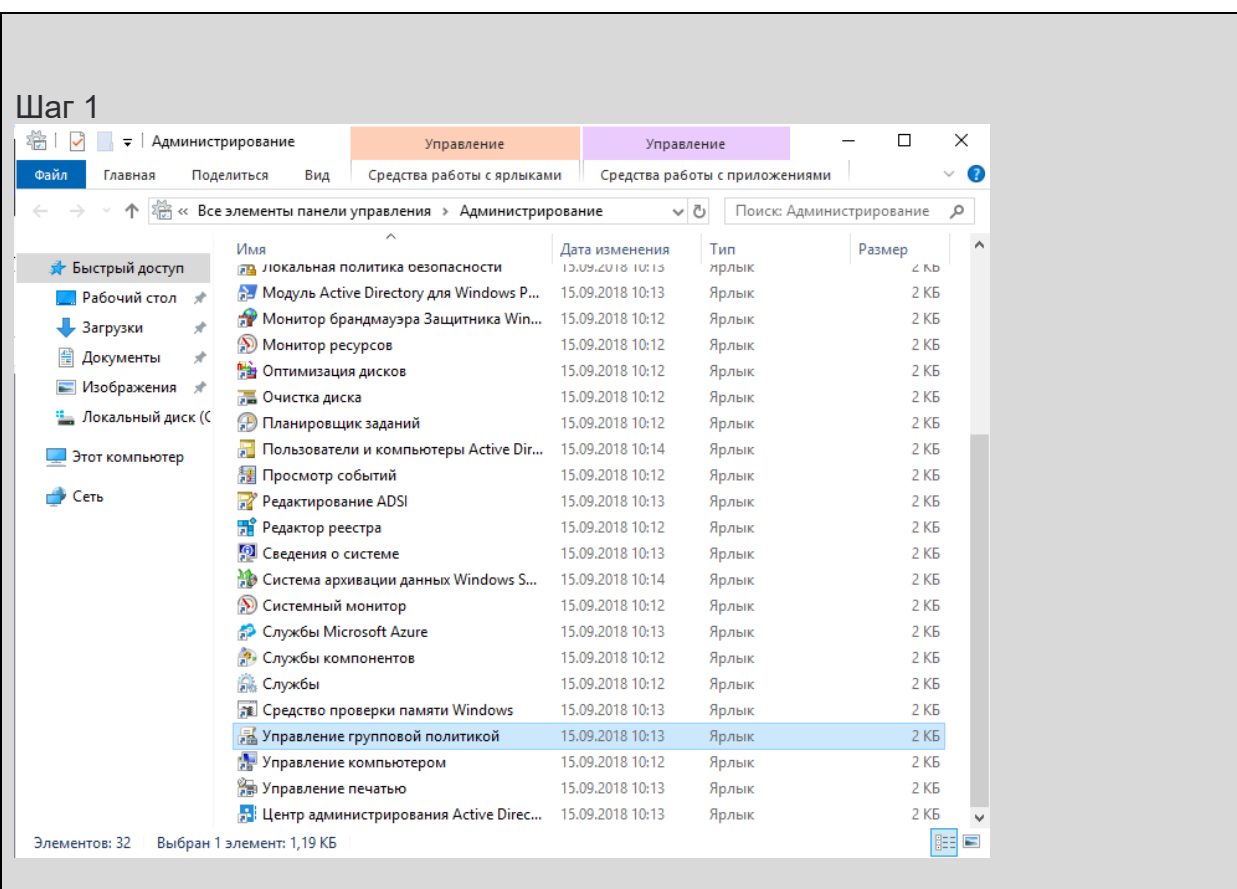


## Шаг 3. Снял галочку защиты от случайного удаления

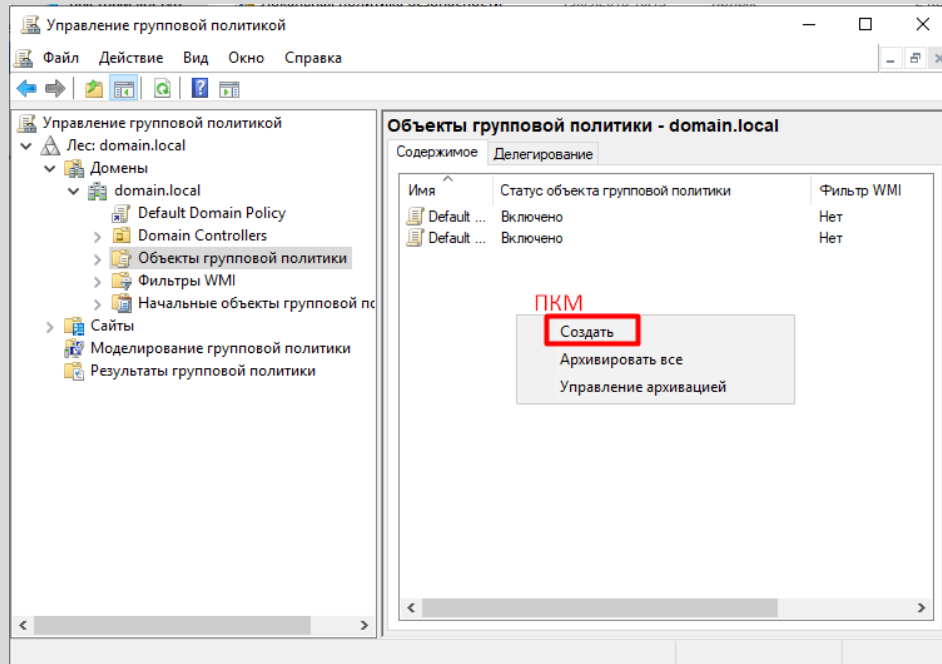




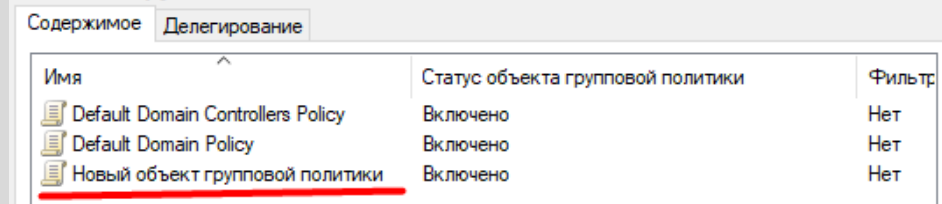
8. Создайте групповую политику (GPO) с блокировкой ссылки "Игры" и подключите к любой OU



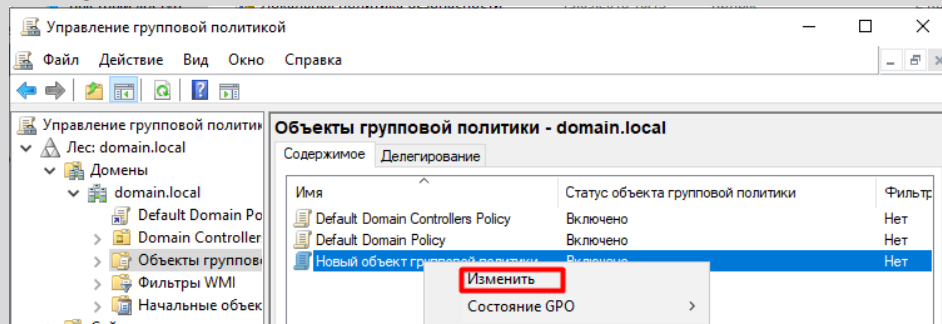
## Шаг 2



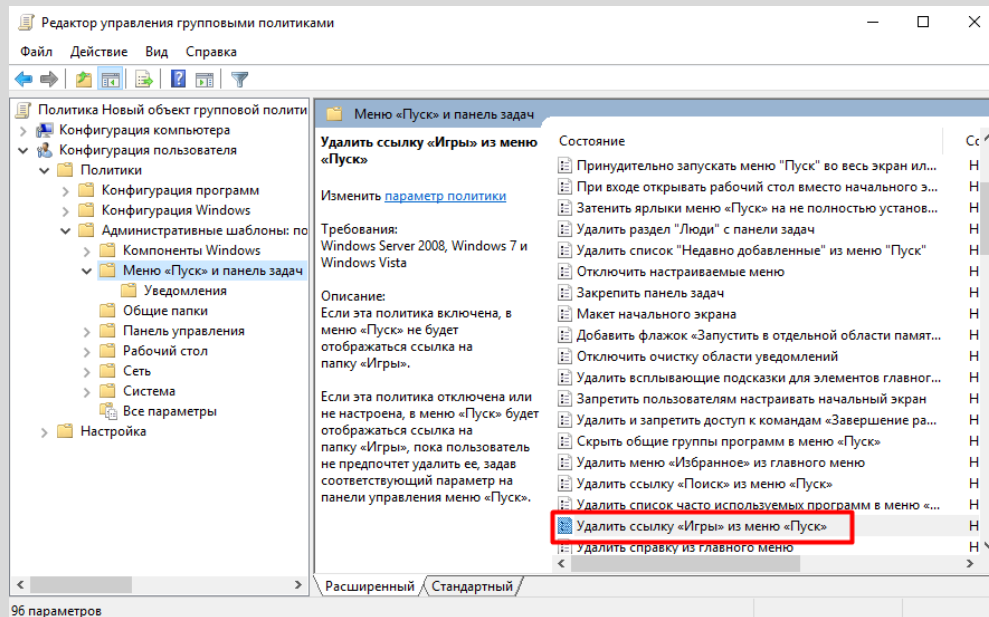
## Объекты групповой политики - domain.local



## Шаг 3



#### Шаг 4.

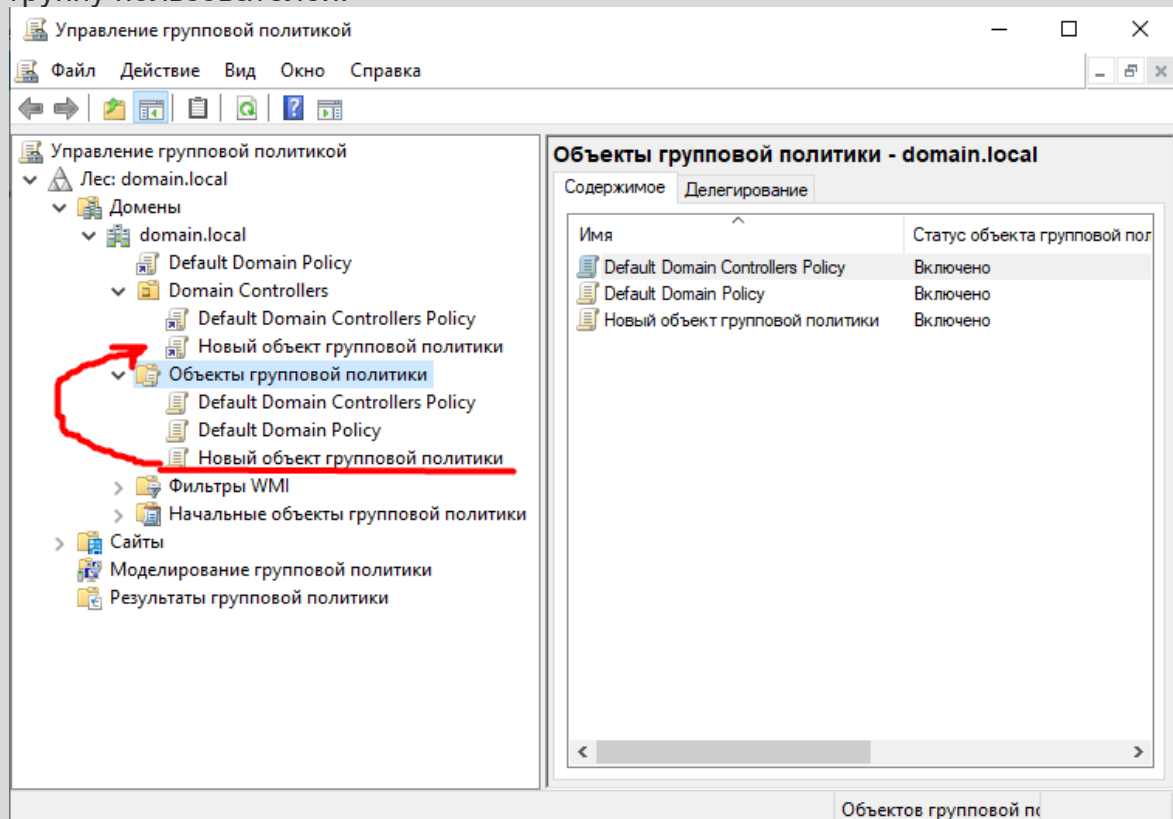


#### Шаг 5

Удалить список часто используемых программ в меню «...	Не задана
<b>Удалить ссылку «Игры» из меню «Пуск»</b>	<b>Включена</b>
Удалить справку из главного меню	Не задана

Настроил

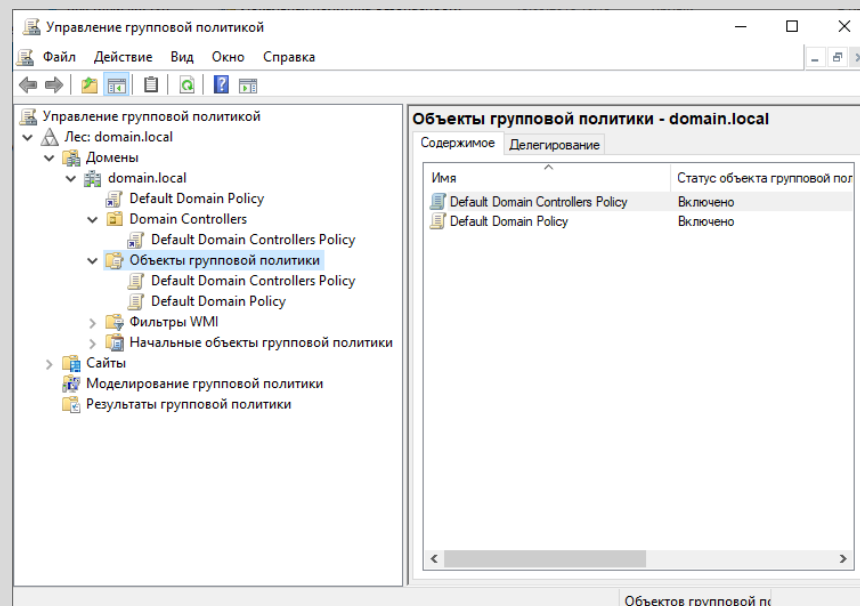
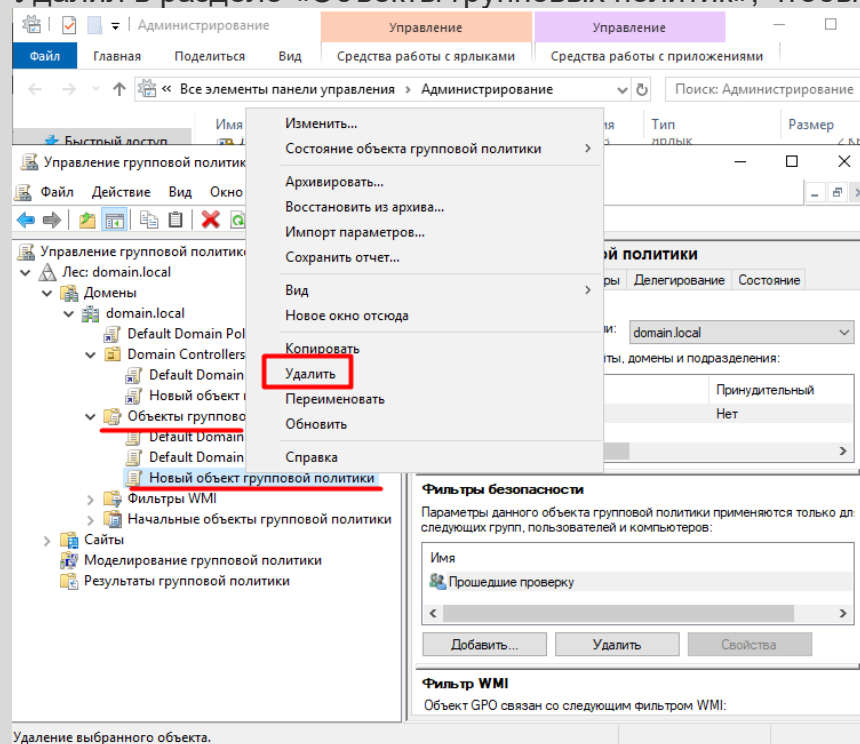
Шаг 6. После настройки зажал нужную политику и перенес в необходимую группу пользователей.



Готово

## 9. Удалите созданную GPO

Удалил в разделе «Объекты групповых политик», чтобы сразу удалить отовсюду



10. Добавьте в качестве сервера пересылки адрес 8.8.8.8

Диспетчер серверов

Администрирование

Управление

Управление

Файл

Главная

Поделиться

Вид

Средства работы с ярлыками

Средства работы с приложениями

« Все элементы панели управления »

Администрирование

Поиск: Администрирование

Быстрый доступ

Рабочий стол

Загрузки

Документы

Изображения

Локальный диск (C:)

Этот компьютер

Сеть

Имя

Дата изменения

Тип

Размер

Terminal Services

15.09.2018 10:19

Папка с файлами

Active Directory - домены и доверие

15.09.2018 10:14

Ярлык

2 КБ

Active Directory — сайты и службы

15.09.2018 10:13

Ярлык

2 КБ

DNS

15.09.2018 10:13

Ярлык

2 КБ

ODBC Data Sources (32-bit)

15.09.2018 10:12

Ярлык

2 КБ

Диск восстановления

15.09.2018 10:12

Ярлык

2 КБ

Диспетчер DNS

Файл

Действие

Вид

Справка

DNS

WIN-SERVER1

Зоны прямого просмотра

Зоны обратного просмотра

Точки доверия

Серверы условной пересылки

Создать сервер условной пересылки...

Вид

Обновить

Экспортировать список...

Справка

Элементов: 32

Выбран 1 элемент: 1,2

Создать сервер условной пересылки

DNS-домен:

IP-адреса основных серверов:

IP-адрес

FQDN сервера

Проверка выполнена

Удалить

Вверх

Вниз

8.8.8.8

dns.google

OK

Сохранять условный сервер пересылки в Active Directory и реплицировать ее следующим образом:

Все DNS-серверы в этом лесу

Время ожидания пересылки (сек): 5

Полное доменное имя сервера будет недоступно, если не настроены соответствующие зоны обратного просмотра и записи.

OK

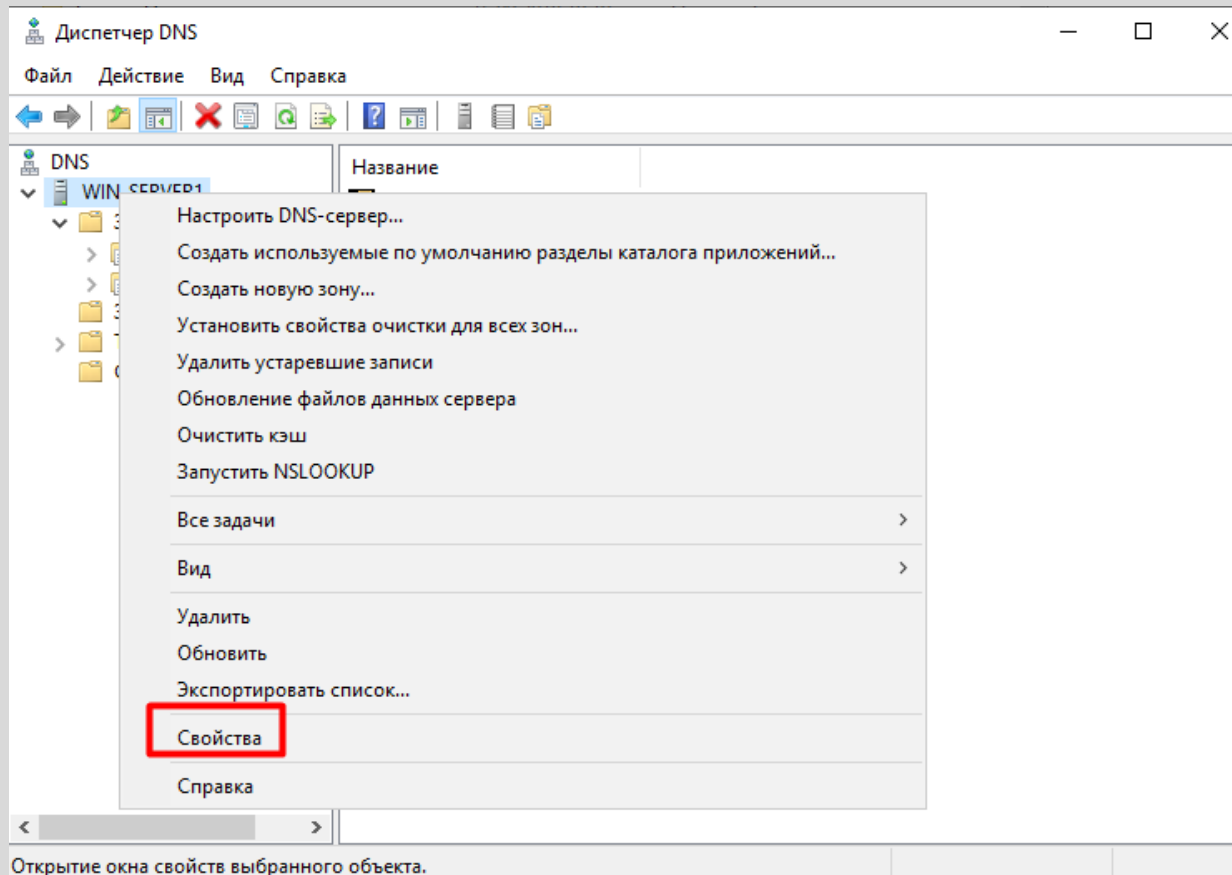
Отмена

1 нов

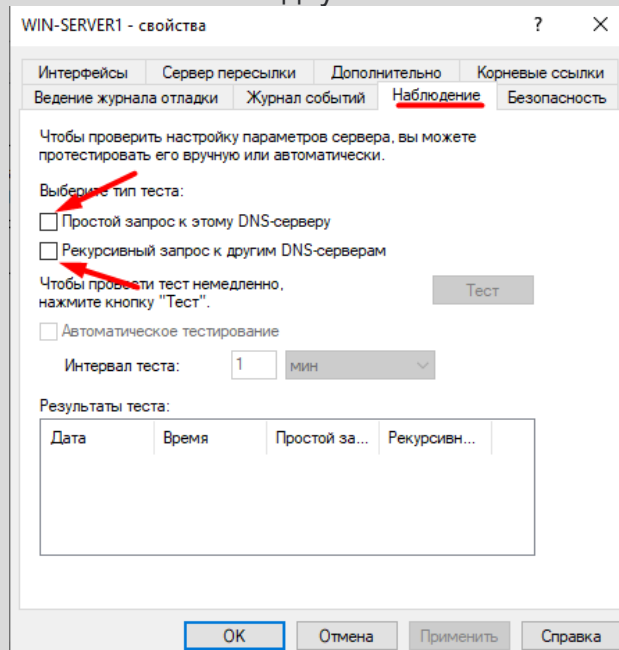
Готово

## 11. Сделайте простой и рекурсивный запросы к DNS серверу

### Шаг 1

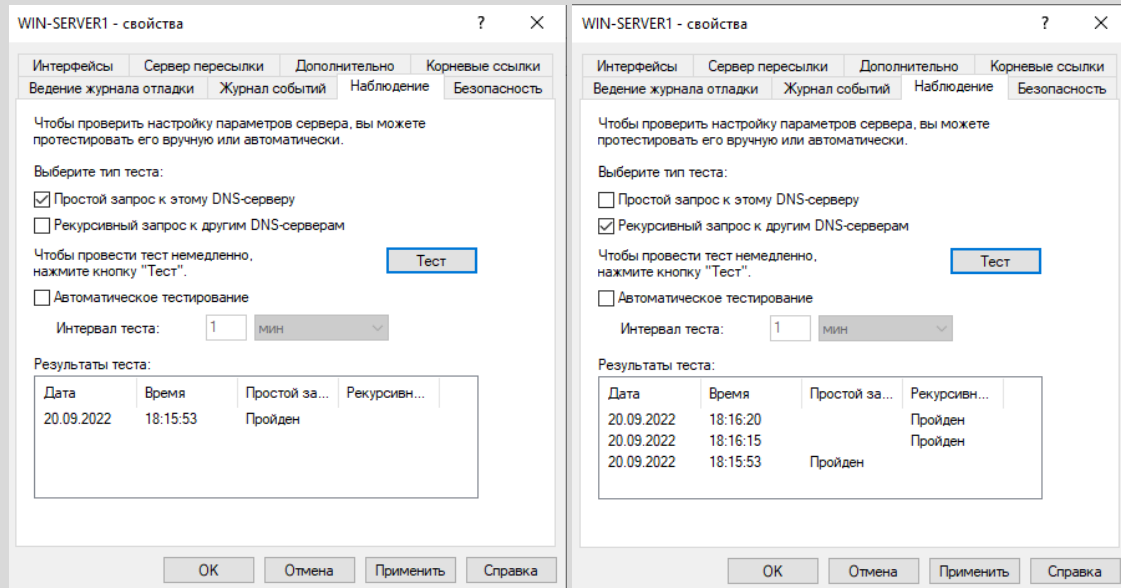


### Шаг 2. Поставил одну из галочек и нажал «Тест»





### Шаг 3



12. Используя утилиту NTDSUtil и оснастки AD передайте две роли на второй контроллер домена

Проверил, на каких доменах какие роли

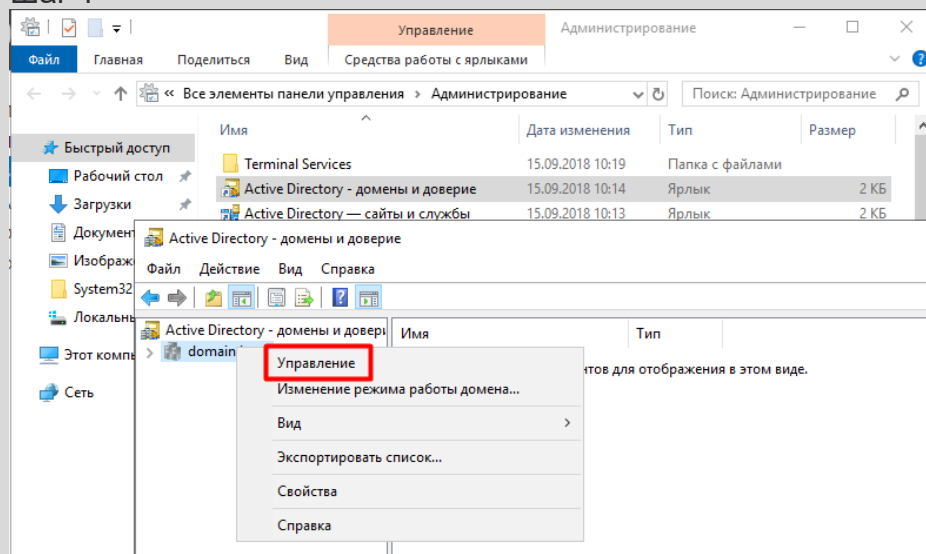
netdom query fsmo

```
PS C:\Users\Администратор> netdom query fsmo
Хозяин схемы                WIN-Server1.domain.local
Хозяин именования доменов   WIN-Server1.domain.local
PDC                          WIN-Server1.domain.local
Диспетчер пула RID           WIN-Server1.domain.local
Хозяин инфраструктуры       WIN-Server1.domain.local
Команда выполнена успешно.
```

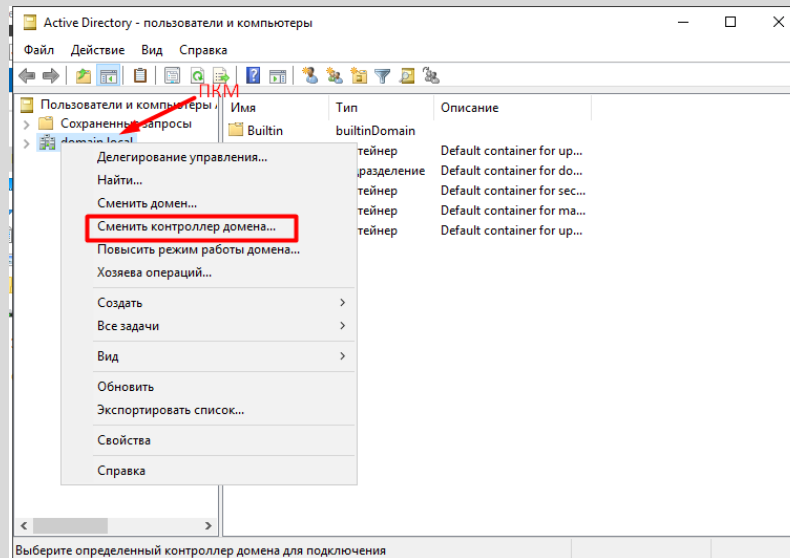
Все роли на сервере 1

Оснастка AD

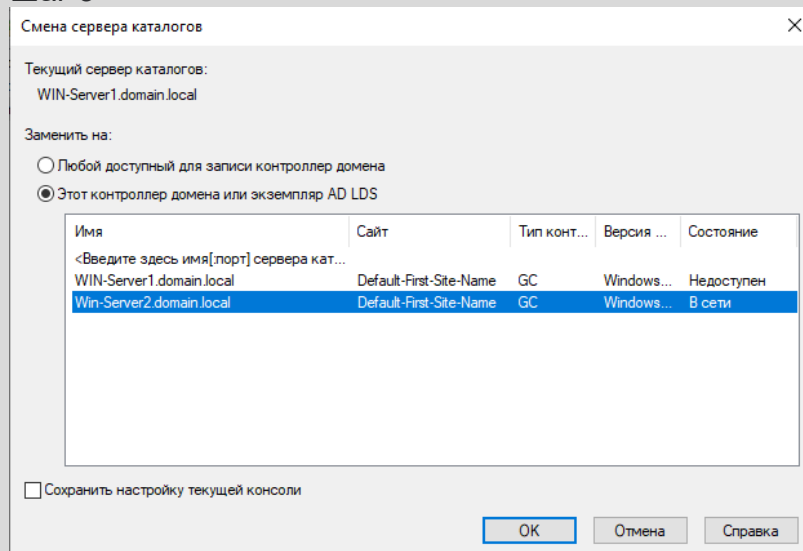
Шаг 1



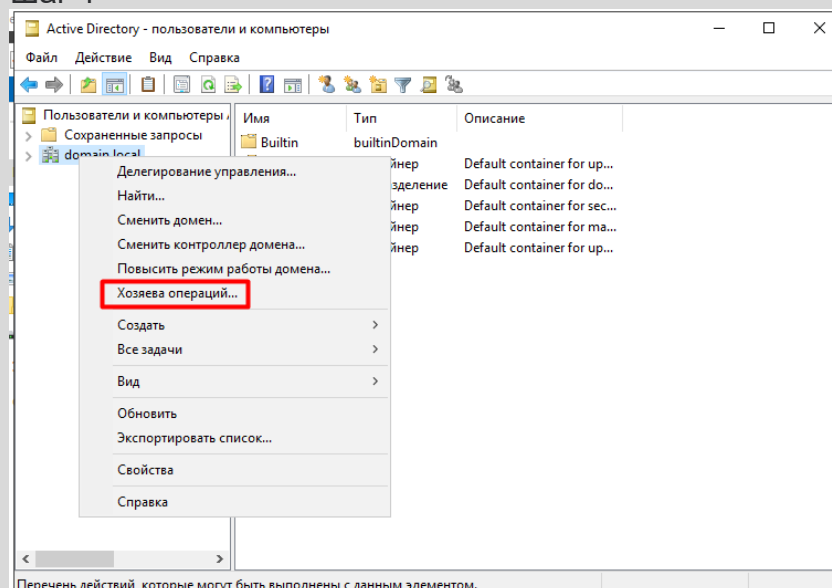
## Шаг 2



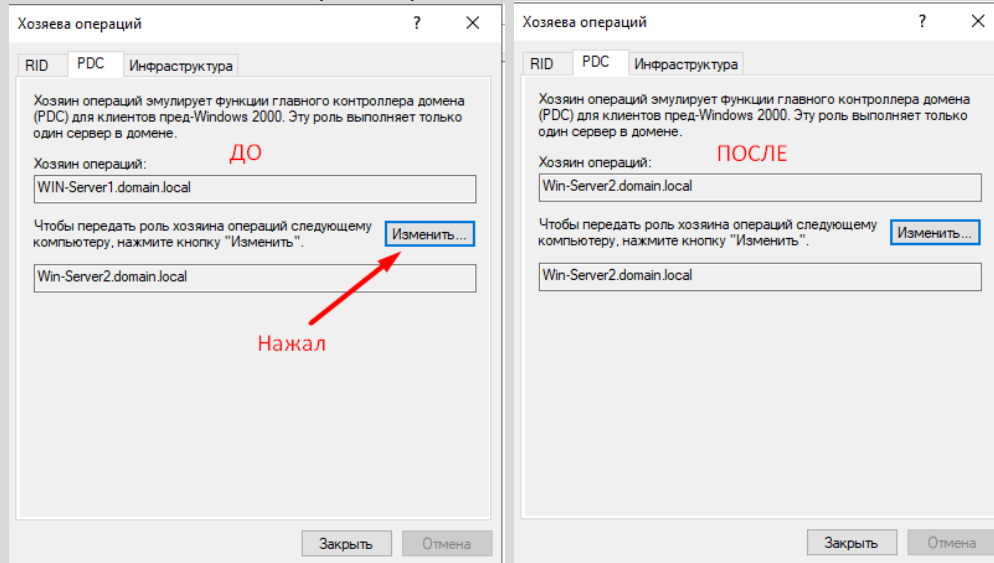
## Шаг 3



## Шаг 4



## Шаг 5. Изменил контроллер на вкладках RID и PDC



Проверил командой netdom query fsmo

```
PS C:\Users\Администратор> netdom query fsmo
Хозяин схемы                WIN-Server1.domain.local
Хозяин именования доменов   WIN-Server1.domain.local
PDC                          Win-Server2.domain.local
Диспетчер пула RID           Win-Server2.domain.local
Хозяин инфраструктуры       WIN-Server1.domain.local
Команда выполнена успешно.
```

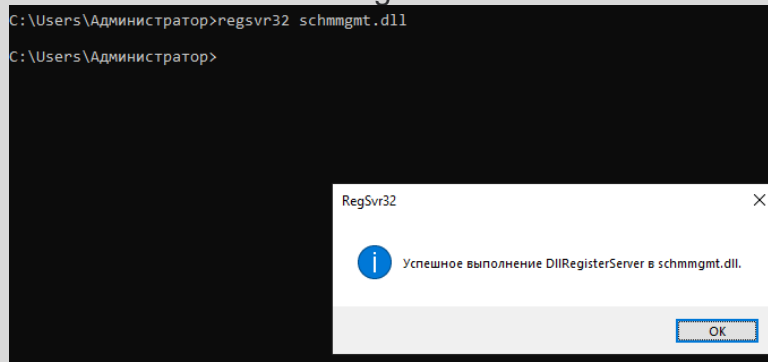
Готово

## Утилита NTDSUtil

Вернул контроллер RID и PDC на сервер 1

Шаг 1. Зарегистрировал необходимую библиотеку

Win +R -> cmd -> schmmgmt.dll



Шаг 2. Ввёл ряд команд

```
ntdsutil
roles
connections
connect to server win-server1    #здесь указал имя сервера, на которой надо
```

передать контроллер!

q  
transfer pdc                    ДА  
transfer rid master            ДА

Шаг 3. Проверил

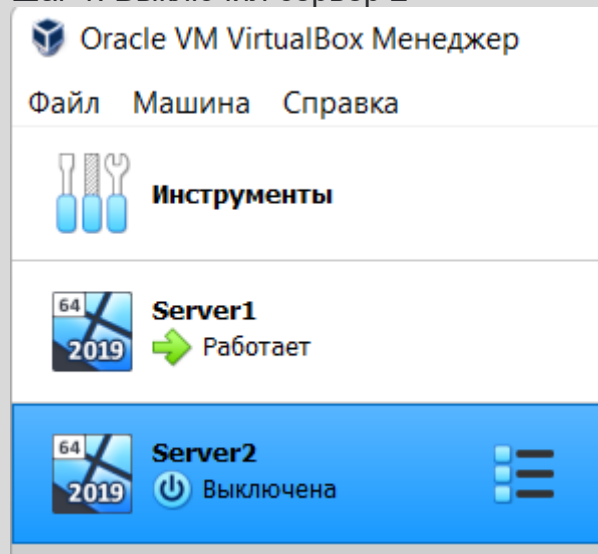
netdom query fsmo

```
PS C:\Users\Администратор> netdom query fsmo
Хозяин схемы                    WIN-Server1.domain.local
Хозяин именования доменов    WIN-Server1.domain.local
PDC                             WIN-Server1.domain.local
Диспетчер пула RID            WIN-Server1.domain.local
Хозяин инфраструктуры        WIN-Server1.domain.local
Команда выполнена успешно.
```

Готово

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

Шаг 1. Выключил сервер 2



Шаг 2. Открыл Powershell

ntdsutil  
roles  
connections  
connect to server win-server1  
  
q

seize pdc *#принудительная передача роли seize, в отличии от согласованного transfer*

seize rid master

Т.к. в предыдущем задании я уже передал роли, то соответствующий вывод:

```
fsmo maintenance: Seize PDC
Попытка безопасной передачи PDC FSMO перед захватом.
Успешная передача FSMO - захват не требуется.
Серверу "win-server1" известно о 5 ролях
Схема - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Хозяин именования - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
PDC - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
RID - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Инфраструктура - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
fsmo maintenance: Seize RID master
Попытка безопасной передачи RID FSMO перед захватом.
Успешная передача FSMO - захват не требуется.
Серверу "win-server1" известно о 5 ролях
Схема - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Хозяин именования - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
PDC - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
RID - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Инфраструктура - CN=NTDS Settings,CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Активация Windows
```

Шаг 3. Удалил данные о втором контроллере из AD

Запустил Powershell

```
ntdsutil
metadata cleanup
connections
connect to server win-server1
q
```

```
select operation target
list domain
```

```
select operation target: list domain
Найдено доменов: 1
0 - DC=domain,DC=local
```

*#нашёл лишь один, с номером 0*

```
select domain 0
```

```
select operation target: select domain 0
Нет текущего сайта
Домен - DC=domain,DC=local
Нет текущего сервера
Нет текущего контекста именования
```

```
list sites
```

```
select operation target: list sites
Найдено сайтов: 1
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
```

```
select site 0
```

```
select operation target: select site 0
Сайт - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Домен - DC=domain,DC=local
Нет текущего сервера
Нет текущего контекста именования
```

```
list servers in site
```

```
select operation target: list servers in site
Найдено серверов: 2
0 - CN=WIN-SERVER1,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
1 - CN=WIN-SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local

select server 1
select operation target: select server 1
Сайт - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Домен - DC=domain,DC=local
Сервер - CN=WIN-SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Объект DSA - CN=NTDS Settings,CN=WIN-SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local
Имя DNS-узла - Win-Server2.domain.local
Объект-компьютер - CN=WIN-SERVER2,OU=Domain Controllers,DC=domain,DC=local
Нет текущего контекста именования
```

q

## remove selected server

```
metadata cleanup: remove selected server
Передача или захват ролей FSMO от выбранного сервера.
Удаление метаданных FRS для выбранного сервера.
Поиск членов FRS в "CN=WIN-SERVER2,OU=Domain Controllers,DC=domain,DC=local".
Удаление поддерева в "CN=WIN-SERVER2,OU=Domain Controllers,DC=domain,DC=local".
Ошибка при попытке удалить параметры FRS на CN=WIN-SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local: "Элемент не найден.";
очистка метаданных продолжается.
"CN=WIN-SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=domain,DC=local" удалена с сервера win-server1"
```

## Шаг 4. Проверил

The screenshot shows the Windows Server 2008 R2 interface. The main window is 'Active Directory - пользователи и компьютеры'. The left pane shows the 'domain.local' tree with 'Domain Controllers' selected. The right pane shows a table of domain controllers.

Имя	Тип	Тип контроллера	Сайт	Описание
WIN-SERVER1	Компьютер	GC	Default-First-Si...	

Below the table, there is a task list with the following data:

Имя	ИД	Состояние	Описание	Система	Время
WIN-SERVER1	10028	Ошибка	Microsoft-Windows-DistributedCOM	Система	20.09.2022 19:24:30
WIN-SERVER1	1002	Ошибка	Application Hang	Приложение	20.09.2022 19:18:36
WIN-SERVER1	10028	Ошибка	Microsoft-Windows-DistributedCOM	Система	20.09.2022 19:14:30
WIN-SERVER1	10028	Ошибка	Microsoft-Windows-DistributedCOM	Система	20.09.2022 19:14:30

Перешёл в DNS и вычистил все упоминания о win-server2 #это надо делать, чтоб в будущем, если захочу дать такое же имя новому серверу, у меня не возникло конфликтов

Диспетчер DNS

ФайлДействиеВидСправка

DNS

WIN-SERVER1

Зоны прямого просмотра

\_msdcs.domain.local

dc

\_sites

\_tcp

domains

3868eaf9-7a5f-46f4-9...

\_tcp

gc

\_sites

Default-First-Site-Name

\_tcp

pdc

\_tcp

domain.local

\_msdcs

\_sites

Default-First-Site-Name

\_tcp

\_udp

DomainDnsZones

\_sites

Default-First-Site-Name

\_tcp

\_udp

ForestDnsZones

Зоны обратного просмотра

Точки доверия

Серверы условной пересылки

Название	Тип	Значение	Отметка времени
_ldap	Располож...	[0][100][3268] WIN-Server1.domai...	15.09.2022 13:00:00

Активация Windows  
Чтобы активировать Windows, перейдите в раздел "Параметры" и выберите "Активация".  
20 с

Готово