

Выполнил Мешечкин Д. Инфобез-2345

Перед выполнением ДЗ№4 были созданы точки резервного копирования на обеих машинах. Так же по рекомендации к ДЗ№3 были выполнены команды в PS
Set-Item WSMAN:\localhost\Client\TrustedHosts -Value '*'
Ситуация координальным образом не поменялась:
Сервер GUI видит сервер GUI2 как через WAC, так и через диспетчер серверов, в том числе через AD, но сервер GUI2 не видит сервер GUI через WAC, но видит через диспетчер серверов и через AD.

Задание 1/2: Запустите утилиты repadmin /showrepl. Запустите утилиту dcdiag /test:dns , /test:topology.

Не уверен, корректно ли будет работать в PowerShell вместо cmd, но на сервере GUI выполнил всё через cmd от имени админа, на GUI2 через PowerShell от имени админа.

Администратор: Командная строка

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

Repadmin: выполнение команды /showrepl контроллере домена localhost с полным доступом
Default-First-Site-Name\WINSERV2019GUI
Параметры DSA: IS_GC
Параметры сайта: (none)
DSA - GUID объекта: d0237a2a-e747-401c-ad60-6b3d29e6185f
DSA - код вызова: d0237a2a-e747-401c-ad60-6b3d29e6185f

==== ВХОДЯЩИЕ СОСЕДИ =====

DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: 54d3624a-7b39-4ad7-96f8-2e1257f9a5ca
  Последняя попытка @ 2022-09-16 11:58:17 успешна.

CN=Configuration,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: 54d3624a-7b39-4ad7-96f8-2e1257f9a5ca
  Последняя попытка @ 2022-09-16 12:03:53 успешна.

CN=Schema,CN=Configuration,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: 54d3624a-7b39-4ad7-96f8-2e1257f9a5ca
  Последняя попытка @ 2022-09-16 11:58:17 успешна.

DC=DomainDnsZones,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: 54d3624a-7b39-4ad7-96f8-2e1257f9a5ca
  Последняя попытка @ 2022-09-16 11:58:17 успешна.

DC=ForestDnsZones,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: 54d3624a-7b39-4ad7-96f8-2e1257f9a5ca
  Последняя попытка @ 2022-09-16 11:58:17 успешна.

C:\Users\Администратор>
```

Администратор: Windows PowerShell

```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

PS C:\Users\Администратор.TESTGBDOMAIN> repadmin /showrepl

Repadmin: выполнение команды /showrepl контроллере домена localhost с полным доступом
Default-First-Site-Name\WINSERV2019GUI2
Параметры DSA: IS_GC
Параметры сайта: (none)
DSA - GUID объекта: 54d3624a-7b39-4ad7-96f8-2e1257f9a5ca
DSA - код вызова: db68de56-fff3-44d4-a3aa-0aa9bc3f6b78

==== ВХОДЯЩИЕ СОСЕДИ =====

DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: d0237a2a-e747-401c-ad60-6b3d29e6185f
  Последняя попытка @ 2022-09-16 12:19:29 успешна.

CN=Configuration,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: d0237a2a-e747-401c-ad60-6b3d29e6185f
  Последняя попытка @ 2022-09-16 12:03:38 успешна.

CN=Schema,CN=Configuration,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: d0237a2a-e747-401c-ad60-6b3d29e6185f
  Последняя попытка @ 2022-09-16 11:58:43 успешна.

DC=DomainDnsZones,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: d0237a2a-e747-401c-ad60-6b3d29e6185f
  Последняя попытка @ 2022-09-16 11:58:43 успешна.

DC=ForestDnsZones,DC=testgbdomain,DC=com
  Default-First-Site-Name\WINSERV2019GUI2 через RPC
  DSA - GUID объекта: d0237a2a-e747-401c-ad60-6b3d29e6185f
  Последняя попытка @ 2022-09-16 11:58:43 успешна.

PS C:\Users\Администратор.TESTGBDOMAIN>
```

Администратор: Командная строка

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

Диагностика сервера каталогов

Выполнение начальной настройки:
Выполняется попытка поиска основного сервера...
Основной сервер = WinServ2019GUI
* Определен лес AD.
Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI
Запуск проверки: Connectivity
..... WINSERV2019GUI - пройдена проверка Connectivity

Выполнение основных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI

Запуск проверки: DNS

Проверки DNS выполняются без зависания. Подождите несколько минут...
..... WINSERV2019GUI - 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: testgbdomain

Выполнение проверок предприятия на: testgbdomain.com
Запуск проверки: DNS
Результаты проверки контроллеров домена:

Контроллер домена: WinServ2019GUI.testgbdomain.com
Домен: testgbdomain.com

Администратор: Windows PowerShell

Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

PS C:\Users\администратор.TESTGBDOMAIN> dcdiag /test:dns

Диагностика сервера каталогов

Выполнение начальной настройки:
Выполняется попытка поиска основного сервера...
Основной сервер = WinServ2019GUI2
* Определен лес AD.
Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI2
Запуск проверки: Connectivity
..... WINSERV2019GUI2 - пройдена проверка Connectivity

Выполнение основных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI2

Запуск проверки: DNS

Проверки DNS выполняются без зависания. Подождите несколько минут...
..... WINSERV2019GUI2 - 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: testgbdomain

Выполнение проверок предприятия на: testgbdomain.com
Запуск проверки: DNS
Результаты проверки контроллеров домена:

Контроллер домена: WinServ2019GUI2.testgbdomain.com
Домен: testgbdomain.com

TEST: Basic (Basc)
Внимание! У адаптера 00:15:5D:01:26:05 динамический IP-адрес(возможна неправильная настройка)

TEST: Records registration (RReg)
Сетевой адаптер [00000001] Microsoft Hyper-V Network Adapter:
Внимание!
Отсутствует запись A на DNS-сервере 192.168.1.153:
gc._msdcs.testgbdomain.com

Внимание! Не удастся найти регистрации записей для некоторых сетевых адаптеров

WinServ2019GUI PASS WARN PASS PASS PASS PASS n/a
..... testgbdomain.com - пройдена проверка DNS

TEST: Basic (Basc)
Внимание! У адаптера 00:15:5D:01:26:06 динамический IP-адрес(возможна неправильная настройка)

WinServ2019GUI2 PASS WARN PASS PASS PASS PASS n/a
..... testgbdomain.com - пройдена проверка DNS

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

Диагностика сервера каталогов

Выполнение начальной настройки:
Выполняется попытка поиска основного сервера...
Основной сервер = WinServ2019GUI
* Определен лес AD.
Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI
Запуск проверки: Connectivity
..... WINSERV2019GUI - пройдена проверка Connectivity

Выполнение основных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI
Запуск проверки: Topology
..... WINSERV2019GUI - 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: testgbdomain

Выполнение проверок предприятия на: testgbdomain.com

PS C:\Users\администратор.TESTGBDOMAIN> dcdiag /test:topology

Диагностика сервера каталогов

Выполнение начальной настройки:
Выполняется попытка поиска основного сервера...
Основной сервер = WinServ2019GUI2
* Определен лес AD.
Сбор начальных данных завершен.

Выполнение обязательных начальных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI2
Запуск проверки: Connectivity
..... WINSERV2019GUI2 - пройдена проверка Connectivity

Выполнение основных проверок

Сервер проверки: Default-First-Site-Name\WINSERV2019GUI2
Запуск проверки: Topology
..... WINSERV2019GUI2 - 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: testgbdomain

Выполнение проверок предприятия на: testgbdomain.com
PS C:\Users\администратор.TESTGBDOMAIN>

По результатам вывода команд тесты пройдены на обоих серверах, за исключением записей A на DNS-сервере 192.168.1.153.

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

Аналогично предыдущим заданиям, будет всё выполняться в командной строке и PS.

C:\Users\Администратор>whoami
testgbdomain\администратор

C:\Users\Администратор>whoami /user

Сведения о пользователе

Пользователь SID

testgbdomain\администратор S-1-5-21-4013446233-1495740280-1893065651-500

C:\Users\Администратор>

```

PS C:\Users\администратор.TESTGBDOMAIN> whoami
testgbdomain\администратор
PS C:\Users\администратор.TESTGBDOMAIN> whoami /user

Сведения о пользователе
-----

Пользователь          SID
=====
testgbdomain\администратор S-1-5-21-4013446233-1495740280-1893065651-500
PS C:\Users\администратор.TESTGBDOMAIN>

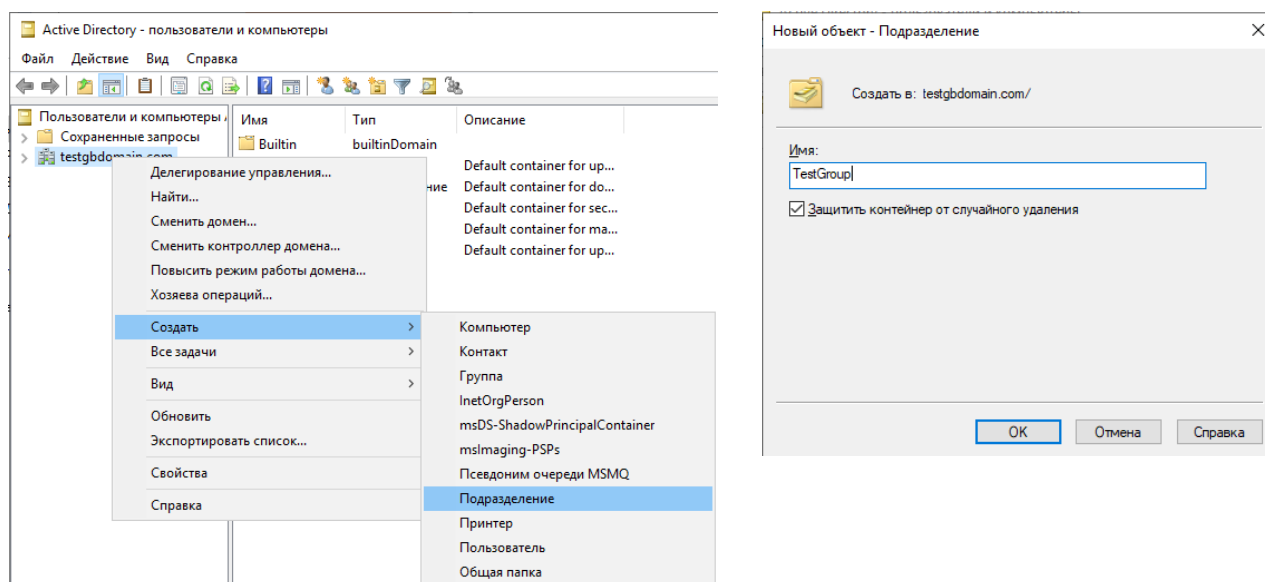
```

Видно, что SID на обеих машинах совпадают, да и изначально было видно, что пользователь, от имени которого выполняются команды - является администратором в домене, а значит по простому - администратором на сервере GUI. Для смены пользователя и просмотра именно SID сервера GUI2, необходимо будет убрать сервер GUI2 из домена, созданного ранее в ДЗ№3. Возможно тут не прав и беглый полчасовой поиск и попытки найти решения - результатов не дали.

Задание 4/5/6/7: Создайте защищенную от удаления ОП (OU). Создайте в ней учетные записи нескольких пользователей, компьютеров, группу. Добавьте пользователей в группу. Удалите созданную OU.

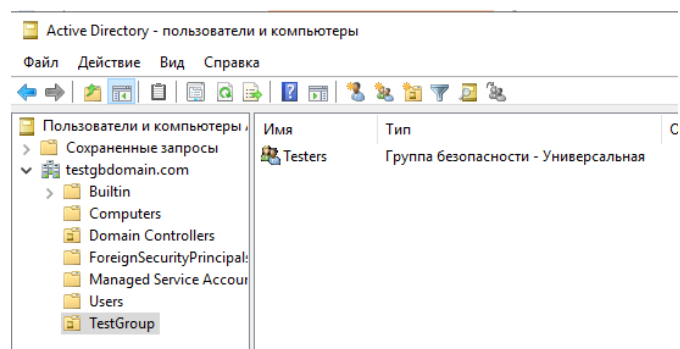
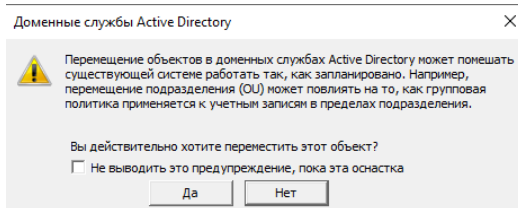
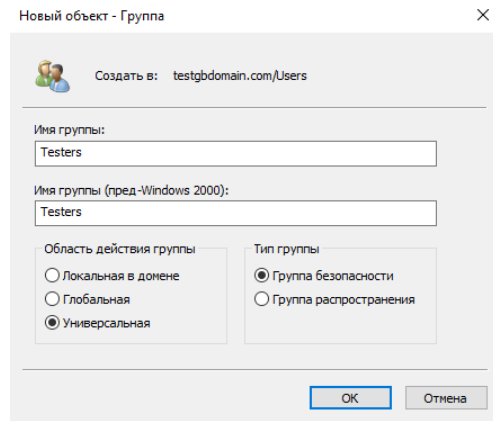
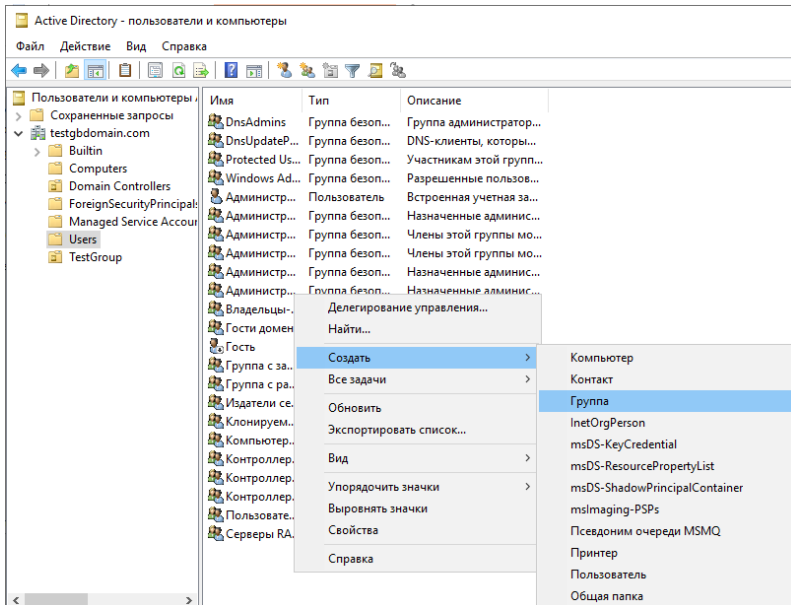
Для выполнения задания необходимо в "Средствах администрирования -> Пользователи и компьютеры Active Directory" открыть необходимый домен и в нём производить действия.

Для создания защищённой от удаления OU, на домене ПКМ -> Создать -> Подразделение и далее в открывшемся окне ставится флаг "Защитить контейнер от случайного удаления".

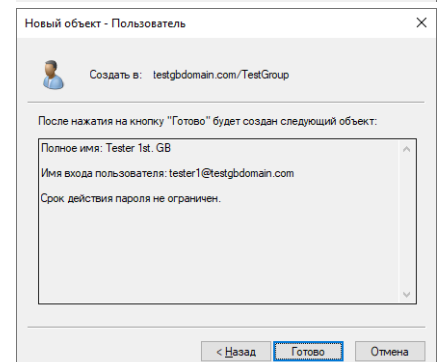
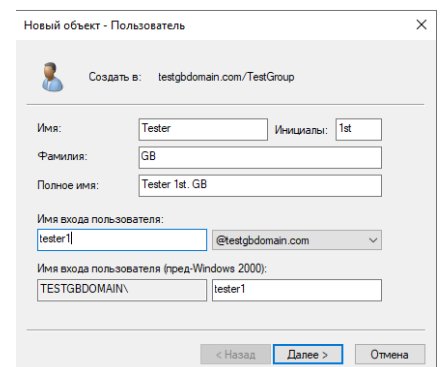
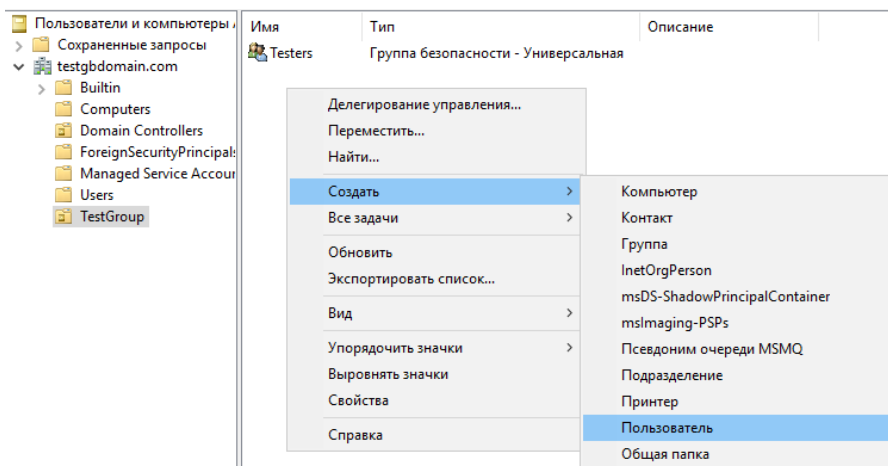


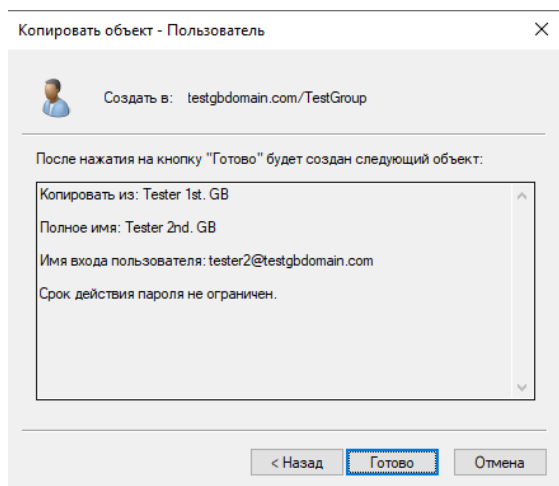
Для создания защищённой от удаления OU, на домене ПКМ -> Создать -> Подразделение и далее в открывшемся окне ставится флаг "Защитить контейнер от случайного удаления".

Для создания группы: в разделе домена -> Users в правом окне ПКМ -> Создать -> Группа. Создается группа Testers с областью действия "Универсальная" для возможного дальнейшего взаимодействия с другими доменами и типом "Группа безопасности" для доступа к различным директориям в домене. После создания, группу можно перетащить в созданное подразделение. После чего группа появится уже в подразделении.

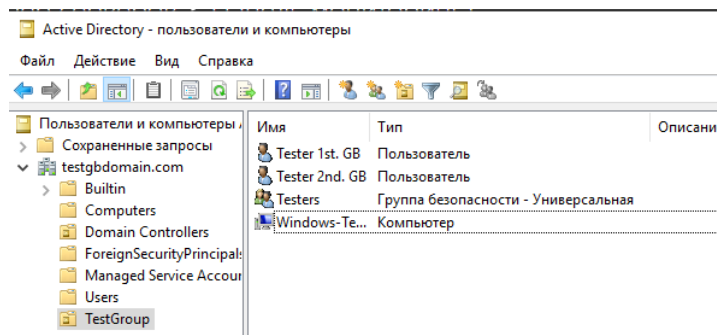
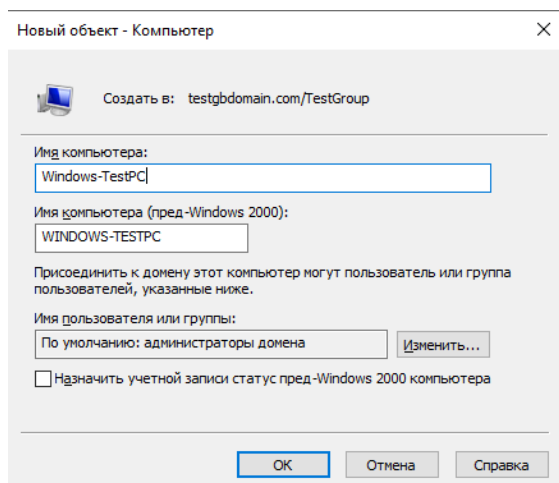


Дальше необходимо создать несколько пользователей. В созданном подразделении ПКМ -> Создать -> Пользователь. И далее заполняются поля. При нажатии "Далее" заполняются поля с паролями. В зависимости от ситуации выбираются различные флаги при создании пароля. После открывается окно с общей информацией по добавлению нового пользователя. Для создания дополнительных пользователей можно изначально создать пользователя-шаблон с установленными общими свойствами, и далее ПКМ -> копировать, после чего заполнить первое окно по созданию с личными данными пользователя, в тоже время уже добавленные данные в свойствах будут добавлены в свойства создаваемого пользователя.

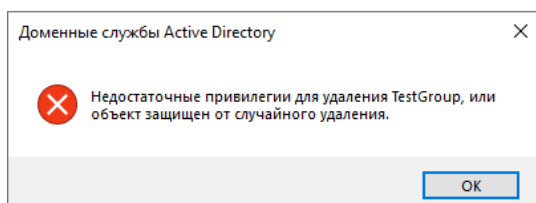




Создание компьютера в том же подразделении производится примерно аналогичным способом, как и с пользователями. ПКМ -> Создать -> Компьютер. Далее заполняются поля. В данной ситуации добавление ПК будет достаточно проблематичным, намного проще будет уже добавить существующий ПК в AD в созданное подразделение.



Стандартное и самое простое удаление данного подразделения через ПКМ -> Удалить - не работает.

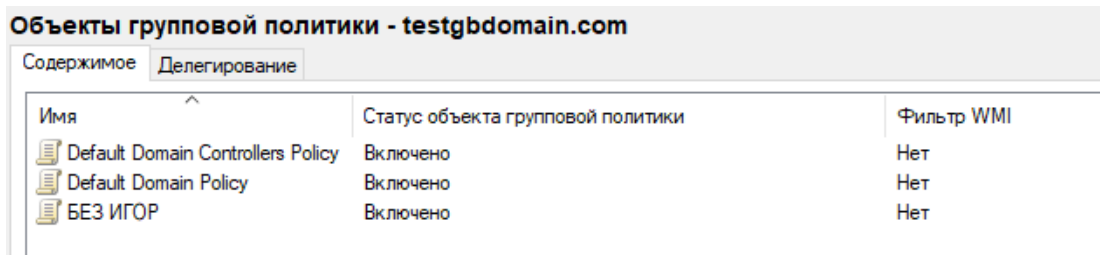
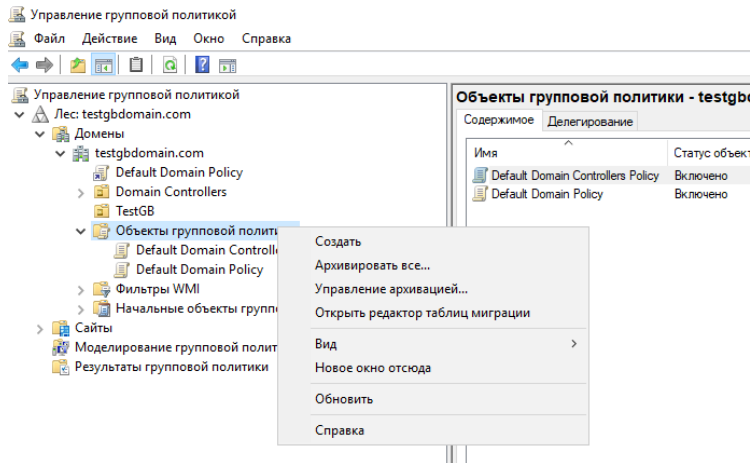


Необходимо в окне "Active directory - Пользователи и компьютеры" нажать "Вид -> Дополнительные компоненты". После в "Свойствах" подразделения будут доступны дополнительные вкладки, где на вкладке "Объект" необходимо убрать флажок "Защитить объект от случайного удаления" и уже после будет возможность удалить данное "защищенное" (уже не совсем) подразделение. После попытки удаления AD выдаст предупреждение. Тестовое подразделение не жалко, сносится без сожалений. После отключаются "Дополнительные компоненты" и окно принимает стандартный вид.

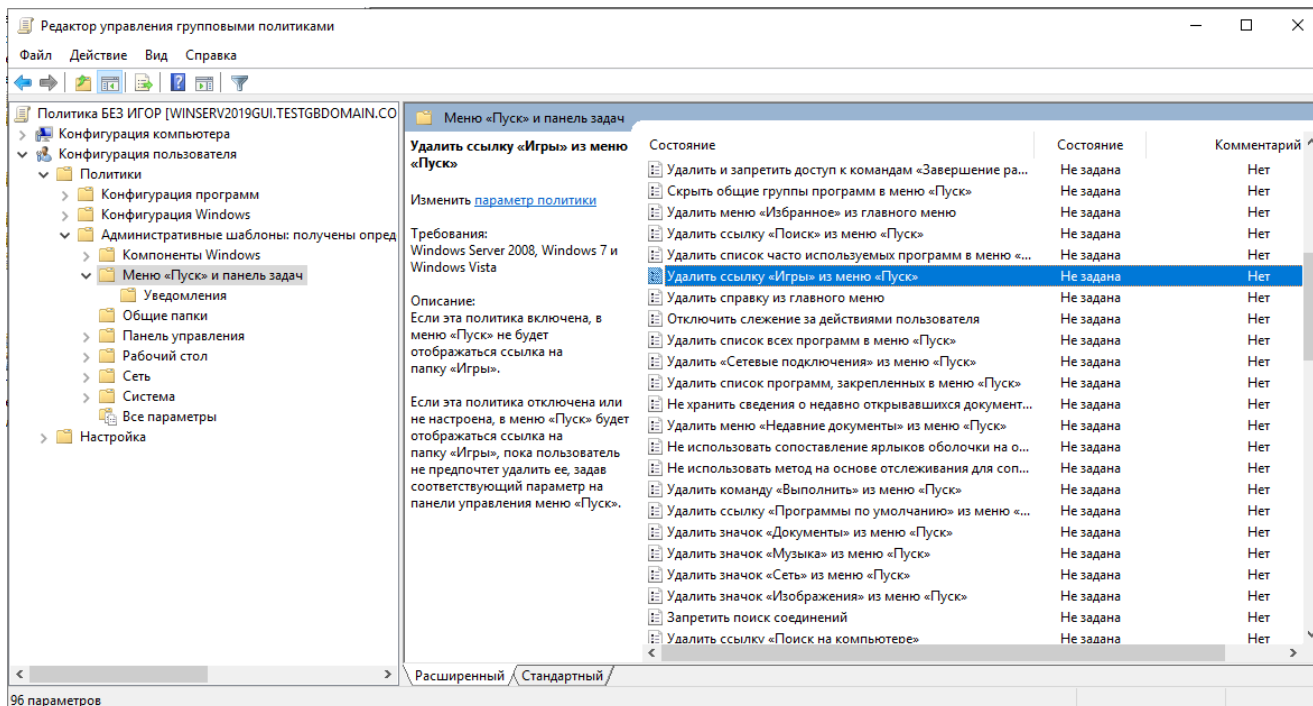


Задание 8/9: Создайте групповую политику (GPO) с блокировкой ссылки "Игры" и подключите к любой OU. Удалите созданную GPO.

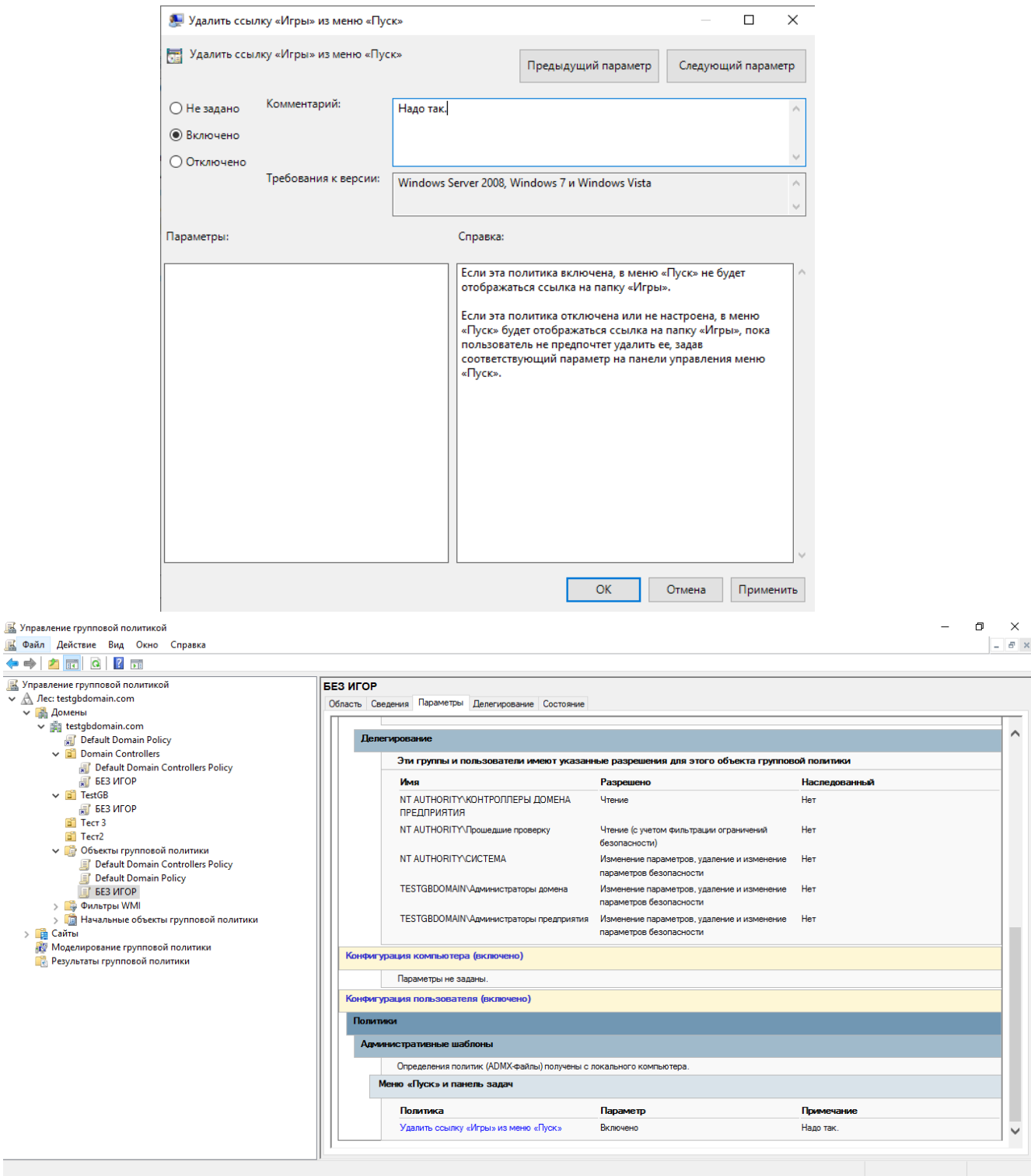
Для создания групповой политики необходимо: "Средства администрирования -> Управление групповой политикой", далее в нашем домене выбираются "Объекты групповой политики -> ПКМ -> Создать" и создать новую политику.



Далее необходимо настроить GPO. На созданной политике ПКМ -> Изменить. Открывается "Редактор управления групповыми политиками", далее для поиска "Игр": "Конфигурация пользователя -> Политики -> Административные шаблоны -> Меню "Пуск" и панель задач" Далее в правом окне необходимо найти "Удалить ссылку "Игры" из меню Пуск".



Двойной клик на данной опции открывает окно, в которой есть возможность отключить данную ссылку. После чего данное отключение можно будет посмотреть в управлении групповой политикой, в созданной политике, в закладке "параметры".



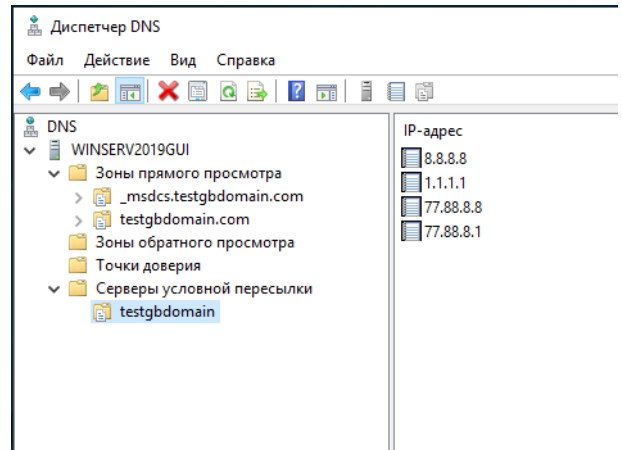
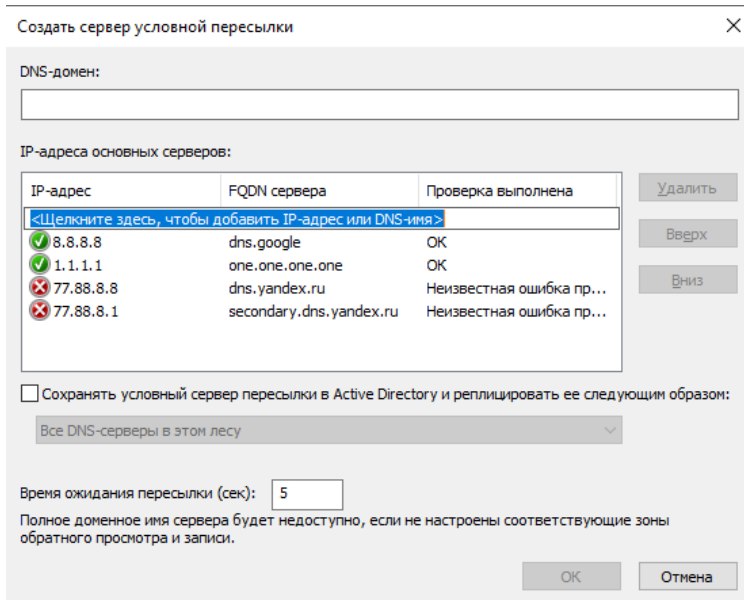
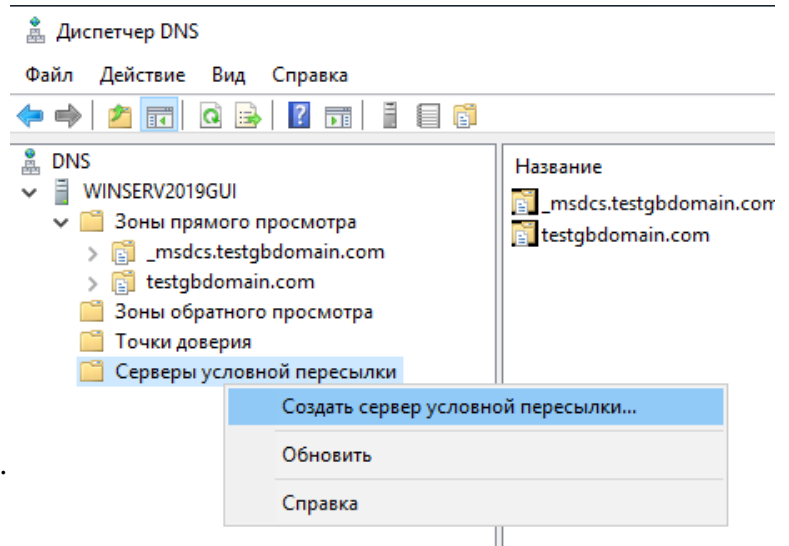
После добавляется данная политика к созданному подразделению. Далее для завершения задания - политика удаляется. Данная политика удаляется сразу со всех добавленных подразделений, если удалять непосредственно саму политику, а не скопированную в подразделение.

Задание 10: Добавьте в качестве сервера пересылки адрес 8.8.8.8

Для выполнения задания необходимо в "Пуск -> Средства администрирования -> DNS" далее в левом окне выбирается сервер, в моём случае GUI, далее на строке "Серверы условной пересылки" ПКМ и "Создать сервер условной пересылки". Далее задаётся адрес 8.8.8.8 - являющийся DND Гугла, 1.1.1.1 - адрес DNS Cloudflare, яндекс свои два DNS отключил. Так же необходимо задать имя, в противном случае создание сервера условной пересылки не хочет сохраняться. Фантазии нет, DNS-домен "testgbdomain".

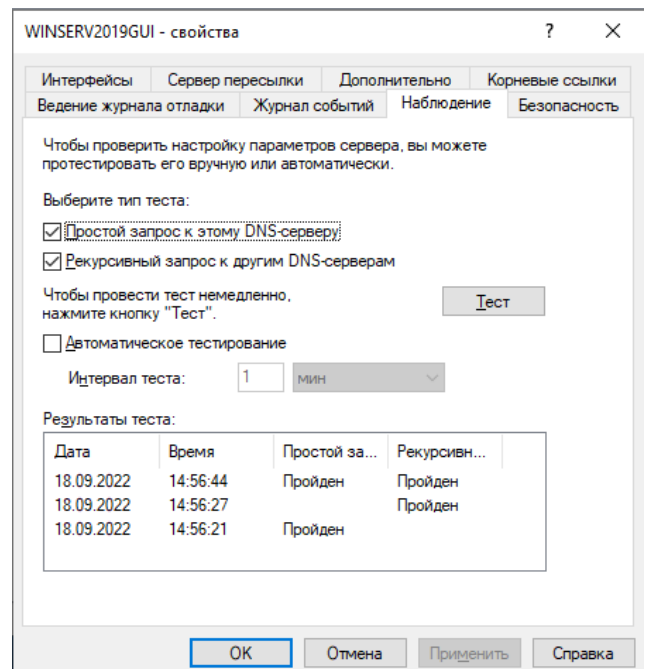
Кстати мертвы ещё 4 DNS сервера яндекса:

безопасный и семейный. 77.88.8.88, 77.88.8.2, 77.88.8.7, 77.88.8.3



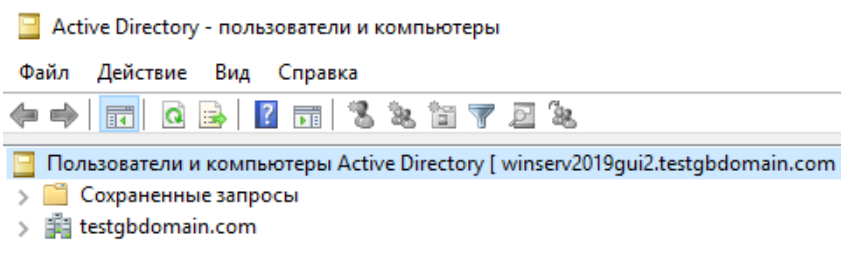
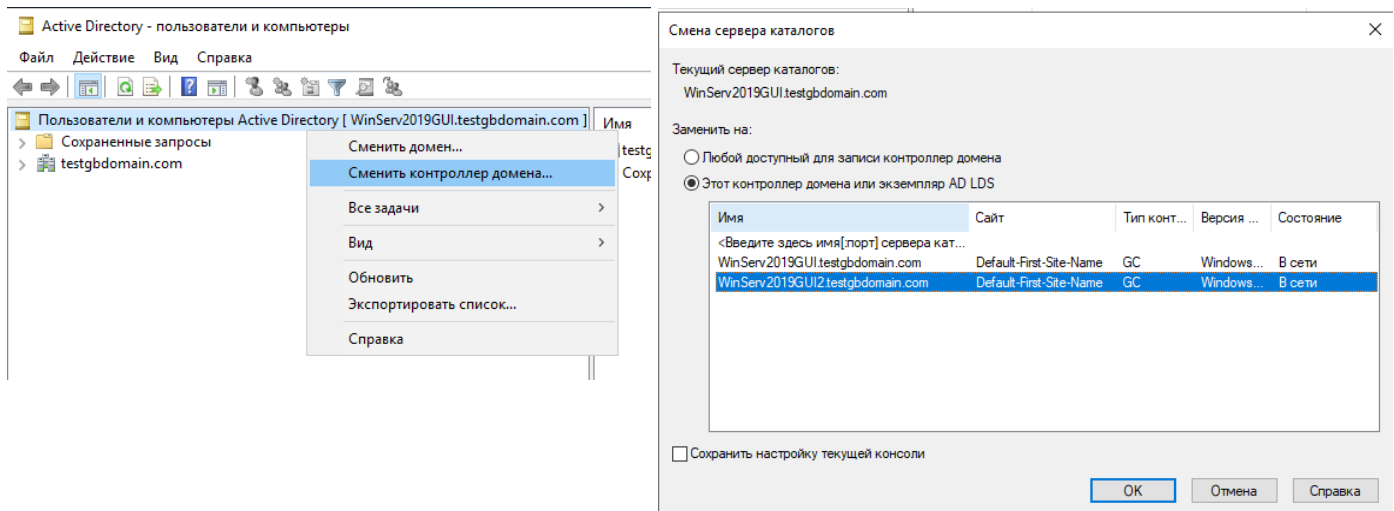
Задание 11: Сделайте простой и рекурсивный запросы к ДНС серверу.

Для выполнения задания, в "Диспетчере DNS" в левом окне на строке с названием сервера ПКМ, далее "свойства". В закладке "интерфейсы" был оставлен сначала только внутренний адрес сервера GUI, после выставлен флаг "По всем IP-адресам". В закладке "Наблюдение" были произведены запросы. В обоих случаях все тесты были пройдены.

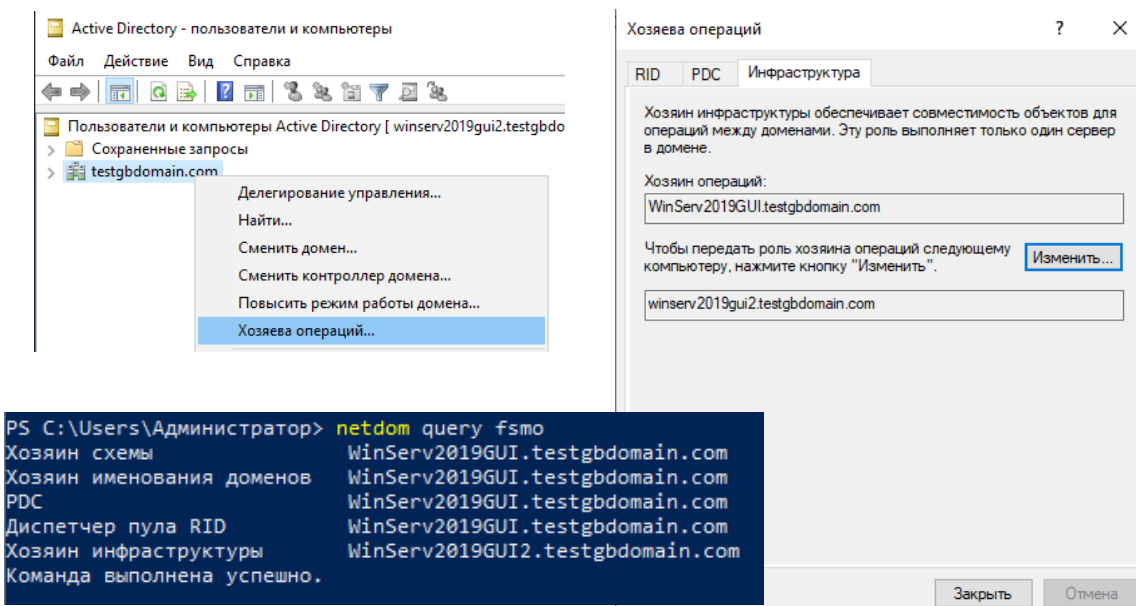


Задание 12: Используя утилиту NTDSUtil и оснастки AD передайте две роли на второй контроллер домена.

В одном случае для выполнения задания необходимо вернуться в "Пользователи и компьютеры AD", далее необходимо переключиться на другой контроллер домена, для этого на ПКМ на "Пользователи и компьютеры -> сменить контроллер домена", далее выбрать сервер GUI2, после чего получаем второй сервер GUI2 в строке активного компьютера в AD.



Для передачи роли на второй контроллер домена необходимо на домене "testgbdomain.com" ПКМ, далее "Хозяева операции", и в закладке "Инфраструктура" прожимается "Изменить". Для проверки в PowerShell вводится команда "netdom query fsmo", в отчёте видно, что "Хозяин инфраструктуры" делегированы серверу GUI2.



Для передачи роли на второй контроллер домена необходимо на домене "testgbdomain.com" ПКМ, далее "Хозяева операции", и в закладке "Инфраструктура" прожимается "Изменить". Для проверки в PowerShell вводится команда "netdom query fsmo", в отчете видно, что "Хозяин инфраструктуры" делегированы серверу GUI2.

Второй способ делегировать через утилиту NTDSUtil. Через "Пуск" запускается с правами администратора. Далее в командной строке:

roles

connections

connect to server winserv2019gui2

q

transfer PDC

Таким образом для второго контроллера домена был передан PDC.

```
PS C:\Users\Администратор> netdom query fsmo
Хозяин схемы WinServ2019GUI.testgbdomain.com
Хозяин именования доменов WinServ2019GUI.testgbdomain.com
PDC WinServ2019GUI.testgbdomain.com
Диспетчер пула RID WinServ2019GUI.testgbdomain.com
Хозяин инфраструктуры WinServ2019GUI.testgbdomain.com
Команда выполнена успешно.
```

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

Происходит "отказ" оборудования в лице схлопывания черной дыры в сервере GUI2, необходимо перехватить управление переданными функциями на сервер GUI. Для этого через NTDSUtil от имени администратора

roles

connections

connect to server winserv2019gui

q

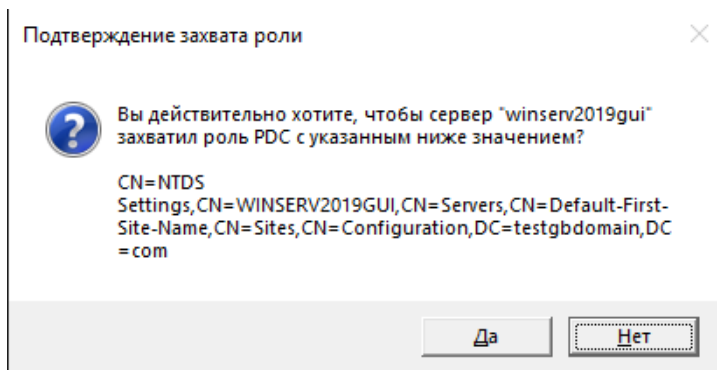
transfer PDC

В данном случае перевод не работает из-за отказа оборудования на сервере GUI2, поэтому необходимо перезаписать роль принудительно.

seize PDC, после аналогично проделывается с инфраструктурой

seize infrastructure master, после проверяется через netdom query fsmo

Перехват ролей выполнен, можно удалять второй контроллер.



```
PS C:\Users\Администратор> netdom query fsmo
Хозяин схемы WinServ2019GUI.testgbdomain.com
Хозяин именования доменов WinServ2019GUI.testgbdomain.com
PDC WinServ2019GUI.testgbdomain.com
Диспетчер пула RID WinServ2019GUI.testgbdomain.com
Хозяин инфраструктуры WinServ2019GUI.testgbdomain.com
Команда выполнена успешно.
```

Для начала необходимо через NTDSUtil - Очистка объектов ликвидированных серверов

metadata cleanup

connections

connect to server winserv2019gui

q

select operation target

list domain

select domain 0

list sites

select site

list servers in site

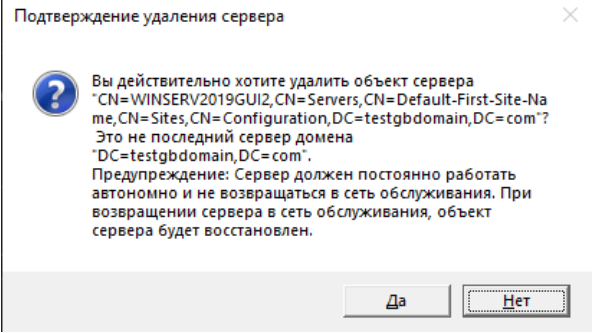
select server 1

q

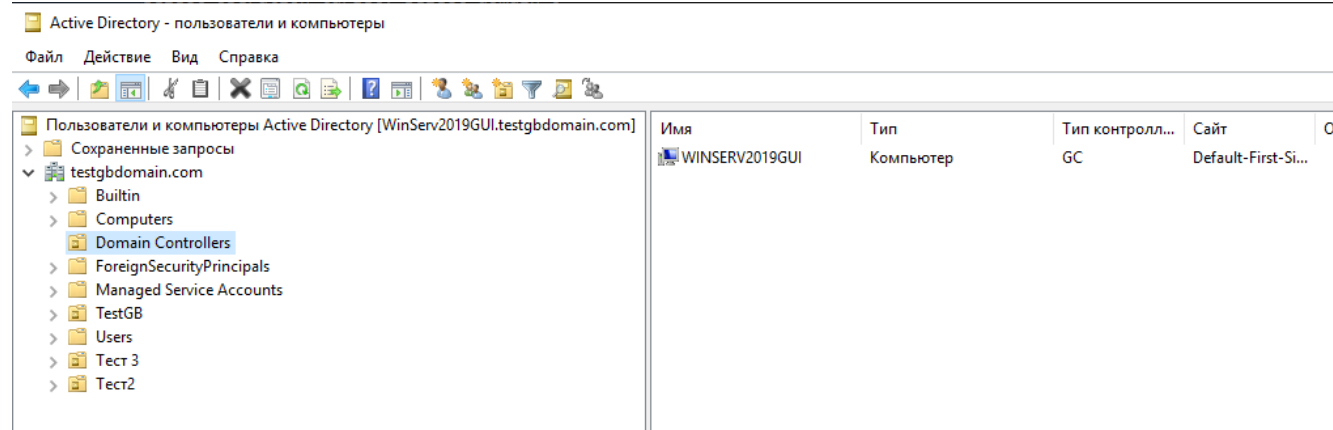
remove selected server

```
C:\Windows\System32\ntdsutil.exe: metadata cleanup
metadata cleanup: connections
server connections: connect to server winserv2019gui
Привязка к winserv2019gui ...
Подключен к winserv2019gui с помощью учетных данных локального пользователя.
server connections: q
metadata cleanup: select operation target
select operation target: list domain
Найдено доменов: 1
0 - DC=testgbdomain,DC=com
select operation target: select domain 0
Нет текущего сайта
Домен - DC=testgbdomain,DC=com
Нет текущего сервера
Нет текущего контекста именования
select operation target: list sites
Найдено сайтов: 1
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
select operation target: select site 0
Сайт - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
Домен - DC=testgbdomain,DC=com
Нет текущего сервера
Нет текущего контекста именования
select operation target: list servers in site
Найдено серверов: 2
0 - CN=WINSERV2019GUI,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
1 - CN=WINSERV2019GUI2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
select operation target: list servers in site
Найдено серверов: 2
0 - CN=WINSERV2019GUI,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
1 - CN=WINSERV2019GUI2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
select operation target: select server 1
Сайт - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
Домен - DC=testgbdomain,DC=com
Сервер - CN=WINSERV2019GUI2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
Объект DSA - CN=NTDS Settings,CN=WINSERV2019GUI2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=testgbdomain,DC=com
Имя DNS-узла - WinServ2019GUI2.testgbdomain.com
Объект-компьютер - CN=WINSERV2019GUI2,OU=Domain Controllers,DC=testgbdomain,DC=com
Нет текущего контекста именования
select operation target: _
```

Активация Wind
Чтобы активировать
раздел "Параметры":



После завершения удаления данных, возвращаюсь в AD - пользователи и компьютеры, обновляется директория Domain Controllers и остается один сервер в AD.



Далее в "Диспетчере DNS" необходимо пройтись по всем директориями и удалить любое упоминание о сервере GUI2.