Создание виртуальной сети вымышленного предприятия «COMPANY» на базе Windows Server 2016.

Часть 3. RSAT, дальнейшее знакомство с групповой политикой, удаленный рабочий стол.

Задание.

На базе развернутой и настроенной в предыдущих работах виртуальной сети (контроллера домена, интернет-шлюза и клиента) необходимо выполнить следующие задачи:

1. Установка на компьютере Win10 средств администрирования Windows Server. Проверка подключения и возможности управления серверами.
2. Средствами ГП создать группу лаборантов имеющих права локального администратора на компьютерах домена (на примере Win10). Отключить учетные записи локального администратора и гостя на компьютере Win10.
3. Настроить удаленный рабочий стол на серверах и проверить возможность подключения с компьютера Win10.

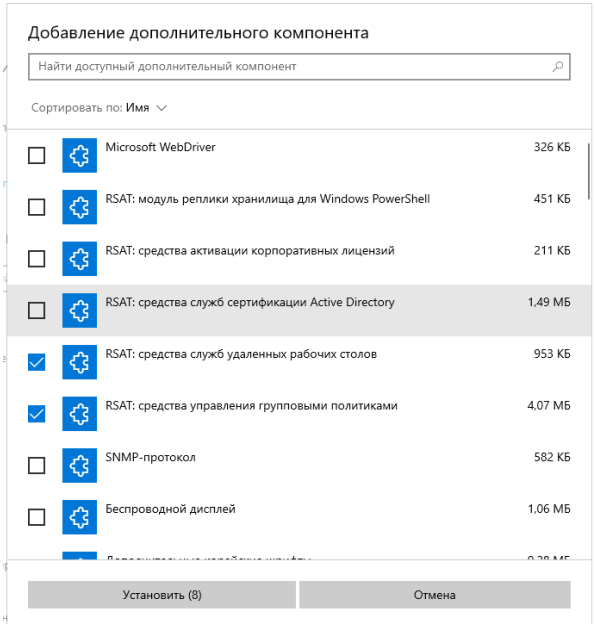
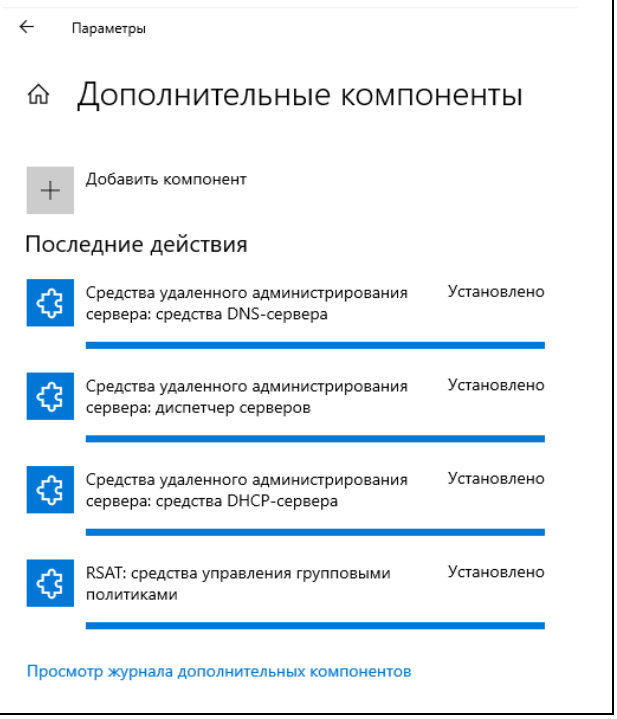
Задача 1.

Набор компонентов RSAT (Remote Server Administration Tools - Средства удаленного администрирования сервера) позволяет удаленно управлять серверными ролями и компонентами на серверах Windows Server с обычной рабочей станции . В RSAT входят как графические MMC оснастки, так и утилиты командной строки, и модули PowerShell. Вы можете установить RSAT как на десктопных версиях Windows 10 или 11, так и на платформе Windows Server.

Установка RSAT (где скачать?)

В современных билдах Windows 10 пакет Remote Server Administration Tools не нужно скачивать вручную. Средства его установки уже встроены в образ Windows 10 и доступны через опцию «**Функции по требованию/Features on Demand**».

Открываем через **«Параметры – Приложения – Дополнительные компоненты – Добавить компонент»**

Выбор компонентов:	Установка:
	

Выбираем для примера компоненты:

RSAT: Средства управления групповыми политиками;

Средства удаленного администрирования сервера: диспетчер серверов;

Средства удаленного администрирования сервера: средства DHCP сервера;

Средства удаленного администрирования сервера: средства DNS сервера.

Средства удаленного администрирования сервера: средства доменных служб Active Directory

Примечание: для подобного способа установки обязательно наличие доступа в Интернет. Соответственно, в предыдущей работе должен быть успешно настроен интернет-шлюз GATE01 и функционировать контроллер домена DCSERVER1.

Если установка через «Дополнительные компоненты - добавить компоненты» не удается, то скачайте и установите 64-битную версию пакета RSAT на Win10 по прямой ссылке:

https://www.microsoft.com/ru-RU/download/details.aspx?id=45520

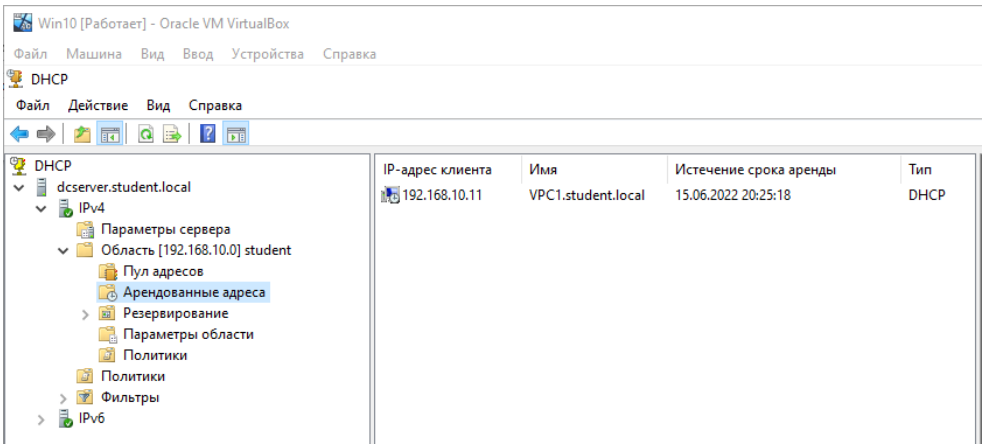
При возникновении ошибки при запуске скачанного пакета необходимо запустить службы «Центр обновления Windows», «Установщик Windows» через «Управление компьютером – Службы и приложения – Службы»

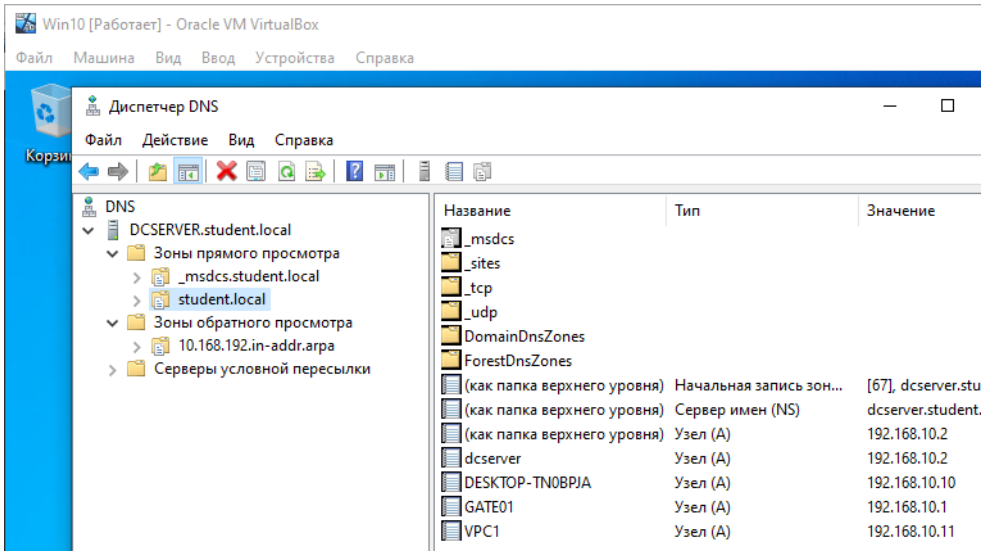
После установки вручную скачанного пакета повторите выбор и установку компонентов через **«Параметры – Приложения – Дополнительные компоненты – Добавить компонент».**

После установки, графические **оснастки RSAT** доступны через **«Пуск – Средства администрирования Windows»**.

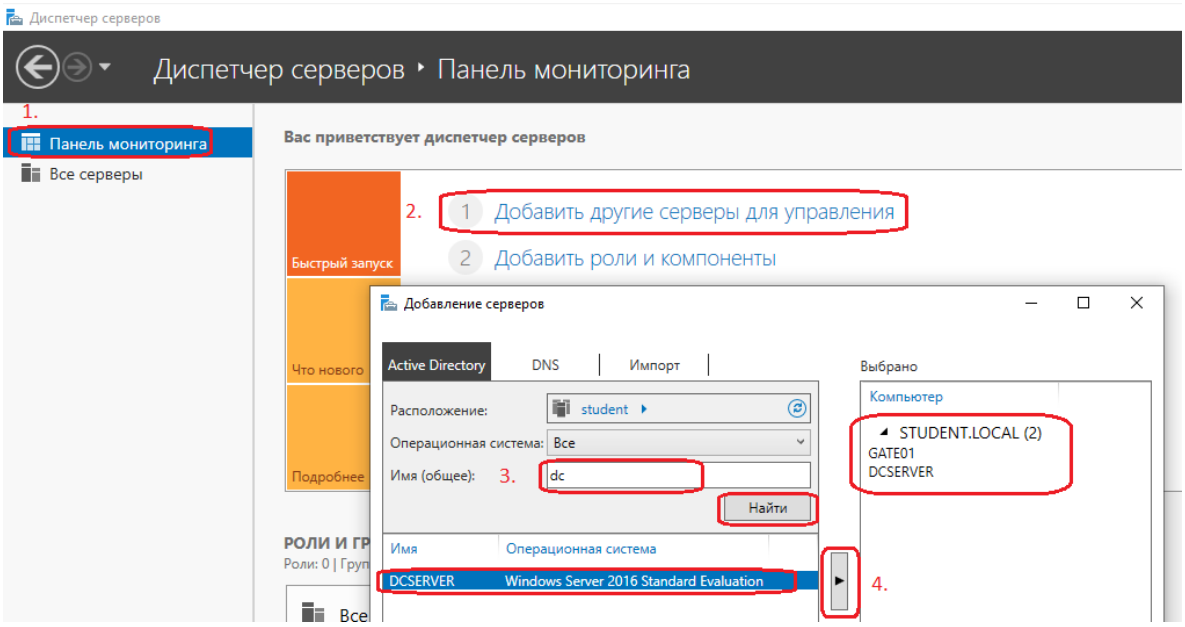
«**Диспетчер серверов**», также доступен через **«Пуск – Диспетчер серверов».**

Самостоятельно проверить возможность подключения с клиента Win10 с помощью оснасток «DNS», «DHCP», «Управление групповой политикой» к серверу DCSERVER1. Продемонстрировать с помощью скриншотов с описаниями успешность подключения к серверу DCSERVER1.



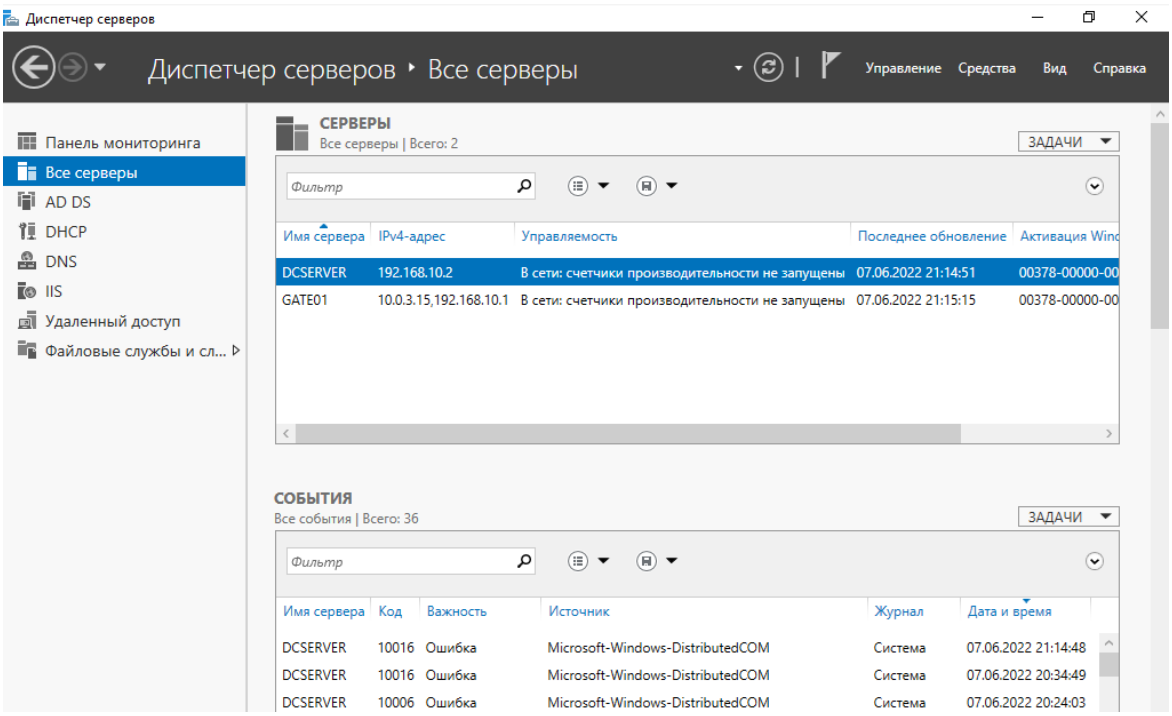


В «Диспетчере серверов» запущенном на Win10 добавить и подключиться к серверам DCSERVER1 и GATE01. Продемонстрировать с помощью скриншотов с описаниями успешность подключения к серверу DCSERVER1:



Примечание: Внимание!!! Будьте внимательны и не выполняйте каких-либо необдуманных действий (удаление и пр.) т.к. удаленные средства управления работают так же как и локально запущенные!!!

После добавления серверов GATE01 и DCSERVER1 Диспетчер Серверов будет выглядеть соответсвенно:

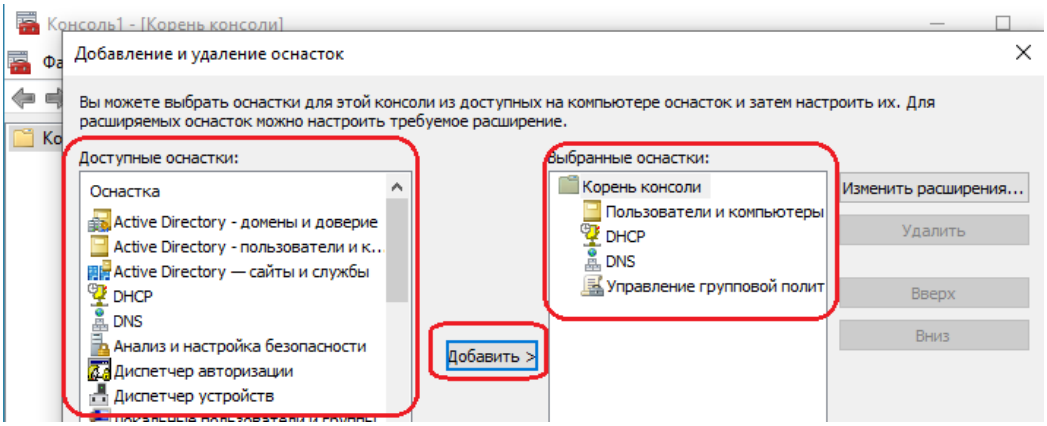


Сохраните настроенную «Консоль управления – MMC» содержащую набор оснасток Пользователи и компьютеры – Active Directory, DHCP, DNS и

Управление групповой политикой на рабочем столе, для удобства использования и быстрого доступа.

Для этого выполните **Пуск-выполнить-mmc:**

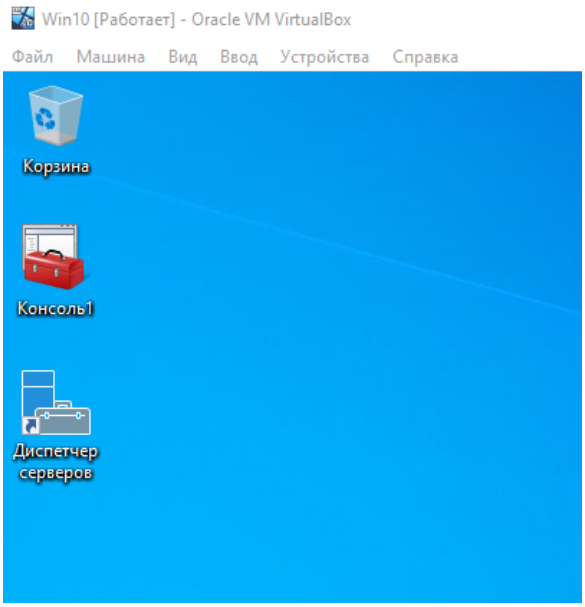
Затем, через меню **«Файл – Добавить или удалить оснастку»** выберите необходимые оснастки:



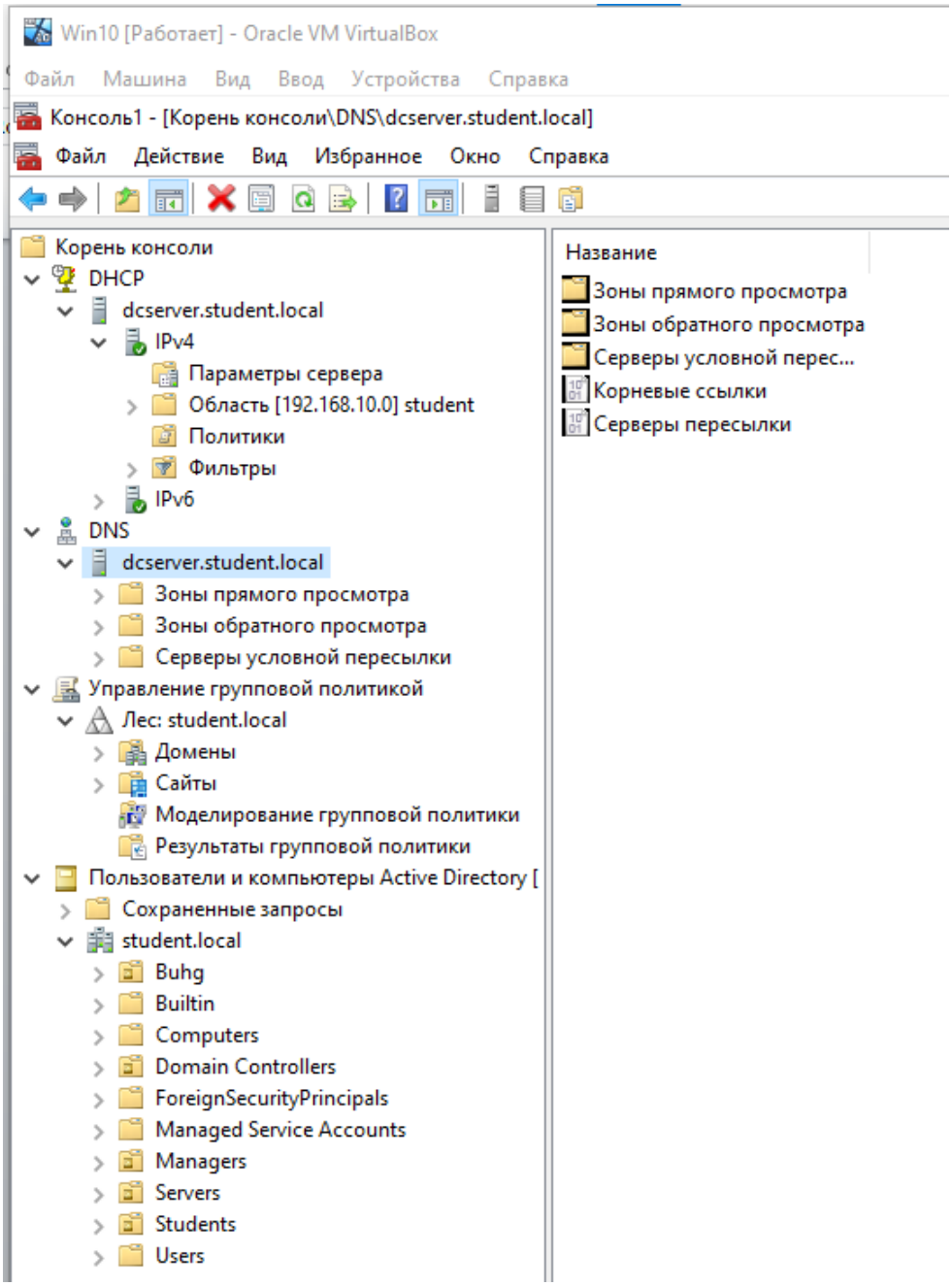
Далее, через меню **«Файл – Сохранить как» сохраните данную консоль управления на рабочем столе** под каким-либо именем.

Также скопируйте ярлык Диспетчера серверов на рабочий стол.

Консоль и Диспетчер серверов на рабочем столе:



Открытая консоль MMC с оснастками **DNS, DHCP, Управление групповой политикой** и **Пользователи и компьютеры Active Directory** подключенными к серверу **DCSERVER1**:



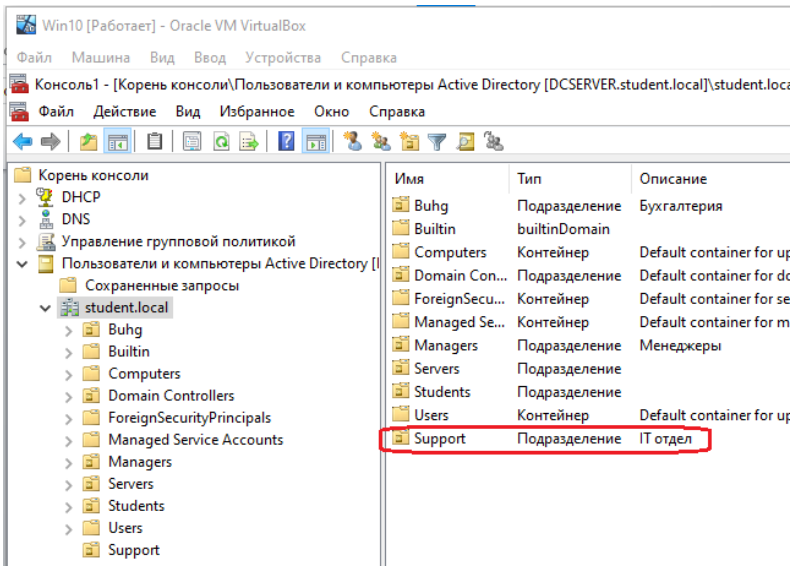
Задача 2.

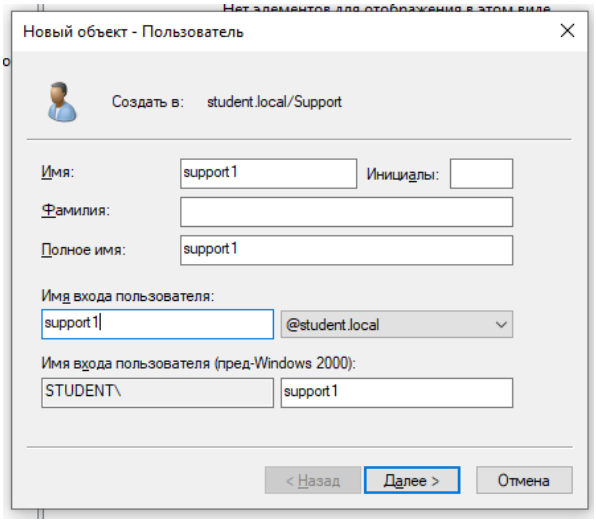
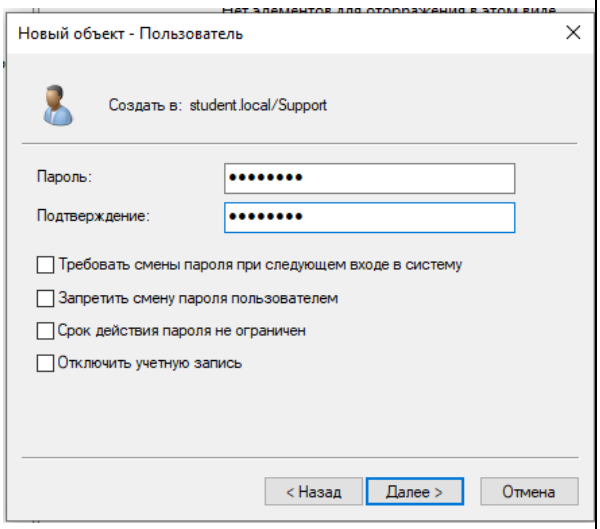
С клиента Win10, с помощью оснасток «**Пользователи и компьютеры Active Directory**» и «**Управление групповой политикой**» создайте и настройте на контроллере домена подразделение «**Support**», члены которой будут осуществлять техническую поддержку пользователей и должны иметь права локального администратора на компьютерах – клиентах домена.

Кроме локального администратора в группу Администраторов входит как минимум первая созданная на компьютере учетная запись, также могут быть и другие учетные записи. В целях безопасности правильно будет удалить их из этой группы, т.е. лишить привилегий локального Администратора.

В группе локальных администраторов должны входить Администраторы домена и члены группы техподдержки.

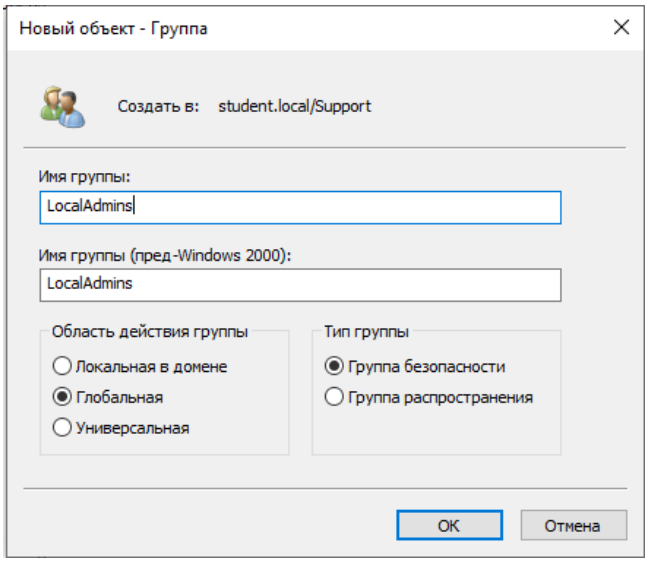
Этап 1. С помощью оснастки «**Пользователи и компьютеры Active Directory**» создаем подразделение «**Support**» в домене **company.local**



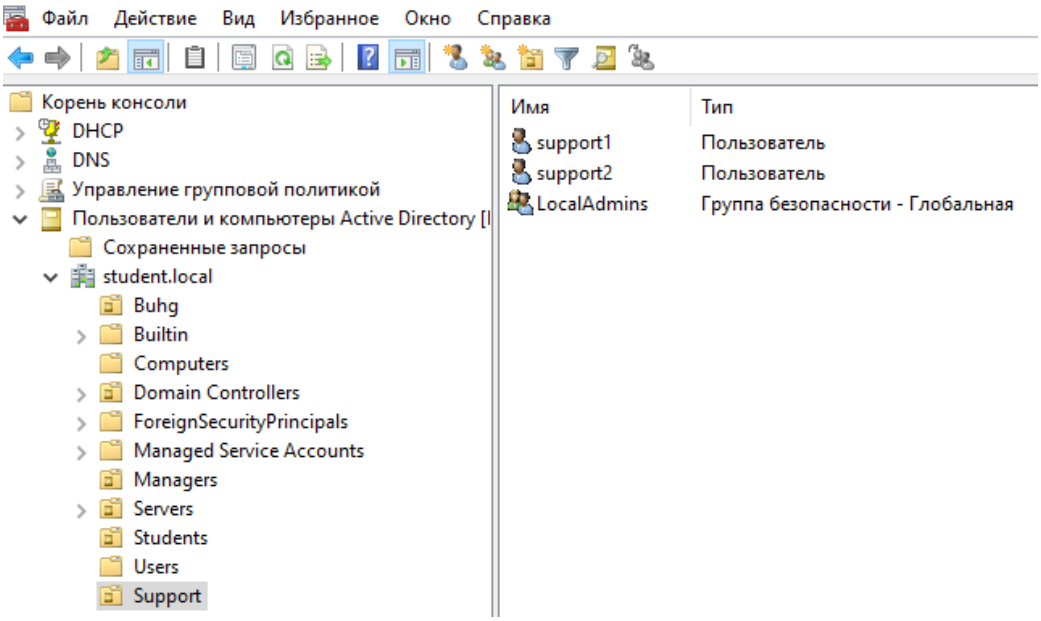
Создаем пользователя:	Задаем пароль:
	

пользователь	**пароль**
support1	support1
support2	support2

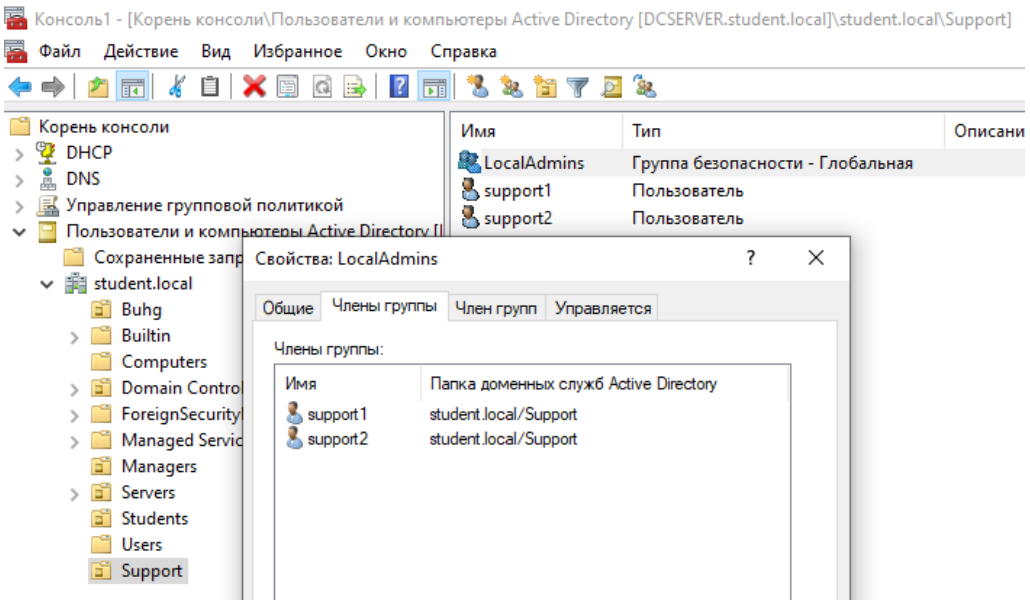
В подразделении «**Support**» создаем группу «**LocalAdmins**»:



В итоге содержимое подразделения «**Support**» должно выглядеть следующим образом:

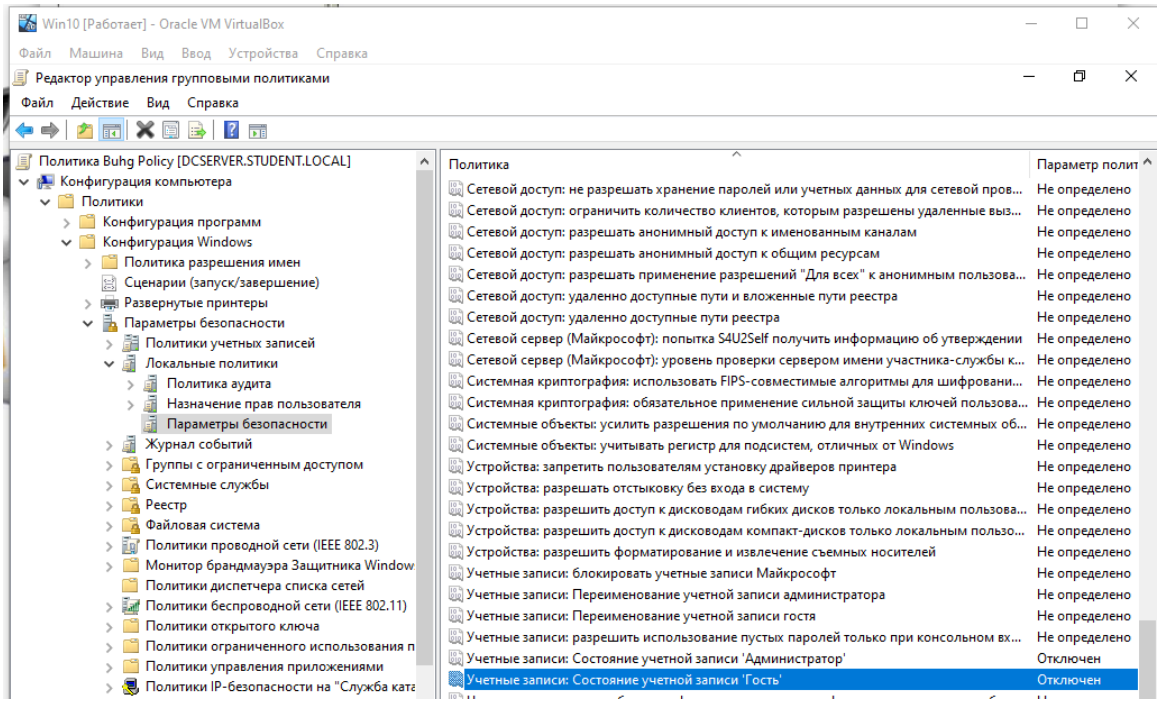


Включаем в данную группу пользователей «**support1**» и «**support2**»



Этап 2. С помощью оснастки «У**правление групповой политикой»** отредактируйте (измените) объекты групповой политики «**Buhg Policy**» и «**Managers Policy**», созданные ранее.

Откройте «**Конфигурация компьютера – Политики - Конфигурация Windows - Параметры безопасности - Локальные политики – Параметры безопасности».**

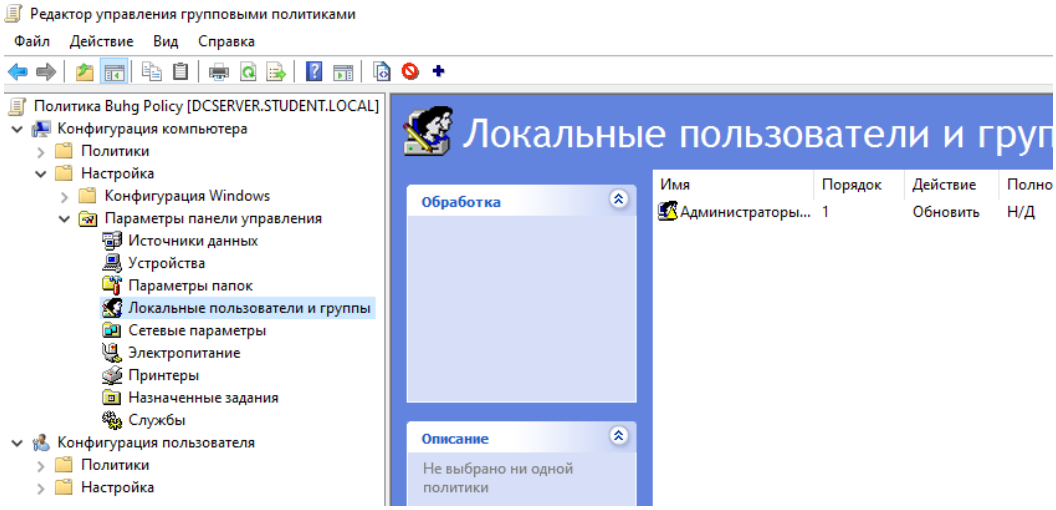


Там находим: «**Учетные записи: Состояние учетной записи Администратор**» и отключаем в свойствах.

«**Учетные записи: Состояние учетной записи Гость**» и отключаем в свойствах.

Данные правила повысят безопасность и отключат локального администратора и гостя.

Далее, открываем «**Конфигурация компьютера - Настройка - Параметры панели управления - Локальные пользователи и группы**»



Где выполняем «**Создать - Локальная группа**».

Затем указываем следующие настройки:

Действие - Обновить,

Имя группы - Администраторы (встроенная учетная запись)

ниже устанавливаем флаги:

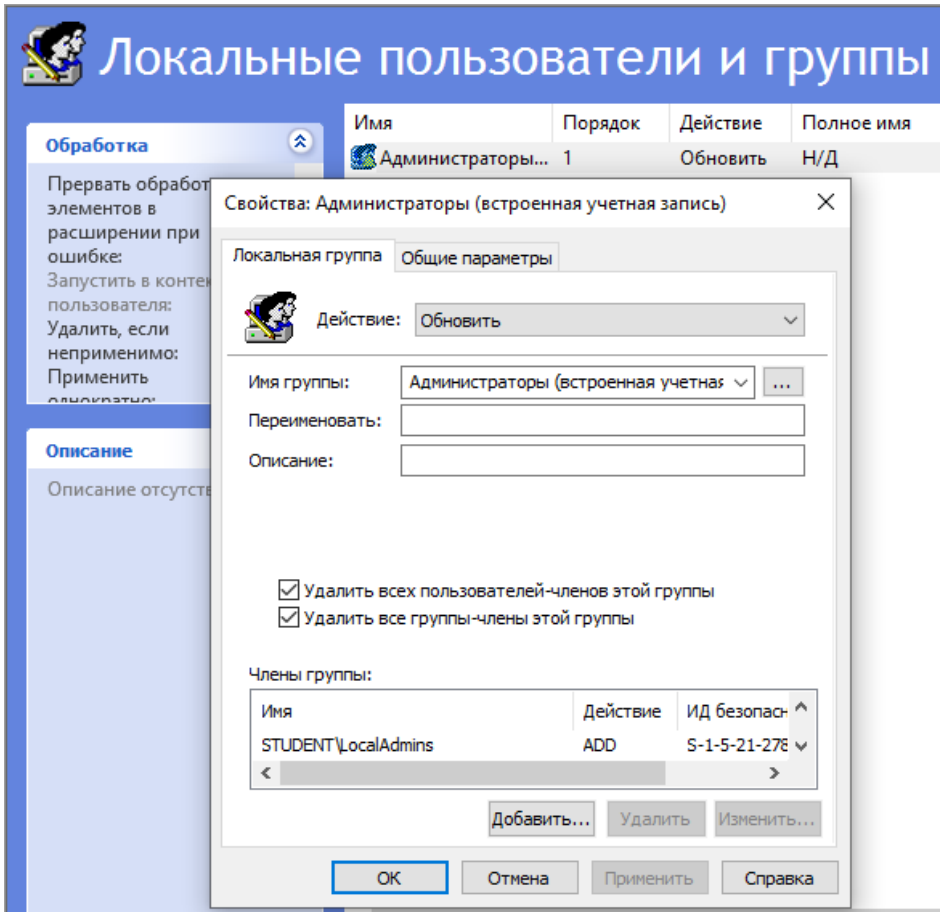
Удалить всех пользователей-членов этой группы

Удалить все группы-члены этой группы.

Затем добавляем в **Члены группы:**

группу «**Администраторы домена»;**

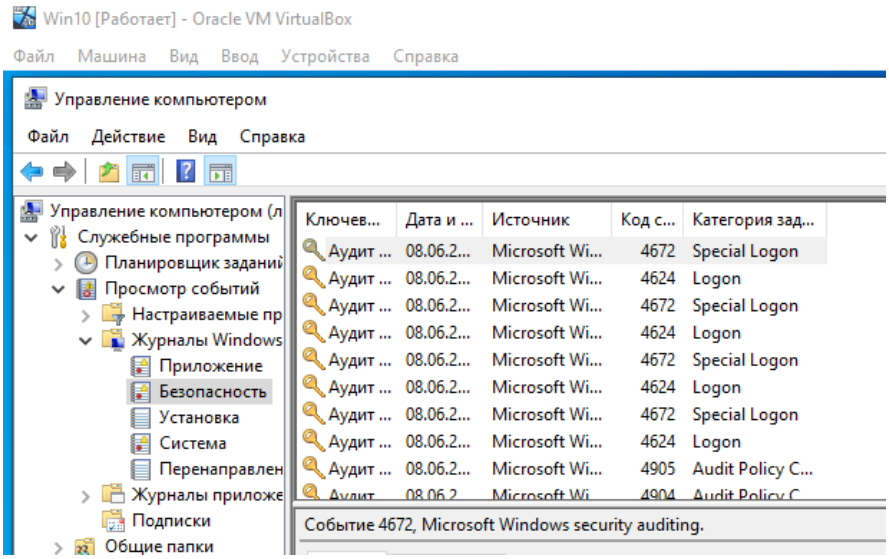
и группу техподдержки «**LocalAdmins» домена.**



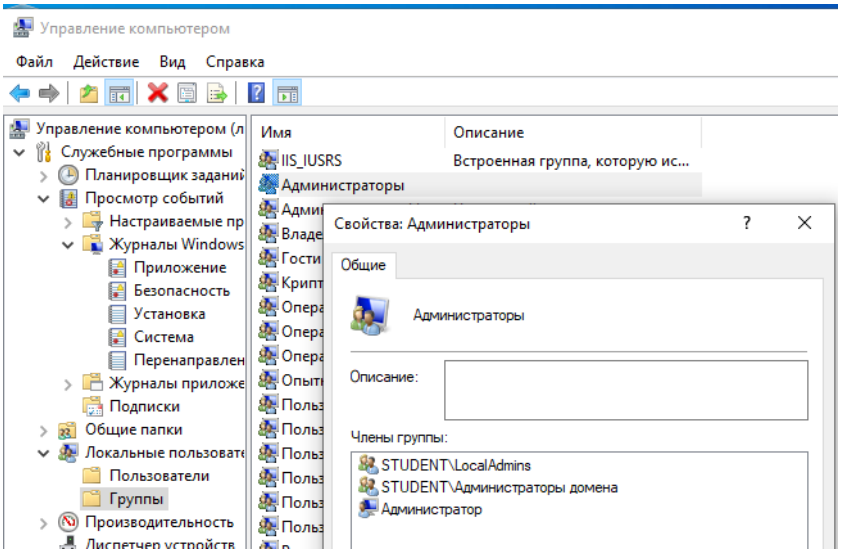
Закройте политику «**Buhg Policy**» и форсируйте обновление группово й политики на Win10 с помощью команды **gpupdate /force.**

После чего перезагрузите **Win10** и **зайдите** под учетной записью сотрудника подразделения ИТ-поддержки **support1** или **support2.**

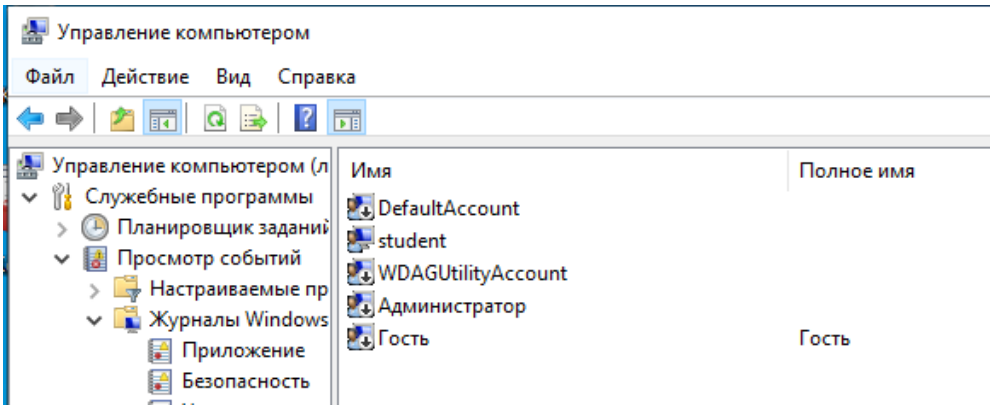
Для демонстрации наличия прав локального администратора, например, откройте в журнал событий безопасности локального компьютера в **«Управление компьютером – Служебные программы – Просмотр событий – Безопасность»:**



Для того чтоб удостовериться что пользователь **support1** входит в локальную группу администраторов откройте там же **«Локальные пользователи и группы»,** затем проверьте кто входит в группу **«Администраторы»:**



Далее, в соседней ветке «**Пользователи**», проверим отключены ли учетные записи локального администратора и гостя**:**



Альтернативным способом получения информации о состоянии групп является командная строка. Последовательно выполните команды:

Whoami – отобразить текущее имя домена и имя пользователя:

```
C:\Users\support1>whoami
student\support1
```

Net user /domain support1 (или support2 в зависимости под кем вошли) – отобразить различную информацию о доменном пользователе, в т.ч. о членстве в доменной группе «**LocalAdmins**»:

```
C:\Users\support1>net user /domain support1
Этот запрос будет обрабатываться контроллером домена student.local.

Имя пользователя                        support1
Полное имя                              support1
Комментарий
Комментарий пользователя
Код страны или региона                  000 (Стандартный системный)
Учетная запись активна                  Yes
Учетная запись просрочена               Никогда

Последний пароль задан                  08.06.2022 17:07:34
Действие пароля завершается             20.07.2022 17:07:34
Пароль допускает изменение              09.06.2022 17:07:34
Требуется пароль                        Yes
Пользователь может изменить пароль      Yes

Разрешенные рабочие станции             Все
Сценарий входа
Конфигурация пользователя
Основной каталог
Последний вход                          08.06.2022 18:06:02

Разрешенные часы входа                  Все

Членство в локальных группах
Членство в глобальных группах           *LocalAdmins
                                        *Пользователи домена
Команда выполнена успешно.
```

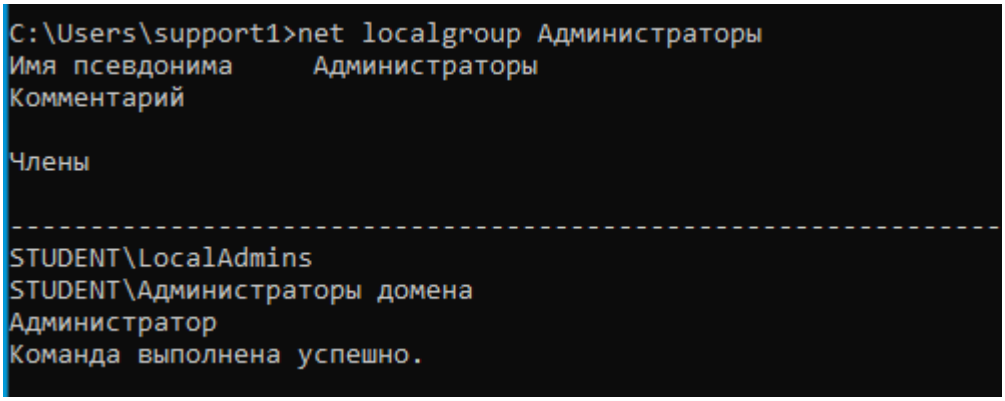
Примечание: команда **Net user /domain имя_пользователя_домена** позволяет получить различные сведения о любых зарегистрированных пользователях домена (в т.ч. об администраторах).

Для получения информации о локальных группах введите:

net localgroup

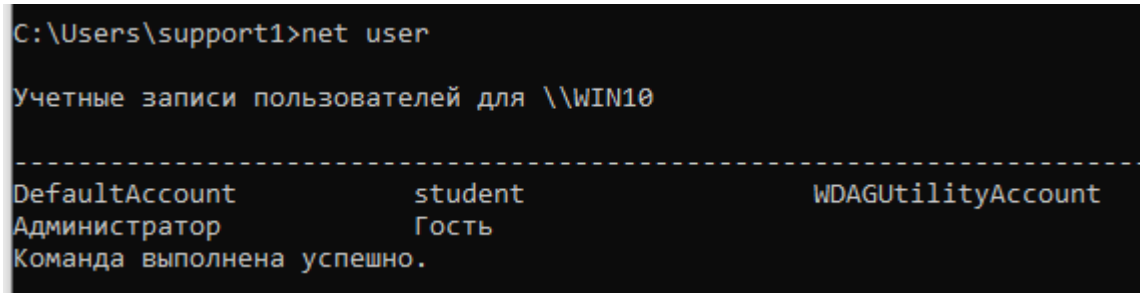
Наконец, для получения информации о конкретной интересующей нас локальной группе администраторов введите:

net localgroup Администраторы

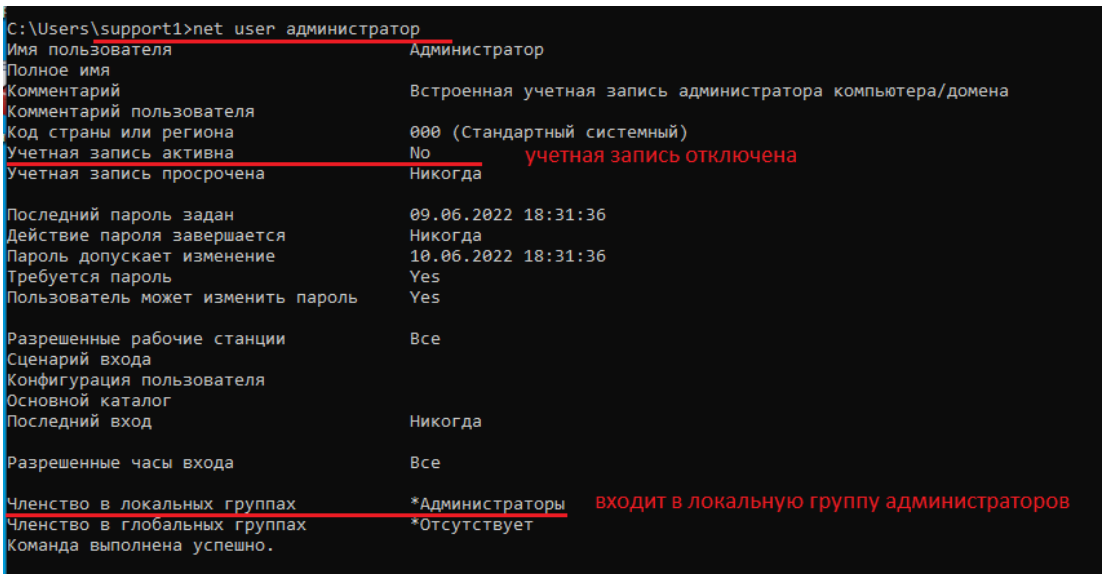


На приведенном скриншоте показано, что членами локальной группы администраторов являются все кто входит в доменную группу «**LocalAdmins» (что нам и было нужно),** а также члены доменной группы **«Администраторы домена»** (к ней принадлежит сам **администратор домена** под которым вам приходилось работать ранее). Локальный администратор, как было показано выше был отключен.

Чтобы узнать с помощью командной строки список локальных пользователей зарегистрированных в системе введите **net user**



Далее, для получения информации о конкретном локальном пользователе введите **net user имя_пользователя**



В случае отсутствия изменений (не изменился состав группы локальных администраторов и отсутствуют права локального администратора у support1 и support2) на Win10 проверьте:

С помощью оснастки «**Пользователи и компьютеры Active Directory**» удостоверьтесь, что компьютер **Win10** входит в подразделение «**Buhg**» **(поскольку, именно для этого подразделения вносим изменения).** Также проверьте входят ли пользователи **support1** и **support2** в группу безопасности «**LocalAdmins**»;

С помощью оснастки «Управление групповой политикой» проверьте правильно ли внесены изменения (согласно заданию) в объект групповой политики **«Buhg Policy» - «Конфигурация компьютера - Настройка - Параметры панели управления - Локальные пользователи и группы».** Отключены ли **Гость** и **Администратор** в **«Конфигурация компьютера - Конфигурация Windows - Параметры безопасности - Локальные политики – Параметры безопасности»**;

С помощью оснастки «У**правление групповой политикой»** проверьте связан ли объект групповой политики «**Buhg Policy**» с подразделением **«Buhg»;**

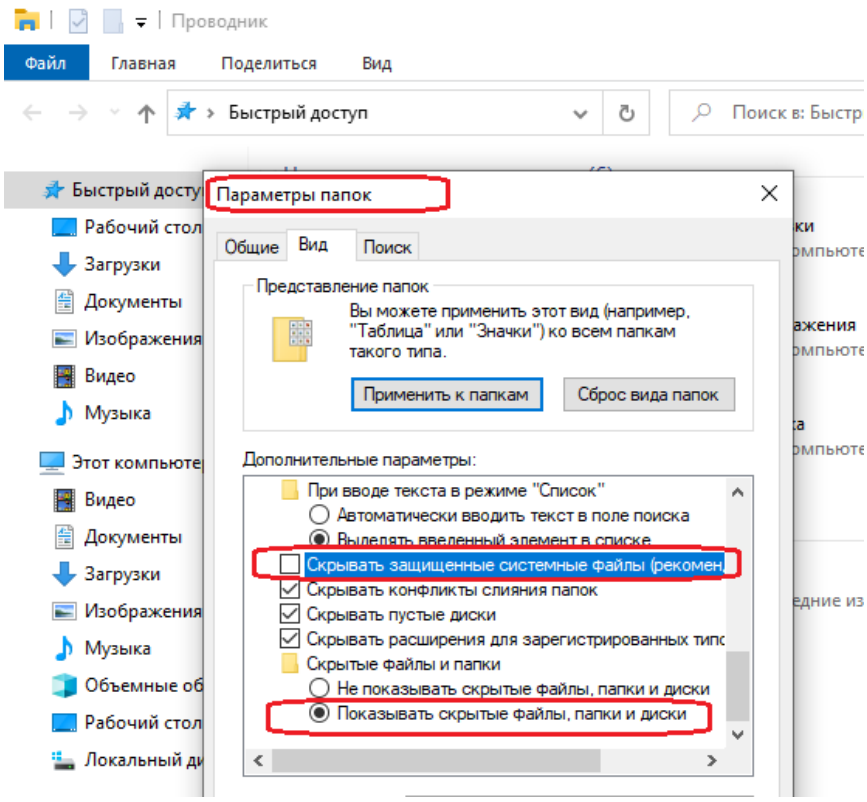
Если пришлось внести изменения в ГП обязательно форсируйте применение ГП с помощью gpupdate /force на DCSERVER1 и Win10.

В случае если ничего не помогает:

В объекте ГП «Buhg Policy» удалите ранее созданную группу локальных администраторов в «**Конфигурация компьютера - Настройка - Параметры панели управления - Локальные пользователи и группы**» и создайте ее заново с заданными параметрами.

Проверьте, отключена (необходимо отключить) ли поддержка IPv6 в свойствах сетевого соединения на DCSERVER1 и Win10. Входит ли вообще в домен company.local компьютер Win10.

Также возможно придется очистить содержимое папок с кэшированной ГП на компьютере Win10. Для этого в **«Параметрах папок – Вид»** необходимо **включить отображение защищенных системных файлов** и **показывать скрытые файлы и папки:**



Далее, **очищаем содержимое следующих папок:**

C:\ProgramData\Microsoft\Group Policy;

C:\ProgramData\Microsoft\GroupPolicy;

C:\Windows\System32\GroupPolicy;

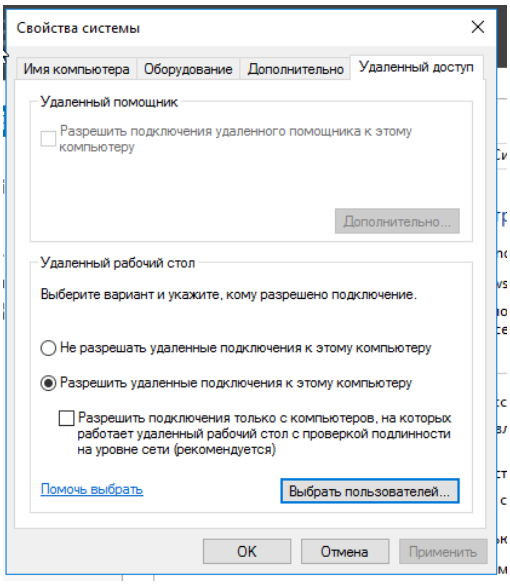
C:\Windows\System32\GroupPolicyUsers.

Задача 3.

Распространенным способом администрирования серверов является **удаленный доступ с помощью удаленного рабочего стола** с рабочих ПК.

Для этого необходимо включить

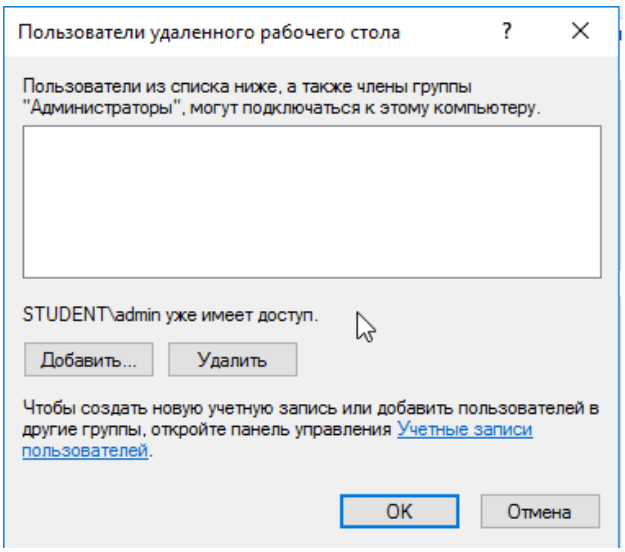
«Система – Дополнительные параметры системы – Удаленный доступ»



Где разрешаем удаленные подключения. Для простоты настройки и быстроты выполнения задания **убираем галочку** «**Разрешить подключение с проверкой подлинности**».

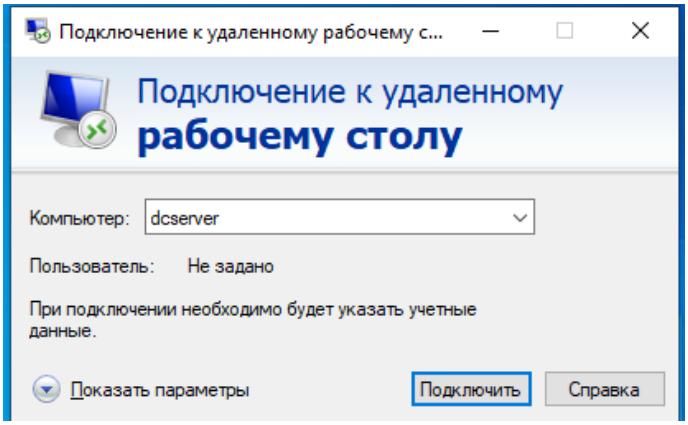
Примечание: подобное снижение уровня безопасности подключения вызвано упрощением

В окне выбора пользователей удостоверяемся что администратор домена уже имеет доступ.



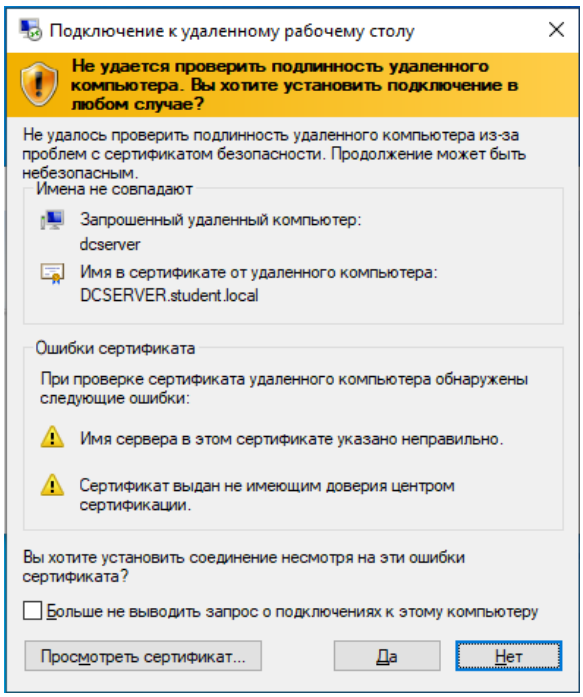
Для проверки возможности подключения к удаленному рабочему столу заходим на компьютер Win10 под учетной записью support1 (или support2).

«Выполняем Пуск-выполнить- mstsc» :

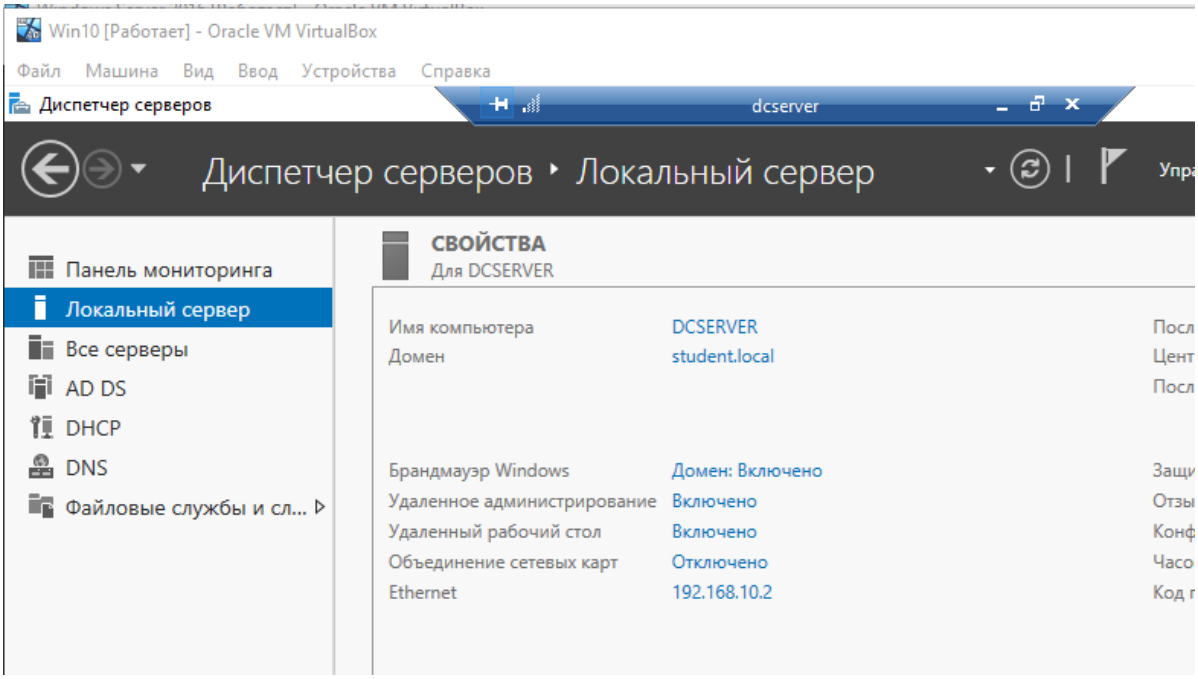


Где вводим имя сервера или его IP-адрес и авторизуемся под учетной записью администратора домена.

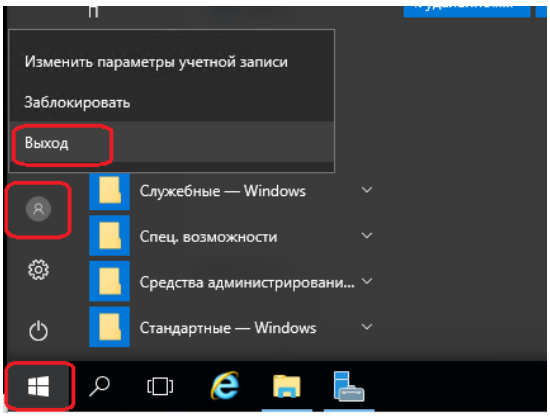
Соглашаемся с сертификатом для подключения.



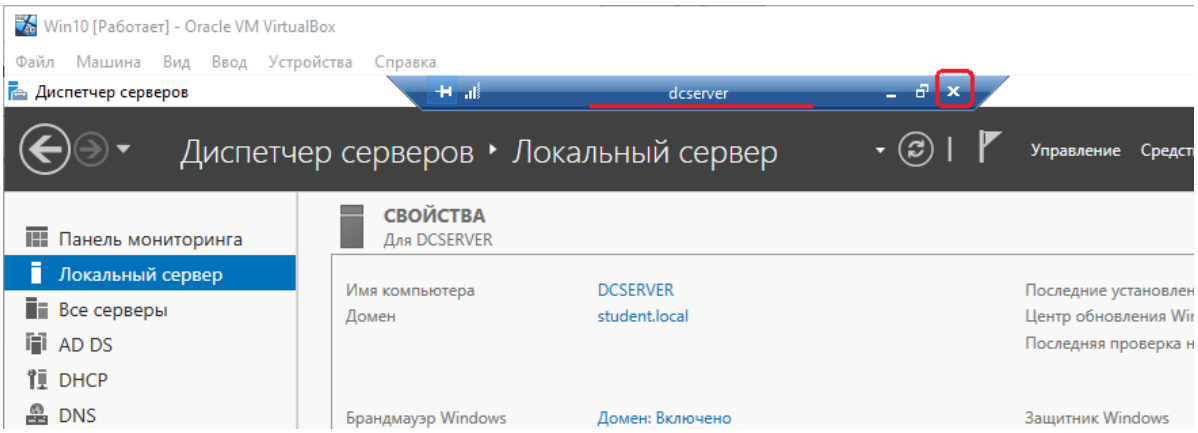
После подключения видим знакомый рабочий стол сервера



Для того чтобы **завершить сеанс подключения к серверу** выполните выход из учетной записи пользователя:



Если вы просто закроете сеанс работы через «крестик» на заголовке, то будет произведено отключение от сеанса с возможностью восстановления работы (на том же состоянии на котором было прервано) при повторном подключении.



Далее, подобным образом необходимо организовать подключение к интернет-шлюзу GATE01. Продемонстрировать открытие на серверах DCSERVER1 и GATE01 различных средства управления, оснасток и пр. и включить необходимые скриншоты с описаниями в отчет.