

## **Лабораторная работа 8. Средства удаленного администрирования в ОС Windows.**

### **Задание.**

Использовать виртуальные машины из предыдущих лабораторных работ. На ОС Windows 10 настроить и протестировать средства удаленного администрирования с подключением к Windows Server 2019 и к доменным службам Active Directory:

- предустановленные средства администрирования, «Computer Management» («Управление компьютером»);
- средства удаленного администрирования сервера — RSAT;
- Windows Admin Center;
- Windows PowerShell.

### **Этапы выполнения.**

1) Запустить виртуальные машины с Windows Server 2019 и Windows 10.

2) Для удаленного управления Windows Server 2019 с помощью различных утилит на Windows 10, необходимо запускать данные утилиты под доменной учетной записью, у которой есть полномочия по администрированию Windows Server 2019. Существует три способа:

- запуск на Windows 10 сеанса пользователя, который входит во встроенную группу «Администраторы» на Windows Server 2019, или группу «Администраторы домена» – т. е. пользователя «Администратор» (встроенного на Windows Server 2019) (не рекомендуется);
- наделение любого доменного пользователя соответствующими полномочиями и запуск его сеанса на Windows 10;
- вход на Windows 10 с любой учетной записью и запуск утилит администрирования от имени привилегированного пользователя (Run as).

В рамках данной лабораторной работы будет использоваться третий способ.

3) В ОС Windows 10 запустить встроенную утилиту для администрирования - «Computer Management» («Управление компьютером») от имени Администратора домена. Ярлык к утилите находится в «Control Panel» («Панели управления»), в разделе «Administration» («Администрирование») - ввести в строке поиска «Средства администрирования Windows» («Windows Administrative Tools»). (рис.1).

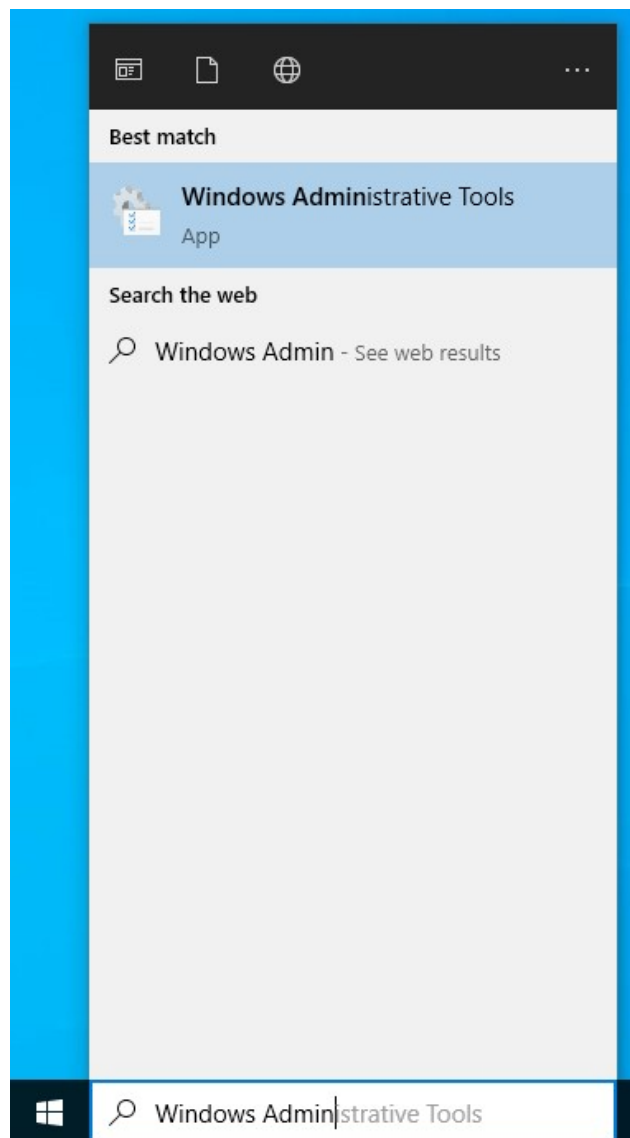


Рис.1. Переход к средствам администрирования Windows.

Выделить ярлык «Computer Management» («Управление компьютером»), зажать клавишу Shift и нажать правой кнопкой мыши, выбрать в меню «Run as a different user» («Запуск от имени другого пользователя») (рис.2).

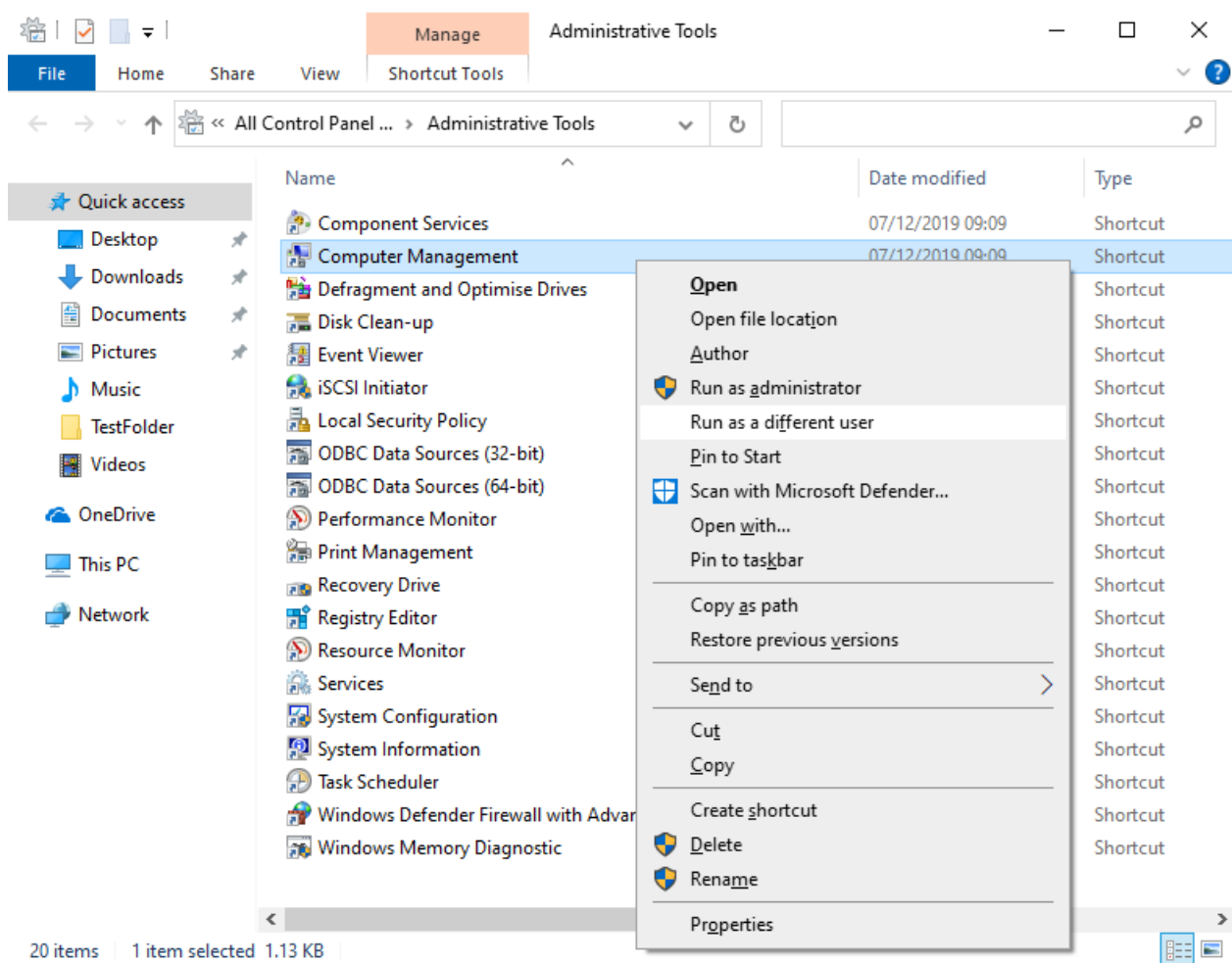


Рис. 2. Запуск от имени другого пользователя.

По запросу ввести учетные данные Администратора домена.

По умолчанию предлагается ряд утилит для администрирования локального компьютера — планировщик задач, просмотр событий, управление локальными пользователями и группами, управление службами и прочее.

4) Из контекстного меню подключиться к другому компьютеру - «Connect to another computer ...» (рис. 3).

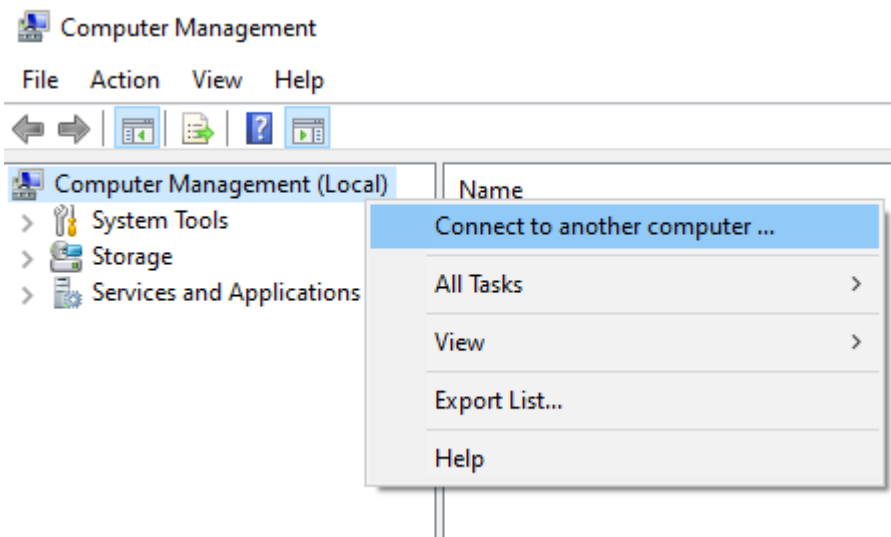


Рис. 3. Подключение к другому компьютеру.

Ввести сетевое имя или IP-адрес удаленного компьютера — Windows Server 2019 (рис.4.)

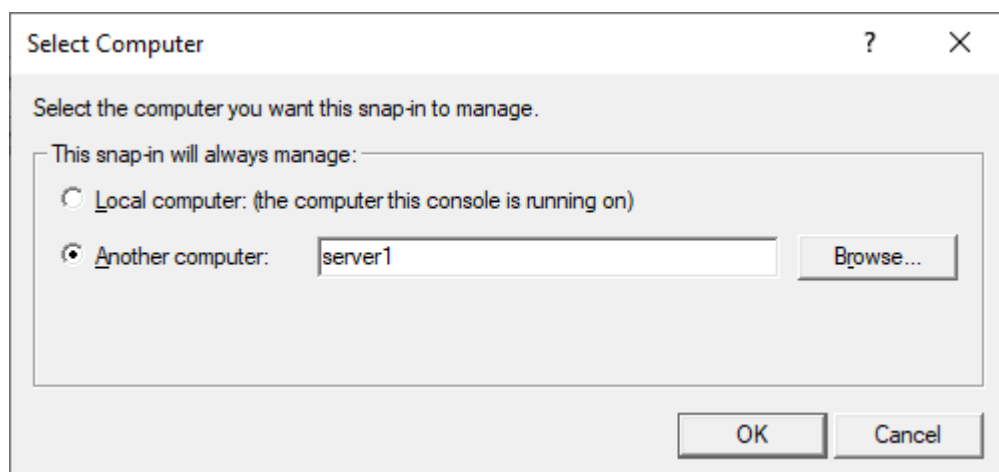


Рис. 4. Выбор компьютера для управления.

Для работы утилиты необходимо добавить разрешающие правила в настройки брандмауэра на Windows Server 2019 (появится окно с подробной информацией) или отключить брандмауэр.

5) Перейти в раздел System Tools – Event Viewer – Windows Logs, просмотреть события Системы. Найти событие системного времени запуска операционной системы, источник (Source) – Kernel-General, код события (Event ID) – 12. Следует искать данное событие в числе первых событий за текущий день, или настроить фильтр.

Снимок с событием системного времени запуска операционной системы в окне «Computer Management» («Управление компьютером») - в отчет.

6) Для подключения к удаленному серверу с помощью других средств администрирования, на данном сервере должно быть разрешено удаленное администрирование (на Windows Server 2019 включено по умолчанию) (рис.5).

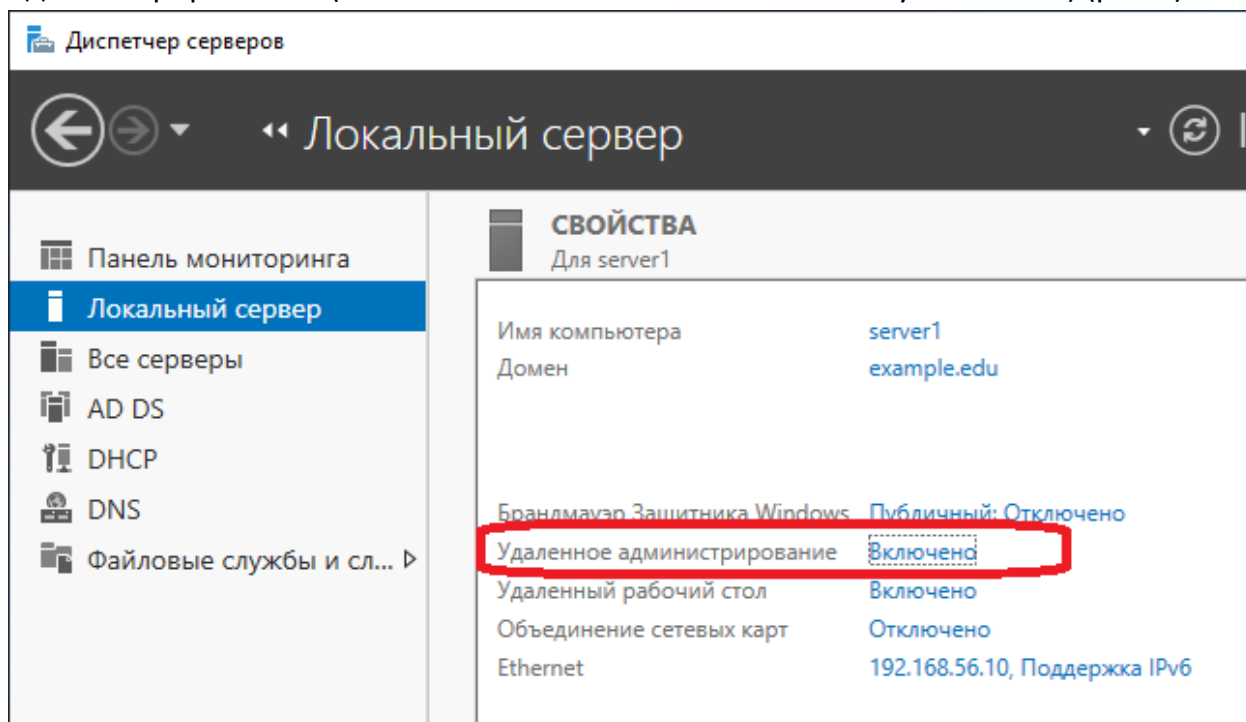


Рис.5. Настройка удаленного администрирования на сервере.

7) Для установки других средств администрирования на Windows 10 необходимо настроить подключение к сети Интернет. Для этого следует выключить VM Windows 10 и в настройках Oracle VirtualBox добавить второй сетевой адаптер с типом подключения NAT. Запустить VM и проверить доступ к сети Интернет.

8) Добавить любого доменного пользователя в локальную группу Администраторов на Windows 10. Для этого следует запустить сеанс пользователя с правами администратора, открыть утилиту «Управление компьютером» (или запустить утилиту от имени такого пользователя). Перейти в раздел System Tools – Local Users and Groups – Groups, добавить доменного пользователя в группу Administrators (рис. 6.)

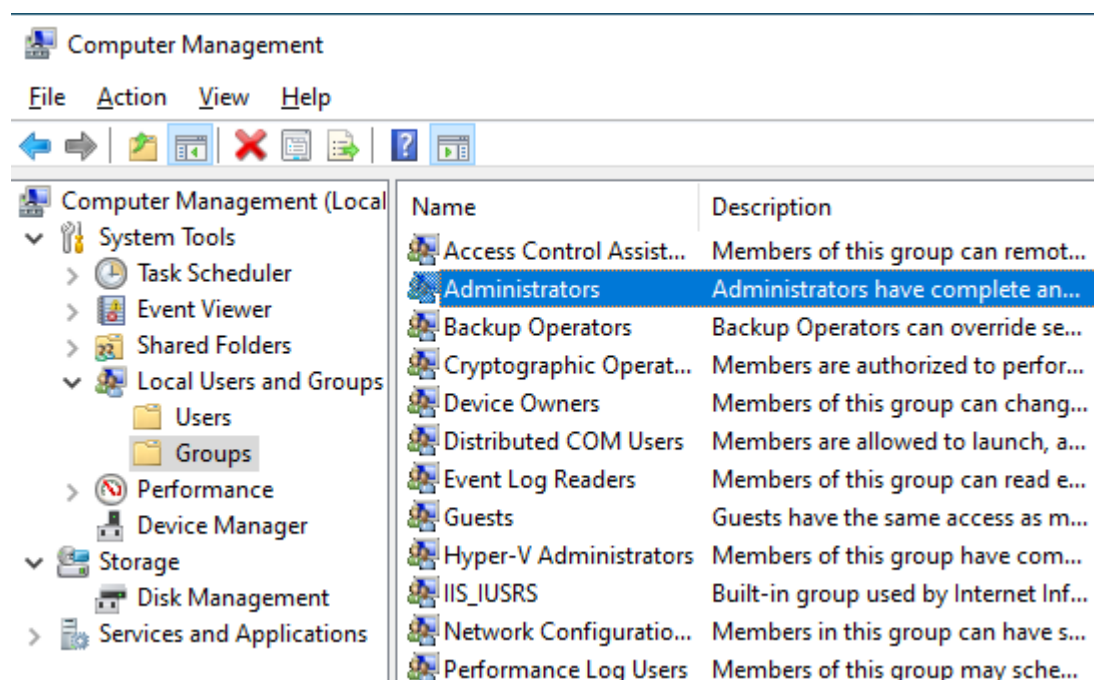


Рис. 6. Редактирование локальных групп пользователей.

В том случае, если настройка проводилась в сеансе указанного доменного пользователя, для применения новых политик необходимо выполнить выход и повторный вход пользователя.

9) Установить на Windows 10 Средства удаленного администрирования сервера — RSAT. Для этого запустить на Windows 10 сеанс пользователя с правами администратора, перейти в Settings – Apps – Optional features (рис.7). Нажать кнопку «Add a feature» (рис.8).

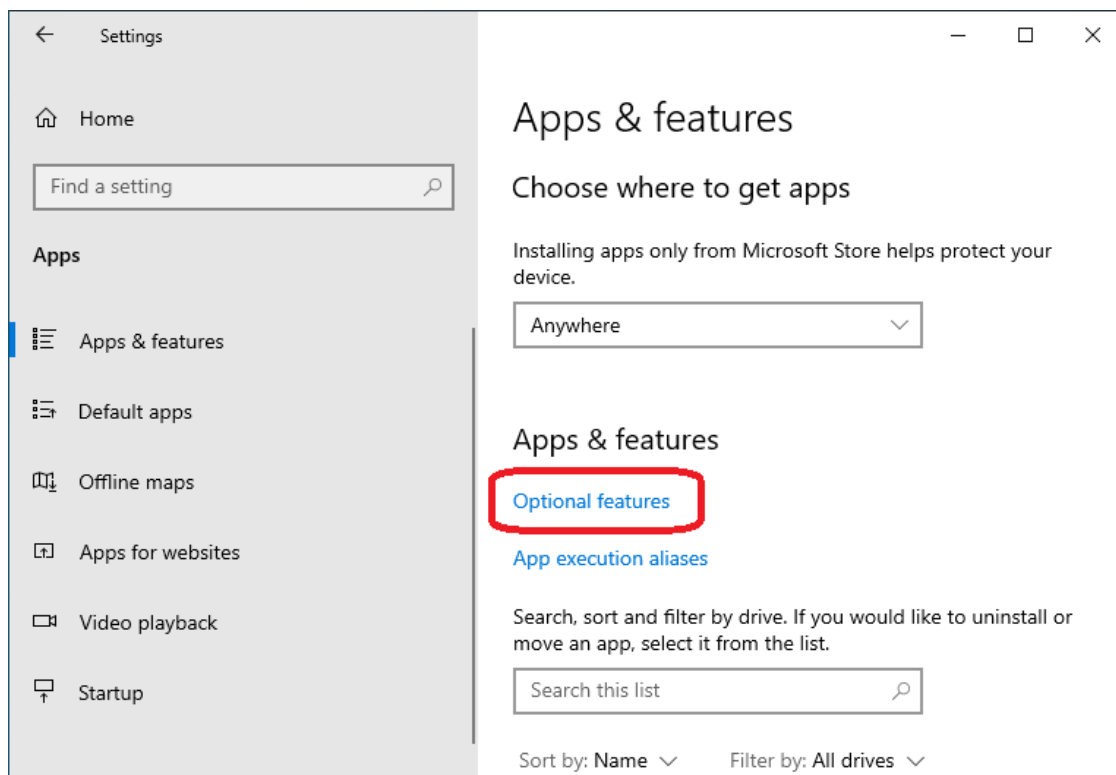


Рис. 7. Приложения и возможности.

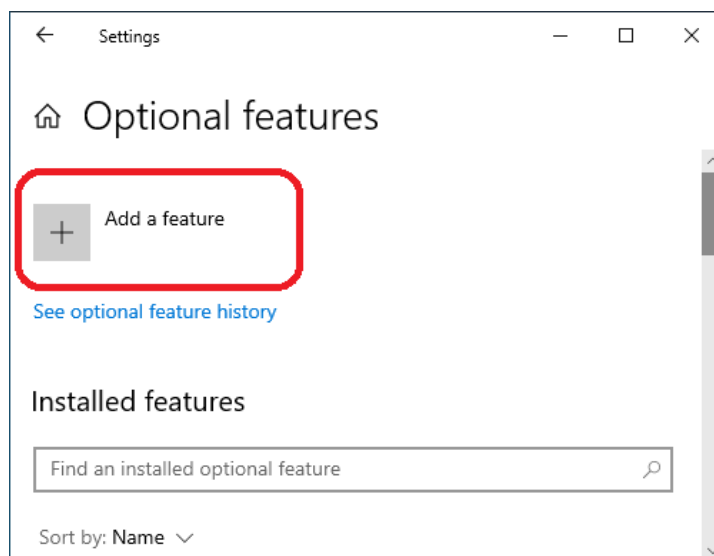


Рис. 8. Дополнительные возможности.

Отфильтровать предлагаемые компоненты по названию «RSAT» (рис.9).

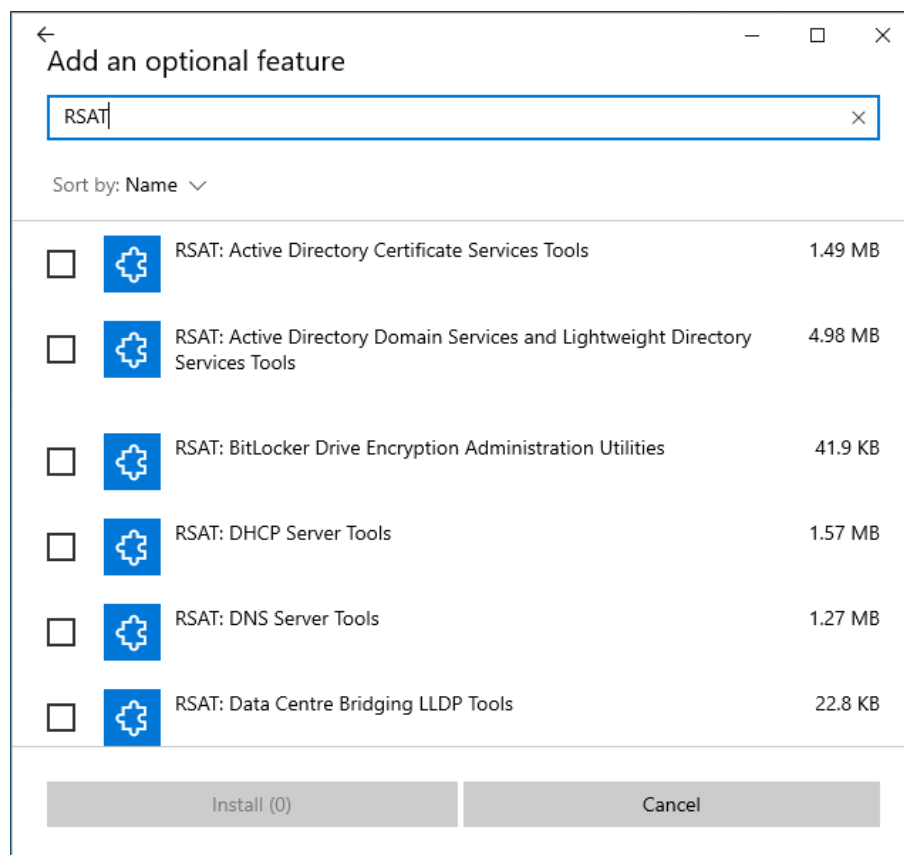


Рис.9. Доступные компоненты RSAT.

Установить следующие компоненты:

- RSAT: Active Directory Domain Services and Lightweight Directory Services Tools
- RSAT: DHCP Server Tools
- RSAT: DNS Server Tools
- RSAT: File Services Tools
- RSAT: Group Policy Management Tools
- RSAT: Server Manager

Установленные компоненты появятся в разделе «Администрирование» («Administration») Панели управления («Control Panel») - ввести в строке поиска «Средства администрирования Windows» («Windows Administrative Tools»). (рис.10).



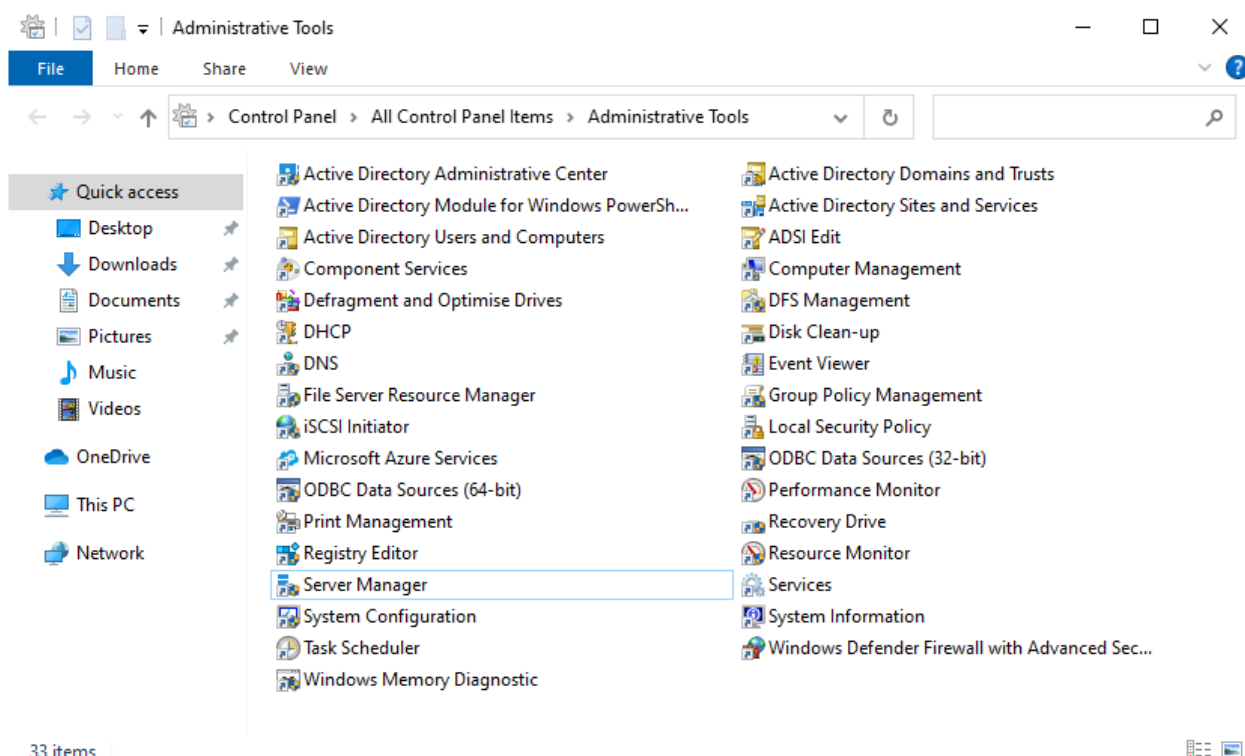


Рис.10. Раздел Администрирование.

10) Запустить на Windows 10 утилиту «Server Manager» (Диспетчер серверов) из состава RSAT под учетной записью администратора домена. Нажать «Add other servers to manage» (рис.11).

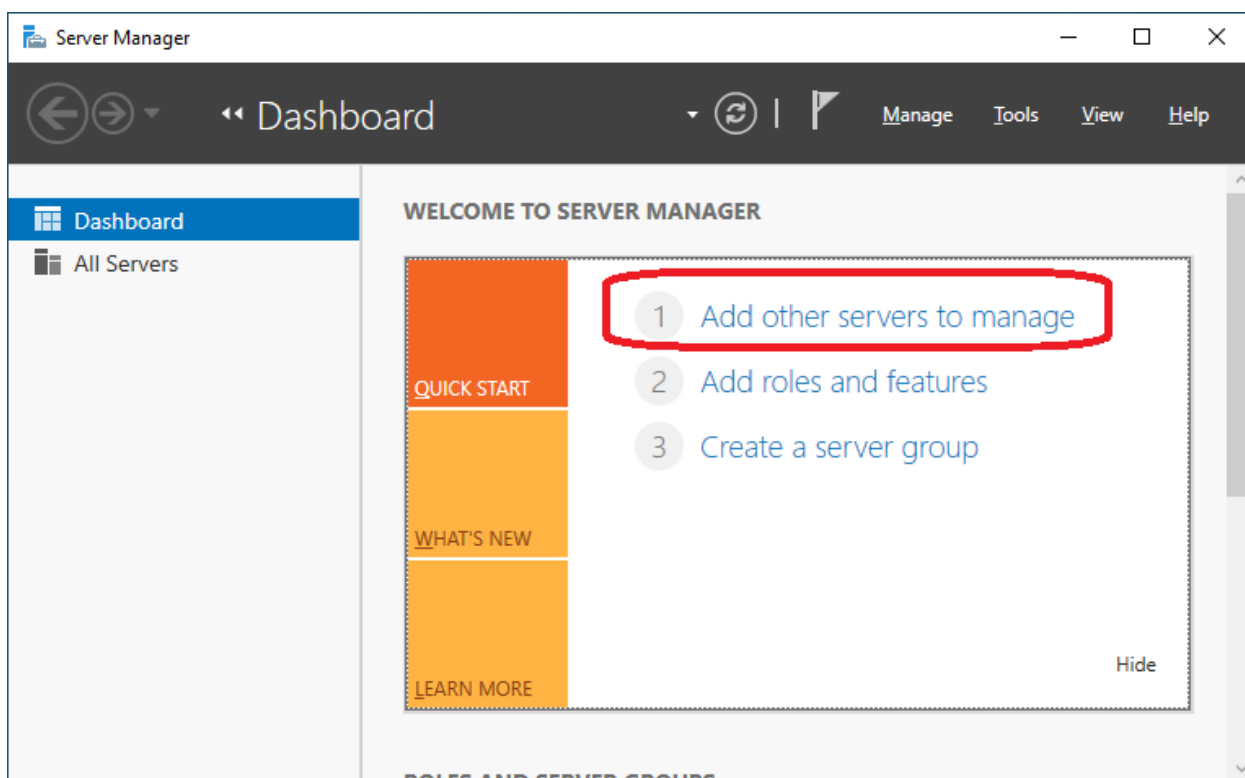


Рис. 11. Диспетчер серверов.

Выполнить поиск сервера в каталоге Active Directory или в настроенной зоне DNS, добавить сервер Windows Server 2019 (рис.12).

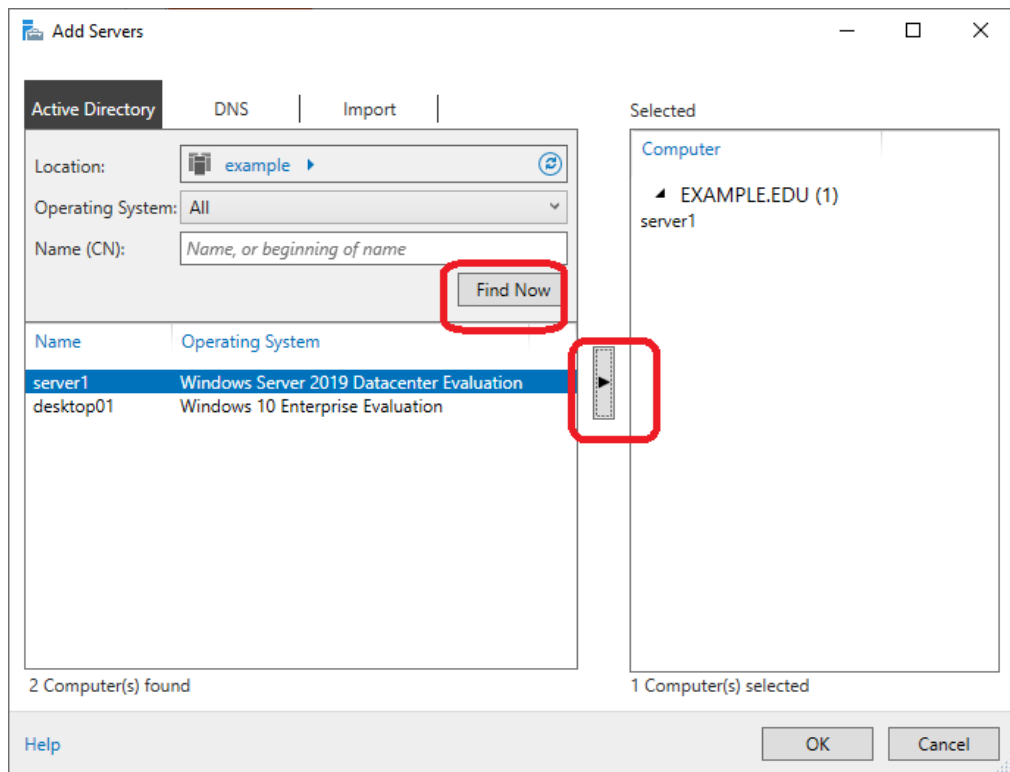


Рис.12. Добавление сервера.

После добавления сервера будут доступны настройки установленных ролей и компонентов. Настройки Диспетчера серверов (список добавленных серверов) сохраняются отдельно для каждого пользователя.

Снимок диспетчера серверов на Windows 10 с добавленным сервером Windows Server 2019 – в отчет.

11) Перейти в оснастку «Active Directory Users and Computers» на Windows 10 (рис.13).

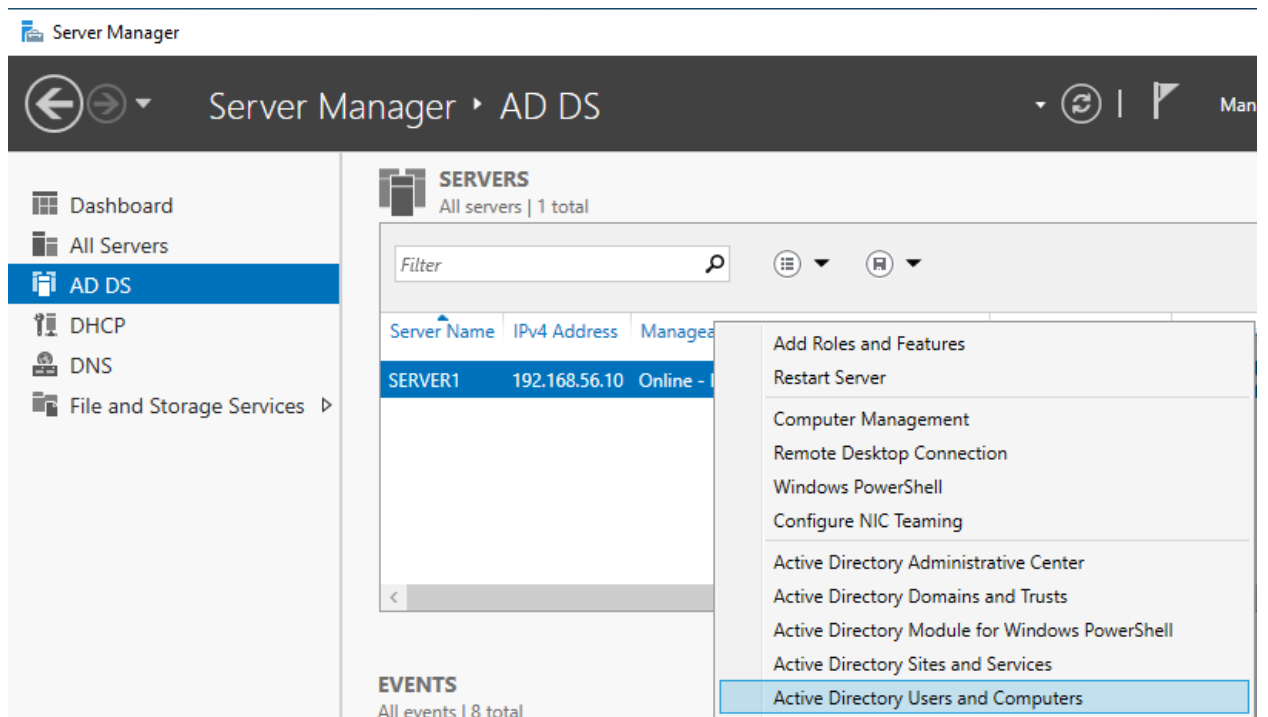


Рис.13. Запуск оснастки в диспетчере серверов.

Создать произвольную доменную учетную запись пользователя в любом подразделении (OU) домена AD.

12) Загрузить и установить на Windows 10 инструмент Windows Admin Center. Ссылка на загрузку дистрибутива появляется при каждом запуске Диспетчера серверов. Существует несколько сценариев установки Windows Admin Center, в данной лабораторной работе установку следует производить на Windows 10. Параметры установки оставить в значениях по-умолчанию. По завершению установки выбрать запуск Admin Center.

После установки Windows Admin Center будет доступен на Windows 10 через веб-браузер по URL адресу (рис.14):

<https://localhost:6516/>

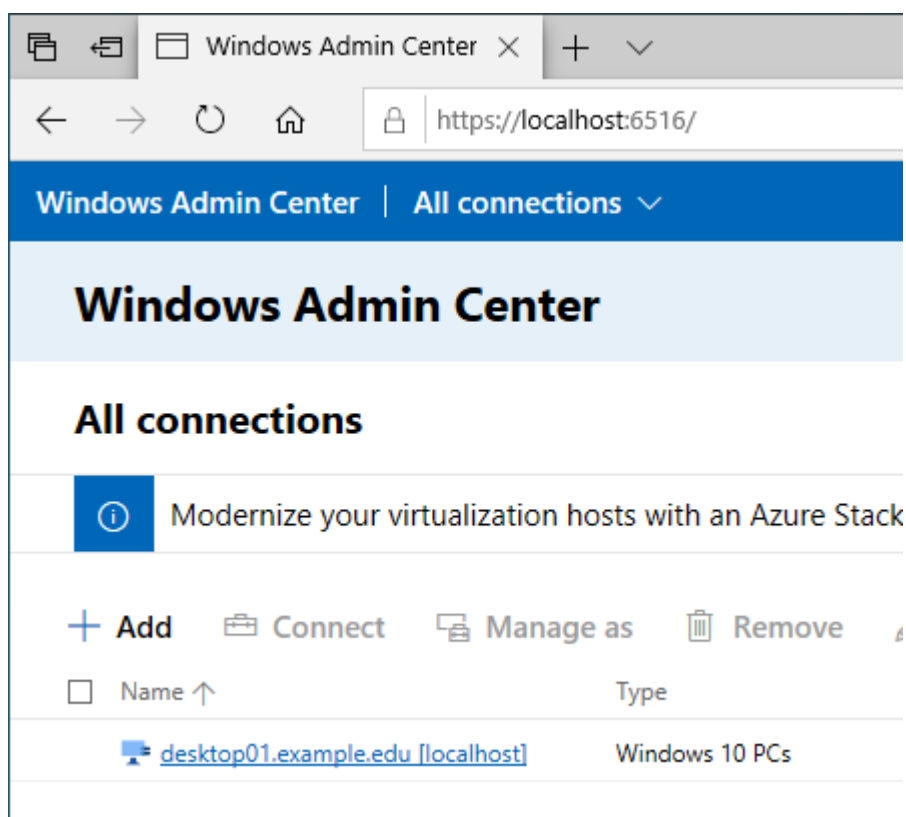


Рис.14. Windows Admin Center.

Первоначально доступно управление локальным узлом, для этого следует перейти по ссылке с сетевым именем узла (например, desktop01.example.edu).

13) Перейти на главную страницу Windows Admin Center и добавить Windows Server 2019 в список управляемых узлов — нажать Add (рис.14).

Выбрать тип узла — сервер, ввести имя сервера или выполнить поиск в Active Directory (рис.15).

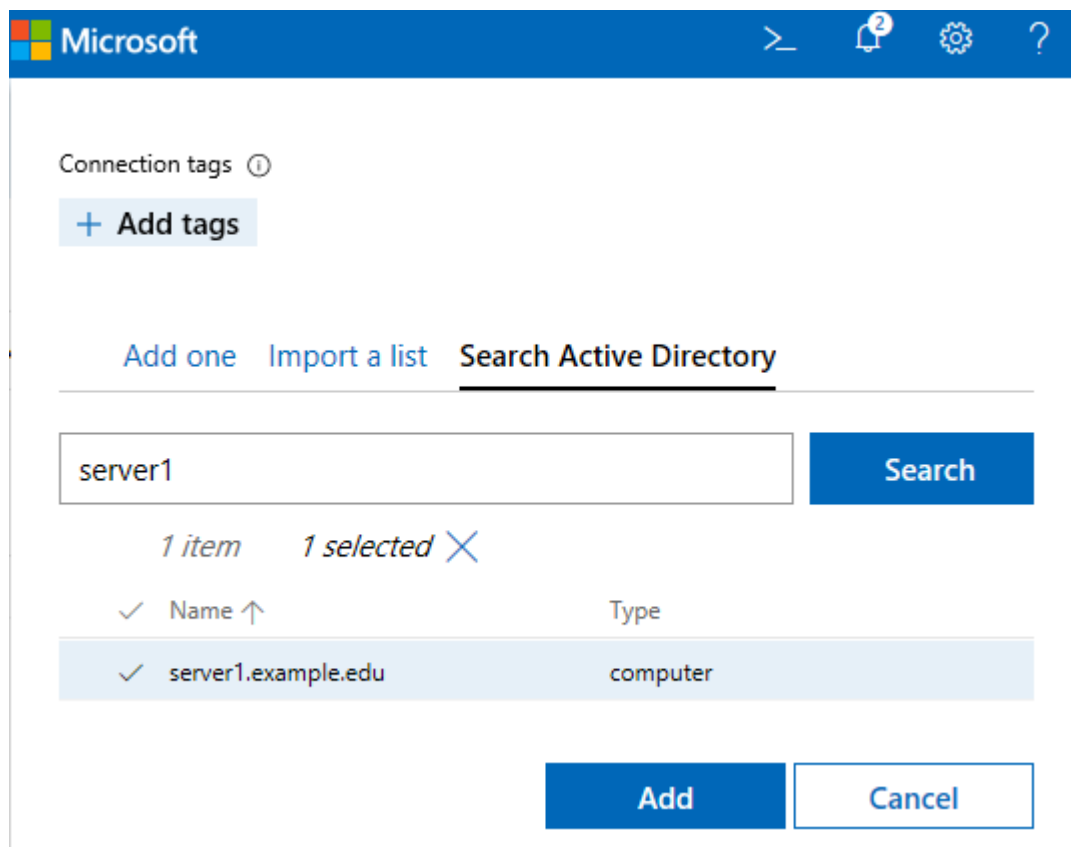


Рис.15. Добавление сервера.

После добавления сервера перейти по ссылке в списке узлов к узлу Windows Server 2019. По запросу ввести учетные данные Администратора домена. Будет выведен раздел с общей информацией о сервере и статистика использования ресурсов, в левой части окна — список доступных разделов. (рис.16).

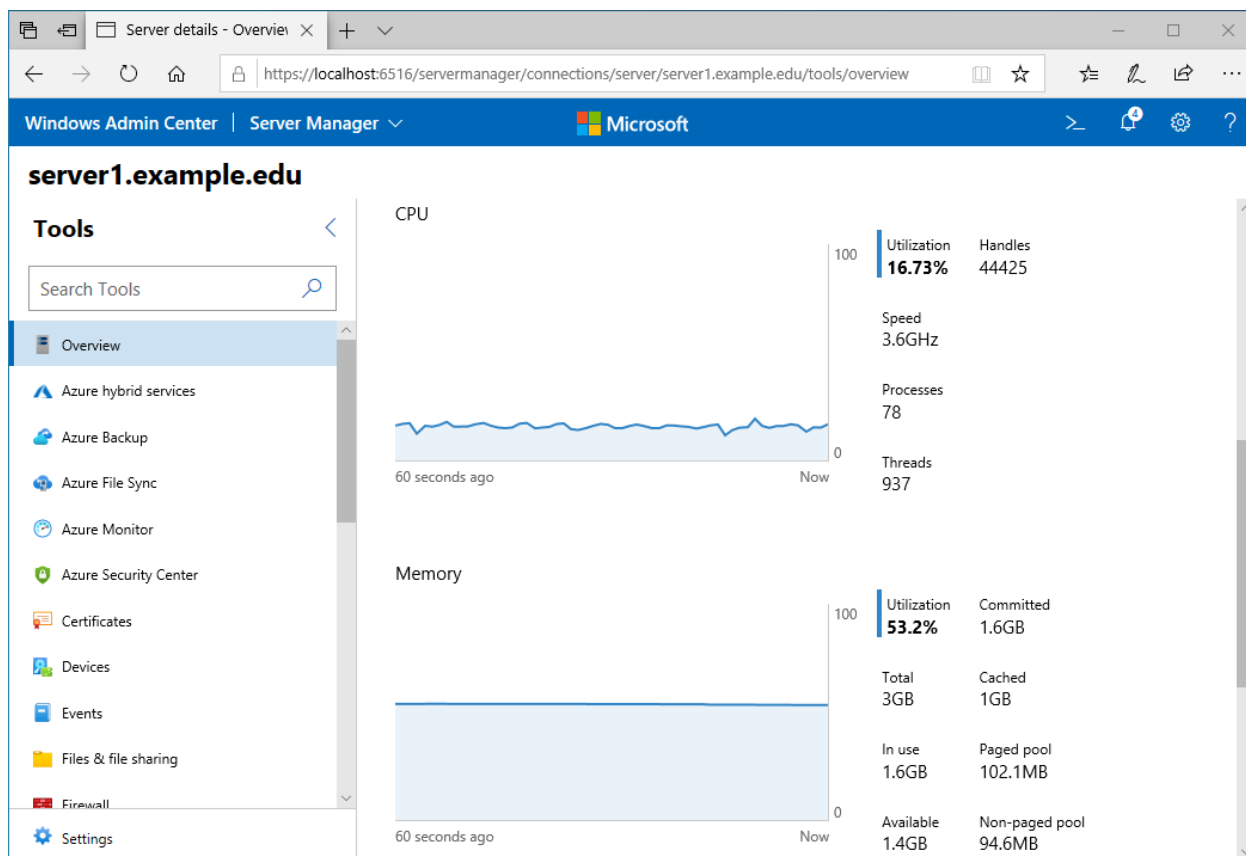


Рис.16. Сведения о сервере.

Снимок Windows Admin Center с общей информацией о сервере Windows Server 2019 (раздел Overview)– в отчет.

14) Запустить на Windows 10 командную оболочку Windows PowerShell, например, через интерфейс Выполнить - «powershell», или через поле поиска на панели задач.

В Windows PowerShell могут выполняться как специальные команды PowerShell (командлеты), так и стандартные команды оболочки Windows, а также встроенные псевдонимы (короткие команды для командлетов PowerShell) (рис.17.)

```
Windows PowerShell
PS C:\Users\user1> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : example.edu
    Link-local IPv6 Address . . . . . : fe80::c4ff:5b49:e9c:d03f%15
    IPv4 Address. . . . . : 192.168.56.22
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.5

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::a8c2:3b13:8d8b:39f2%3
    IPv4 Address. . . . . : 10.0.3.15
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.3.2
PS C:\Users\user1>
PS C:\Users\user1> Get-Alias pwd

CommandType      Name                                Version      Source
-----
Alias             pwd -> Get-Location

PS C:\Users\user1> pwd

Path
----
C:\Users\user1

PS C:\Users\user1> 
```

Рис.17. Команды Windows PowerShell.

Ввести команду подключения к серверу Windows Server 2019 по сетевому имени (например, server1) с указанием на запрос учетных данных :

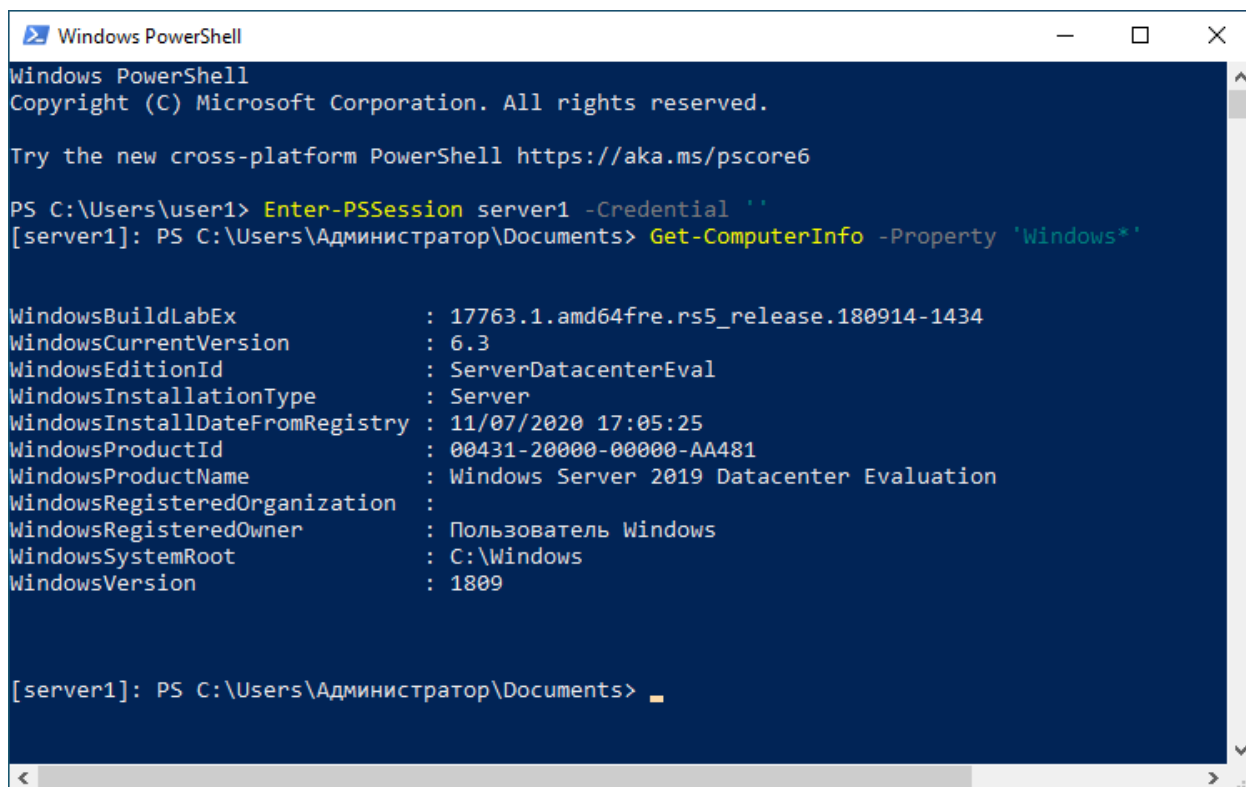
```
Enter-PSSession server1 -Credential "
```

(в конце команды — две одинарные кавычки).

Во всплывающем окне ввести учетные данные администратора домена. После этого будет открыт интерактивный сеанс с сервером.

Ввести команду получения информации об операционной системе сервера с фильтрацией по параметрам (рис.18):

```
Get-ComputerInfo -Property 'Windows*'
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\user1> Enter-PSSession server1 -Credential ''
[server1]: PS C:\Users\Администратор\Documents> Get-ComputerInfo -Property 'Windows*'

WindowsBuildLabEx           : 17763.1.amd64fre.rs5_release.180914-1434
WindowsCurrentVersion       : 6.3
WindowsEditionId            : ServerDatacenterEval
WindowsInstallationType     : Server
WindowsInstallDateFromRegistry : 11/07/2020 17:05:25
WindowsProductId            : 00431-20000-00000-AA481
WindowsProductName          : Windows Server 2019 Datacenter Evaluation
WindowsRegisteredOrganization : 
WindowsRegisteredOwner      : Пользователь Windows
WindowsSystemRoot           : C:\Windows
WindowsVersion              : 1809

[server1]: PS C:\Users\Администратор\Documents>
```

Рис. 18. Получение информации об удаленном сервере.

Снимок окна PowerShell на Windows 10 с открытым сеансом подключения к серверу и вывод информации об ОС сервера— в отчет.

Завершить сеанс с удаленным сервером — ввести команду «exit».

15) Вывести в Powershell список установленных ролей и компонентов на удаленном сервере (например, server1) (рис.19):

```
Get-WindowsFeature -ComputerName server1 -Credential " | Where installed
```



```
Windows PowerShell
PS C:\Users\user1> Get-WindowsFeature -ComputerName server1 -Credential '' | Where installed

Display Name                                     Name                                     Install State
-----
[X] DHCP-сервер                                DHCP                                     Installed
[X] DNS-сервер                                  DNS                                     Installed
[X] Доменные службы Active Directory            AD-Domain-Services                    Installed
[X] Файловые службы и службы хранилища         FileAndStorage-Services               Installed
[X] Службы хранения                            Storage-Services                      Installed
[X] Файловые службы и службы iSCSI             File-Services                         Installed
[X] Файловый сервер                            FS-FileServer                        Installed
[X] Windows Defender Antivirus                 Windows-Defender                      Installed
[X] Windows PowerShell                         PowerShellRoot                        Installed
[X] Windows PowerShell 5.1                     PowerShell                            Installed
[X] Интегрированная среда сценариев Windows PowerShell-ISE PowerShell-ISE                       Installed
[X] XPS Viewer                                 XPS-Viewer                           Installed
[X] Поддержка WoW64                            WoW64-Support                         Installed
[X] Средства удаленного администрирования сервера RSAT                                  Installed
[X] Средства администрирования ролей           RSAT-Role-Tools                      Installed
[X] Средства AD DS и AD LDS                    RSAT-AD-Tools                        Installed
[X] Модуль Active Directory для Windows ... RSAT-AD-PowerShell                  Installed
[X] Средства AD DS                             RSAT-ADDS                           Installed
[X] Оснастки и программы командной с... RSAT-ADDS-Tools                     Installed
[X] Центр администрирования Active D... RSAT-AD-AdminCenter                 Installed
[X] Средства DHCP-сервера                      RSAT-DHCP                           Installed
[X] Средства DNS-сервера                      RSAT-DNS-Server                     Installed
[X] Управление групповой политикой             GPMC                                 Installed
[X] Функции .NET Framework 4.7                 NET-Framework-45-Fea...             Installed
[X] .NET Framework 4.7                        NET-Framework-45-Core               Installed
[X] Службы WCF                                 NET-WCF-Services45                  Installed
[X] Совместное использование портов TCP         NET-WCF-TCP-PortShar...             Installed

PS C:\Users\user1>
```

Рис.19. Выполнение команды на удаленном сервере.

16) Для управления объектами Active Directory в PowerShell нет необходимости открывать интерактивный сеанс работы или отправлять команду на конкретный сервер - контроллер домена.

Для работы с объектами Active Directory необходим дополнительный модуль, который загружается автоматически при вводе команды из состава модуля. В ряде случаев требуется ручная загрузка модуля:

```
Import-Module ActiveDirectory
```

Ввести в PowerShell команду вывода краткой информации об учетной записи доменного пользователя (например, user1):

```
Get-ADUser -identity user1
```

Вывести список всех включенных пользователей домена с отображением только имени и времени последнего входа:

```
Get-ADUser -filter {enabled -eq "True"} -Properties * | select Name, LastlogonDate
```

Снимки результатов выполнения команд получения информации о доменных пользователях — в отчет.

**Отчет:**

- снимок с событием системного времени запуска операционной системы в окне «Computer Management» («Управление компьютером»);
- снимок Диспетчера серверов на Windows 10 с добавленным сервером Windows Server 2019;
- снимок Windows Admin Center с общей информацией о сервере Windows Server 2019 (раздел Overview);
- снимок окна PowerShell на Windows 10 с открытым сеансом подключения к серверу и вывод информации об ОС сервера;
- снимки результатов выполнения команд получения информации о доменных пользователях в PowerShell на Windows 10.