МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра «Вычислительные системы и технологии»

Отчет по лабораторной работе №2

по дисциплине

Программное обеспечение вычислительных сетей

РУКОВОДИТЕЛЬ:

Анисимова Е.С.

СТУДЕНТ:

Малинок С.М.

гр. 21-ПО

Работа защищена « »

С оценкой

Нижний Новгород 2024

Цель работы:

Изучить подготовку и процесс установки Windows Server, изучить варианты настройки сетевых компонентов, ознакомиться с составом и назначением основных служб и системных программ. Изучить состав и основные свойства сетевых служб Windows Sever, ознакомиться со встроенными средствами управления, получить базовые навыки администрирования сетевой среды.

План работы:

1. Windows Server — операционная система, разработанная Microsoft специально для серверных сред и предприятий. Основные требования для установки:

* Аппаратные требования: Эти требования могут варьироваться в зависимости от версии Windows Server, но обычно включают процессор с архитектурой x64, достаточно оперативной памяти (обычно не менее 2 ГБ для минимальной установки), свободное место на жестком диске для установки операционной системы и дополнительные ресурсы для установки и работы приложений и служб.
* Совместимость с оборудованием: Перед установкой Windows Server необходимо убедиться, что серверное оборудование совместимо с требованиями операционной системы. Это включает сетевые адаптеры, дисковые устройства, контроллеры RAID и другое оборудование.
* Лицензирование: Windows Server требует соответствующей лицензии для каждого экземпляра операционной системы, который будет использоваться. Лицензирование может варьироваться в зависимости от версии операционной системы, количества процессоров/ядер и уровня функциональности.
* Сетевые требования: Настройка сетевых параметров также важна для правильной работы Windows Server. Это включает в себя настройку IP-адресов, DNS, DHCP (при необходимости), а также настройку брандмауэров и других средств безопасности.
* Системные требования: Для оптимальной работы операционной системы рекомендуется наличие надежного источника питания, регулярное обновление ПО и драйверов, а также резервное копирование данных.
* Безопасность: Важно обеспечить безопасность операционной системы путем установки антивирусного программного обеспечения, настройки прав доступа и регулярного аудита системы на наличие уязвимостей.

Рассмотрим основные аппаратные требования windows server

* Процессор (CPU):

Минимальные: 1.4 ГГц 64-битный процессор.

Рекомендуемые: Процессор с несколькими ядрами или многоядерный процессор, поддерживающий Hyper-Threading или аналогичную технологию для оптимальной производительности.

* Оперативная память (RAM):

Минимальные: 512 МБ (для Core Install), 2 ГБ (для Server Core), 2 ГБ (для Server с графическим интерфейсом).

Рекомендуемые: 16 ГБ или больше, в зависимости от нагрузки и потребностей сервера.

* Жесткий диск (HDD/SSD):

Минимальные: 32 ГБ свободного пространства.

Рекомендуемые: 40 ГБ или больше для установки операционной системы и установки дополнительных компонентов и приложений.

* Сетевой адаптер (Network Adapter):

Минимальные: 1 Гбит/с Ethernet.

Рекомендуемые: 10 Гбит/с Ethernet для высокопроизводительных серверов или серверов с высокой загрузкой.

* Дисковая подсистема:

Рекомендуемые: Дисковая подсистема с поддержкой RAID для повышения надежности и производительности в случае отказа диска.

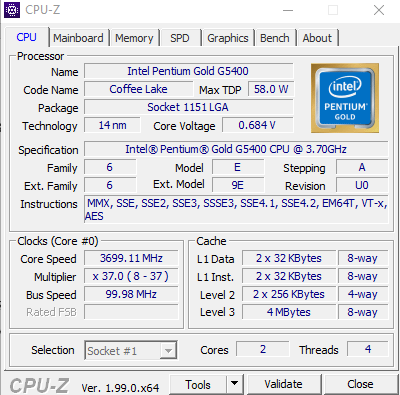
* Графический процессор (GPU):

Минимальные: Не требуется для серверных версий Windows Server. Графический интерфейс может быть отключен для Server Core и Core Install.

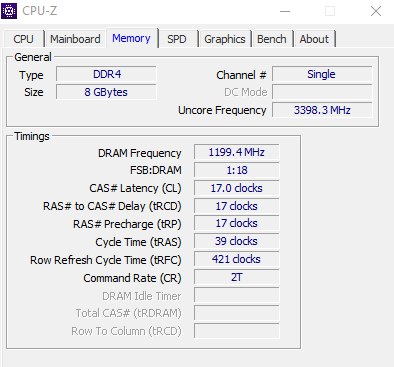
Рекомендуемые: Для некоторых специфических задач, таких как виртуализация с графическими приложениями, может потребоваться поддержка графического процессора.

Рассмотрим аппаратные данные компьютера-хоста с помощью утилиты CPU-Z и Aida64:

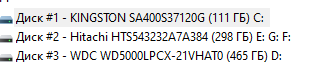
Процессор:



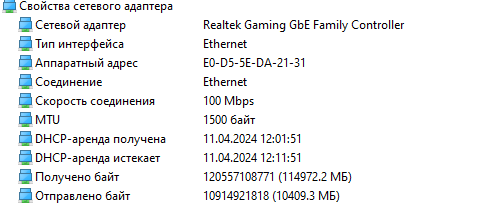
Память:



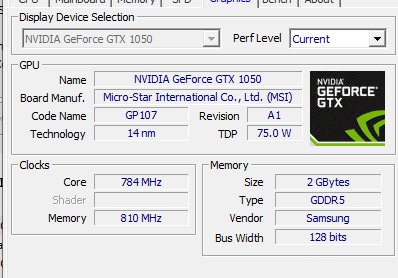
Жесткие диски:



Сетевой адаптер:



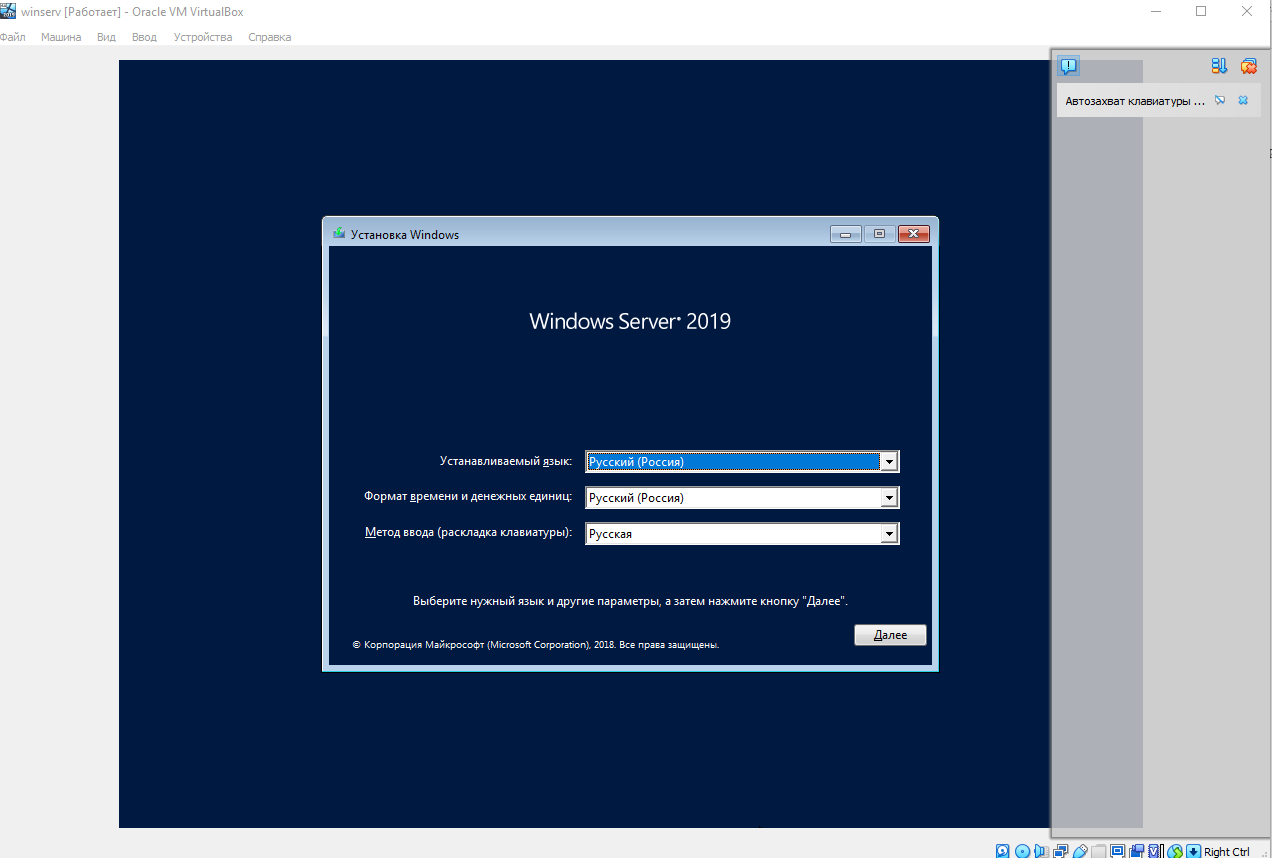
GPU:



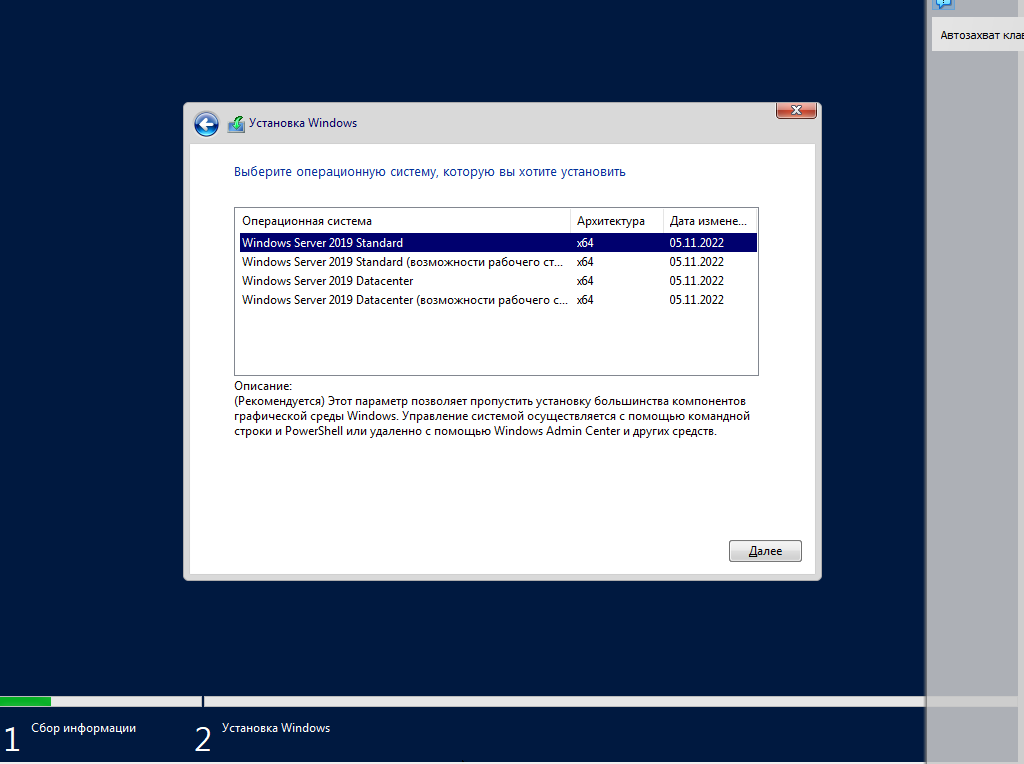
Машина-хост подходит под рекомендуемые системные требования ОС.

1. Планировка установки windows server
2. Мой ПК полностью удовлетворяет требованиям Windows Server 2019
3. Мой ПК полностью соответсвует требованиям виртуальной машины
4. Дистрибутив для установки windows server 2019 был взят из интернета
5. Установка будет производится на внешний диск D, необходимое место – 50 ГБ
6. Тип установки new, так как система ставится с нуля
7. Лицензия будет получена путём генератора ключей
8. В сети сервер будет выступать хранилищем файлов
9. Active Directory, DNS, DHCP.
10. WN-59CBD1TPL06 имя компьютера. Домен - SERVER
11. Настройка производится с нуля
12. Установка windows server

Начальный экран установки похож на win10



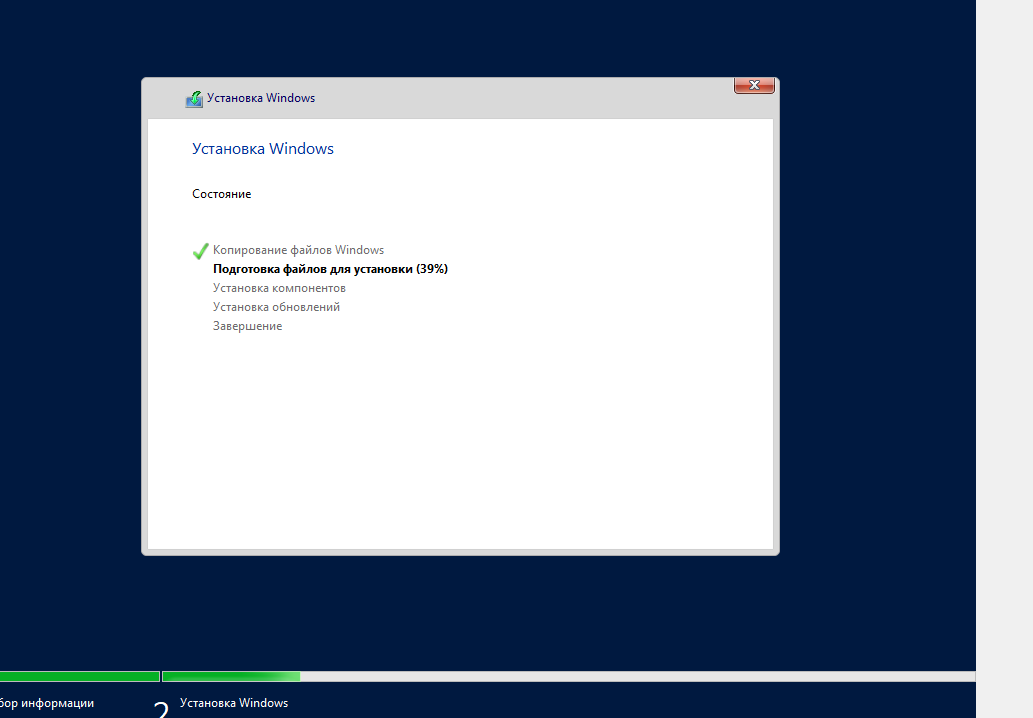
Для установки выбрал Windows Server 2019 standart с возможностями рабочего стола.

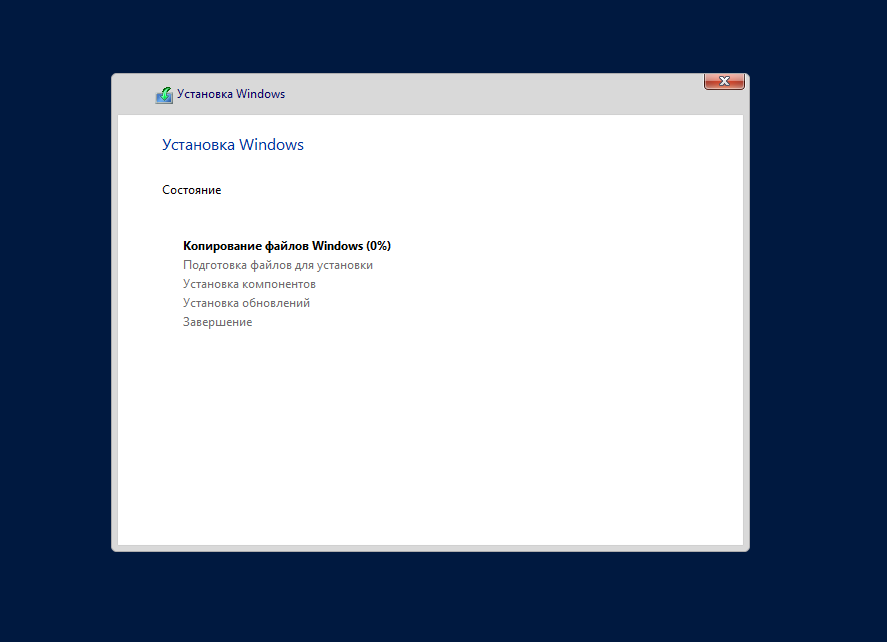
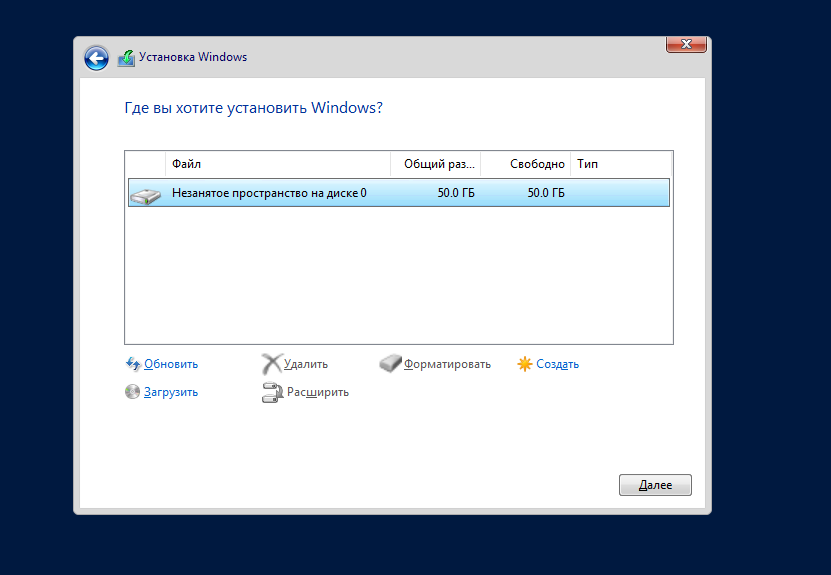


Главные различия между Windows Server Standard и Datacenter заключаются в их возможностях и лицензионной политике:

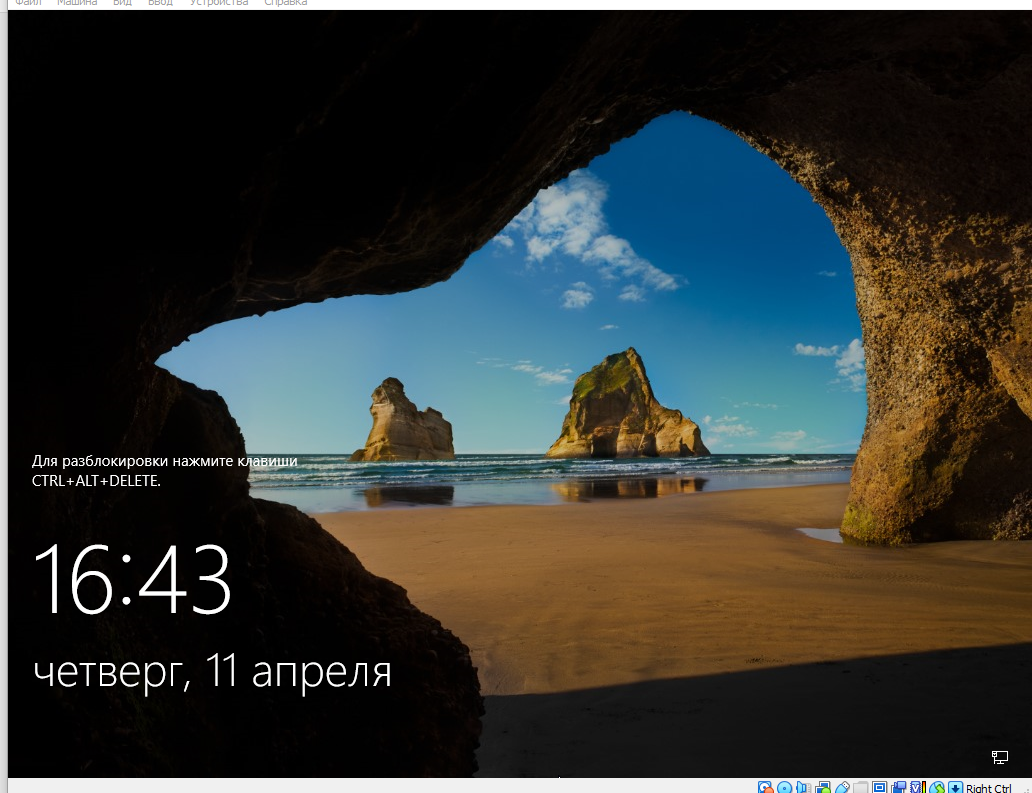
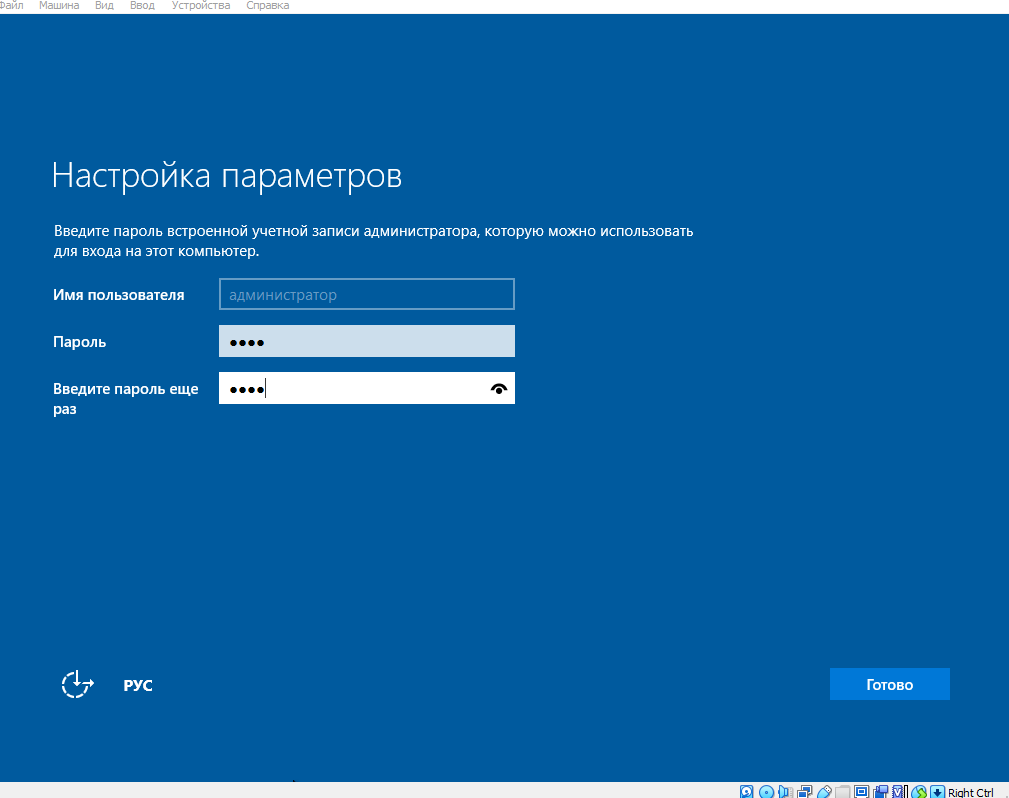
* Лицензирование и цена: Windows Server Standard обычно имеет ограничение на количество виртуальных машин (VM), которые можно запустить на сервере, а также на количество процессоров (обычно до 2). Datacenter, с другой стороны, позволяет неограниченное количество VM и обычно лицензируется на основе количества процессоров на сервере. Datacenter обычно стоит значительно дороже, чем Standard, но если у вас много виртуализированных серверов, Datacenter может быть более выгодным вариантом.
* Возможности: Datacenter обычно включает в себя все функции, доступные в Standard, а также дополнительные функции, которые могут быть полезны в больших средах виртуализации или корпоративных сетях. Например, Datacenter может включать в себя возможности виртуализации на уровне хоста, такие как Hyper-V Replica, а также дополнительные функции управления и безопасности.
* Масштабируемость: Datacenter предназначен для более крупных и сложных сред, где требуется высокая масштабируемость и гибкость. Он предоставляет больше возможностей для управления и виртуализации ресурсов.

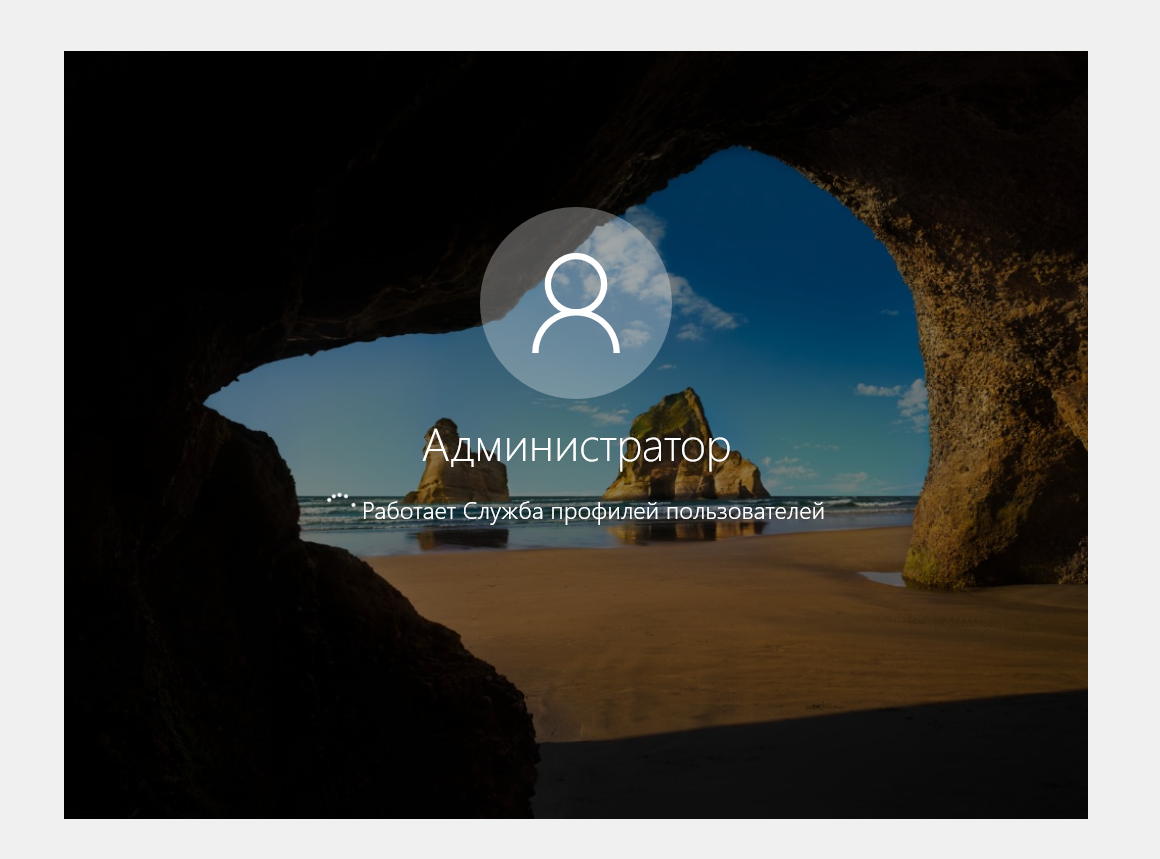
Для моей задачи подойдёт версия Standart с рабочим столом



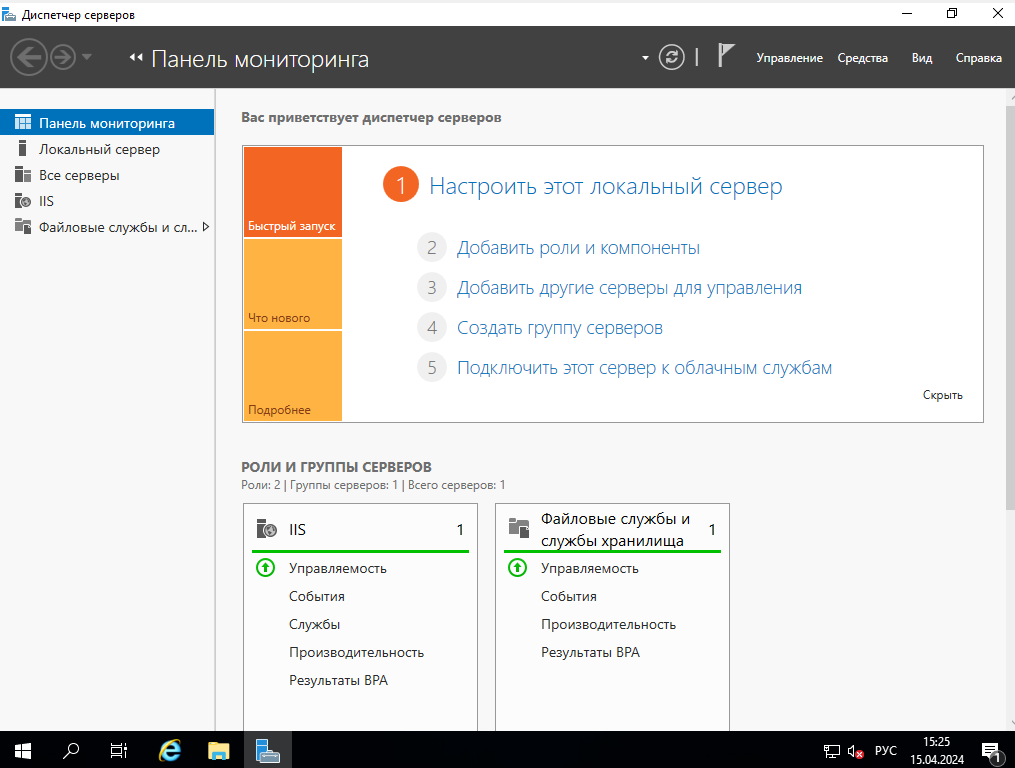


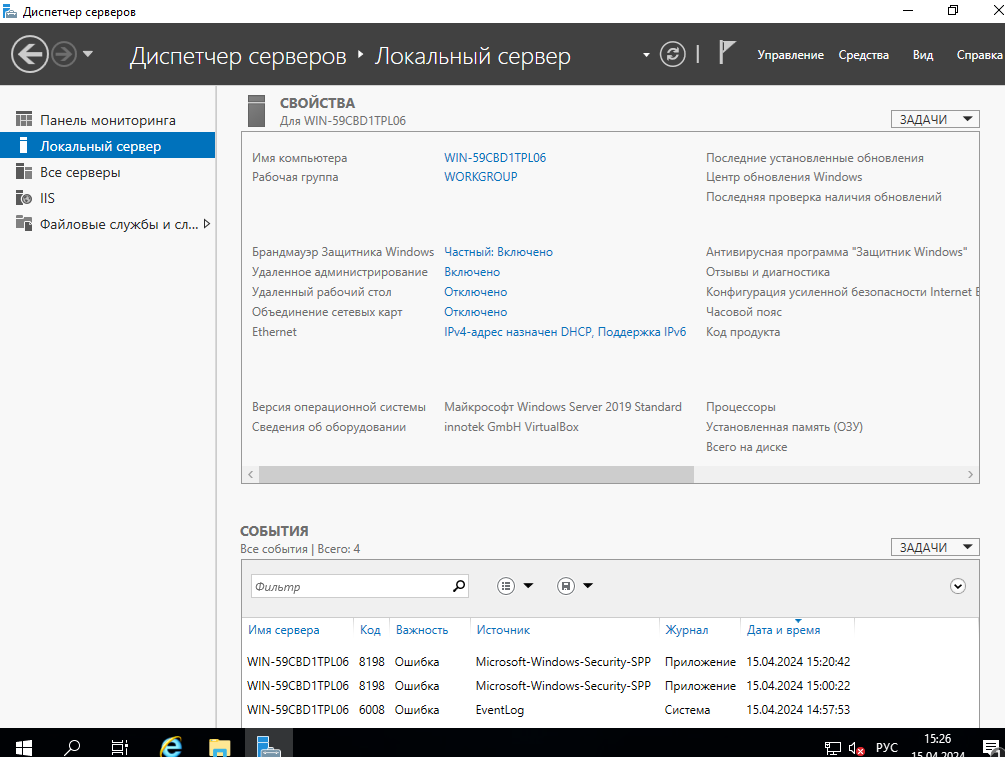
Настройка



Вход в систему 

Мастер настройки сервера





Мастер настройки сервера Windows Server (Windows Server Configuration Wizard) - это инструмент, предоставляемый операционной системой Windows Server для облегчения процесса начальной настройки сервера. Этот мастер позволяет администраторам быстро и удобно настроить основные параметры сервера, такие как сетевые настройки, безопасность, службы и т.д.

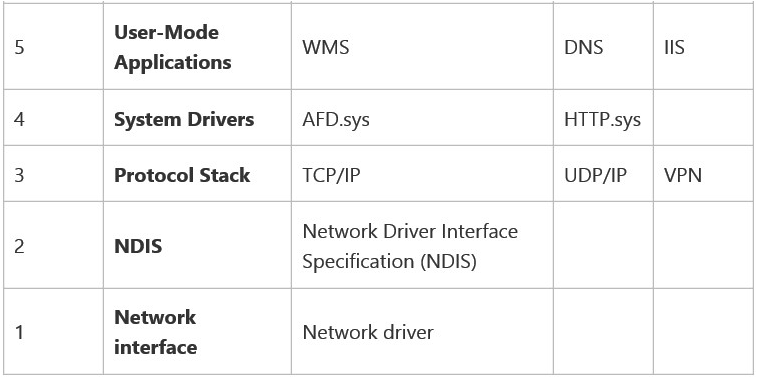
Обычно мастер настройки сервера Windows Server предлагает шаг за шагом инструкции для настройки различных аспектов сервера. Например, он может попросить указать имя сервера, установить пароли администратора, сконфигурировать сетевые подключения, включить или отключить определенные службы и т.д.

Этот инструмент помогает ускорить процесс начальной настройки сервера и обеспечить базовую безопасность и функциональность. Однако после завершения мастера настройки администратор может провести дополнительные настройки в соответствии с требованиями и потребностями конкретной среды.

Настройка производительности сетевой подсистемы, особенно для рабочих нагрузок с интенсивными сетями, может включать каждый слой сетевой архитектуры, который также называется стеком сети. Эти слои широко разделены на следующие разделы.

1. Сетевой интерфейс. Это самый низкий уровень в сетевом стеке и содержит сетевой драйвер, который взаимодействует напрямую с сетевым адаптером.
2. Спецификация интерфейса сетевого драйвера (NDIS). NDIS предоставляет интерфейсы для драйвера под ним и для слоев над ним, таких как стек протоколов.
3. Стек протоколов. Стек протоколов реализует такие протоколы, как TCP/IP и UDP/IP. Эти слои предоставляют интерфейс транспортного слоя для слоев над ними.
4. Системные драйверы. Обычно это клиенты, использующие расширение данных транспорта (TDX) или интерфейс Winsock Kernel (WSK) для предоставления интерфейсов приложениям пользовательского режима.
5. Приложения в режиме пользователя. Обычно это решения Майкрософт или пользовательские приложения.

В приведенной ниже таблице представлена вертикальная иллюстрация слоев сетевого стека, включая примеры элементов, выполняемых в каждом слое.



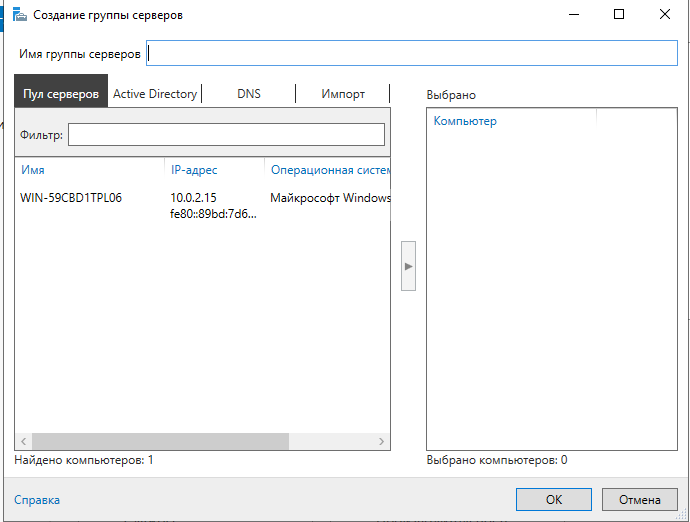
Группа серверов (Server Group) - это совокупность нескольких серверов, объединенных вместе для совместного выполнения определенных задач или для обеспечения отказоустойчивости и масштабируемости системы. Группа серверов может использоваться для различных целей, таких как балансировка нагрузки, отказоустойчивость, высокая доступность и распределение задач.

В зависимости от конкретной конфигурации и целей, группа серверов может включать в себя сервера с одинаковым или различным аппаратным и программным обеспечением. Как правило, группа серверов управляется и контролируется с помощью специального программного обеспечения, такого как системы управления кластерами или программы для балансировки нагрузки.

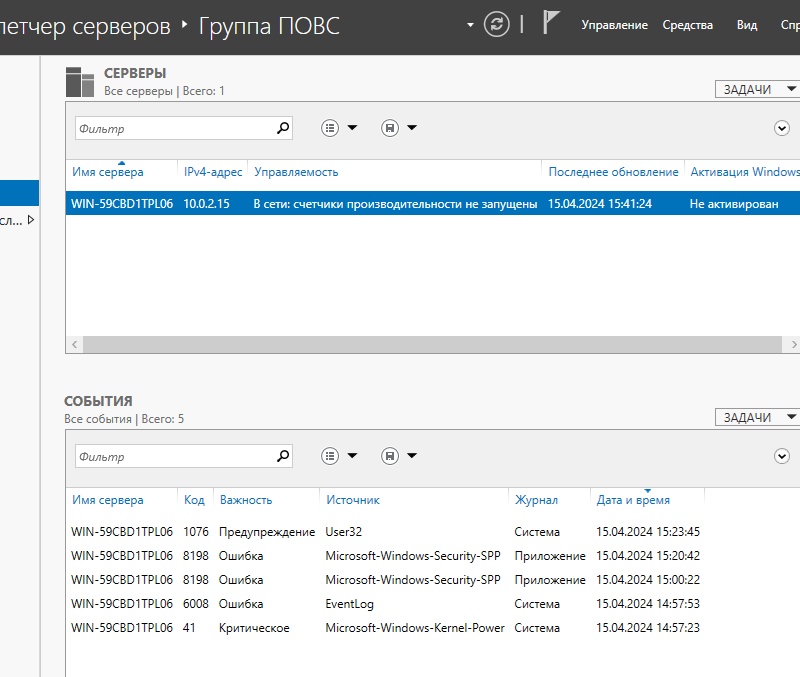
Какие существуют группы серверов:

1. Кластеры высокой доступности (High Availability Clusters): В этих группах несколько серверов работают вместе таким образом, чтобы обеспечить непрерывную доступность сервисов и приложений в случае отказа одного из серверов.
2. Группы серверов для балансировки нагрузки (Load Balancing Server Groups): Здесь несколько серверов используются для распределения нагрузки от клиентов между собой с целью обеспечения равномерного распределения нагрузки и увеличения производительности.
3. Группы серверов для параллельных вычислений (Parallel Computing Server Groups): Эти группы серверов используются для выполнения параллельных вычислений, где задачи могут быть разделены между несколькими серверами для более быстрого выполнения.

Использование групп серверов позволяет повысить надежность, масштабируемость и производительность системы за счет распределения нагрузки и обеспечения резервирования ресурсов.



Создана группа серверов



1. Основные свойства администрирования windows server, Компоненты группы администрирование.

Windows Server предлагает ряд встроенных свойств и инструментов для управления и администрирования серверов. Некоторые из основных встроенных свойств администрирования Windows Server включают:

* Active Directory: Active Directory (AD) представляет собой службу каталогов, которая хранит данные об объектах в сетевой среде, таких как пользователи, компьютеры, группы и ресурсы, и обеспечивает доступ к этим данным другим приложениям и службам в сети.
* Group Policy: Group Policy позволяет администраторам централизованно управлять настройками конфигурации для пользователей и компьютеров в сети. С его помощью можно настроить политики безопасности, сети, программного обеспечения и другие параметры на уровне домена или организационной единицы.
* PowerShell: PowerShell - это мощный язык сценариев и среда командной строки, разработанные для автоматизации административных задач в Windows. Он предоставляет доступ к широкому спектру командлетов и API для управления различными аспектами сервера и его ресурсов.
* Remote Desktop Services (RDS): RDS позволяет пользователям удаленно запускать приложения и рабочие столы на сервере. Это особенно полезно для предоставления доступа к приложениям в виртуальных средах или для удаленной поддержки пользователей.
* Windows Server Update Services (WSUS): WSUS позволяет администраторам управлять процессом обновления для компьютеров и серверов в сети, централизованно устанавливая и управляя обновлениями операционной системы и другими продуктами Microsoft.
* Failover Clustering: Failover Clustering позволяет создавать группы серверов (кластеры), которые могут автоматически обеспечивать отказоустойчивость и высокую доступность для приложений и служб.
* Remote Server Administration Tools (RSAT): Набор инструментов для удаленного администрирования серверов Windows с локальной рабочей станции.

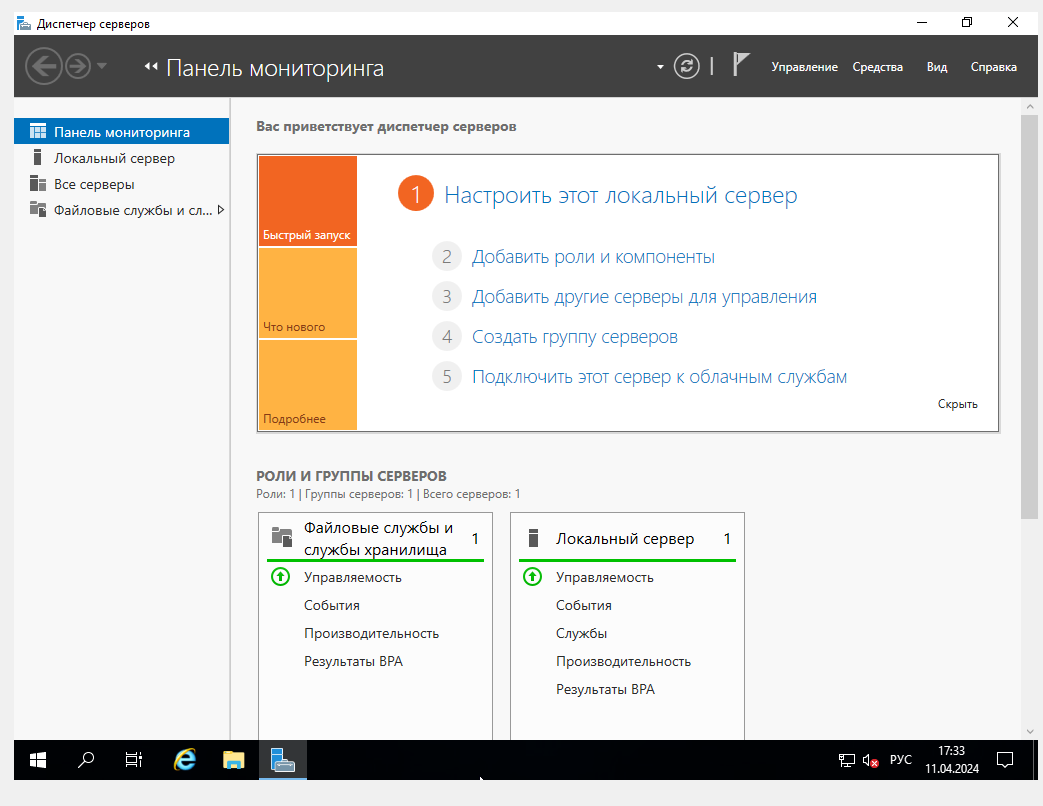
Компоненты группы администрирования включают в себя:

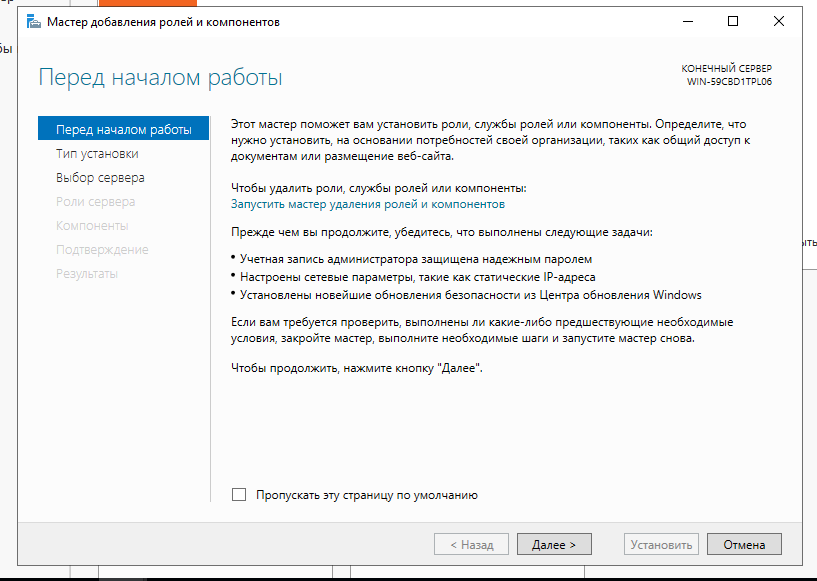
Редактор реестра, системный монитор, редактор служб, планировщик заданий, брандмауэр, диспетчер серверов. Рассмотрим эти компоненты:

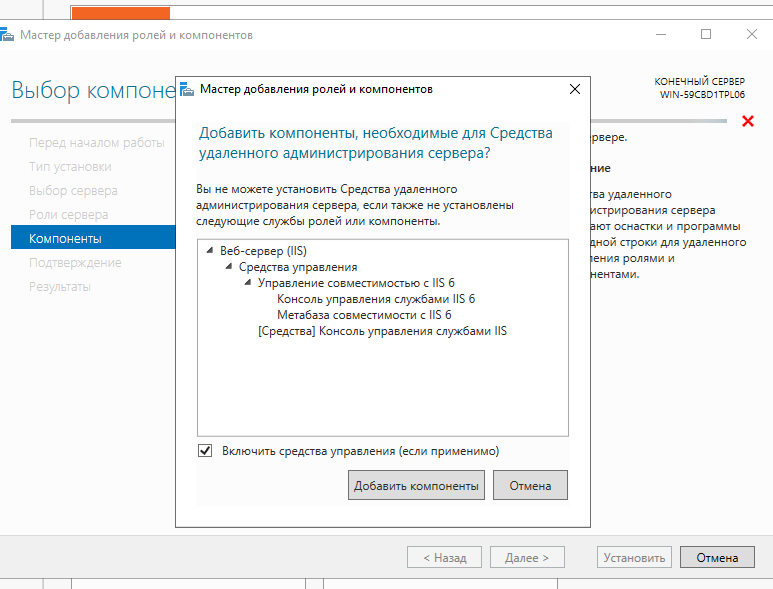
1. Редактор реестра - это инструмент в операционной системе Windows, который позволяет пользователям просматривать, изменять и управлять реестром операционной системы. Реестр - это центральное хранилище настроек и конфигураций операционной системы Windows, включая параметры системы, настройки программ, информацию о установленных приложениях, ассоциации файлов и многое другое.
2. Системный монитор - это инструмент в операционных системах Windows, который позволяет отслеживать и анализировать производительность компьютера в реальном времени. С его помощью можно отображать и анализировать различные параметры и ресурсы системы, такие как загрузка процессора, использование памяти, активность дисков, сетевой трафик и другие метрики.
3. Редактор служб - это инструмент в операционной системе Windows, который позволяет управлять службами (сервисами), запущенными на компьютере. Службы - это фоновые процессы, которые выполняются без участия пользователя и могут выполнять различные функции, такие как запуск веб-серверов, обеспечение сетевого доступа, управление устройствами и т. д.
4. Планировщик заданий - это инструмент в операционной системе Windows, который позволяет настраивать и автоматизировать выполнение различных задач в определенное время или при наступлении определенных событий. Через Планировщик заданий можно создавать и управлять заданиями, такими как запуск приложений, выполнение сценариев, отправка электронных сообщений, обновление программного обеспечения и многое другое.
5. Брандмауэр - это программное или аппаратное устройство, которое служит для защиты компьютерных сетей от несанкционированного доступа и контроля трафика, проходящего через сеть. Брандмауэр может блокировать или разрешать соединения на основе заданных правил безопасности. В операционной системе Windows, Брандмауэр является встроенной функцией, которая может быть настроена для фильтрации входящего и исходящего сетевого трафика. Это позволяет контролировать доступ к ресурсам компьютера из локальной сети или интернета.
6. Диспетчер серверов (Server Manager) - это удобный инструмент управления в операционной системе Windows Server, который позволяет администраторам управлять различными аспектами сервера, включая установку и настройку ролей сервера, управление удаленными серверами, мониторинг состояния сервера, настройку служб и многое другое.
7. Выполнить установку инструментального пакета администратора

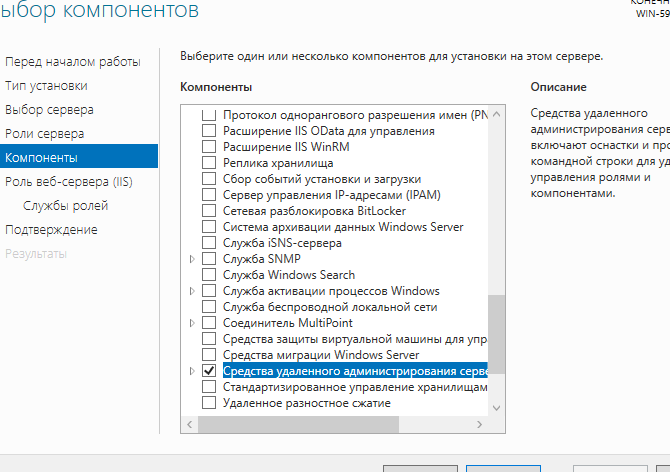
В Windows Server 2019 Microsoft изменила подход к инструментам администратора, включенным в операционную систему. Support Tools, которые были представлены в предыдущих версиях Windows Server, больше не поставляются вместе с Windows Server 2019. Вместо этого Microsoft предоставляет набор инструментов, известный как Remote Server Administration Tools (RSAT), которые позволяют администраторам управлять удаленными серверами из клиентских компьютеров под управлением Windows.

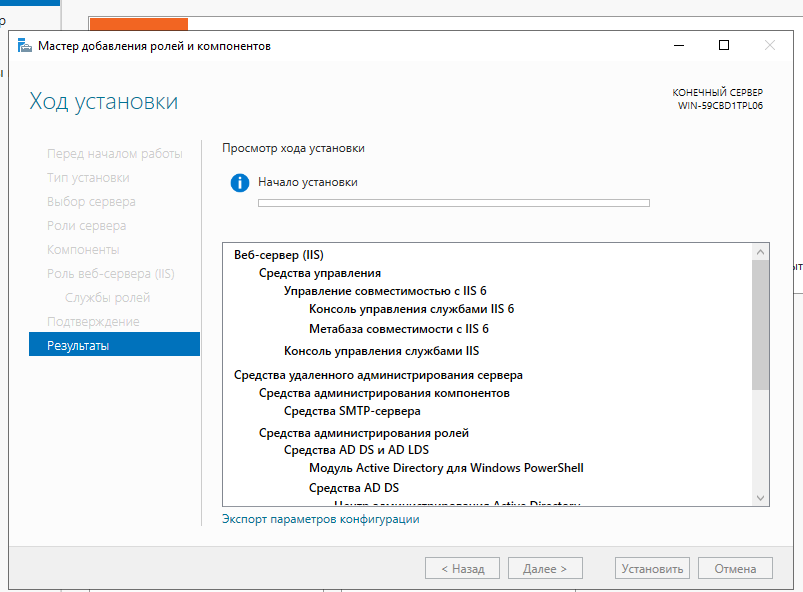
В Windows Server для установки RSAT не нужен доступ в интернет. Компоненты RSAT можно устанавливать при установке соответствующих ролей или фич Windows Server, либо можно установить их через Server Manager (Add roles and Features -> Features -> Remote Server Administration Tools). Все компоненты RSAT разбиты на две секции: Feature Administration Tools и Role Administration Tools. Выберите необходимые компоненты и нажмите Next -> Next.

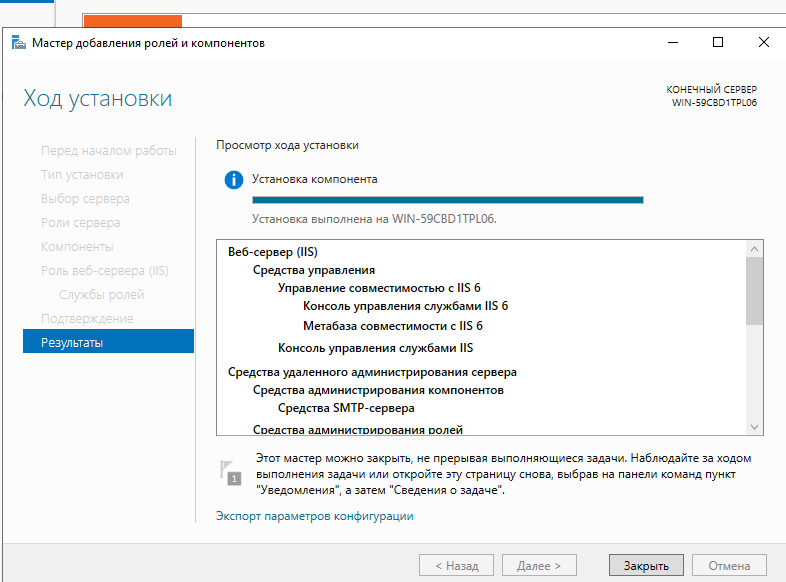




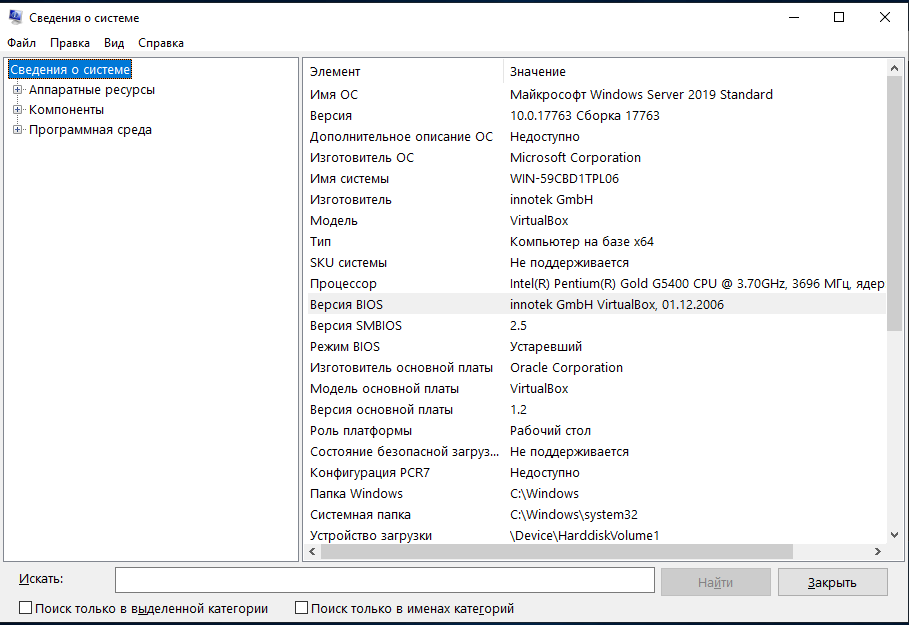




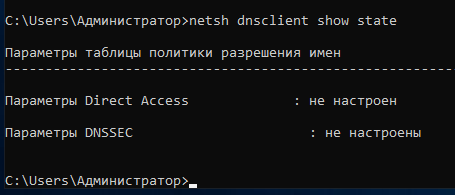




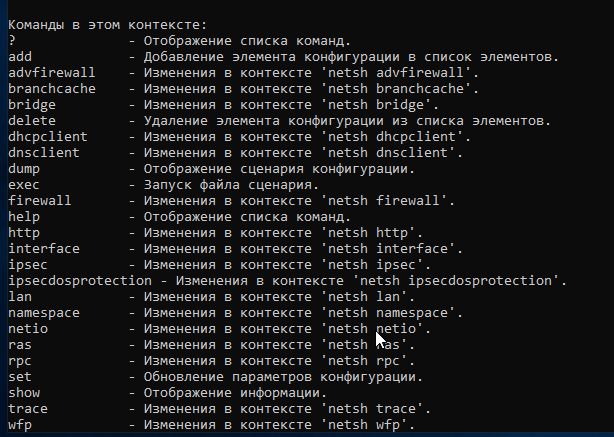
Msinfo32



Команда netdiag была заменена на netsh в последних версиях windows



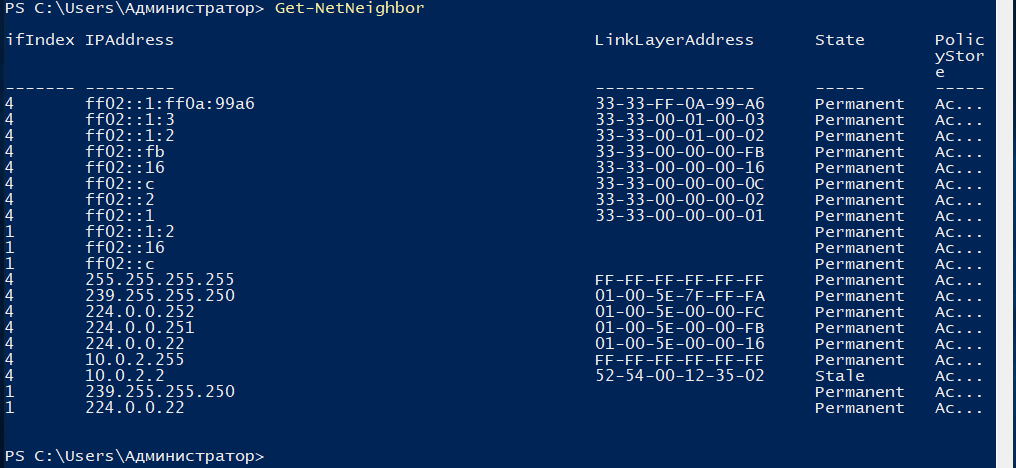
С помощью netsh мы можем изменять конфигурацию сети



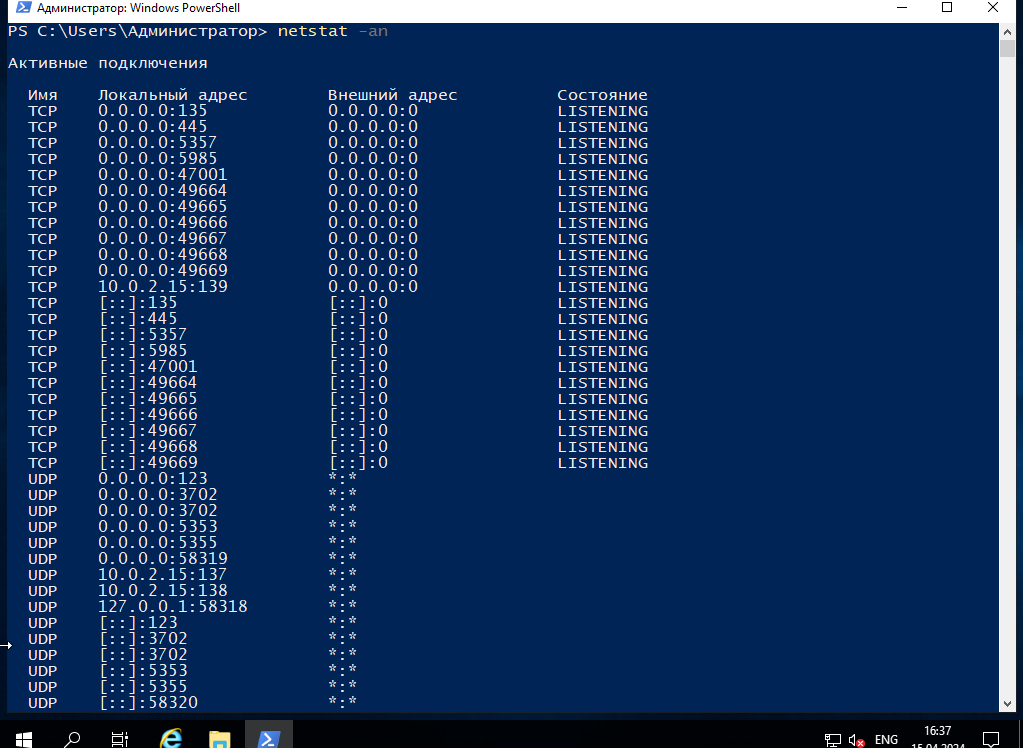
Browstat - это утилита, которая использовалась в более ранних версиях Windows Server для анализа состояния браузера домена (Domain Browser) в сети. Этот инструмент был часто использован администраторами для диагностики проблем с мастером браузера (Browser Master) или для отображения списка компьютеров в домене.

В Windows Server 2019 и в других современных версиях Windows Server Microsoft перешла к другим средствам диагностики и администрирования, в частности, к инструментам PowerShell и утилитам из Remote Server Administration Tools (RSAT).

Заменим команду Browstat командой Powershell Get-NetNeighbor



Проанализируем сетевое окружение командой netstat Команда netstat выводит информацию о сетевых соединениях, сетевых портах, маршрутах и других сетевых параметрах.

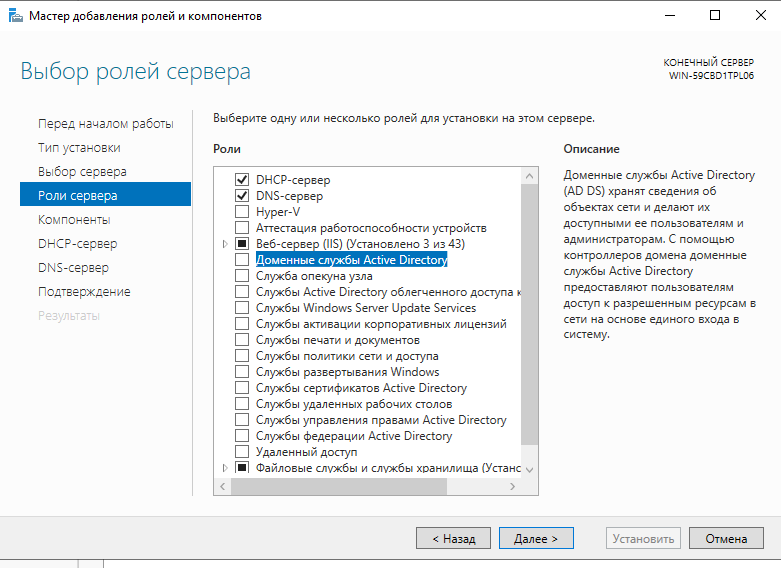


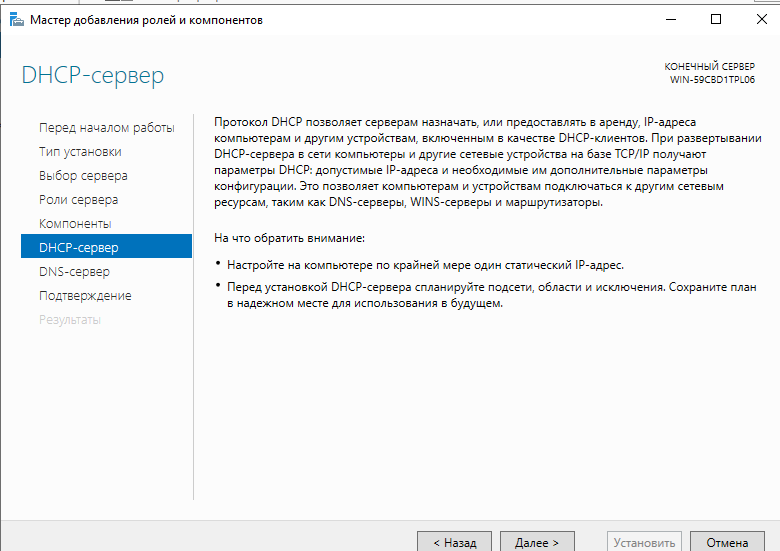
1. Выбрать распределение сетевых сервисов DNS, WINS, DHCP по серверам. Установить соответствующие службы на выбранных серверах.

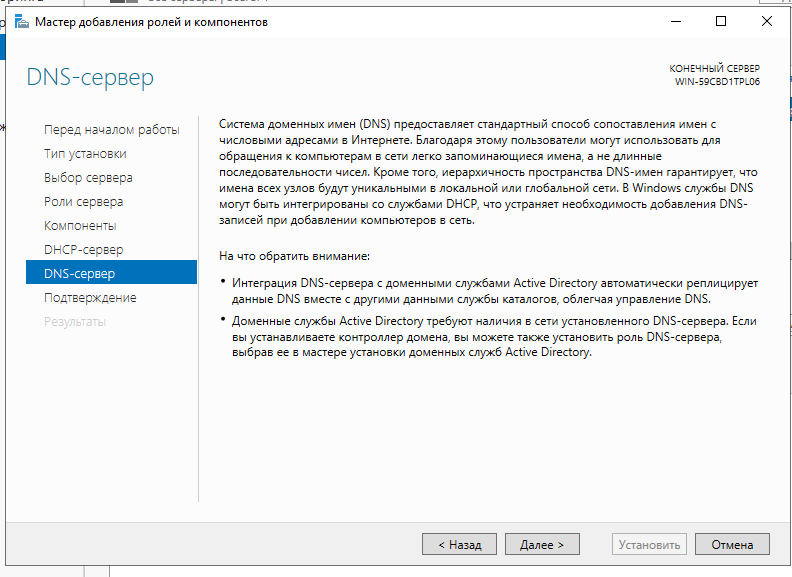
С официального сайта Microsoft мы узнаём: Служба имен Интернета Windows (WINS) — это устаревшая служба регистрации имен компьютера и разрешения, которая сопоставляет имена компьютеров NetBIOS с IP-адресами.

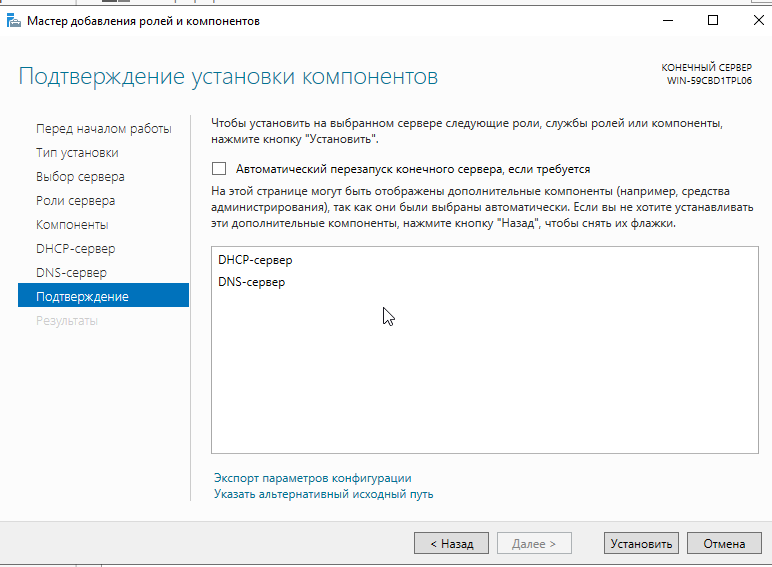
Если у вас еще нет WINS, развернутых в сети, не развертывайте WINS. Вместо этого разверните систему доменных имен (DNS). DNS также предоставляет службы регистрации и разрешения имен компьютера и включает в себя множество дополнительных преимуществ по сравнению с WINS, такими как интеграция с службами домен Active Directory.

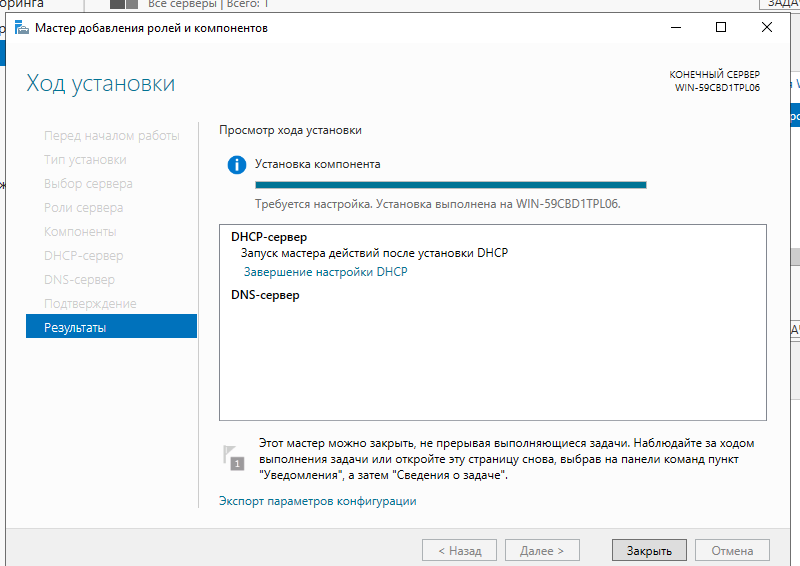
Более того, при настройке ролей виртуальной машины не было обнаружено этой роли, так что используем роли DHCP и DNS: так как мы используем одну виртуальную машину, то присваиваем нашему серверу обе роли



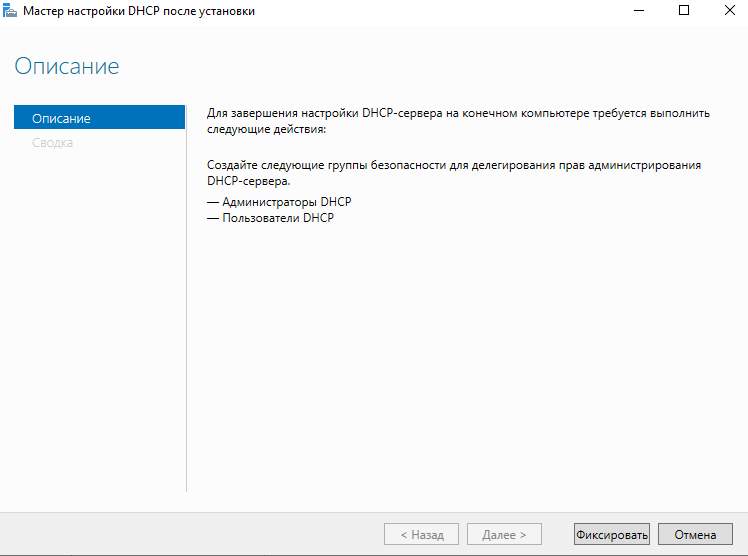


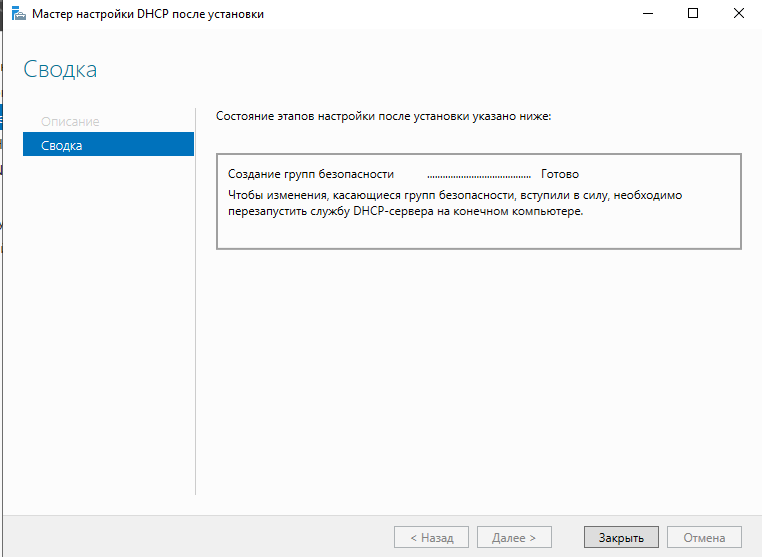






Запустим мастер настрйоки DHCP





1. Конфигурирование и использование DHCP

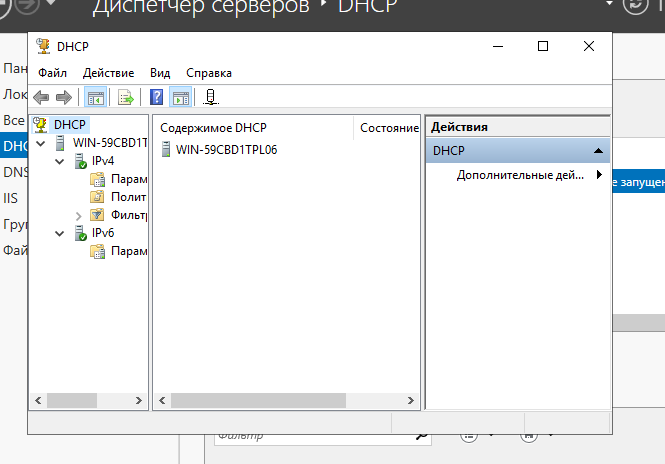
Базовая настройка DHCP сервера произошла при установке мастером настройки.

IPv4 содержит в себе область адресов, параметры сервера и фльтры.

Область включает в себя пул адресов, список арендованных адресов, зарезервированные адреса (позволяют назначать клиенту один и тот же IP-адрес) и параметры области (можно настроить вручную с помощью вкладки Дополнительные действия – Настроить параметры)

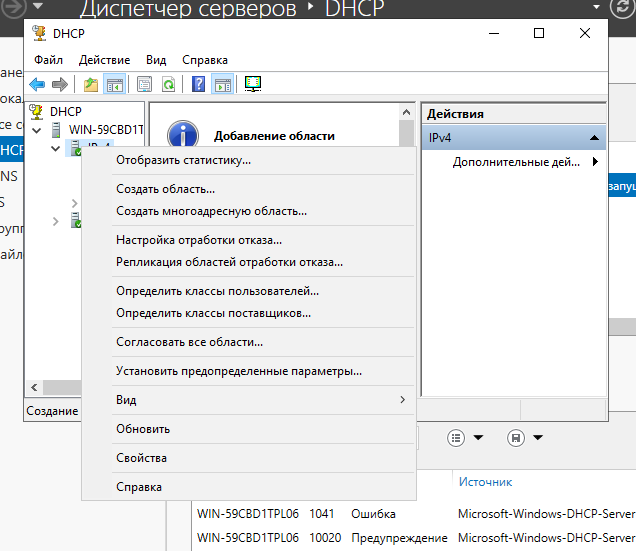
Настройка DHCP-сервера (Dynamic Host Configuration Protocol) в Microsoft Windows Server 2019 позволяет автоматически назначать IP-адреса и другие сетевые параметры клиентам в сети. Вот пошаговое руководство по настройке DHCP-сервера в Windows Server 2019:

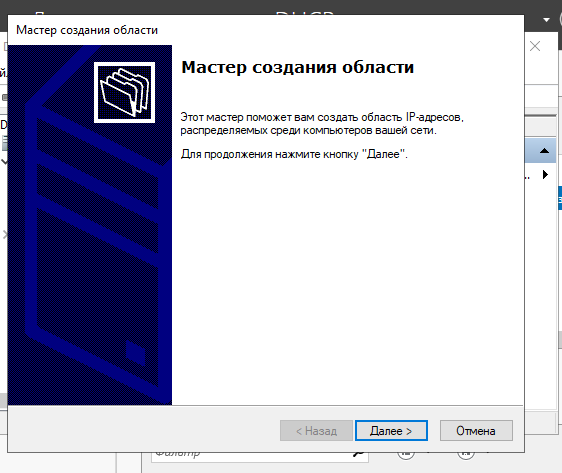
1. Установка роли службы DHCP:
   * 1. Запустите "Server Manager" на сервере с установленной Windows Server 2019.
     2. Нажмите на "Manage" в верхнем правом углу и выберите "Add Roles and Features".
     3. Пройдите мастер установки, выбрав роль "DHCP Server", и добавьте требуемые дополнительные компоненты.
     4. Завершите установку, следуя инструкциям мастера.
2. Настройка DHCP-службы:
   * 1. После установки роли службы DHCP откройте "Server Manager" и выберите "Tools" в верхнем правом углу.
     2. Выберите "DHCP" для открытия DHCP Manager.
3. Настройка DHCP-сервера:
   * 1. В DHCP Manager щелкните правой кнопкой мыши на сервере и выберите "Configure DHCP Server".
     2. Следуйте инструкциям мастера настройки, выбрав сетевой интерфейс, на котором DHCP-сервер будет выдавать адреса, а также указав диапазоны IP-адресов для выдачи.
4. Настройка диапазонов адресов:
   * 1. В DHCP Manager выберите сервер и разверните "IPv4".
     2. Щелкните правой кнопкой мыши на "IPv4" и выберите "New Scope".
     3. Следуйте мастеру создания нового диапазона, указав диапазон IP-адресов, маску подсети, шлюз по умолчанию, DNS-серверы и другие параметры.
     4. Настройте параметры аренды адресов, такие как время аренды (Lease Duration), и другие параметры, включая опции DHCP, если это необходимо.
5. Настройка параметров области:
   * 1. При необходимости настройте параметры области (Scope Options), такие как адрес DNS-сервера, шлюз по умолчанию, DNS-суффикс и т. д., для того чтобы клиенты могли правильно настраиваться.
6. Активация DHCP-сервера:
   * 1. После завершения настройки DHCP-сервера убедитесь, что он активирован. Если DHCP-сервер не активирован, щелкните правой кнопкой мыши на сервере в DHCP Manager и выберите "Authorize".
7. Мониторинг и отладка:
   1. После настройки DHCP-сервера важно следить за его работой и мониторить выдачу адресов клиентам. Для этого можно использовать различные инструменты, включая DHCP Manager.

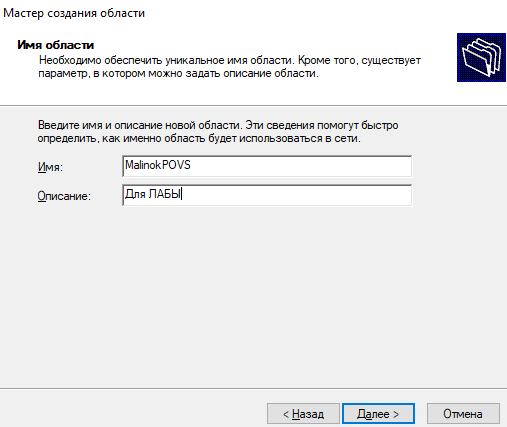
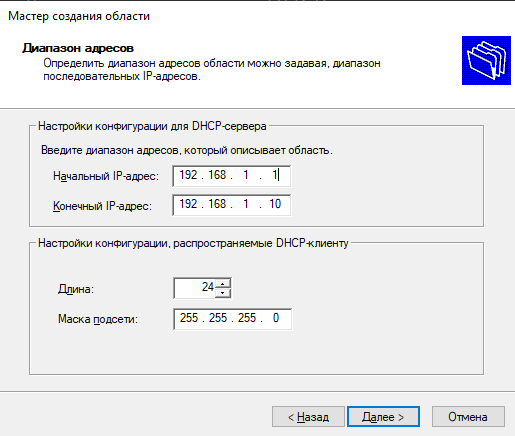


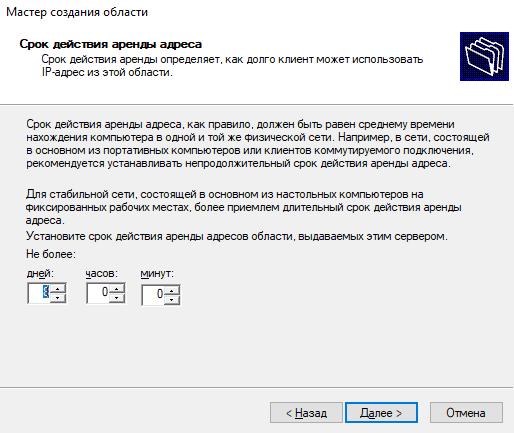
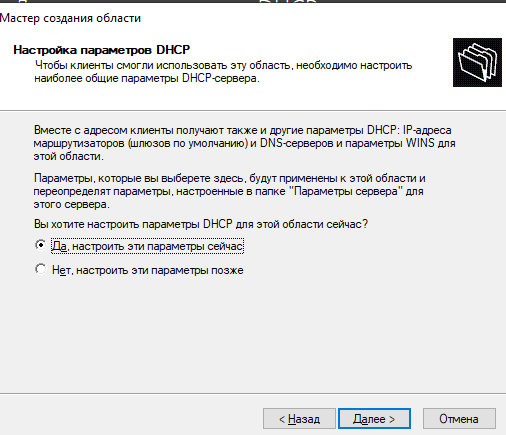
Настроим пулы областей

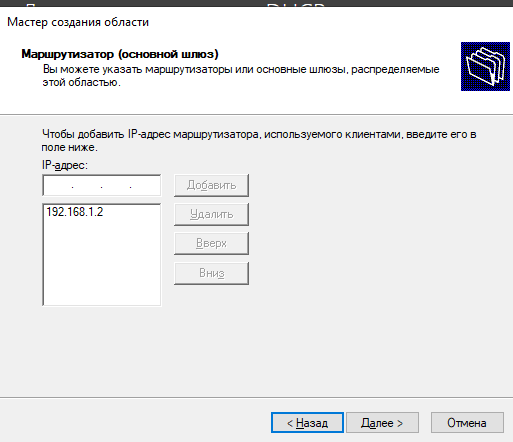
Так как у нас одна ВМ, и сервер имеет несколько ролей, мастер настройки не глупый и даёт нам возможность сконфигурировать сразу все роли (DNS, DHCP, WINS)

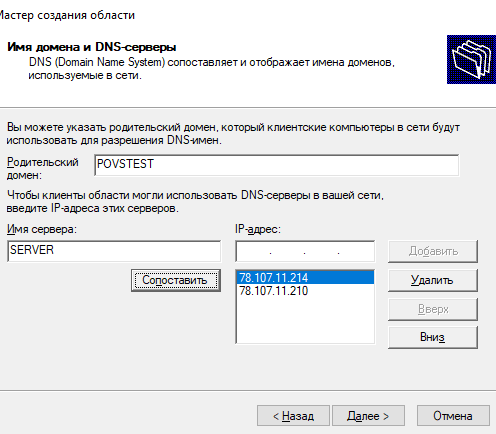


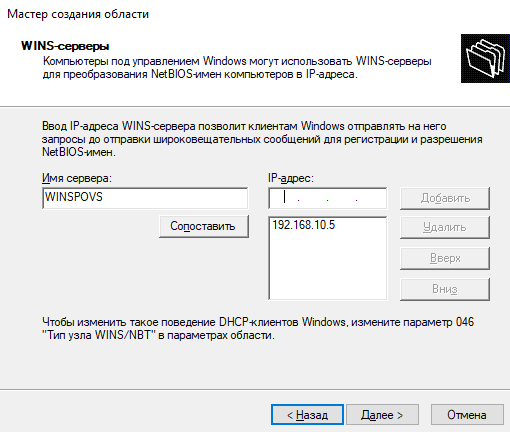
э

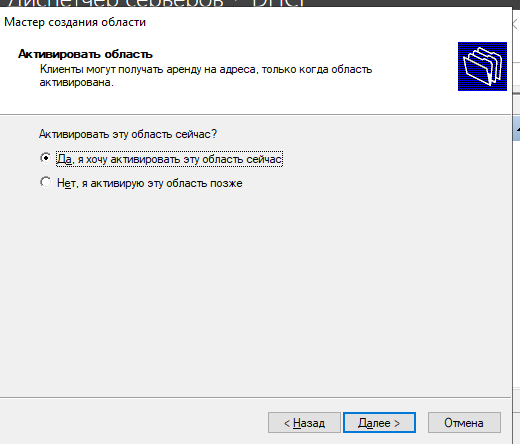
 

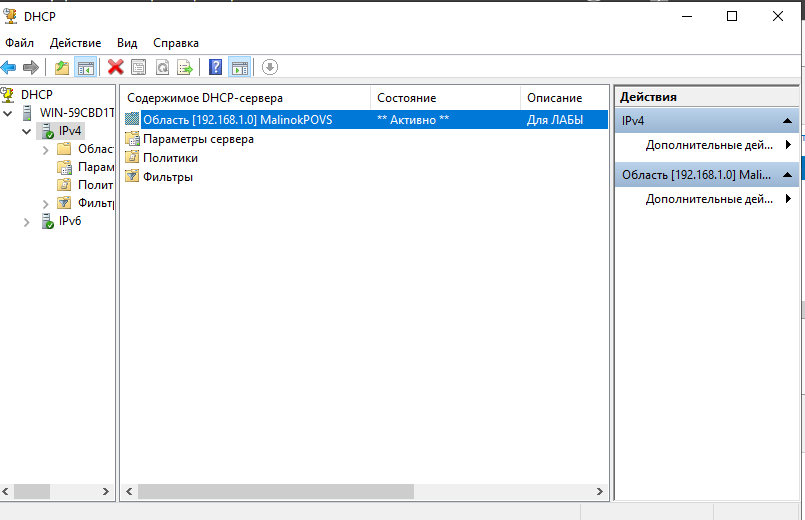




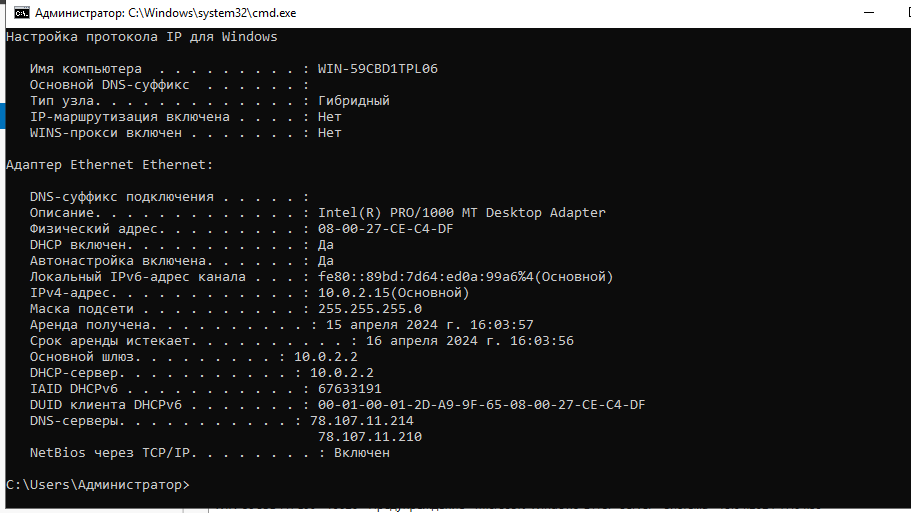




Область создана и активирована



Теперь проверим конфигурацию DHCP сервера и подключение протоколов TCP\IP с помощью ipconfig

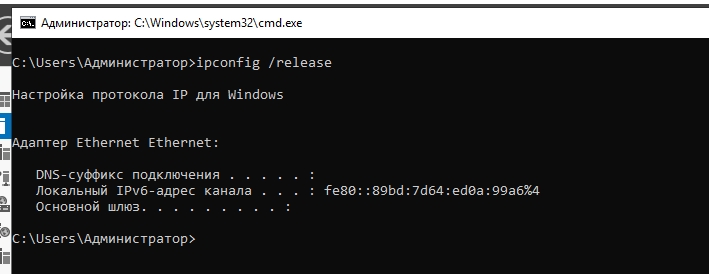


Компьютер автоматически получил IP-адрес и адрес DNS-сервера после изменения настроек.

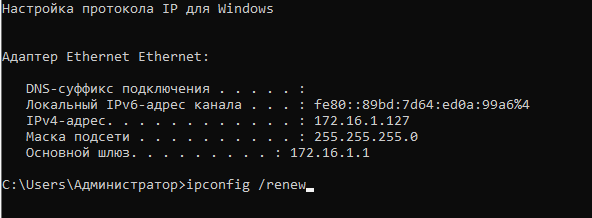
IP-адрес был назначен автоматически в формате. В данной случае была активирована APIPA (автоматическая частная IP-адресация, Automatic Private IP Addressing). То есть, система сама себе назначила IP-адрес, основываясь на MAC-адресе и ГПСЧ. APIPA позволяет избежать сбоев в компьютерной системе при отказе DHCP-сервера. В данной ситуации был назначен адрес 10.0.2.15, маска 255.255.255.0.

Используя протокол ARP, клиенты проверяют уникальность сгенерированного адреса перед использованием. Если на других компьютерах не был сгенерирован такой же адрес, то компьютер использует свой, иначе генерирует новый. Также, пока используется адрес, назначенный APIPA, компьютер проверяет DHCP-сервер. Как только DHCP-сервер снова будет обслуживать запросы, система автоматически обновит свой адрес на назначенный DHCP-сервером.

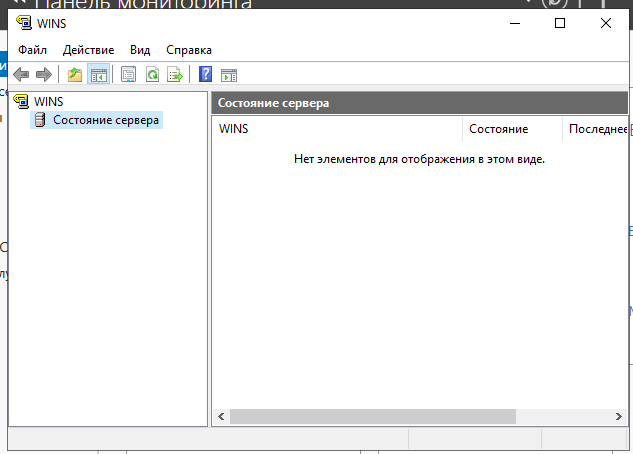
Используя команду ipconfig /release освободим выданный нам ip адрес



С помощью ipconfig /renew выдадим новый



1. Конфигурирование и использование сервера WINS

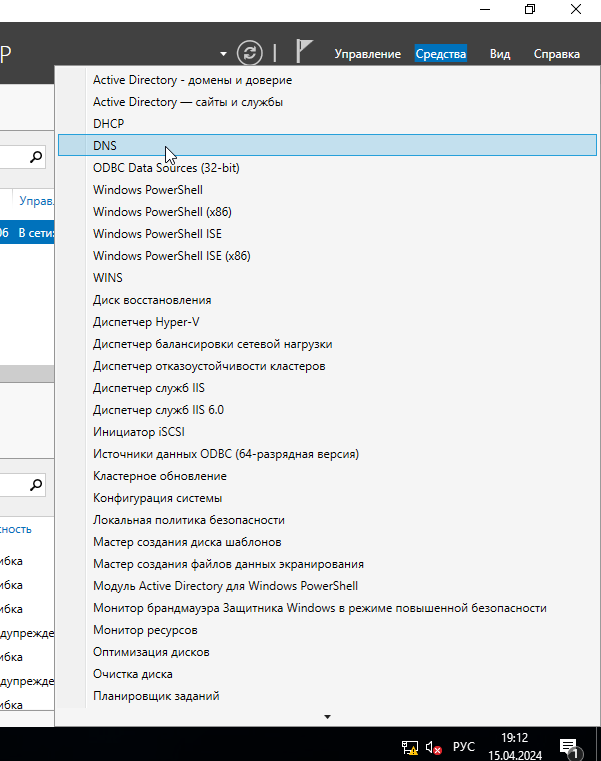


В ОС windows server 2019 функционал wins был объединён с DNS

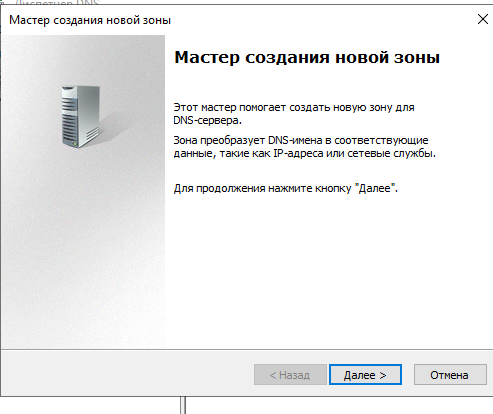
1. Конфигурирование и использование DNS и WINS

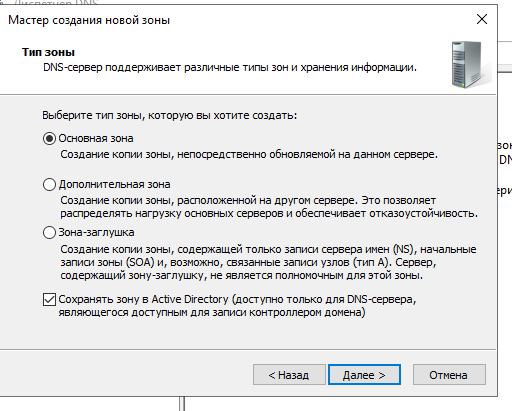
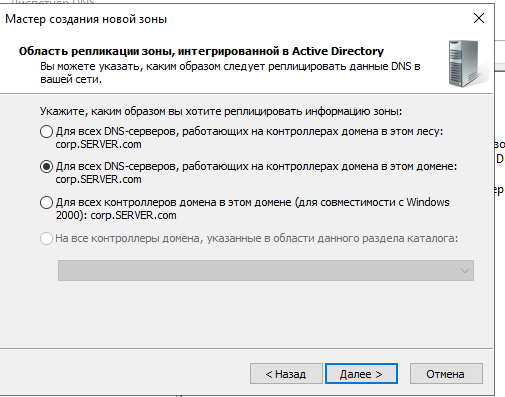
Настройка DNS-сервера в Microsoft Windows Server 2019 может быть выполнена с использованием инструмента управления DNS (DNS Manager) в составе роли службы доменных контроллеров (Domain Controller Role). Вот пошаговое руководство для настройки DNS-сервера в Windows Server 2019:

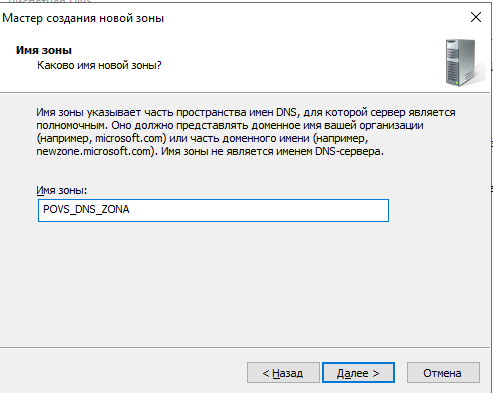
* 1. Установка роли службы доменных контроллеров (Domain Controller Role):
     1. Запустите "Server Manager" на сервере с установленной Windows Server 2019.
     2. Нажмите на "Manage" в верхнем правом углу и выберите "Add Roles and Features".
     3. Пройдите мастер установки, выбрав роль "Active Directory Domain Services" и добавив требуемые дополнительные компоненты, включая DNS-сервер.
     4. Завершите установку, следуя инструкциям мастера.
     5. Запуск инструмента управления DNS (DNS Manager):
     6. После завершения установки роли перейдите к "Server Manager".
     7. Нажмите на "Tools" в правом верхнем углу и выберите "DNS" для запуска DNS Manager.
  2. Настройка зон DNS:
     1. В DNS Manager откройте раздел "Forward Lookup Zones".
     2. Щелкните правой кнопкой мыши на папке "Forward Lookup Zones" и выберите "New Zone".
     3. Следуйте мастеру создания новой зоны, выбрав тип зоны (Primary, Secondary или Stub), затем укажите имя зоны и другие параметры по вашему усмотрению.
     4. Повторите этот процесс для создания обратных зон, если это необходимо.
  3. Добавление записей ресурсов (Resource Records):
     1. В созданных зонах выберите "New Host (A or AAAA)" для добавления записи A (для IPv4-адресов) или AAAA (для IPv6-адресов).
     2. Введите имя хоста и соответствующий IP-адрес.
     3. Для других типов записей ресурсов выберите соответствующий тип записи из контекстного меню.
  4. Настройка обратных зон:
     1. В обратных зонах выберите "New Pointer (PTR)" для создания обратной записи (PTR).
     2. Введите последний октет IP-адреса и соответствующее имя хоста.
  5. Проверка и тестирование:
     1. После завершения настройки DNS протестируйте его, выполнив различные запросы к серверу DNS и убедившись, что он корректно разрешает имена хостов.
     2. Убедитесь, что клиенты могут успешно регистрироваться и обращаться к серверу DNS для разрешения имен.

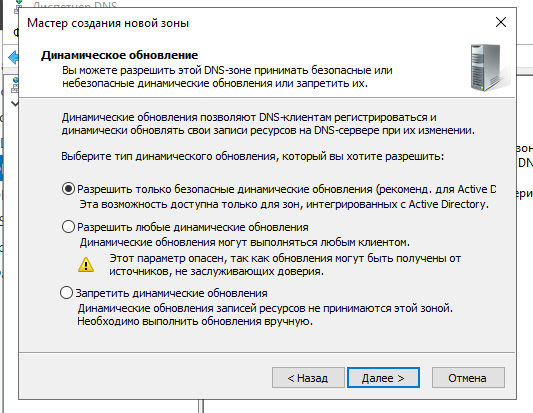
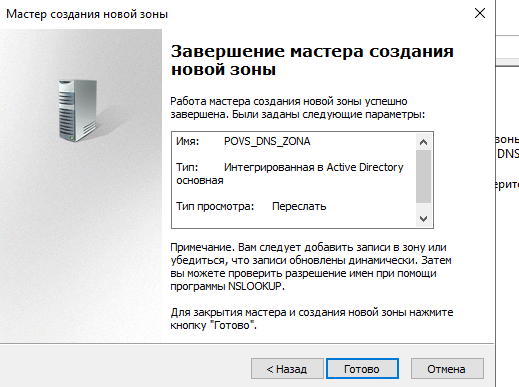


Сначала создадим зону DNS



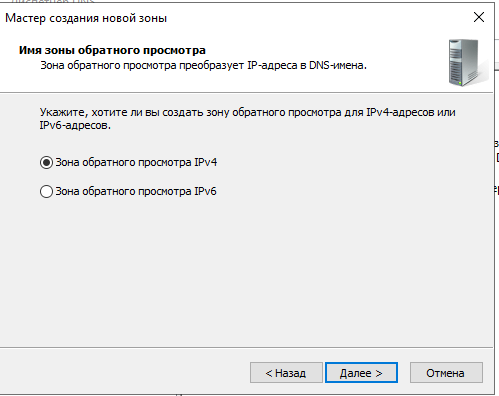
 

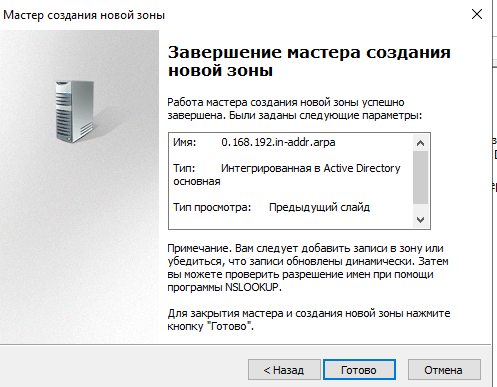


Зона создана

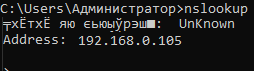
Так же создадим зону обратного просмотра



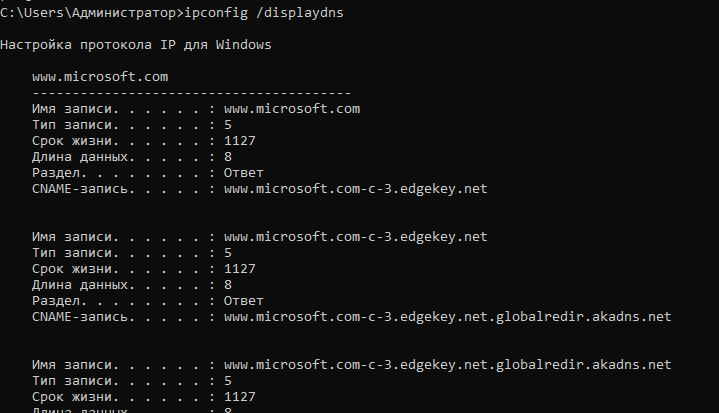


Команда nslookup — инструмент сетевого администрирования для запросов в доменной системе имен (DNS) с целью получения доменного имени, IP-адреса или другой информации из записей DNS.

Проверка работоспособности DNS с помощью nslookup

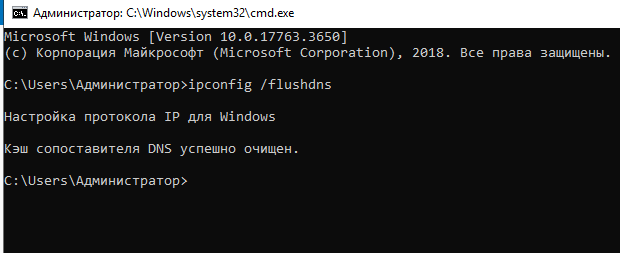


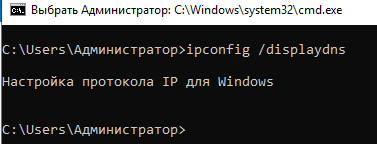
Отобразим DNS соединения с помощью ipconfig



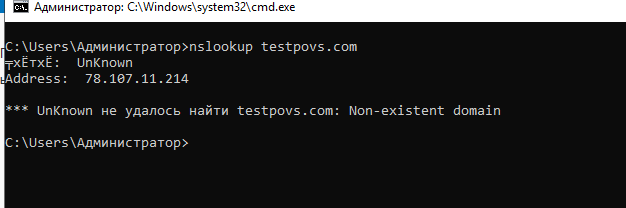
Манипулируя кэшем DNS-клиента, показать его влияние на результат разрешения имени

Очистим кэш DNS



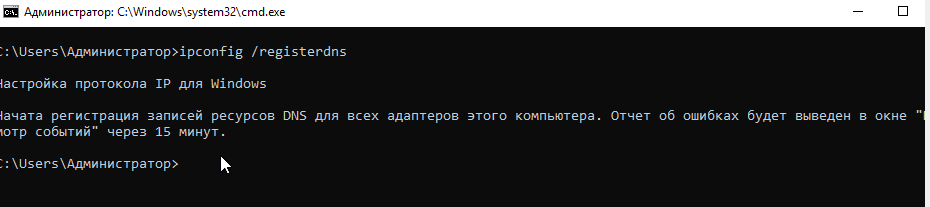


Как мы видим, кэш DNS пуст

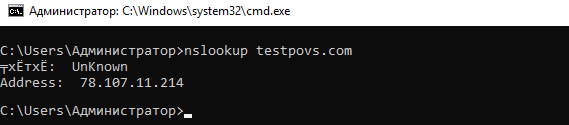


После чистки кэша DNS нет доступа к testpovs.com

Восстановим имена DNS



Попробуем снова



Доступ появился.

Вывод:

В ходе выполнения лабораторной работы были изучены процесс установки Windows Server 2019, варианты настройки сетевых компонентов, работа с DHCP и DNS сервером, изучен состав и свойства сетевых служб windows server, получены базовые навыки администрирования сетевой среды.