**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ**

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ«ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ № 50 ИМЕНИ ДВАЖДЫ ГЕРОЯ СОЦИАЛИСТИЧЕСКОГО ТРУДА Н.А. ЗЛОБИНА»

(ГБПОУ ПК № 50 ИМЕНИ ДВАЖДЫ ГЕРОЯ

СОЦИАЛИСТИЧЕСКОГО ТРУДА Н.А. ЗЛОБИНА)

**КУРСОВОЙ ПРОЕКТ**

на тему

«Обеспечение удалённого доступа к ОС Windows Server 2016 с помощью средств RDP.»

Выполнена студентом Антоновым Иваном Геннадиевичем

(группы) ОКС-302

по специальности 09.02.02 Компьютерные сети

Форма обучения очная

Курсовой проект

допускается к защите с оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Руководитель Котляревская А. В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись, дата)

Москва 2020

**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ**

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ«ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ № 50 ИМЕНИ ДВАЖДЫ ГЕРОЯ СОЦИАЛИСТИЧЕСКОГО ТРУДА Н.А. ЗЛОБИНА»

(ГБПОУ ПК № 50 ИМЕНИ ДВАЖДЫ ГЕРОЯ

СОЦИАЛИСТИЧЕСКОГО ТРУДА Н.А. ЗЛОБИНА)

РАССМОТРЕНО и СОГЛАСОВАНО

на заседании ПЦК

Протокол от «\_\_\_» \_\_\_\_\_\_\_20\_\_г. № \_\_\_\_

Председатель ПЦК

Федотова Н.П. ( )

**Задание**

**на курсовой проект**

Тема: Обеспечение удалённого доступа к ОС Windows Server 2016 с помощью средств RDP.

По ПМ 02 МДК 02.02. Организация администрирования компьютерных систем

Выполнил студент: Антонов Иван Геннадиевич

(Ф.И.О. полностью)

Курса 3 группы ОКС-302

Специальности 09.02.02 Компьютерные сети

(шифр и наименование специальности)

Срок сдачи студентом курсового проекта «\_\_» \_\_\_\_\_\_ 2020 г.

Перечень подлежащих разработке вопросов:

ВВЕДЕНИЕ

ОСНОВНАЯ ЧАСТЬ

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

|  |  |
| --- | --- |
| Дата выдачи проекта  «\_\_» \_\_\_\_\_\_ 2020 г.  Подпись студента\_\_\_\_\_\_\_\_\_ | Руководитель курсовой проекта  Котляревская А. В. (                        ) |

**СОДЕРЖАНИЕ**

Введение 4

**ВВЕДЕНИЕ**

Я устроился на работу в новый магазин X, где мне потребовалось настроить роли DNS, AD DS и DHCP на их сервере с операционной системой Windows Server 2016. В связи с ситуацией, было принято решение работать удаленно. Для этой цели мне потребовалось настроить на удаленной машине протокол удаленного доступа RDP.

Цель: Обеспечение удаленного доступа к ОС Windows Server 2016 с помощью средств RDP.

Для выполнения цели поставлены следующие задачи:

* Настроить протокол удаленного доступа (RDP);
* Настроить роль AD DS:
  + Создать новый лес;
  + Создать новый домен;
  + Ввести сервер в домен и сделать его контроллером домена.
* Настроить роль DNS:
  + Настроить зоны прямого и обратного просмотра.
* Настроить роль DHCP:
  + Настроить пул выдаваемых адресов;
  + Настроить пул зарезервированных адресов.

Актуальность данной темы заключается в том, что удаленный доступ обеспечивает гибкость в работе с ОС Windows Server. Это позволяет нам настраивать удаленную машину, даже если она у нас не под рукой.

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 Операционная система

Операционная система, сокр. ОС (англ. operating system, OS) — комплекс взаимосвязанных программ, предназначенных для управления ресурсами компьютера и организации взаимодействия с пользователем.

Давайте сравним две популярные серверные ОС:

* Windows Server 2016;
* Linux Ubuntu Server.

1.1.1 Windows Server 2016

Windows Server 2016 (кодовое имя Windows Server vNext) — серверная операционная система от Microsoft. Система является частью семейства Windows NT и разрабатывается одновременно с Windows 10.

Преимущества Windows Server 2016:

* Механизм обновления ОС хостов кластера без его остановки (Cluster Operating System Rolling Upgrade) — это происходит через создание смешанного кластера Windows Server 2012 R2 и Windows Server vNext;
* Синхронная репликация хранилищ на уровне блоков с поддержкой географически распределенных кластеров;
* Виртуальный сетевой контроллер (software-defined networking stack) для одновременного управления физическими и виртуальными сетями;
* Новый формат файлов конфигурации виртуальных машин (.VMCX и .VMRS), с более высокой степенью защиты от сбоев на уровне хранилища. Также можно будет обновлять версии конфигурационных файлов;
* Можно создавать снимки состояния системы прямо из гостевой ОС;
* Полноценный Storage Quality of Service (QoS) — возможность динамического отслеживания производительности хранилищ и горячая миграция виртуальных машин при превышении этими хранилищами пороговых значений (IOPS);
* Изменения в самом Hyper-V: использование альтернативных аккаунтов (хранение нескольких учётных данных одного человека, возможность использования по времени), возможность управления предыдущими версиями Hyper-V в корпоративной инфраструктуре, обновление и улучшение протокола удалённого управления, возможность безопасной загрузки гостевых операционных систем Linux;
* Возможность обновления Integration Services через Windows Update;
* «Горячее» добавление сетевых карт и оперативной памяти;
* Поддержка OpenGL и OpenCL для Remote Desktop;
* Возможности публикации приложений;
* Совместимость с режимом Connected Standby. • Windows Defender: Windows Server Antimalware теперь установлена и включена по умолчанию без графического интерфейса • IIS 10: Добавлена поддержка протокола HTTP/2 • Windows PowerShell 5.0 • Убран Telnet сервер.

1.1.2 Ubuntu Server LTS

Ubuntu Server LTS — это серверная операционная система на базе ядра Linux. Ubuntu более известна, как отличный дистрибутив для знакомства с linux и установки его на рабочий компьютер или ноутбук.

Приставка к названию LTS означает Long Term Support — расширенное время поддержки. Это значит, что к LTS релизу будут выходить обновления безопасности значительно дольше, чем к обычным версиям.

Основной упор в Ubuntu делался на удобство и простоту использования, чтобы каждый желающий без проблем мог познакомиться с операционной системой на базе Linux и начать ее использовать в повседневной жизни.

Ubuntu Server какой-то особенной простотой и удобством, по сравнению с другими серверными дистрибутивами не обладает, так что особенности desktop версии, где упор идет на удобное графическое окружение, не применимы к серверному варианту. Серверная система обладает другими отличительными признаками, которые я перечислю ниже:

* Минималистичный консольный установщик системы на сервер;
* Периодические новости в консоли;
* По умолчанию Ubuntu Server подключает во время установки swap в виде отдельного файла (его можно отключить, изменить размер и т. д.) (Рисунок 1);
* в Ubuntu одно из самых свежих ядер среди серверных операционных систем (все новинки приходят быстрее на Ubuntu Server).

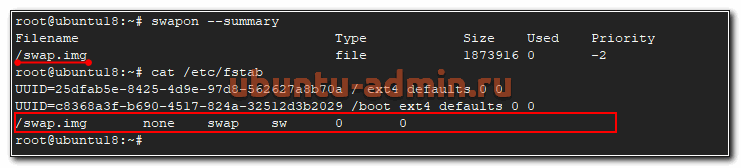


Рисунок 1 – swap файл во время установки

1.1.3 Вывод

Я выбираю ОС Windows Server 2016, потому что в ней есть Active Directory Domain Controller и встроенные средства ля работы по протоколу RDP.

1.2 Протоколы удаленного доступа

С появлением и распространением компьютерных сетей появляется насущная необходимость управления компьютером с удаленного терминала. С помощью программ удаленного управления администратор может решать, например, такие задачи, как запуск программ на удаленном хосте, добавление/удаление пользователей, осуществлять какие-либо настройки системы и другие подобные задачи. То есть, программы удаленного управления в идеале позволяют администратору делать с софтом компьютера, который может находится от него на значительном расстоянии, все то, что он мог бы сделать в непосредственной близости от этого компьютера.

1.2.1 Протокол RDP

Как известно, протокол удаленного рабочего стола (Remote Desktop Protocol или RDP) позволяет удаленно подключаться к компьютерам под управлением Windows и доступен любому пользователю Windows, если у него не версия Home, где есть только клиент RDP, но не хост. Это удобное, эффективное и практичное средство для удаленного доступа для целей администрирования или повседневной работы. Поддержка RDP включена в ОС Windows, начиная еще с NT 4.0 и XP, однако далеко не все знают, как ею пользоваться. Между тем можно открывать удаленный рабочий стол Microsoft с компьютеров под Windows, Mac OS X, а также с мобильных устройств с ОС Android или с iPhone и iPad.

Если должным образом разбираться в настройках, то RDP будет хорошим средством удаленного доступа. Он дает возможность не только видеть удаленный рабочий стол, но и пользоваться ресурсами удаленного компьютера, подключать к нему локальные диски или периферийные устройства. При этом компьютер должен иметь внешний IP, (статический или динамический), или должна быть возможность «пробросить» порт с маршрутизатора с внешним IP-адресом.

Серверы RDP нередко применяют для совместной работы в системе 1С, или на них разворачивают рабочие места пользователей, позволяя им подключаться к своему рабочему месту удаленно. Клиент RDP позволяет дает возможность работать с текстовыми и графическими приложениями, удаленно получать какие-то данные с домашнего ПК. Для этого на роутере нужно пробросить порт 3389, чтобы через NAT получить доступ к домашней сети. Тоже относится к настройке RDP-сервера в организации.

RDP многие считают небезопасным способом удаленного доступа по сравнению с использованием специальных программ, таких как RAdmin, TeamViewer, VNC и пр. Другой предрассудок – большой трафик RDP. Однако на сегодня RDP не менее безопасен, чем любое другое решение для удаленного доступа, а с помощью настроек можно добиться высокой скорости реакции и небольшой потребности в полосе пропускания.

1.2.2 Вывод

Протокол RDP отлично нам подходит, потому что в ОС Windows Server есть встроенные средства для обеспечения удаленного доступа по протоколу RDP.

1.3 Active Directory Domain Controller

Доменные службы Active Directory (AD DS) —­ это реализация службы каталогов Microsoft, которая предоставляет централизованные службы проверки подлинности и авторизации. AD DS в Windows Server предоставляет мощную службу каталогов для централизованного хранения и управления безопасностью, например пользователями, группами и компьютерами, а также обеспечивает централизованный и безопасный доступ к сетевым ресурсам. Active Directory Domain Services используется для организации локальных вычислительных сетей.

Представление решения состоялось в 1999 году, впервые продукт был выпущен вместе с Windows 2000 Server, а затем развит в рамках выпуска Windows Server 2003. Впоследствии новые версии продукта вошли в Windows Server 2003 R2, Windows Server 2008 и Windows Server 2008 R2 и переименован в Active Directory Domain Services. Ранее служба каталогов называлась NT Directory Service (NTDS), это название до сих пор можно встретить в некоторых исполняемых файлах.

В отличие от версий Windows до Windows 2000, которые использовали в основном протокол NetBIOS для сетевого взаимодействия, служба Active Directory интегрирована с DNS и работает только поверх TCP/IP. Для аутентификации по умолчанию используется протокол Kerberos. Если клиент или приложение не поддерживает Kerberos-аутентификацию, используется протокол NTLM.

1.4 DNS

DNS — Domain Name System (доменная система имён) - отвечает за преобразование имени сайта в IP-адрес веб-сервера, на котором он находится. Можно привести сравнение с телефонной книгой, в которой каждому имени соответствет телефонный номер.

Когда вы в браузере вводите адрес сайта (например, vk.com), браузер делает запрос DNS-серверу, который возвращает IP-адреса, принадлежащие этому имени (например, 87.240.190.67 или 87.240.190.72 для доменного имени vk.com). В дальнейшем с этим адресом и происходит обмен информацией, а для пользователя это выглядит как посещение сайта vk.com.

Основой DNS является представление об иерархической структуре имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

DNS обладает следующими характеристиками:

* Распределённость администрирования. Ответственность за разные части иерархической структуры несут разные люди или организации.
* Распределённость хранения информации. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его зону ответственности, и (возможно) адреса корневых DNS-серверов.
* Кэширование информации. Узел может хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
* Иерархическая структура, в которой все узлы объединены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или делегировать (передавать) их другим узлам.
* Резервирование. За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

1.5 DHCP

DHCP - протокол динамического конфигурирования хостов. DHCP позволяет сетевым устройствам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Протокол DHCP используется в большинстве сетей TCP/IP.

Можно включить сервер на роутере и тогда это будет сервер. Альтернативный вариант — установить DHCP и на компьютере, например настроить в Windows 10. Можно включать или отключать эти службы на одном из компьютеров сети — это будет уровень клиента или сетевого протокола.

Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи протокола UDP. По умолчанию запросы от клиента делаются на 67 порт к серверу, сервер в свою очередь отвечает на порт 68 к клиенту, выдавая адрес IP и другую необходимую информацию, такую, как сетевую маску, маршрутизатор и серверы DNS.

2 ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1 Исходные данные ПК

В нашем случае будет два ПК: первый, к которому мы подключаемся (далее сервер), также он будет контроллером нашего домена, и будет служить DHCP и DNS сервером (рис. 2); и второй (далее клиент), которым мы подключаемся (рис. 3).

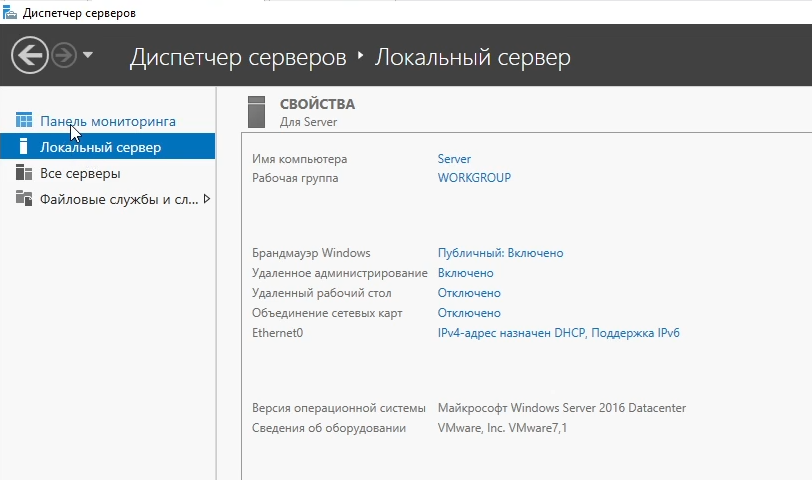


Рисунок – Данные сервера

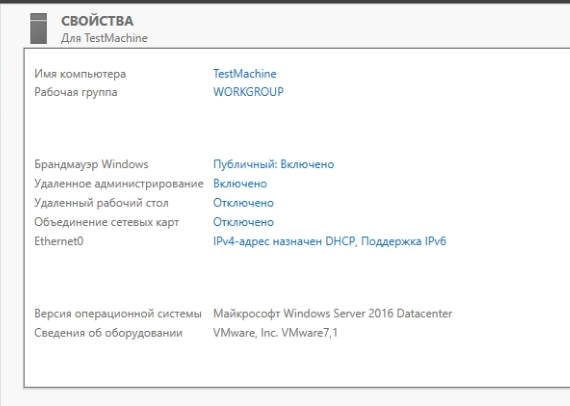


Рисунок – Данные клиента

2.2 Установка ролей на сервер

Приступим к установке ролей на сервер. Зайдем в диспетчер серверов и нажмем на “Добавить роли и компоненты”. Нам высветится окошко утилиты Мастер добавления ролей и компонентов (рис. 4).

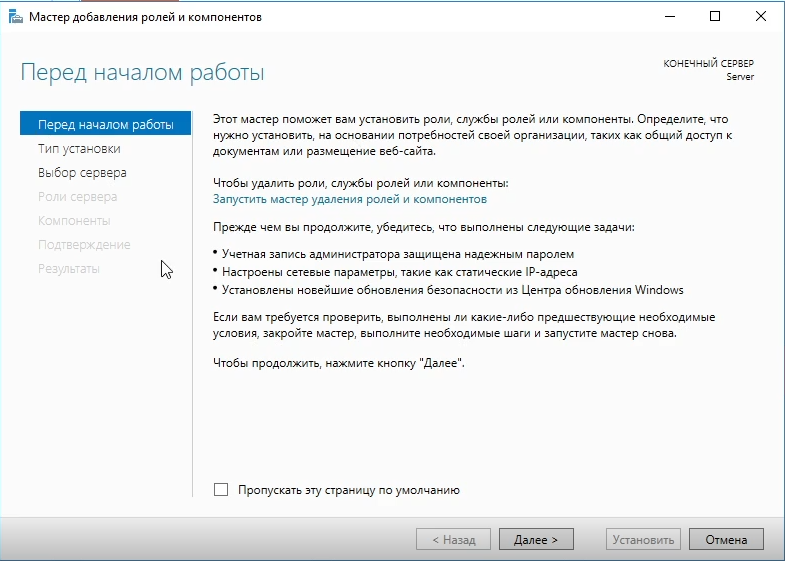


Рисунок – Мастер добавления ролей и компонентов

Далее выбираем наш сервер (рис.5).

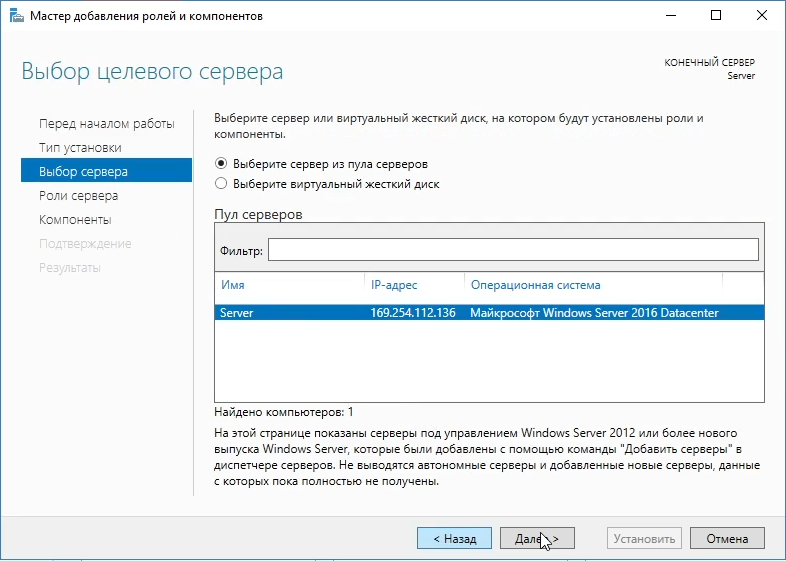


Рисунок – Выбор сервера

Далее выбираем DHCP-сервер (рис. 6), DNS-сервер (рис. 7), AD DC (рис. 8).

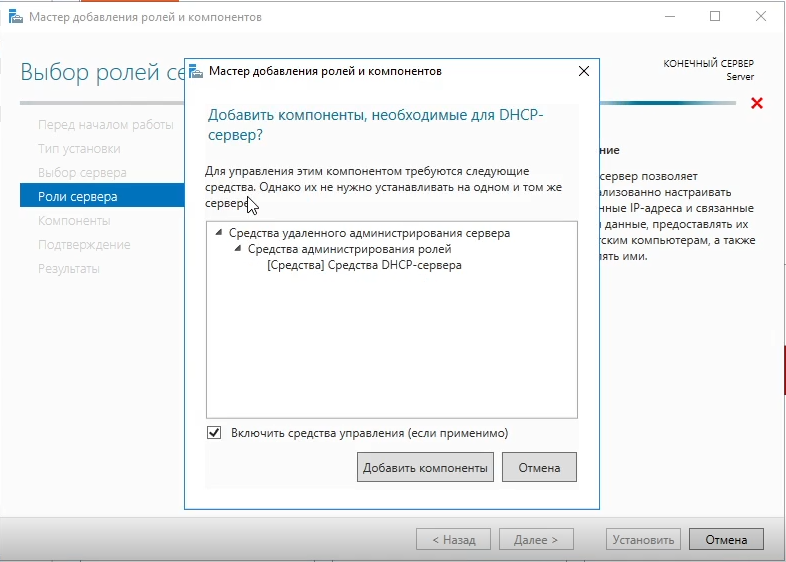


Рисунок – Добавление роли DHCP-сервера

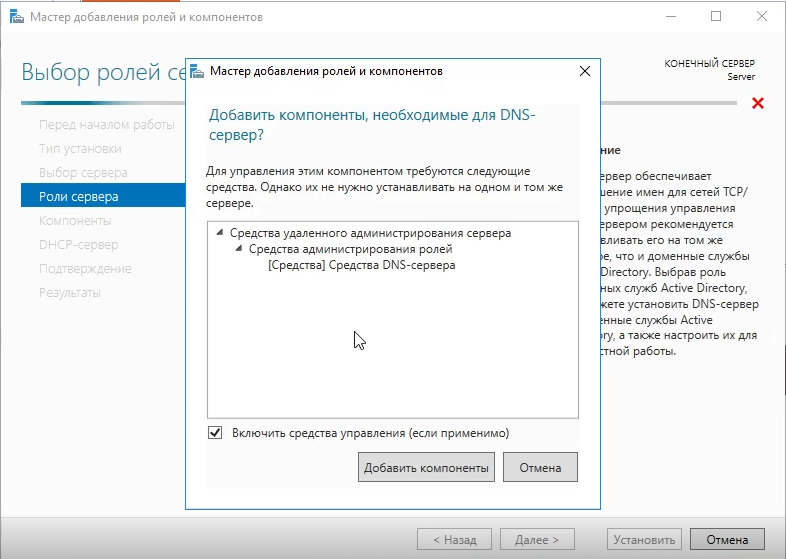


Рисунок –Добавление роли DNS-сервера

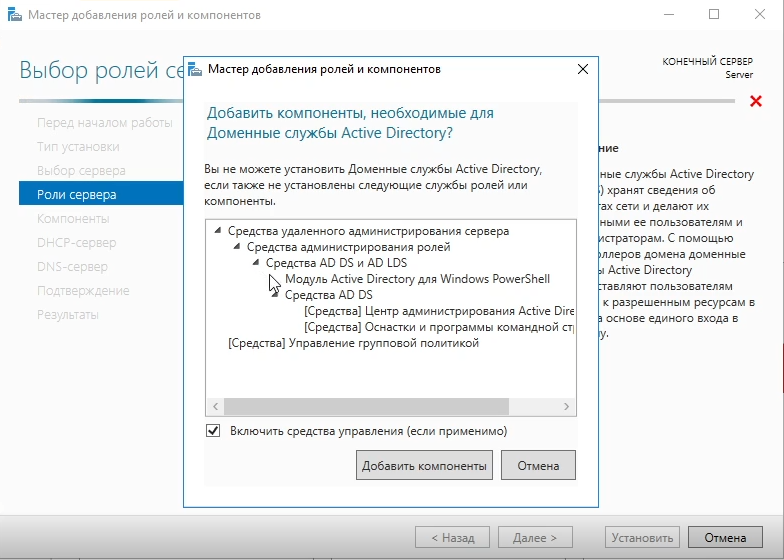


Рисунок – Добавление роли для доменных служб Active Directory

Далее мы должны отметить Службы удаленных рабочих столов (рис. 9).

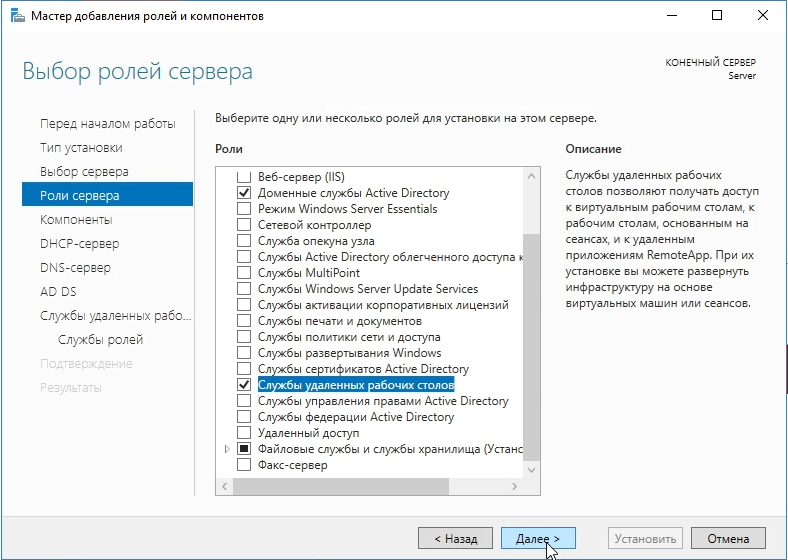


Рисунок – Выбор службы удаленных рабочих столов

Также в компонентах добавляем службу беспроводной локальной сети (рис. 10).

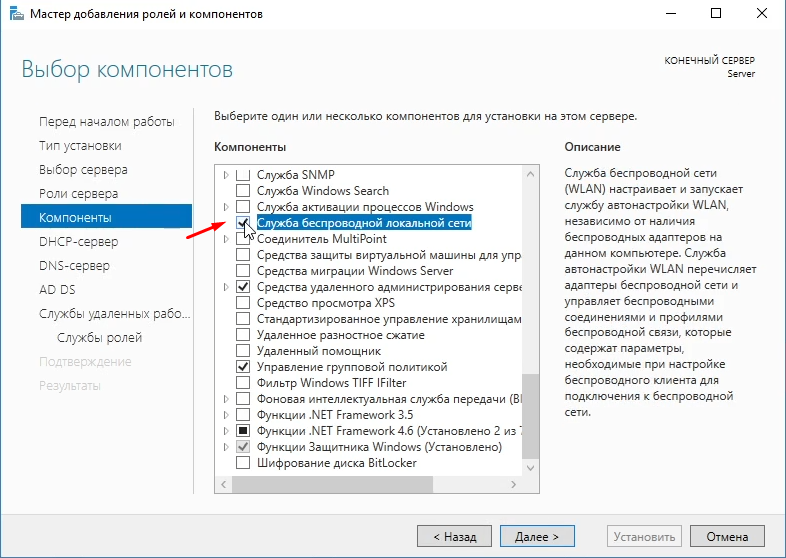


Рисунок – Выбор службы беспроводной локальной сети

В меню службы удаленных рабочих столов – службы ролей мы выбираем Лицензирование удаленных рабочих столов, узел сеансов удаленных рабочих столов и шлюз удаленных рабочих столов (рис. 11).

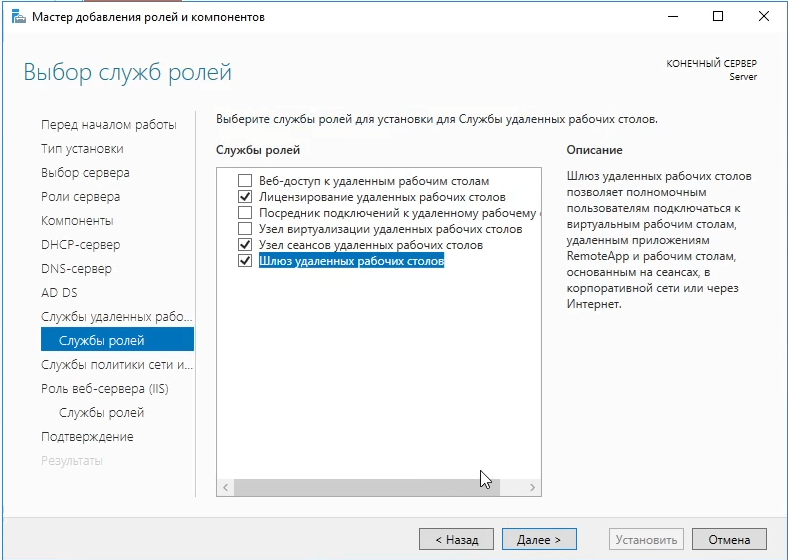


Рисунок – Выбор служб ролей

На рисунке 12 показано, что должно устанавливаться.

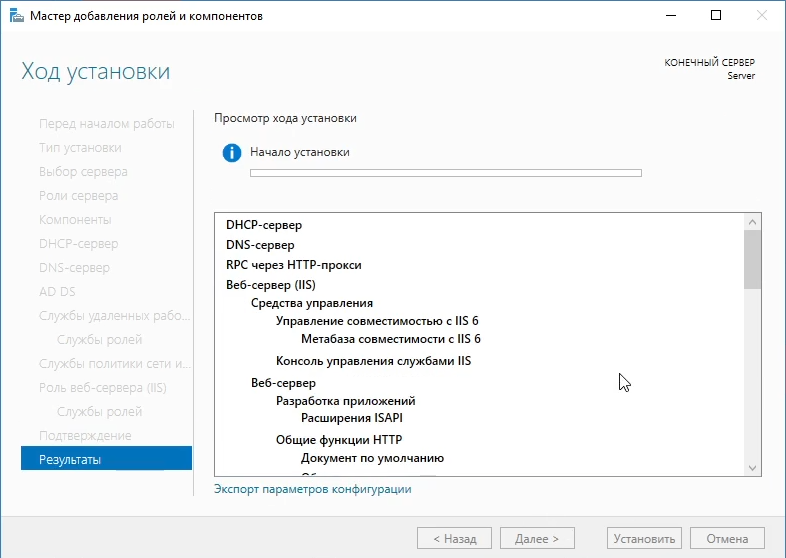


Рисунок – Процесс установки ролей

2.3 Настройка AD DC на сервер

В диспетчере серверов в разделе Задачи выбираем “Повысить роль этого сервера до уровня контроллера домена” (рис. 13), далее добавляем новый лес с корневым именем “local.ru” (рис. 14).

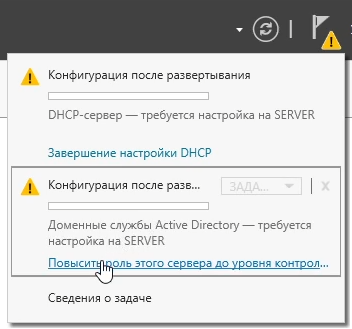


Рисунок – Выбор задачи настройки AD DC

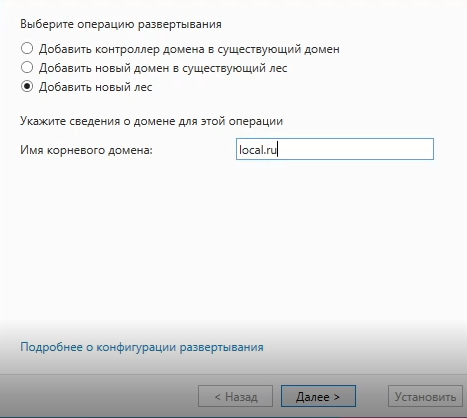


Рисунок – Выбор имени корневого домена

Вводим пароль для режима восстановления служб каталогов (рис. 15) и выбираем NetBIOS-имя домена (рис. 16).

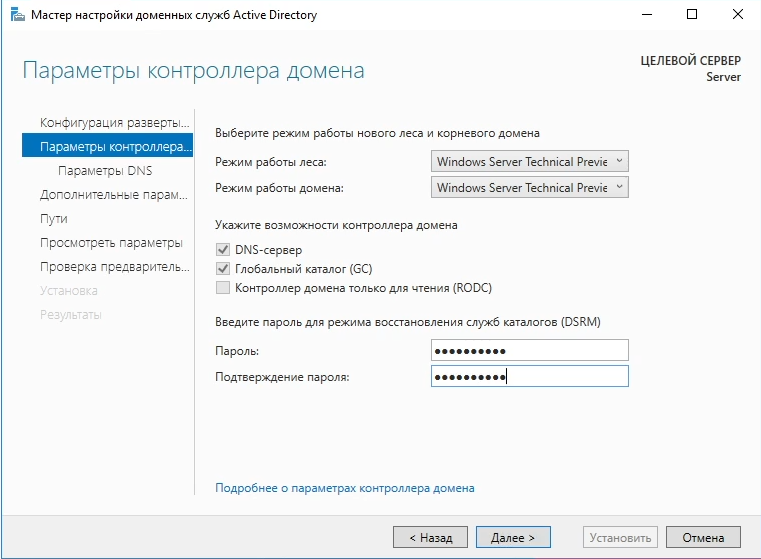


Рисунок – Ввод пароля для DSRM

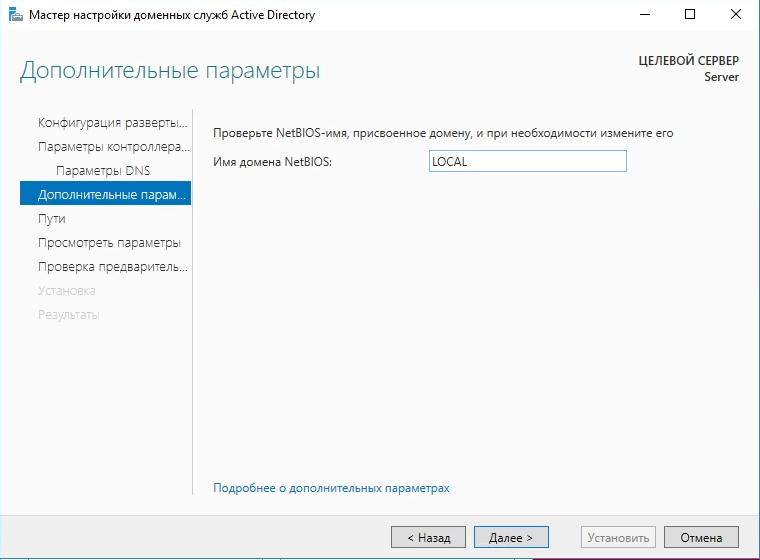


Рисунок – выбор NetBIOS-имени домена

На рисунке 17 изображены результаты проверки нашего выбора, на рисунке 18 показан процесс установки. Далее нашс уведомят о том, что нужно перезагрузиться (рис. 19), соглашаемся на это.

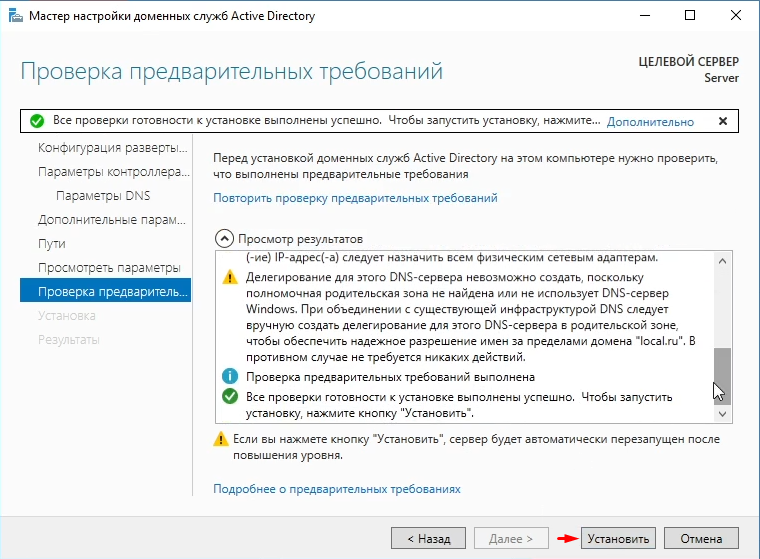


Рисунок – Проверка предварительных требований

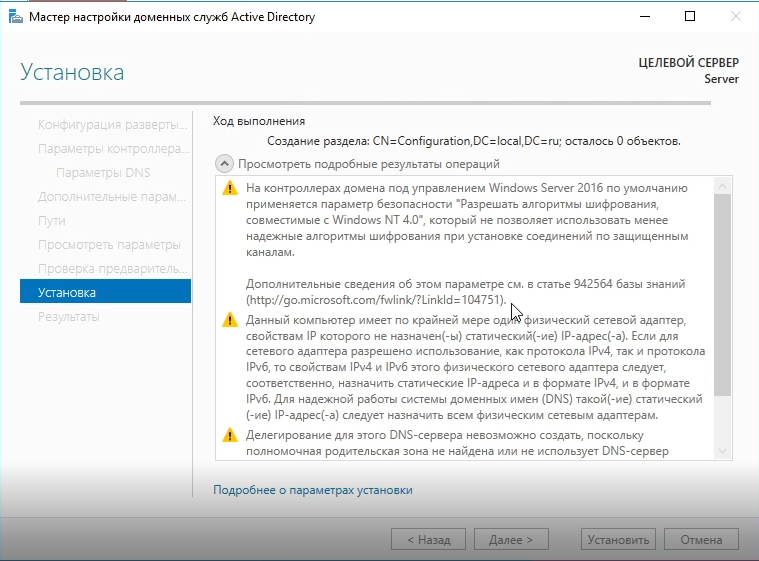


Рисунок – Процесс установки

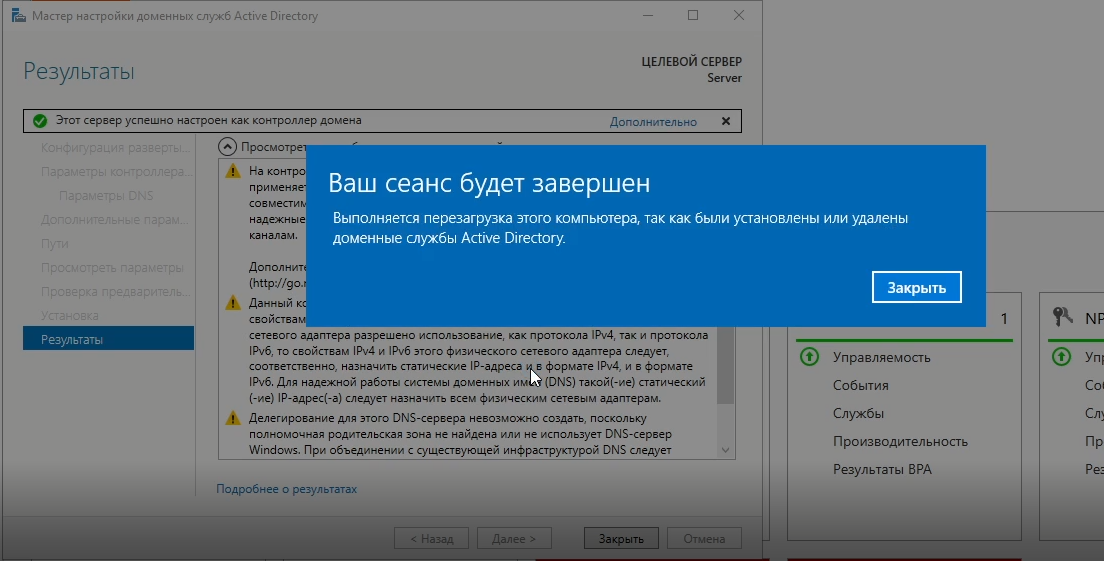


Рисунок – Предупреждение о перезагрузке