ЛАБОРАТОРНАЯ РАБОТА №1

«ACTIVE DIRECTORY»

1. Цель работы

Исследование возможностей, предоставляемых Windows Active Directory.

2. Постановка задачи

Необходимо установить и настроить работу службы AD, а также распределить роли пользователей. Задание для выполнения уточняется преподавателем в ходе проведения лабораторного занятия.

3. Ход работы

До установки ролей сервера требовалось задать имя будущему серверу и IP-адрес. На рисунках 1-3 представлен данный процесс.

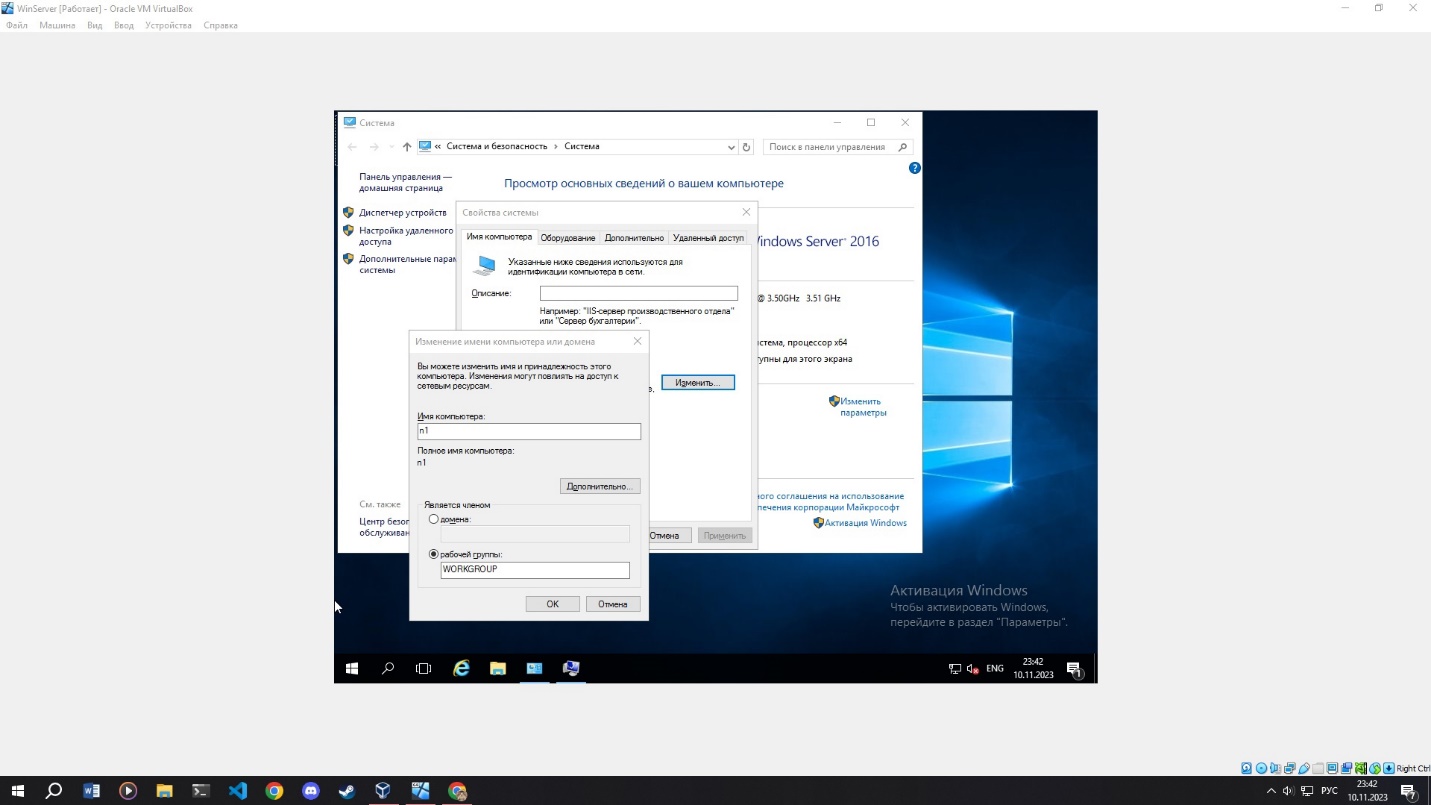


Рисунок 1 – Установка имени сервера

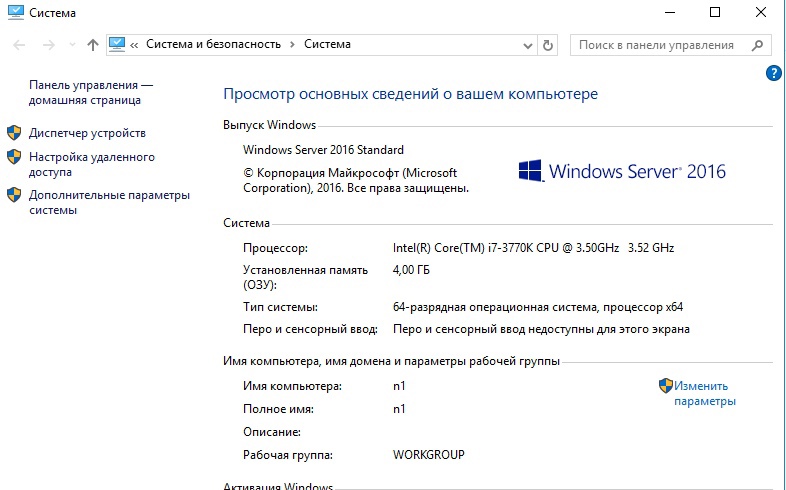


Рисунок 2 – Проверка поменянного имени сервера после перезагрузки

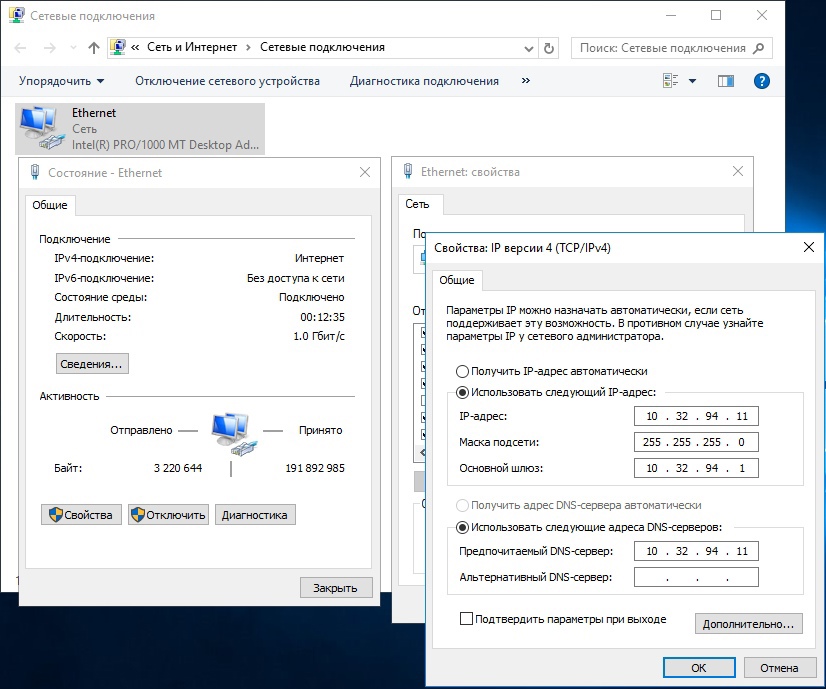


Рисунок 3 – Установка статического IP-адреса сервера

Далее требовалось произвести установку ролей сервера. Для этого необходимо было выбрать "Диспетчер серверов" (рисунок 4), затем следующем окне выбрать пункт "Добавить роли и компоненты" и выбрать наш сервер (рисунок 5).

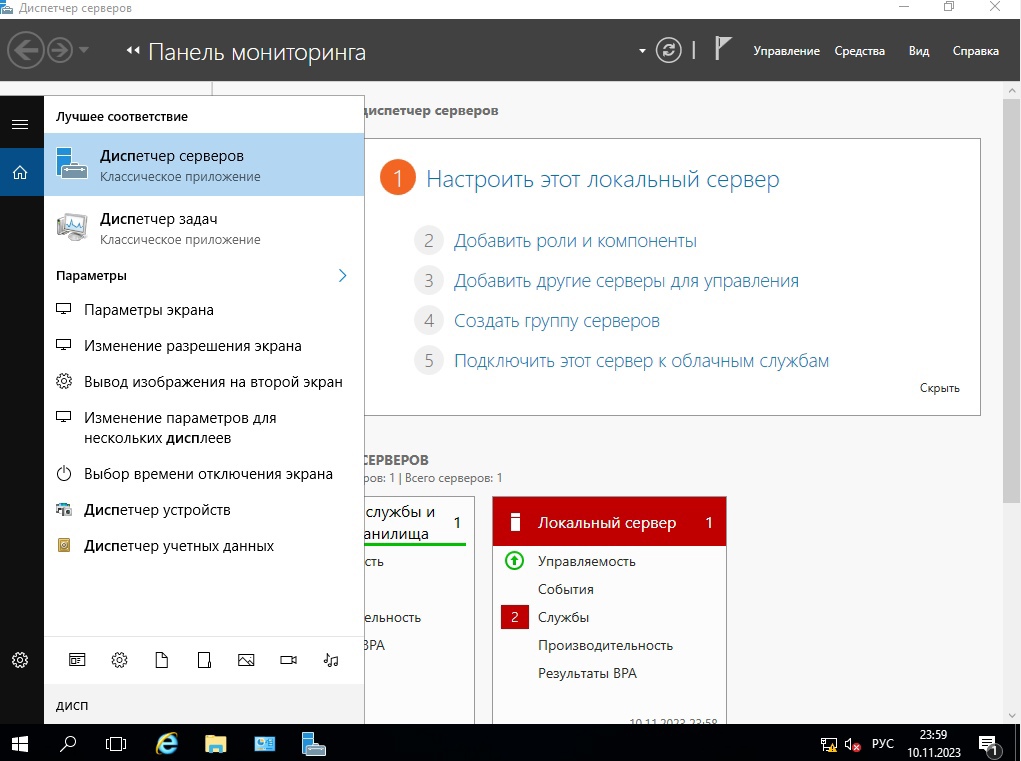


Рисунок 4 – Выбор «Диспетчер серверов»

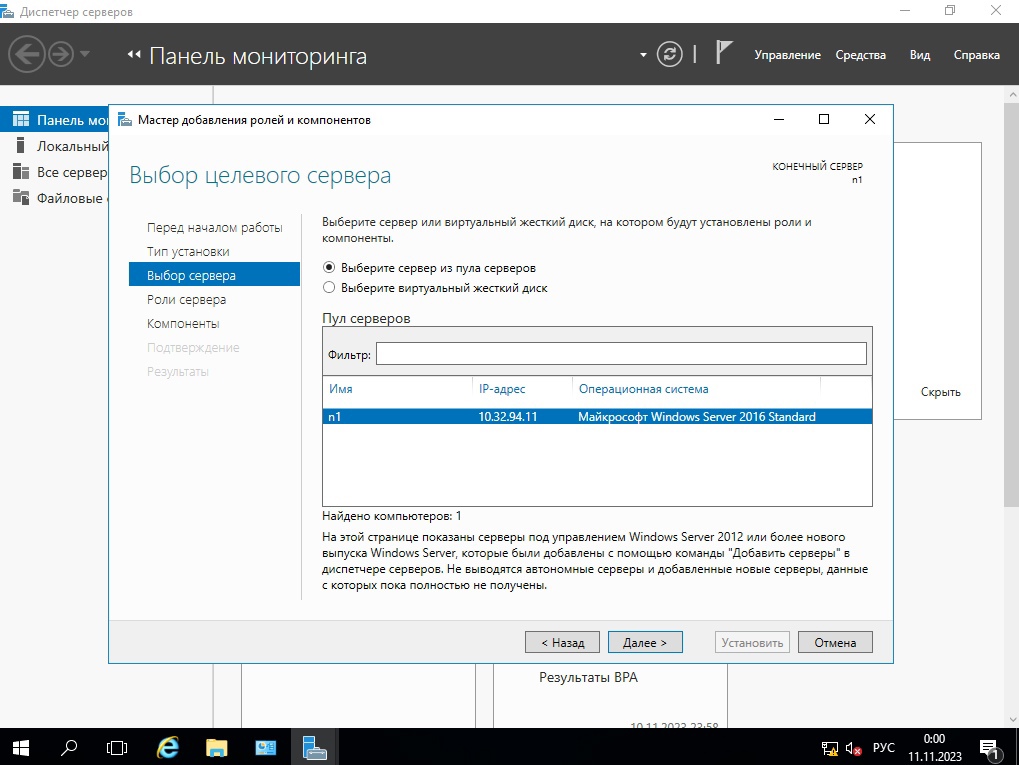


Рисунок 5 – Мастер добавление ролей и компонентов

Для выбора ролей сервера необходимо установить галочки напротив "DNS-сервера" и "Доменные службы Active Directory". При появлении запроса о добавлении компонентов – "Добавить компоненты". Результат процедуры изображен на рисунке 6.

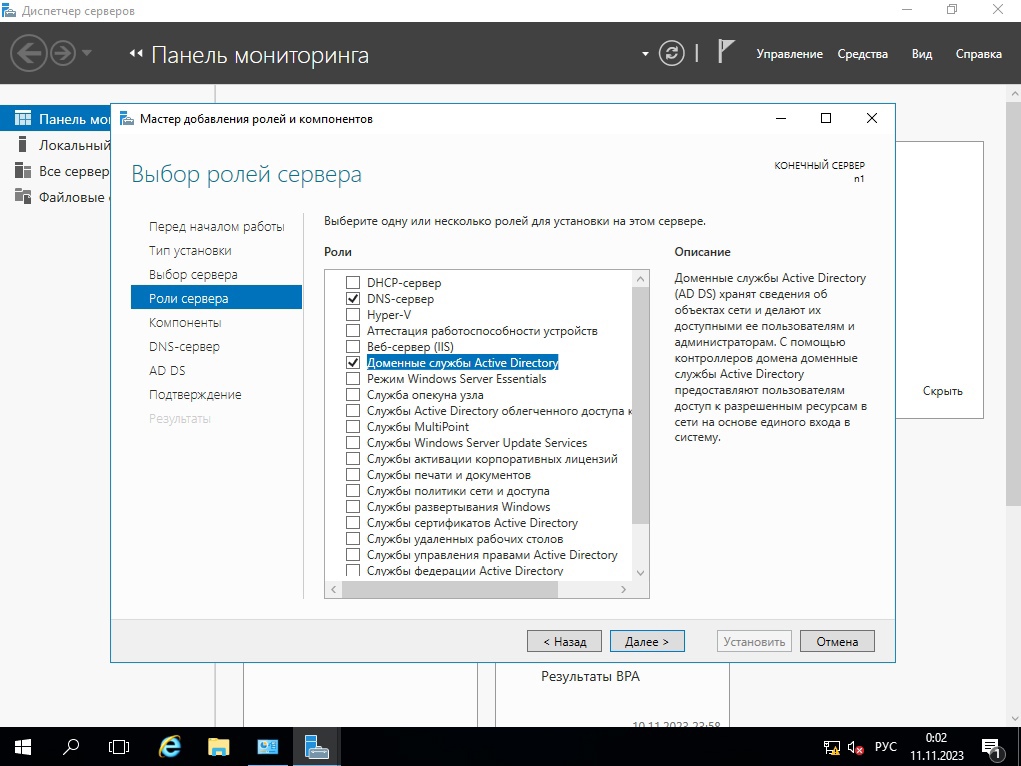


Рисунок 6 – Выбор ролей для сервера

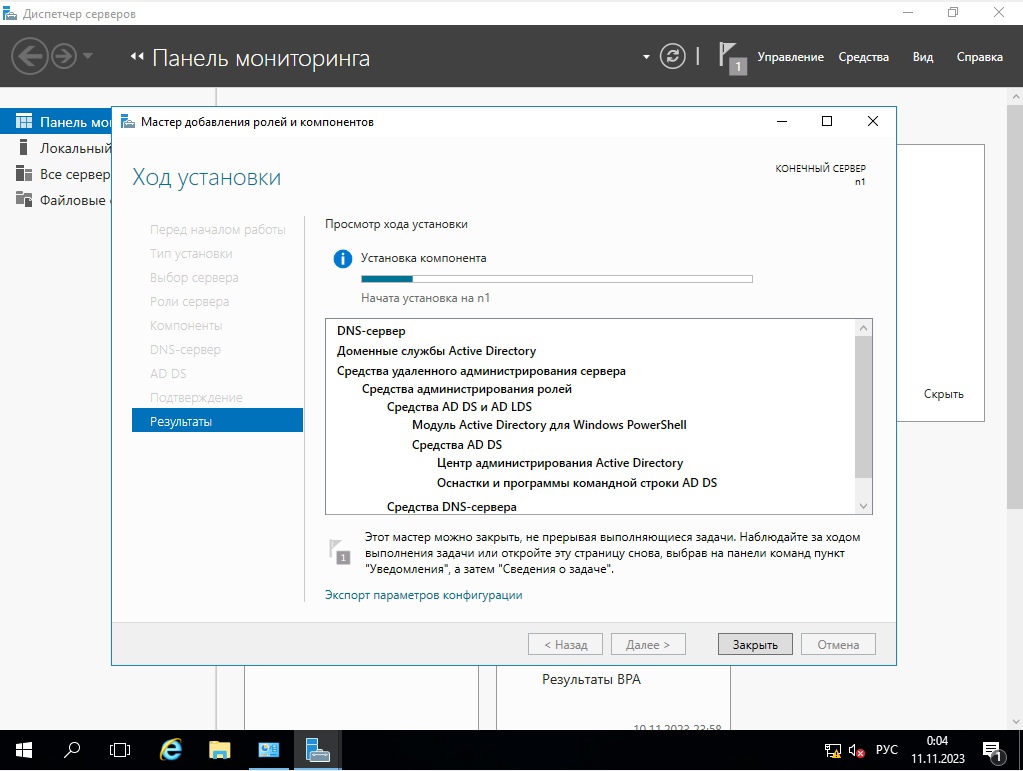


Рисунок 7 – Установка компонентов

После окончания установки выбранных ролей сервера необходимо было нажать на значок предупреждения в "Диспетчере серверов" и выбрать "Повысить роль этого сервера до уровня контроллера домена".

В следующем окне необходимо выбрать "Добавить новый лес". Имя корневого домена – уникальное имя вашего домена (рисунок 8).

Далее требовалось ввести пароль для режима восстановления служб каталогов (DSRM) (рисунок 9).

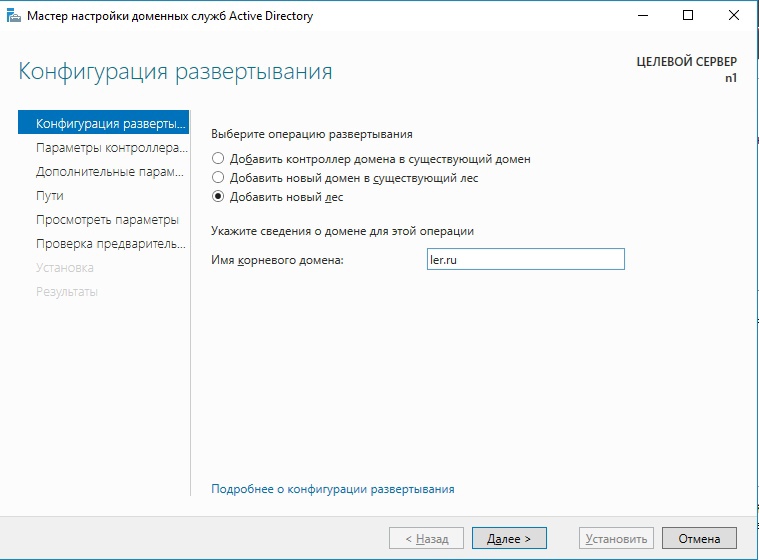


Рисунок 8 – Добавление нового леса и указание имени корневого домена

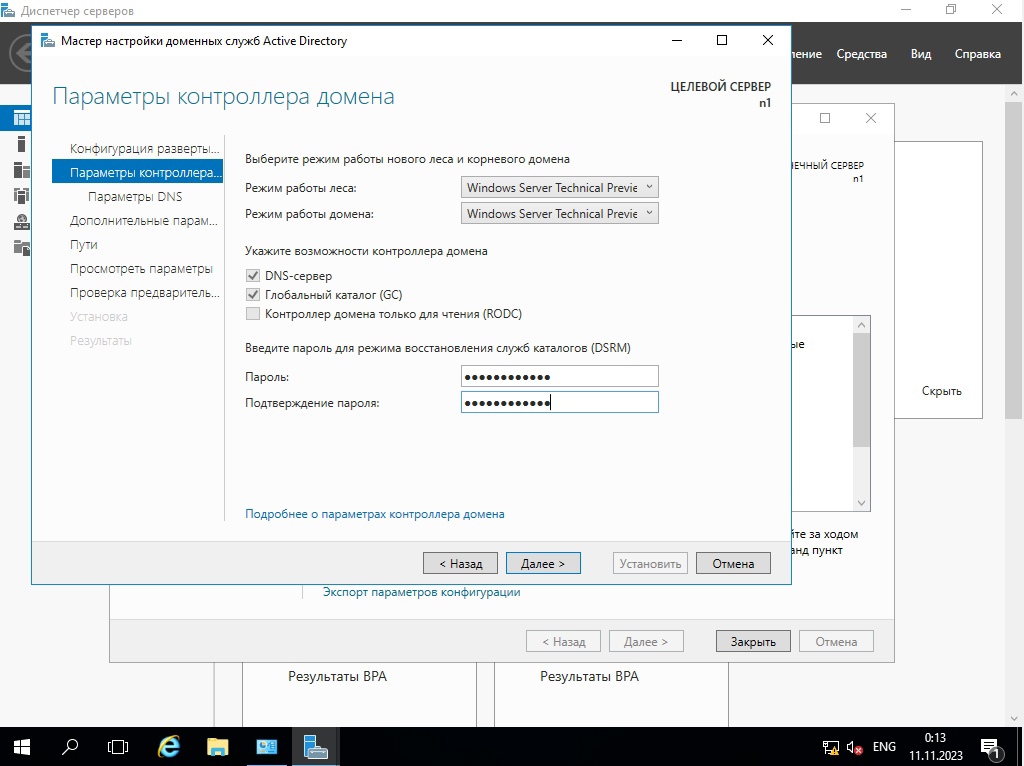


Рисунок 9 – Установление пароля

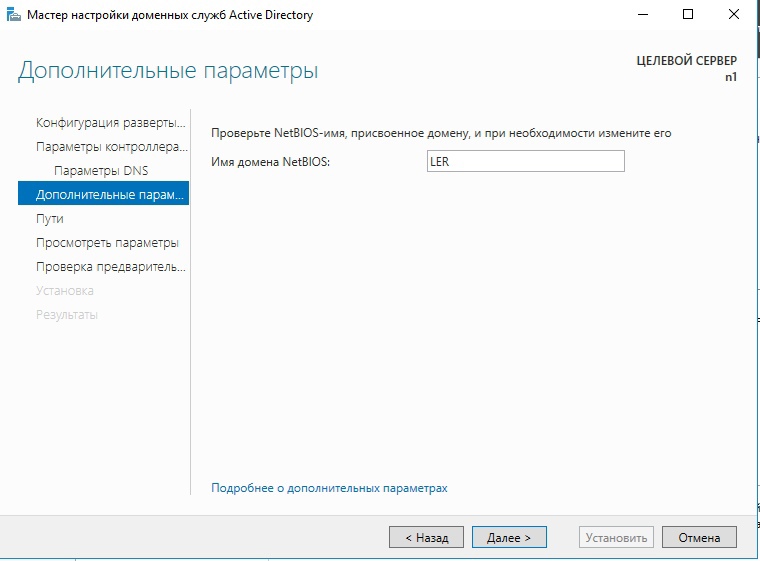


Рисунок 10 – Дополнительные параметры

В открывшемся окне необходимо было оставить по умолчанию расположение базы данных AD DS, файлов журналов и попок SYSVOL, а после нажать на "Далее" (рисунок 11).

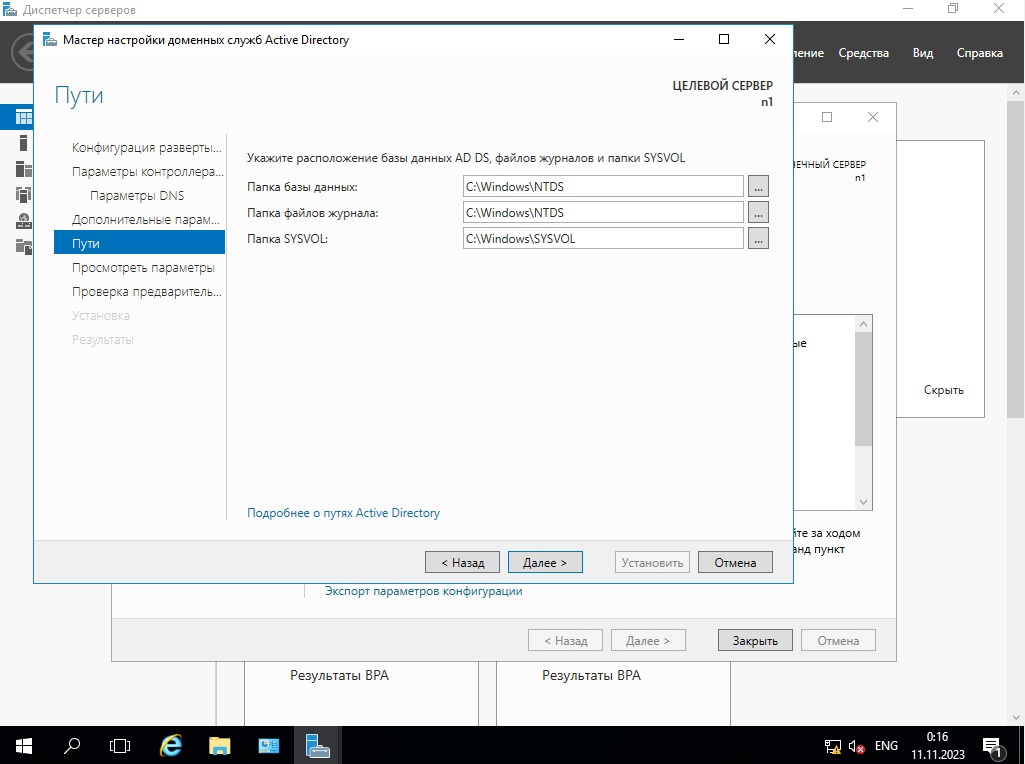


Рисунок 11 – Окно «Пути»

После настройки контроллера домена можно перейти к настройке обратной зоны DNS-сервера. Для этого в "Диспетчер серверов" требовалось выбрать "Средства", а далее "DNS".

В открывшемся окне необходимо выбрать созданный ранее сервер, затем "Зона обратного просмотра". Правой клавишей мыши - "Создать новую зону..." (рисунок 12).

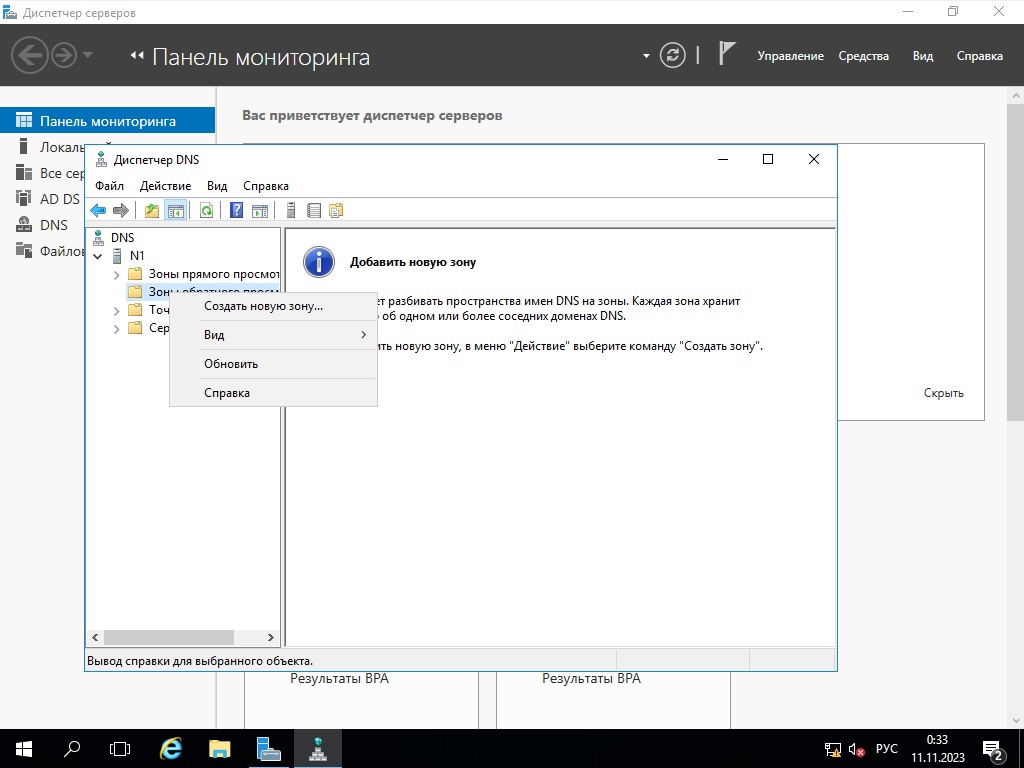


Рисунок 12 – Добавление новой зоны

Необходимо оставить по умолчанию чекбокс на пункте «Для всех DNS-серверов, работающих на контроллерах домена в этом домене» (рисунок 13).

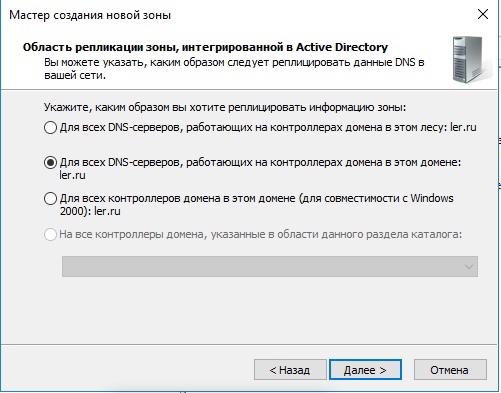


Рисунок 13 – Установка области репликации, интегрированной в Active Directory

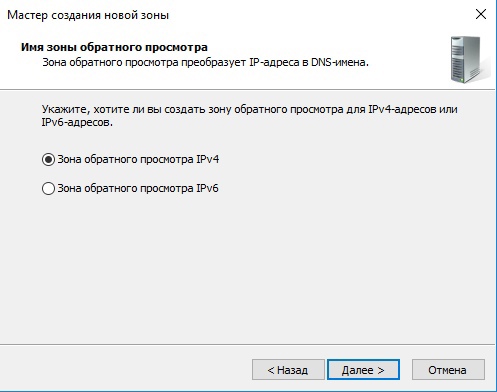


Рисунок 14 – Выбор зоны обратного просмотра

Далее для настройки зоны обратного просмотра требуется задать"Идентификатор сети", был задан следующий: 10.32.94 (рисунок 15).

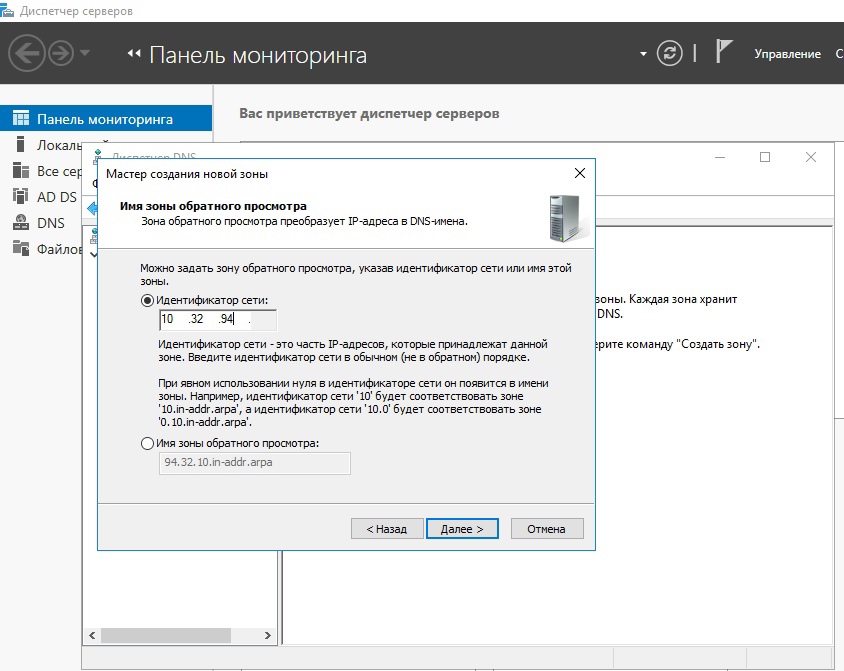


Рисунок 15 – Установка идентификатора сети и имени зоны

В следующем окне необходимо было оставить по умолчанию «Разрешить только безопасные динамические обновления» (рисунок 16).

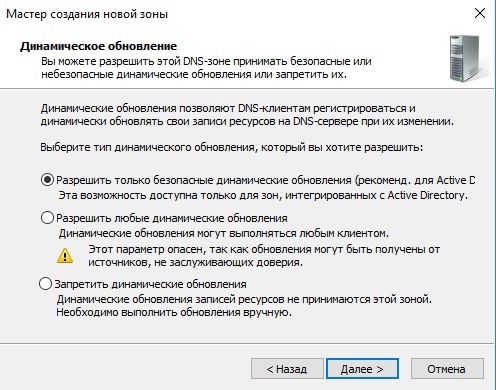


Рисунок 16 – Разрешение безопасных динамических обновлений

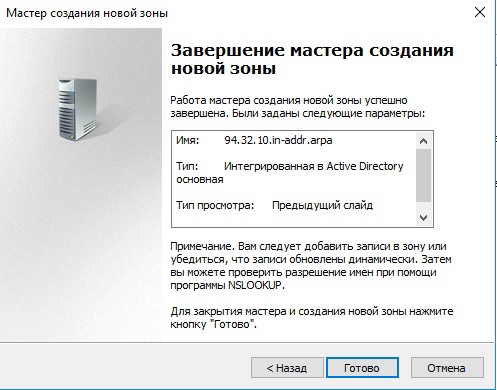


Рисунок 17 – Завершение мастера создания новой зоны

Далее было проверено появление зоны обратного просмотра для домена (рисунок 18).

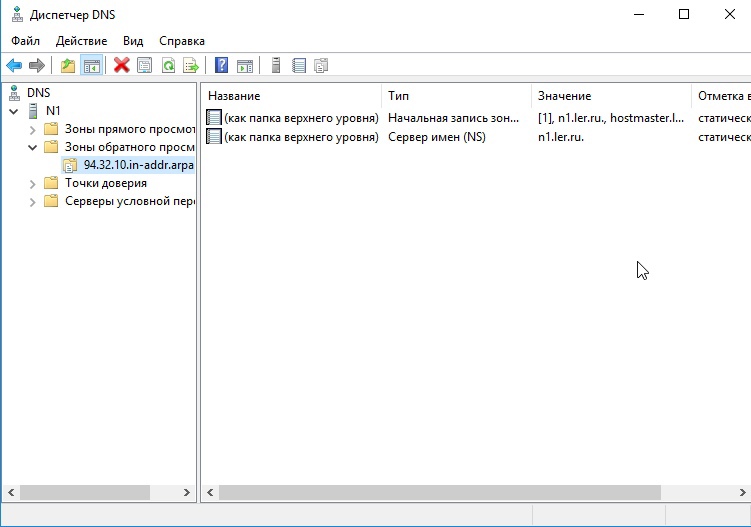


Рисунок 18 – Просмотр зон обратного просмотра

Наконец, в "Диспетчере серверов" необходимо было выбрать "Пользователи и компьютеры Active Directory" и проверить работу Active Directory (рисунок 19).

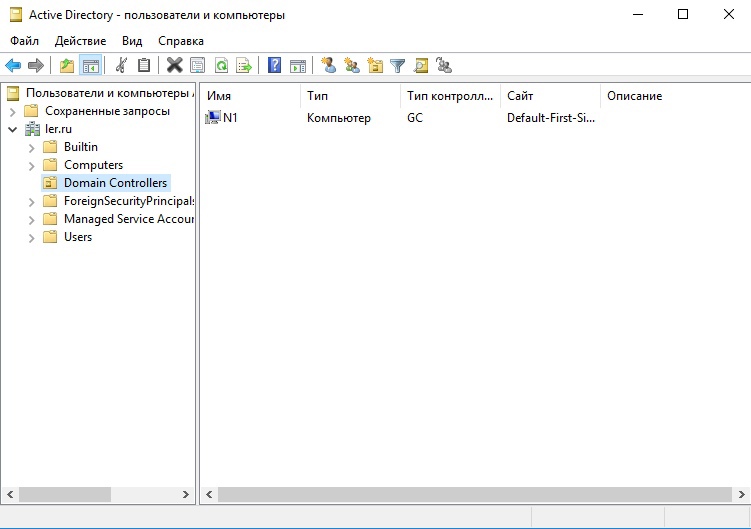


Рисунок 19 - Проверка работы Active Directory

4. Выводы

В ходе выполнения лабораторной работы была настроена работа службы Active Directory, а также распределены роли пользователей.

**1. Что такое Active Directory и каковы её основные возможности?**

Active Directory – служба каталогов от корпорации Microsoft для операционных систем семейства Windows Server. Служба позволяет администраторам использовать групповые политики для обеспечения единообразия настройки пользовательской рабочей среды, разворачивать ПО на множестве компьютеров через групповые политики или посредством System Center Configuration Manager, устанавливать обновления операционной системы, прикладного и серверного программного обеспечения на всех компьютерах в сети, используя службу обновления Windows Server. AD хранит данные о ресурсах (компьютерах, пользователях, серверах, сетевых и периферийных устройствах и т.д.) и настройки среды в централизованной базе данных.

**Основные возможности Windows AD**:

− единая база регистрации пользователей, которая хранится централизованно на одном либо нескольких серверах; таким образом, при появлении нового сотрудника в офисе вам нужно будет всего лишь завести ему учетную запись на сервере и указать, на какие рабочие станции он сможет получать доступ;

− поскольку все ресурсы домена индексируются, это дает возможность простого и быстрого поиска для пользователей; например, если нужно найти цветной принтер в отделе;

− совокупность применения разрешений NTFS, групповых политик и делегирования управления позволит вам тонко настроить и распределить права между участниками домена;

− перемещаемые профили пользователей дают возможность хранить важную информацию и настройки конфигурации на сервере; фактически, если пользователь, обладающий перемещаемым профилем в домене, сядет работать за другой компьютер и введет свои имя пользователя и пароль, он увидит свой рабочий стол с привычными ему настройками;

− с помощью групповых политик вы можете изменять настройки операционных систем пользователей, от разрешения пользователю устанавливать обои на рабочем столе до настроек безопасности, а также распространять по сети программное обеспечение, например, Volume Shadow Copy client и т. п.;

− многие программы (прокси-серверы, серверы баз данныхи др.) не только производства Microsoft на сегодняшний день научились использовать доменную аутентификацию, таким образом, вам не придется создавать еще одну базу данных пользователей, а можно будет использовать уже существующую;

− использование Remote Installation Services облегчает установку систем на рабочие места, но, в свою очередь, работает только при внедренной службе каталогов.

**2. Для чего необходим контроллер домена, какие функции он выполняет?**

Для реализации данного решения, необходим специальный сервер –контроллер домена. Именно он будет выполнять функции аутентификации пользователей и устройств в сети, а также выступать в качестве хранилища базы данных. При попытке использовать любой из объектов (ПК, сервер, принтер) сети, выполняется обращение к контроллеру домена, который либо разрешает это действие (есть необходимые права), либо блокирует его.

**3. Что такое «рабочие группы» и чем вызваны сложности эксплуатации их в крупных сетях?**

Рабочая группа – это логическая группировка компьютеров, объединенных общим именем для облегчения навигации в пределах сети, при этом принципиально важно, что каждый в рабочей группе равноправен (т. е. сеть получается одноранговой) и поддерживает собственную локальную базу данных учетных записей пользователей (Security Accounts Manager, SAM).

Действительно, вход в защищенную систему является обязательным, а непосредственный и сетевой входы принципиально различаются (непосредственный контролируется локальным компьютером, а сетевой —удаленным), то, например, пользователю, вошедшему на компьютер Comp1 под локальной учетной записью User1, будет отказано в доступе к принтеру, установленному на компьютере Comp2, поскольку в его локальной базе нет пользователя с именем User1.

**4. Какие группы выделяют в рамках схемы AD и как они подразделяются по области действия?**

Группы безопасности (применяются для разграничения прав доступа к объектам сети) и группы распространения (применяются в основном для рассылки почтовых сообщений, например, в сервере Microsoft Exchange Server).

Они подразделяются по области действия:

− универсальные группы могут включать в себя пользователей в рамках леса, а также другие универсальные группы или глобальные группы любого домена в лесу;

− глобальные группы домена могут включать в себя пользователей домена и другие глобальные группы этого же домена;

− локальные группы домена используются для разграничения прав доступа, могут включать в себя пользователей домена, а также универсальные группы и глобальные группы любого домена в лесу;

− локальные группы компьютеров – группы, которые содержит SAM (security account manager) локальной машины. Область их распространения ограничивается только данной машиной, но они могут включать в себя локальные группы домена, в котором находится компьютер, а также универсальные и глобальные группы своего домена или другого, которому они доверяют. Например, вы можете включить пользователя из доменной локальной группы Users в группу Administrators локальной машины, тем самым дав ему права администратора, но только для этого компьютера.

**5. Что такое лес AD и какую структуру он имеет?**

**Лес Active Directory** – определяет набор одного или нескольких доменов, использующих одни и те же схему, конфигурацию и глобальный каталог. Кроме этого, все домены участвуют в двусторонних транзитивных отношениях доверия. Обратим внимание на термины, которые используются в определении леса:

**Схема** – схема Active Directory используется совместно всеми доменами в пределах леса. Схема — это конфигурационная информация, которая управляет структурой и содержимым каталога.

**Конфигурация** – конфигурация определяет логическую структуру леса, например, число и конфигурацию сайтов в пределах леса.

**Глобальный каталог** – глобальный каталог можно воспринимать в виде справочника для леса. Глобальный каталог содержит информацию о всех объектах леса включая информацию о расположении объектов.

**6. Объясните понятие «доверие» и назовите основные виды отношения доверия.**

Предоставляет различным доменам возможность работать вместе. Без доверия домены работают как отдельные сущности, то есть пользователи из домена A не смогут получать доступ к ресурсам в домене B.

Существует три основных типа отношений доверия:

**Транзитивные** – транзитивные отношения доверия создаются автоматически между доменами одного леса. Они позволяют пользователям любого домена потенциально получать доступ к ресурсам любого другого домена этого леса, если у пользователей есть соответствующие права доступа.

**Shortcut** – это отношение доверия между доменами одного леса, которые уже имеют транзитивное отношение доверия. Такое отношение доверия предоставляет более быструю аутентификацию и проверку доступа к ресурсам между не соседними доменами леса.

**Внешние** – внешние отношения доверия позволяют доменам из различных лесов совместно использовать ресурсы. Такие отношения доверия не являются транзитивными, то есть они относятся только к тем доменам, для которых они создавались.

**7. Что такое «транзитивное» отношение доверия и назовите доверие, которое не является транзитивным.**

Транзитивные – транзитивные отношения доверия создаются автоматически между доменами одного леса. Они позволяют пользователям любого домена потенциально получать доступ к ресурсам любого другого домена этого леса, если у пользователей есть соответствующие права доступа.

Внешние – внешние отношения доверия позволяют доменам из различных лесов совместно использовать ресурсы. Такие отношения доверия не являются транзитивными, то есть они относятся только к тем доменам, для которых они создавались.

**8. Что такое глобальный каталог леса Active Directory?**

Глобальный каталог – глобальный каталог можно воспринимать в виде справочника для леса. Глобальный каталог содержит информацию о всех объектах леса включая информацию о расположении объектов.

**9. Что такое ресурсная запись и какие элементы она включает?**

Ресурсная запись (RR – Resource Record) – единица хранения и передачи информации в DNS, включающая в себя следующие элементы (поля):

− Имя (Name) – имя домена, к которому относится запись;

− TTL (Time To Live) – допустимое время хранения записи неответственным сервером;

− Тип (Type) – параметр, определяющий назначение и формат записи в поле данных (Rdata);

− Класс (Class)– тип сети передачи данных (подразумевается возможность DNS работать с типами сетей, отличных от TCP/IP);

− Длина поля данных (Rdlen);

− Поле данных (Rdata) – содержание и формат поля зависят от типа записи.

**10. Какие типы ресурсных записей бывают?**

− A (IPv4 Address Record – адресная запись) – связывает доменное имя с IPv4-адресом хоста;

− AAAA (IPv6 Address Record) – связывает доменное имя с IPv6-адресом хоста (аналогично А-записи);

− CNAME (Canonical Name Record – каноническая запись имени) –используется для перенаправления на другое доменное имя;

− MX (Mail Exchange – почтовый обменник) – ссылается на почтовый сервер, обслуживающий домен;

− NS (NameServer– сервер имен) – ссылается на DNS-сервер, ответственный за домен;

− TXT – текстовое описание домена. Зачастую требуется для выполнения специфических задач (например, подтверждения права собственности на домен при привязке его к почтовому сервису);

− PTR (Point to Reverse – запись указателя) – связывает IP-адрес машины с доменом, используется преимущественно для проверки сторонними почтовыми сервисами отправляемых через эту машину электронных писем на отношение к домену, указанному в параметрах почтового сервера. При несоответствии этих параметров письмо проверяется более тщательно по другим критериям.

**11. Что такое обратный просмотр DNS и для чего он используется?**

Обратный просмотр DNS (англ. reverseDNSlookup)–обращение к особой доменной зоне для определения имени узла по его IP-адресу c помощью PTR-записи.

**12. Чем ограничивается количество PTR-записей, описывающих разные имена, на один адрес и почему?**

не ограничивается спецификациями, но может ограничиваться размером UDP-пакета, так как DNS-сервер инкапсулирует свой ответ в UDP.