Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Практическое занятие № 6. Развертывание службы Active Directory

Студент: Мозолевский А. Д.

ФИТ 4 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2023

# Выполнение упражнений

Для работы с Active Directory необходимо установить соответствующий компонент, представленный на рисунке 1.1.

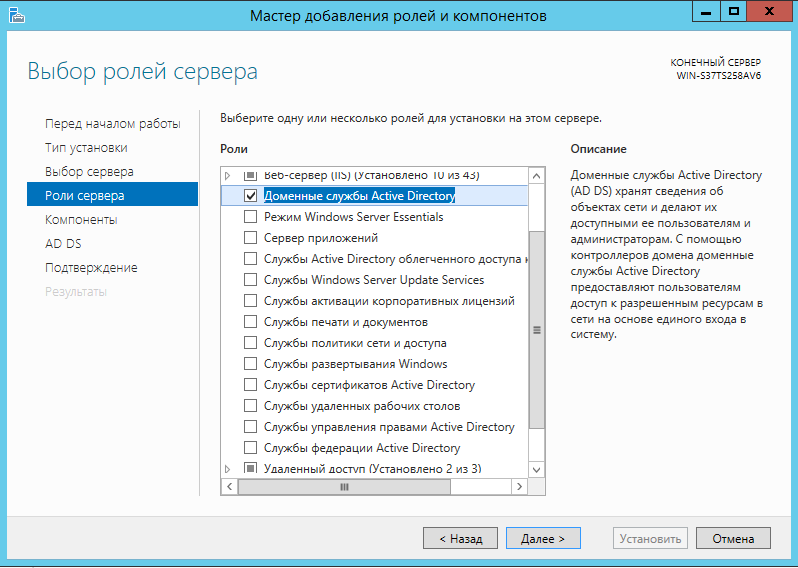


Рисунок 1.1 – Компонент для работы с Active Directory

Далее необходимо выбрать имя корневого каталога, что представлено на рисунке 1.2.

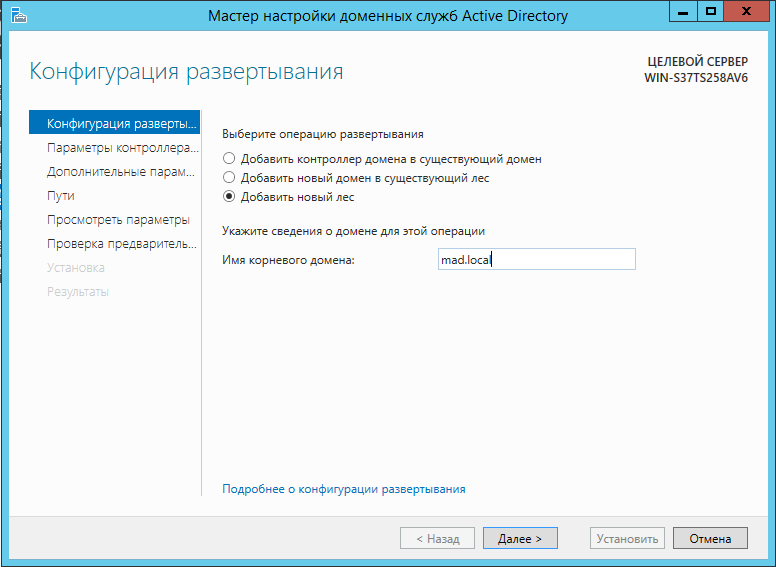


Рисунок 1.2 – Настройка имени корневого компонента AD

Такое же имя представлено на NetBIOS, что представлено на рисунке 1.3.

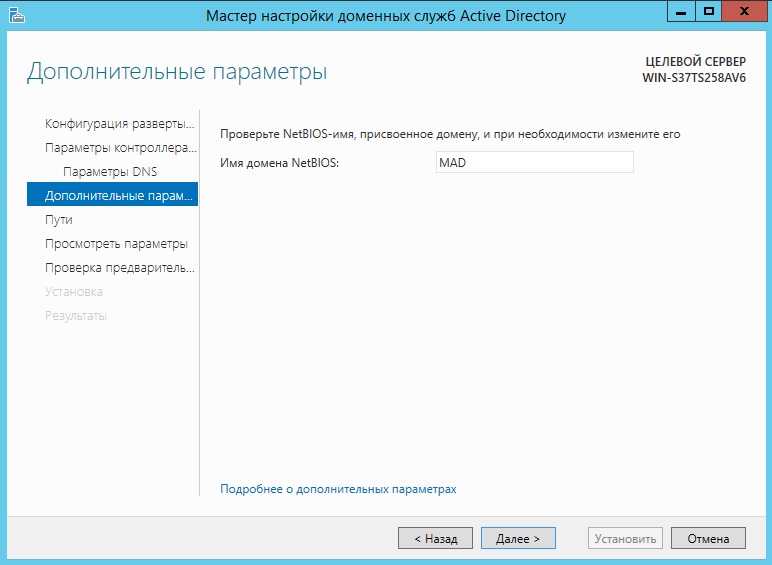


Рисунок 1.3 – Доменное имя NetBOIS

После корректной установки будет выведено окно, которое представлено на рисунке 1.4.

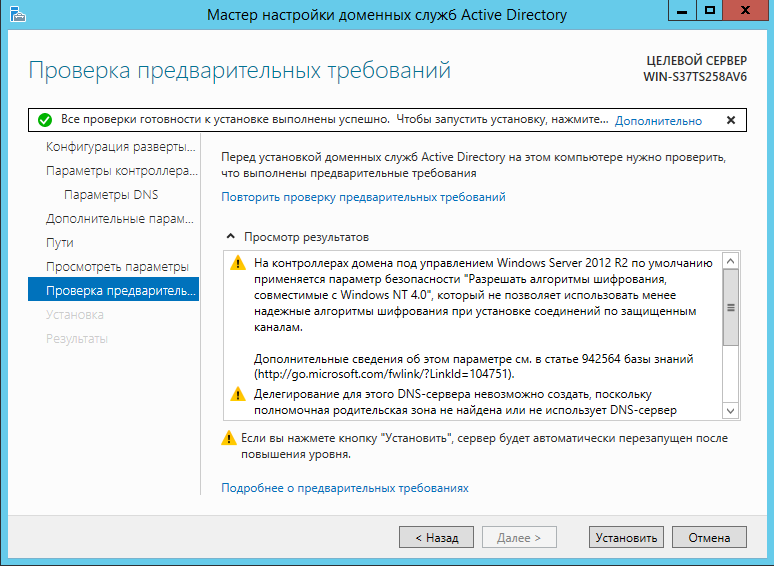


Рисунок 1.4 – Корректная установка AD

После перезагрузки можно проверить, что компонент был установлен. Содержимое данной папки представлено на рисунке 1.5.

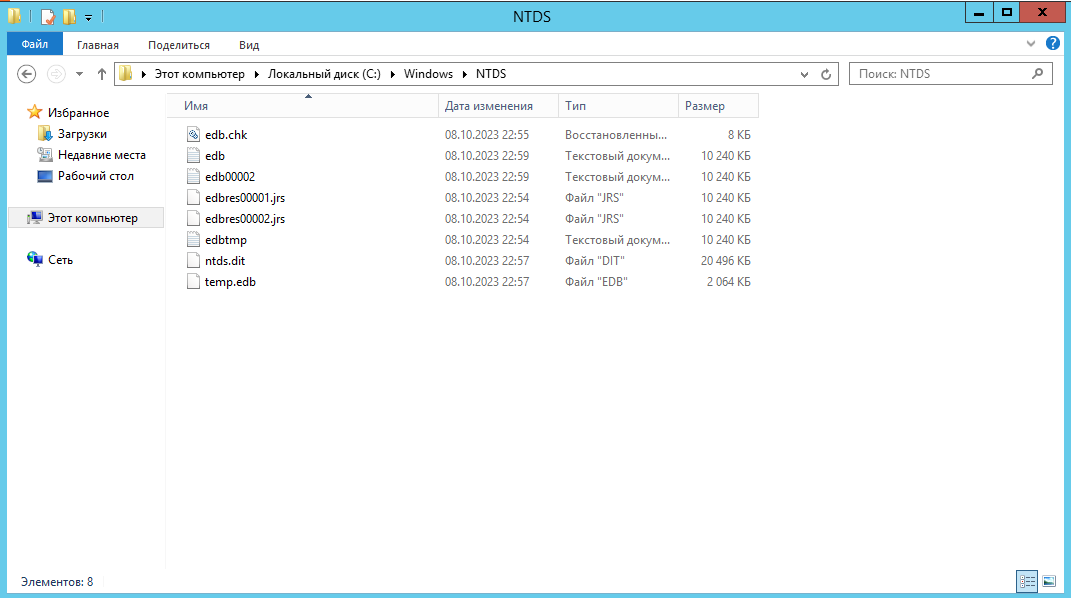


Рисунок 1.5 – Содержимое папки NTDS

Затем можно воспользоваться утилитой net для проверки работы sysvol, что представлено на рисунке 1.6.

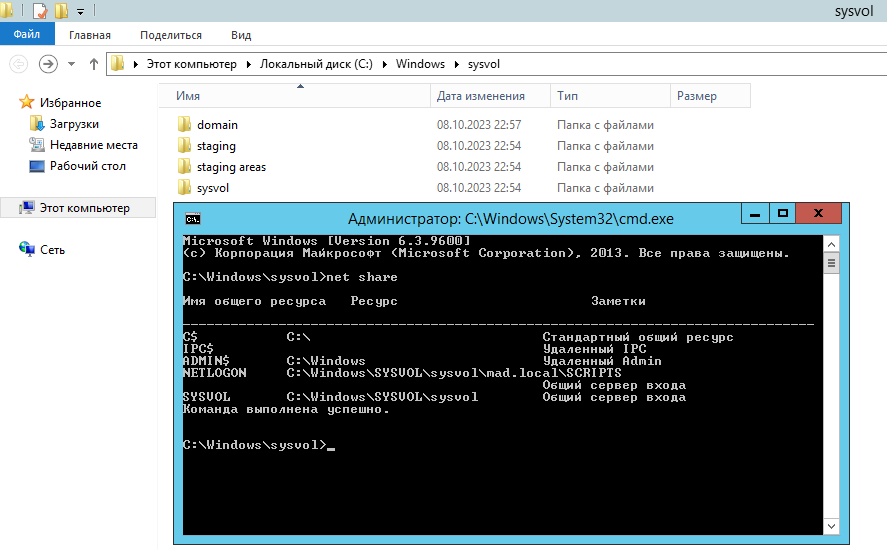


Рисунок 1.6 – Проверка работы sysvol

2. Контрольные вопросы

1. **Как служба DNS связана со службой активного каталога (Active Directory)?**

Служба DNS (Domain Name System) играет важную роль в Active Directory, так как AD использует DNS для разрешения имен компьютеров и ресурсов в сети. Каждый контроллер домена в Active Directory имеет DNS-записи, которые позволяют клиентам и другим контроллерам домена находить и связываться с ним. Правильная настройка DNS необходима для функционирования AD.

1. **Какие типы контроллеров AD бывают?**

Существуют два основных типа контроллеров домена в Active Directory:

1. Контроллеры домена (Domain Controllers, DC): Они содержат базу данных AD и службы для аутентификации и авторизации пользователей в домене.
2. Контроллеры домена с управлением участниками (Read-Only Domain Controllers, RODC): Эти контроллеры предоставляют только ограниченный доступ к базе данных AD и используются в ситуациях, где требуется уменьшить риск компрометации базы данных AD на удаленных местах или в ненадежных средах.
3. **Что такое база данных AD?**

База данных Active Directory (AD) представляет собой центральное хранилище данных о пользователях, группах, компьютерах и других ресурсах в сети. Она содержит информацию о структуре и организации домена, а также обеспечивает доступ и аутентификацию пользователей в домене.

1. **Кратко опишите процесс повышения статуса одиночного сервера до уровня контроллера домена?**

Процесс повышения статуса одиночного сервера до контроллера домена включает в себя следующие шаги:

* Установка роли службы Active Directory Domain Services (AD DS).
* Запуск мастера установки контроллера домена.
* Выбор опций для создания нового домена или присоединения к существующему.
* Предоставление информации о новом домене, включая его имя и пароль администратора.
* Перезагрузка сервера после завершения процесса установки.

1. **В каком месте файловой системы (в каком каталоге) ОС Windows располагаются:**

* файла базы данных AD: %SystemRoot%\NTDS
* файлы журналов AD: %SystemRoot%\NTDS
* системный разделяемый том AD: %SystemRoot%\SYSVOL

1. **С помощью какой консоли ММС можно управлять пользователями и компьютерами входящими в AD?**

Для управления пользователями и компьютерами в Active Directory можно использовать "Active Directory Users and Computers" (ADUC), которая доступна через Microsoft Management Console (MMC).

1. **С помощью какой консоли ММС можно управлять репликациями в домене?**

Управление репликациями в домене можно осуществлять с помощью "Active Directory Sites and Services" (ADSS), также доступной через Microsoft Management Console (MMC).

1. **Почему служба AD предполагает необходимость репликаций между контроллерами одного домена?**

Репликация между контроллерами домена необходима для обеспечения согласованности и доступности данных в разных частях домена. Она позволяет обновлениям, внесенным на одном контроллере, распространяться на все остальные контроллеры домена, что обеспечивает единое представление данных и уменьшает возможность конфликтов.

1. **Какой транспортный протокол используют службы LDAP и Керберос?**

Службы LDAP (Lightweight Directory Access Protocol) используют протокол TCP (Transmission Control Protocol) для передачи данных. Обычно LDAP работает на порту 389 (LDAP) и 636 (LDAPS, LDAP Secure).

Службы Керберос (Kerberos) также используют TCP, но они работают на разных портах. Основной порт для аутентификации Керберос - 88 (Kerberos), а также 464 (Kerberos Change/Set Password).

1. **Какие порты используют службы LDAP и Керберос?**

Службы LDAP обычно используют порт 389 для незащищенной передачи данных и порт 636 для защищенной (SSL/TLS) передачи данных (LDAPS).

Службы Керберос используют порт 88 для аутентификации и порт 464 для смены или установки пароля (Kerberos Change/Set Password).