Министерство образования Республики Беларусь

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра программной инженерии

«Администрирование и безопасность Интернет-систем»

**Отчет к лабораторной работе №5:**

«Развертывание службы Active Directory»

Выполнил:

Студент 4 курса 6 группы ФИТ

Хлыстов Глеб Георгиевич

Проверила:

Сазонова Дарья Владимировна

Минск 2023

# **Теоретические сведения**

**1.1 Создание контроллера домена Active Directory**

**Подготовка к установке**

Чтобы повысить статус сервера Windows Windows 2019 до уровня контроллера домена, сначала нужно полностью завершить процесс установки ОС. Затем войти в систему с учетной записью администратора. Для размещения AD сервер должен иметь раздел NTFS. Последним требованием является наличие доступа к серверу DNS.

Windows Server 2019 представляет новое поколение Active Directory упрощенное администрирование доменных служб и является наиболее радикальную модернизацию системы управления доменами с момента выпуска Windows 2000 Server.

Упрощенное администрирование AD DS (Active Directory Domain Service) представляет новый подход к развертыванию доменов. Ниже перечислены некоторые из этих возможностей.

* Развертывание роли AD DS теперь является частью архитектуры диспетчера сервера и допускает удаленную установку.
* Модуль развертывания и настройки AD DS теперь основан на Windows PowerShell, даже при использовании графического интерфейса установки.
* При повышении роли сервера теперь проводится проверка предварительных требований с помощью которой подтверждается готовность леса и домена для нового контроллера домена, что снижает вероятность сбоев.

**1.2 Установка роли контроллера домена Active Directory**

**Установка роли контроллера домена Active Directory**

С помощью мастера управления серверными ролями добавляем новую роль **Server Manager** — **Manage** — **Add Roles and Features**. Отмечаем галочкой пункт **Skip this page by default** (чтобы в будущем не видеть эту страницу) и нажимаем **Next**.

Выбираем первый пункт **Role-based or feature-based installation** (Базовая установка ролей и компонентов). Второй пункт **Remote Desktop Service installtion**предназначен только для установки роли удаленных рабочих столов. Нажимаем **Next**.

Выбираем **Select a server from the server pool** и выбираем сервер на котором будет развернута роль. Пункт **Select a virtual hard disk** позволяет указать сервер, расположенный на **VHD**-диске. Нажимаем **Next**.

Отмечаем галочкой роль**Active Directory Domain Services**, в подтверждающем запросе добавления роли и компонентов, необходимых для установки **AD** нажимаем **Add Features** и после нажимаем **Next**.

В этом окне предлагается выбрать дополнительные компоненты, в данном случае дополнительные компоненты не нужны, поэтому нажимаем **Next**.

Информационная страница, на которой обращается внимание на то что желательно иметь несколько контроллеров домена, на случай выхода из строя основного. Служба **AD DS** требует установленного в сети **DNS-сервера**, если он не установлен, то будет предложено его установить, а так же **AD DS** требует установки дополнительных служб **DFS Namesspases** (пространства имен), **DFS Replication** (DFS репликации) и **File Replication** (Файловой репликации). Нажимаем **Next**.

На завершающей странице мастера отображается информация по устанавливаемым компонентам. Так же здесь можно экспортировать конфигурацию в xml-файл (**Export configuration settings**), на случай если нужно развернуть идентичный сервер. Нажимаем **Install**.

После установки Роли, в **Server Manager** нажимаем на значок Флажка с восклицательным знаком и выбираем **Promote this server to a domain controller** (Повысить этот сервер до контроллера домена). Запустится мастер конфигурирования **AD DS**.

Необходимо выбрать вариант развертывания **AD DS**.

* **Add a domain controller to an existing domain** — добавить дополнительный контроллер домена в существующем домене.
* **Add a new domain to an existing forest** — добавить новый домен в существующем лесу:
* *Tree Domain* —  корневой домен нового дерева в существующем лесу
* *Child Domain* — дочерний домен в существующем лесу
* **Add New Forest** — создать новый корневой домен в новом лесу.

Выбираем вариант **Add New Forest**, указываем корневое имя домена, нажимаем **Next**.

В параметрах контроллера домена оставляем по умолчанию функционал леса и домена, проверяем отмечен ли галочкой пункт **Domain Name System** (**DNS**), будет автоматически поднята роль DNS и задаем пароль для режима восстановления служб каталогов. Нажимаем **Next**.

Не обращаем внимание на предупреждение ошибки делегирования для этого **DNS-сервера**, т.к. роль DNS поднимается в процессе конфигурации **AD DS**. Нажимаем **Next**.

Оставляем подставленное мастером **NetBIOS** имя. Нажимаем **Next**.

Пути к каталогам оставляем по-умолчанию. Нажимаем **Next**.

Вывод сводной информации по настройке **AD DS**. Нажимаем **Next**.

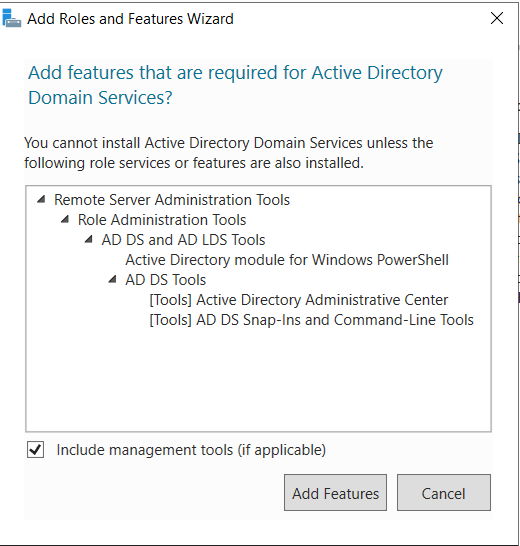
Дожидаемся выполнения предварительной проверки и если проверка прошла успешно, то мастер нам сообщит об этом: **All prerequisite checks are passed successfully. Click «install» to begin installation.** (Все предварительные проверки пройденыуспешно. Нажмите кнопку «установить», чтобы начать установку.). Нажимаем **Install**.

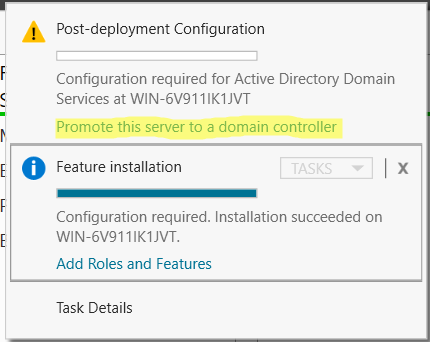
В ходе установки конфигурации **AD DS**, система будет перезагружена.

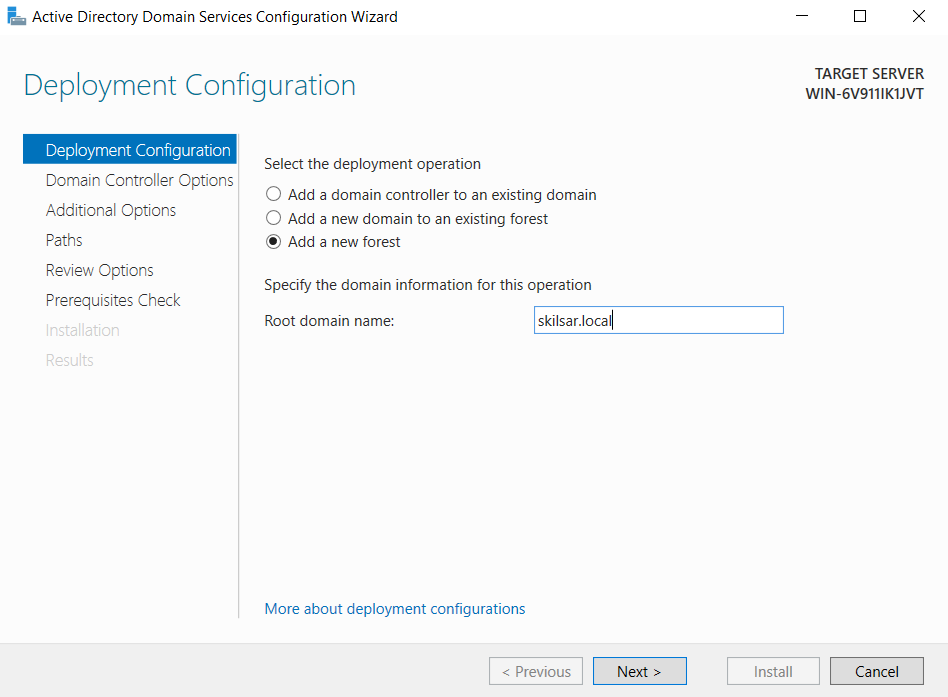
# **Выполнение практического задания**

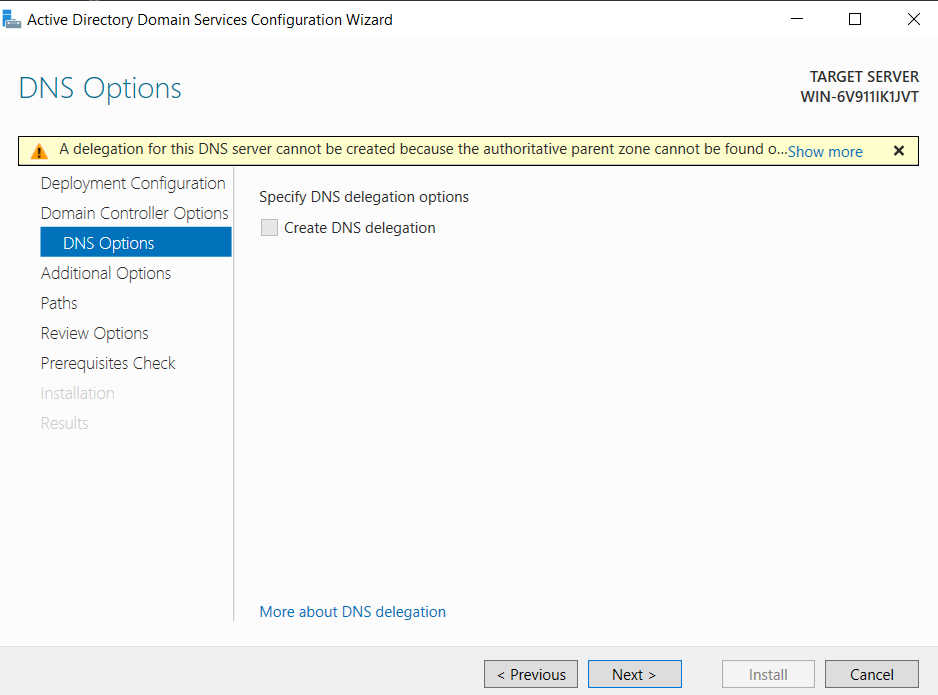
В рамках выполнения данной лабораторной работы было необходимо выполнить развертывания Active Directory. Результат из выполнения представлен на рисунках ниже.

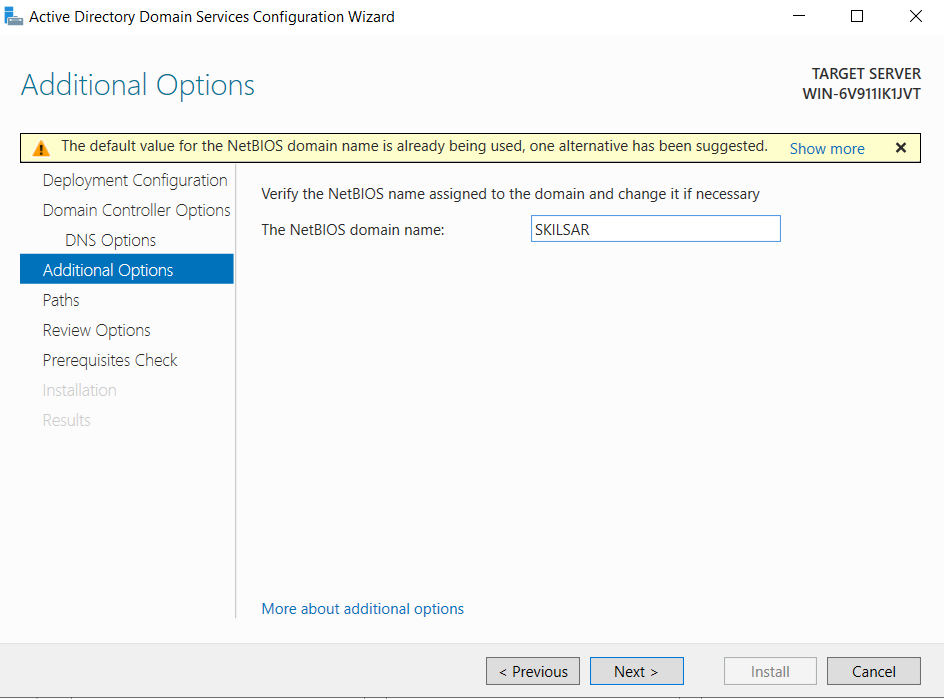
**2.1 Установка Active Directory**

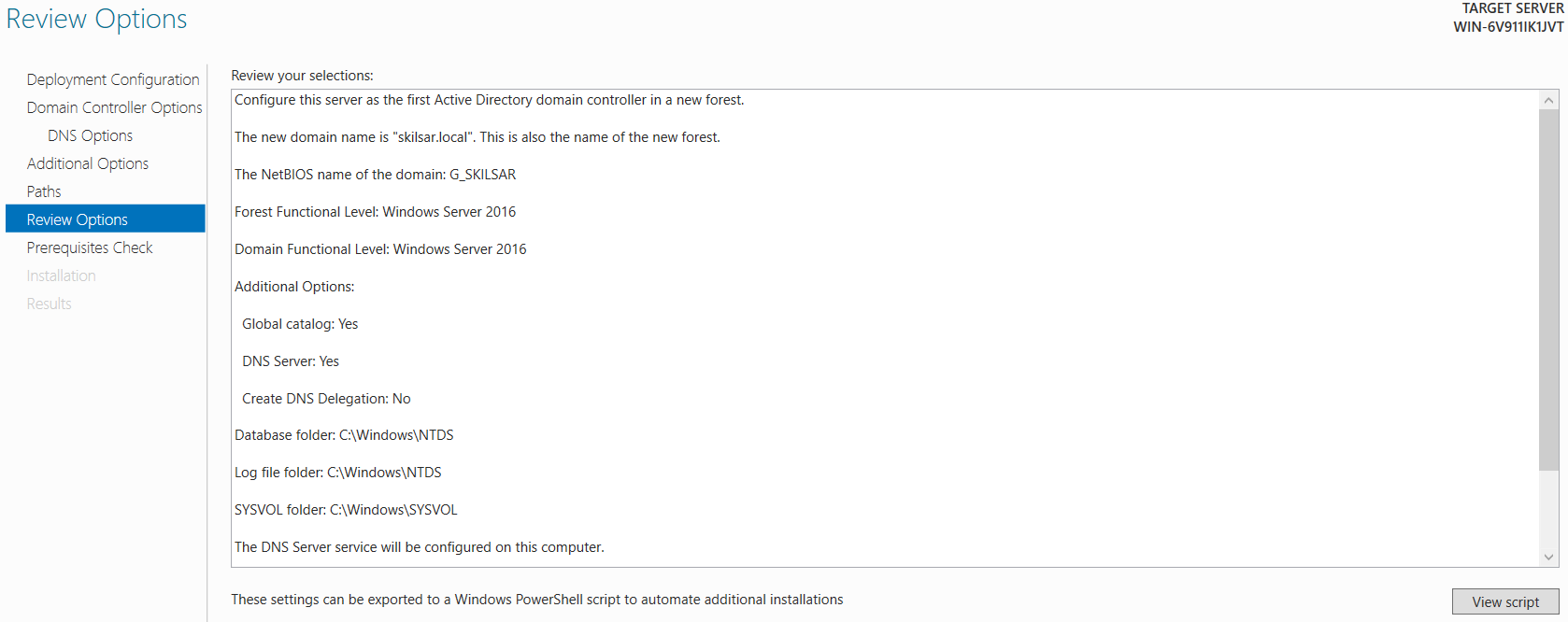


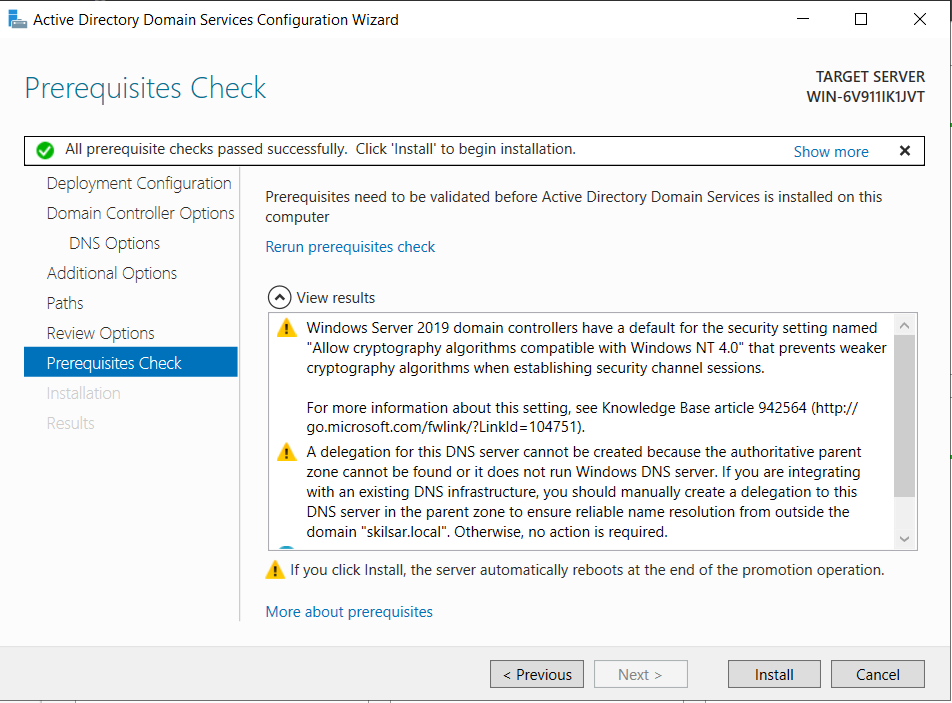




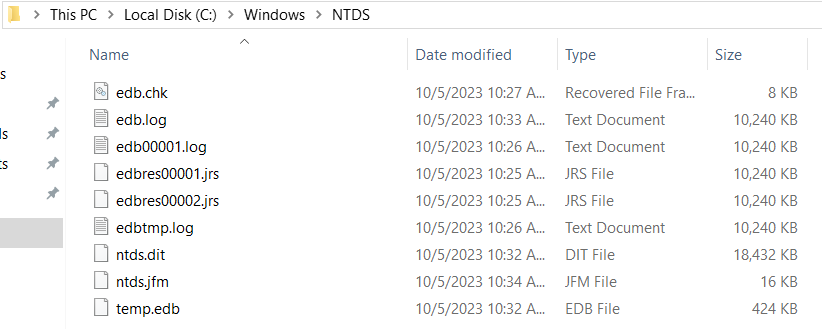








**2.2 Проверка установки Active Directory**



# **Ответы на 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).

# **Вывод**

В данной лабораторной работе я изучил и выполнил развертывания службы Active Directory в виртуальной сети, разработанной в ходе выполнения предыдущих лабораторных работ. Разобрался как выполнять процесс установки контроллера домена в ОС Windows Windows 2019. По итогам лабораторной работы выполнил проверку правильности настройки Active Directory в созданной виртуальной сети.