

---

## Управление контроллерами домена в Active Directory

---

**Цель работы:** Получить дополнительные навыки по управлению контроллерами домена Active Directory на основе Windows Server, работу с событиями и процессами.

**Необходимо:**

- Установленная на компьютере среда виртуализации **ORACLE Virtual Box**
- Образы виртуальных жёстких дисков операционных систем **Windows Server 2012/2016.**
- Доступ к Microsoft Evaluation Center (<https://www.microsoft.com/ru-ru/evalcenter>)

**Краткие теоретические сведения:**

Основной единицей хранения в AD является домен. Домен – контейнерный объект, представляющий собой фрагмент AD хранящийся на специальном компьютере с Windows Server. Домен может содержать объекты-контейнеры (Organization Unit) и конечные объекты (User, Group, Computer и т.п.). Домены AD могут объединяться в деревья, деревья в конгломераты более высокого уровня – леса. В AD относительно домена может строиться распределенная система в которых копии домена хранятся на нескольких Windows Server, работающих в режиме контроллера домена.

Служба Active Directory Directory Service является распределенной. Домен хранится на одном или нескольких контроллерах доменов, которые являются равнозначными.

Однако существуют особые роли контроллеров домена – FSMO и функция

глобального каталога. Эту функцию и каждую из ролей выполняет единственный контроллер. FSMO и функция глобального каталога могут быть перенесены или принудительно захвачены.

*Совет 1. После выполнения работы необходимо сохранить снимки состояния виртуальных машин, для использования в последующих работах.*

*Совет 2. Перед выполнением работы ознакомьтесь с требованиями к содержанию отчета, чтобы собирать необходимые артефакты выполнения.*

## **Порядок выполнения работы:**

### **Часть 1. Подготовительная.**

1. Для выполнения работы понадобится две виртуальные машины Windows Server и Windows 10 Pro или Enterprise и Windows Server одной из версий: 2012 R2\2016\2019.
2. Дистрибутивы операционных систем со сроком действия 90 дней можно скачать с сайта Microsoft Evaluation Center (<https://www.microsoft.com/ru-ru/evalcenter>).
3. Для выполнения работы вы можете использовать готовую инфраструктуру из работы №4.
4. Если таковая инфраструктура имеется, установите дополнительный Windows Server с именем as-srv-2 со статическим адресом и в той же локальной сети, что и предыдущие машины. Введите его в домен.
5. Если инфраструктуры нет, то:
  - a. Подготовьте виртуальные машины с windows server ad-srv и as-srv-2, и ad-client с Windows 10.
  - b. Настройте виртуальные машины так, чтобы они оказались в одной, изолированной LAN. Для сервера выберите и настройте адрес из сети 10.0.0.0/8. В качестве DNS сервера установите

адресе сервера ad-srv.

- c. Подготовьте компьютер «AD-Srv» к развертыванию AD (новый домен, новый лес) с установкой DNS на «Ad-srv». С помощью мастера добавления ролей и компонентов и диспетчера серверов развернуть домен с именем: «ваши\_FIO».local. Автоматически установите и настройте DNS.
  - d. Введите в домен as-srv-2 и ad-client
6. Сделайте снапшоты всех машин.

## Часть 2. Добавление контроллера домена

1. На компьютере ad-srv-2 установите роль AD DS.
2. Настройте на нем дополнительный контроллер домена в том же лесу, домене.
3. После установки перезагрузить компьютер.

## Часть 3. Получение информации о домене

1. С помощью PowerShell установите, на каком контроллере домена функционируют FSMO
2. С помощью dsquery установите, на каком контроллере домена функционируют FSMO
3. Выясните, какие записи DNS появились с вводом нового контроллера домена.
4. На контроллере ad-srv-2 создайте пользователя в AD. Убедитесь, что от имени этого пользователя можно запускать процессы на ad-client с помощью GUI, утилиты runas и PowerShell.

## Часть 4. Архивация Active Directory

1. С помощью PowerShell установите службу архивации windows на ad-srv.

2. С помощью консольной утилиты wbadmín создайте архивную копию ActiveDirectory.

## Часть 5. Замена контроллера домена

Реализуйте сценарий замены контроллера домена, при котором все роли и гс будут переданы на ad-srv-2, а роль AD DS будет удалена с ad-srv.

1. Создайте снапшоты всех виртуальных машин.
2. Перенесите FSMO и гс на ad-srv-2 или с помощью утилиты ntdsutil, PowerShell или GUI. Убедитесь, что перенесен и DNS.
3. Подготовьте описание процесса для отчета.
4. С помощью утилиты dcdiag проверьте AD на ошибки.
5. С помощью PowerShell установите, на каком контроллере домена функционируют FSMO
6. Удалите роль AD DS на ad-srv. Перегрузите компьютер.
7. С помощью утилиты dcdiag проверьте AD на ошибки.
8. Убедитесь, что пользователи могут регистрироваться на ad-client.

## Содержание отчета

Требуется подготовить отчеты в формате DOC\DOCX или PDF. Отчет содержит титульный лист, артефакты выполнения и ответы на вопросы.

Вопросы:

1. Перечислите FSMO. Кратко раскройте их назначение.
2. Опишите, что произойдет, если не будет доступна каждая из ролей.
3. Как с помощью утилиты dcdiag проверить корректность настройки только dns?
4. Как с помощью утилиты dcdiag исправить ошибки в конфигурации?
5. Как ввести компьютер в домен с помощью утилиты netdom?
6. Как ввести компьютер в домен с помощью утилиты PowerShell?
7. Как запустить процесс от имени другого пользователя с помощью утилиты runas?

8. Как запустить процесс от имени другого пользователя с помощью командлета Invoke-Command?

Артефакты:

1. Консольные выводы по Части 3, п. 1-2.
2. Ответ на вопрос из Части 3., п. 3.
3. Командные строки из Части 4, п. 1-2.
4. Приведите описание процесса переноса ролей из Части 5. п.2
5. Командные строки и консольный вывод из Части 5, п. 5.

Отчет выслать в течении 2-х недель на адрес [edu-net@yandex.ru](mailto:edu-net@yandex.ru).

В теме письма: Негруппы ФИО (латинскими буквами) №работы (например: 5555  
Fedor Sumkin 5)