ПРАКТИЧЕСКАЯ РАБОТА №3

# 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 сроиться 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 ознакомитесь с требованиями к содержанием 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 №2.
4. Если таковая инфраструктура имеется, установите дополнительный Windows Server с именем ad-srv-2 со статическим адресом и в той же локальной сети, что и предыдущие машины. Введите его в домен.

* Ну тут либо клонировать старую версию сервера, но потом менять SID с помощью sysprep, либо просто заново еще один установить, но по факту это тот же самый сервак, так что точно sysprep)
* Клонируем сервак
* Входим, Win+R
* Sysprep
* exe
* OOBE + галочку на подготовку
* Перезагружаемся, все, у нас новый сид, но у меня улетел VSC(
* Переименовываем комп, перезагружаем
* Вводим его в домен (там же, где и переименовывание)

1. Если инфраструктуры нет, то:
   1. Подготовьте 2 виртуальные машины с windows server: ad-srv-1 и as-srv-2, а также машину ad-client c Windows 10.
   2. 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 севера установите адрес самого сервера ad-srv.
   3. Подготовьте компьютер «AD-Srv-1» к развертыванию AD (новый домен, новый лес) с установкой DNS на «Ad-srv-1». С помощью мастера добавления ролей и компонентов и диспетчера серверов развернуть домен с именем: «ваши\_FIO».local. Автоматически установите и настройте DNS.
   4. Введите в домен as-srv-2 и ad-client
2. Сделайте снапшоты всех машин.

* Это дело в самом виртуабоксе
* (около название машины менюшка, там снимки сделать)

**Часть 2. Добавление контроллера домена**

1. На компьютере ad-srv-2 [установите роль AD DS](http://pyatilistnik.org/kak-dobavit-kontroller-domena-s-windows-server-2012-r2-v-sushhestvuyushhiy-les-active-directory-windows-server-2008-r2/).

**Лучше 5 раз проверьте правильные ли адреса и DNS адреса стоят на обоих серваках, пожалуйста. И сделайте снапшоты, когда просто все настроите.**

[**Норм статья**](https://jakondo.ru/razvorachivaem-dopolnitelnyj-kontroller-domena-na-baze-windows-server-2012-r2-replikatsiya-nastrojka-raboty-dhcp-s-osnovnym-kontrollerom-domena/)

* Дуем на первый сервак
* Добавить сервер
* DNS, находим второй сервер по имени или IP
* Добавляем, теперь в домене у нас 2 сервера
* Добавить роли и компоненты
* Просто выбираем второй сервер
* Доменные службы AD, там предложит установить и дополнения, ставим и их тоже
* Устанавливаем

1. Настройте на нем дополнительный контроллер домена в том же лесу, домене.

* Когда установилось, повышаем роль, существующий домен, там автоматом нужный домен
* Указываем админа с основного сервака (админа домена)
* Устанавливаем

1. После установки перезагрузить компьютер (второй сервак, который повысили).

* Можно посмотреть все кон-ры домена через dsquery Server -domain ad-training.loc

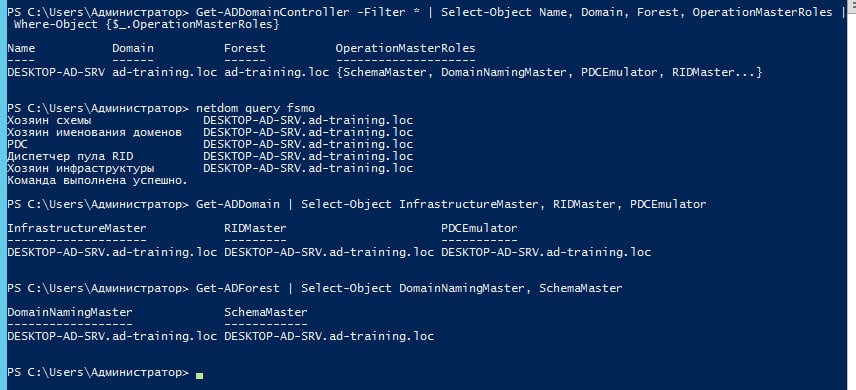


1. На всякий случай сделаем еще снапшотики.

**Часть 3. Получение информации о домене**

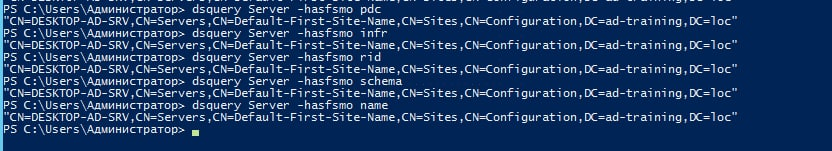
1. С помощью PowerShell [установите](https://winitpro.ru/index.php/2012/03/06/peredacha-rolej-fsmo/), на каком контроллере домена функционируют FSMO

* Powershell от админа
* netdom query fsmo == для всего сразу, удобно
* Или можно получить FSMO роли уровня леса и уровня домена так, явно указывая:
  + Get-ADDomain | Select-Object InfrastructureMaster, RIDMaster, PDCEmulator
  + Get-ADForest | Select-Object DomainNamingMaster, SchemaMaster
  + Get-ADDomainController -Filter \* | Select-Object Name, Domain, Forest, OperationMasterRoles |Where-Object {$\_.OperationMasterRoles} - общая



1. С помощью [dsquery](https://abeliy.wordpress.com/2012/04/26/определение-fsmo-ролей/) [установите](https://vmblog.ru/komanda-dsquery-dlya-poiska-obektov-v-active-directory/), на каком контроллере домена функционируют FSMO

* все контролеры домена в лесу AD - dsquery Server -o rdn –Forest
* все контролеры домена в указанном домене - dsquery Server -domain ad-training.loc
* dsquery server -hasfsmo (pdc|infr|rid|schema|name) (Подставить что-то одно)



1. Выясните, какие записи DNS появились с вводом нового контроллера домена.

* Таак, ну [тут](https://habr.com/ru/post/214439/) и [тут](https://www.wordpress-abc.ru/hosting/dns/dns-zapisi.html) можно почитать немного теории, чтоб хоть буквы примерно понимать
* [Здесь](http://onreader.mdl.ru/MasteringActiveDirectory.2ed/content/Ch04.html) теория для гигачадов
* Диспетчер серверов
* Управление
* DNS
* Шаримся, если есть желание, просто смотрим где примерно чего
* [Зоны обратного](https://serverspace.by/support/help/configuring-a-dns-server-on-windows-server-2012-or-later/) просмотра – пкм – создать
* Основная
* Для всех в домене (2 пункт)
* 4 версия
* Ставим 10.0.0
* Разрешить
* Готово
* .
* Прямая зона – наш домен
* Пкм – создать Узел (А или АААА)
* Имя как у первого сервака, без домена, его адрес
* Такой уже есть, так и надо, ок
* Аналогично со вторым серваком
* .
* Снова наша созданная обратная зона
* Пкм – перезагрузить – пкм- обновить
* Должны появиться указатели на контроллеры
* Обратная зона для того, чтобы можно было наоборот, по адресу восстановить имя контроллера
* Скриним записи в forestName
* Скриним записи в \_mscds.forestName
* Скриним записи в обратной зоне
* Если надо, я в своём отчете немного попытался теории раздобыть

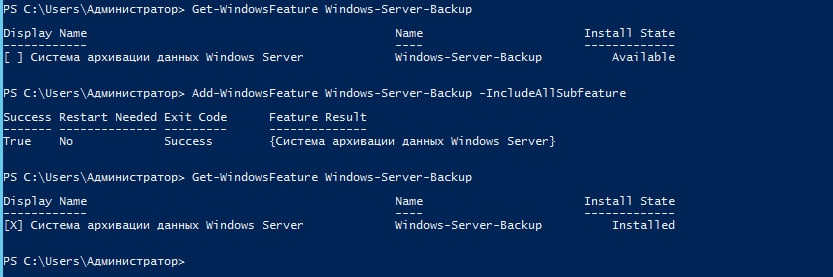
1. На контроллере ad-srv-2 создайте пользователя в AD. Убедитесь, что от имени этого пользователя можно запускать процессы на ad-client с помощью GUI, утилиты runas и PowerShell.

* На втором серваке создаем пользователя
* Видим его в пользователях на первом серваке
* Запускаем машину-клиента, входим там за созданного пользователя
* Проверяем какие-либо штучки

**Часть 4. Архивация Active Directory**

1. С помощью PowerShell [установите](https://winitpro.ru/index.php/2019/10/10/nastraivaem-backup-active-directory/) службу архивации windows на ad-srv.

* Get-WindowsFeature Windows-Server-Backup для проверки
* Если нет, то устанавливаем: Add-WindowsFeature Windows-Server-Backup –IncludeAllSubfeature



1. С помощью консольной утилиты [wbadmin](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/cc742124(v=ws.10)) создайте архивную копию ActiveDirectory.

* wbadmin start SystemStateBackup -backupTarget:[\\Desktop-ad-srv\sysvol](file:///\\Desktop-ad-srv\sysvol) -quiet
* (sysvol для примера, т.к. к ней есть сетевой доступ и она служебная)
* Получаем ошибку, скриним для отчета
* Идем в сетевые папки, sysvol
* Открываем ее свойства, безопасность, даем админам полный доступ (а то мы не можем, и там проблемы будут)
* Повершелл от имени админа
* wbadmin start SystemStateBackup -backupTarget:[\\Desktop-ad-srv\sysvol](file:///\\Desktop-ad-srv\sysvol) –quiet
* Кайфуем, скриним, типа мы умные

**Часть 5. Замена контроллера домена**

Реализуйте сценарий замены контроллера домена, при котором все роли и gc 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 gc на ad-srv-2 с помощью утилиты [ntdsutil](https://itsecforu.ru/2019/05/17/%E2%9C%94%EF%B8%8F-%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5-ntdsutil-%D0%B4%D0%BB%D1%8F-%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F-active-direct/), [PowerShell](https://winitpro.ru/index.php/2012/03/06/peredacha-rolej-fsmo/) или [GUI](http://pyatilistnik.org/kak-peredat-fsmo-roli-drugomu-kontrolleru-domena-active-directory/). Убедитесь, что перенесен и DNS.

* Я выбрал PowerShell ([command](https://learn.microsoft.com/ru-ru/powershell/module/activedirectory/move-addirectoryserveroperationmasterrole?view=windowsserver2022-ps))
* netdom query fsmo
* Второй сервер, то есть тот, кому мы даем роли
* Повершелл от имени админа

**Move-ADDirectoryServerOperationMasterRole -Identity \_имяСервака\_ -OperationMasterRole 0,1,2,3,4**

* netdom query fsmo
* Идем в DNS второго сервера и убеждаемся, что записи те же

1. Подготовьте описание процесса для отчета.
2. С помощью утилиты dcdiag проверьте AD на ошибки.

* Чтобы получить состояние всех контроллеров домена, воспользуемся dcdiag /s:ad-training.loc /a (ну или просто dcdiag)
* Молимся, что ошибок нет
* У меня в начале было много, пару раз назад по снапшотам откатился, в итоге всего 2 ошибки

1. С помощью PowerShell установите, на каком контроллере домена функционируют FSMO

* netdom query fsmo

1. [Удалите](https://winitpro.ru/index.php/2022/01/13/udalenie-kontrollera-domena-active-directory/) роль AD DS на ad-srv. Перегрузите компьютер.

* На первом серваке **Test-ADDSDomainControllerUninstallation**, если успешно, значит можно удалять
* Диспетчер серверов
* Удалить роли
* Первый сервак
* Удаляем AD DS и его компоненты
* Ошибка – надо понижать роль
* Понижаем
* Наша учетка по умолчанию, хорошо, далее
* Ставим галочку на продолжении
* Ставим новый пароль
* Понижаем, комп перезагрузится
* Входим на локального админа первого сервера с новым паролем
* Снова удаляем роль AD DS и его компоненты
* Смотрим через «пользователи и компьютеры» на первом серваке, все как надо

1. С помощью утилиты dcdiag проверьте AD на [ошибки](https://www.youtube.com/watch?v=HelwL9XHvQk).
2. 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: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 5)