ПРАКТИЧЕСКАЯ РАБОТА №3

Основы работы с Active Directory в Windows Server.

Цель работы: Получить базовые навыки развертывания службы каталогов Active Directory на основе Windows Server, управления объектами AD, их правами и групповыми политиками.

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:

Для централизованного управления ресурсами сети применяют распределенные системы – службы каталогов. Эти системы позволяют хранить данные об объектах и субъектах безопасности в специализированной распределенной, защищенной базе данных - службе каталогов. На рынке существуют несколько популярных служб каталогов. Например, Novell eDirectory, OpenLDAP и Microsoft Active Directory (далее AD). Последняя является службой каталогов для сетей Windows. Структурно AD построена по принципу DNS и имеет подобную древовидную структуру. Сама AD использует механизмы DNS для поиска служб и организации взаимодействия компонентов сервиса.

Доступ к объектам каталога осуществляется по протоколу LDAP. В службах каталогов присутствуют объекты двух типов - контейнеры и листья (по ассоциации с деревом).

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.

Домены и другие контейнеры предназначены для объединения других объектов и распространения групповых политик. Групповые политики это шаблоны, которые накладываются на реестр Windows и применяются для ассоциированных с ними объектов. Так, если в домене firma.loc создан Organization Unit с именем dev , а в нем пользователь supervisor, то при регистрации пользователя supervisor к его рабочей станции применяются среди прочих, групповые политики, привязанные к контейнеру dev.

Для управления объектами AD используются средства GUI, консольные утилиты dsquery, dsmod, dsadd, dsrm, dsget и набор командлетов Power Shell.

Для разграничения прав на доступ к файловым объектам на платформе Windows используется механизм ACL в файловой системе NTFS, в которой реализована возможность достаточно гибкого управления правами доступа к файлам и каталогам.

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.
2. Дистрибутивы операционных систем со сроком действия 90 дней можно скачать с сайта Microsoft Evaluation Center (https://www.microsoft.com/ru-ru/evalcenter).
3. Установите операционные системы, сделайте снапшоты машин. Переименуйте виртуальные машины в ad-srv, и ad-client соответственно версии операционной системы.
4. 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 адресе самого сервера.

Часть 2. Развертывание Active Directory

1. 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.
2. После установки перезагрузить компьютер.
3. Установить DHCP-сервер и произвести его настройку (использовать адресный пул 10.0.0.100-10.0.0.110, обеспечьте получение клиентами адреса DNS и шлюза равных адресу сервера). Проведите авторизацию DHCP сервера. После установки перезагрузить компьютер.
4. Убедитесь, что компьютер ad-client получил необходимую

конфигурацию ip. Подключите компьютер ad-client к домену.

5. Войдите на ad-client с учетной записью администратора домена.
6. На контроллере домена ad-srv в оснастке «Active Directory пользователи и компьютеры» найдите объект компьютера ad-client и компьютера ad-srv.

Часть 3. Объектами AD и правами на NTFS и SMB.

1. Используя административную оснастку «Active Directory пользователи и компьютеры», создайте в новом домене 2 подразделения (Organization Unit): ouSellers, ouManagers. В каждом подразделении создайте пользователя: uSeller1, uManager1 и группы gSellers и gManagers.
2. На сервере на диске C:\ создайте каталог «AllUsers» и дайте всем пользователям домена право на чтение этого каталога. В нем создайте каталоги Sellers и Managers, дайте членам групп gSellers и gManagers все права на уровне NTFS для соответствующих каталогов кроме возможностей изменения прав и удаления самих каталогов. При этом следует сохранить возможность создавать, удалять и модифицировать файлы и каталоги внутри самих каталогов. Создайте каталог AllUsers\BlackHole, в который пользователи созданных групп смогли бы копировать файлы "drag-and-drop", но не просматривать содержимое. Создайте каталог AllUsers\Common, в который все пользователи домена смогли бы писать файлы, но удалять смогли бы только свои. Открыть общий доступ через сеть к каталогу AllUsers с необходимыми разрешениями и назначить сетевое имя AllUsersCom.
3. На диске C: сервера создайте папку UsersHome. Для каждого созданного в п. 1 части 3 пользователя создайте домашнюю папку c:\UsersHome\”имя пользователя“. Обеспечьте пользователю возможность записи через сеть (протокол SMB) в свой домашний каталог, причем имя сетевой папки должно быть скрытым, т.е. при просмотре списка папок компьютера в «Сетевом окружении» папку не

должно быть видно.

4. В свойствах каждого пользователя задайте подключение домашней папки на диск X: и место хранения перемещаемого профиля. Обратите внимание на то, что необходимо использовать сетевые пути UNC.
5. Используя машину «Ad-client», авторизуйтесь в системе под пользователем uSeller1, перегрузить клиентский компьютер, выполнить повторную аутентификацию и изучить данные в каталоге x:_profile.

Часть 4. Работа с групповыми политиками.

1. С помощью консоли Управление групповой политикой измените групповую политику домена, так чтобы пароли могли быть длиной 6 символов без контроля сложности.

   Примечание: После создания необходимо принудительно обновить групповую политику командой gpupdate.
2. Создайте групповую политику для контейнера ouSellers, с помощью которой будет:
   a. Запрещен доступ к Панели управления,
   b. Установлена блокировка экрана при периоде неактивности 1 минута, с отключением возможности менять этот параметр.
   c. Запретить пользователю редактировать реестр
   d. Скрыть в проводнике диск C:
3. Создайте групповую политику в контейнере ouManagers, которая будет определять приложения, которые может запускать пользователь:
   a. Paint;
   b. calc;
   c. Notepad.
4. Создайте контейнер для объектов – компьютеров и создайте в нем групповую политику, которая:
   a. отключает сбор и передачу в Microsoft сообщений об ошибках,
   b. отключит локальные учетные записи Администратор

(Administrator)

c. запретит пользователю пользоваться механизмом Offline Files
d. установит на клиентских компьютерах для всех файловых объектов на диске C:\ следующий ACL (Администраторы, Система – полный доступ, Пользователи домена – чтение, просмотр каталогов, выполнение файлов).

5. Создайте отдельную групповую политику с помощью которой разверните на клиентском компьютере программу 7-zip (инсталлятор MSI).
6. Проверьте функционирование политик.

Часть 5. Автоматизация работы с объектами AD

1. Напишите скрипт на PowerShell, получающий в качестве параметра путь к CSV файлу, содержащему:
    a. ФИО пользователя,
    b. Должность
    c. Название отдела
    d. E-mail
    e. Телефон
    f. Логин
    g. Пароль
    h. Имя контейнера, в который надо поместить пользователя
    i. Список групп, в которые нужно поместить пользователя
    j. Путь до домашней папки (подключается на диск X:).
    k. Путь до перемещаемого профиля.
2. Скрипт читает файл и создает необходимые объекты.
3. Существование групп и контейнеров необходимо проверять и создавать их в случае отсутствия.
4. Формирует в формате HTML отчет в котором указано сколько и каких

групп, контейнеров и пользователей создано.

5. Все объекты создаются в домене, в котором запущен скрипт.

Часть 6. Восстановление удаленных объектов

1. Включите корзину AD (с помощью PowerShell или Центра администрирования AD).
2. С помощью скрипта из части 5 создайте 5 пользователей в контейнере unit-for-delete.
3. С помощью команд dsquery и dsrm удалите всех пользователей в контейнере unit-for-delete.
4. С помощью PowerShell восстановите всех удаленных пользователей в контейнере unit-for-delete.

Содержание отчета

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

Вопросы:

1. Раскройте смысл терминов дерево доменов, лес и схема Active Directory?
2. Где на контроллере домена хранится данные об объектах Active Directory в виде файлов? Какие файлы за что отвечают?
3. Где на контроллере домена хранятся файлы, содержащие групповые политики домена?
4. Какие компоненты устанавливаются мастером при добавлении ролей Active Directory?
5. Для чего нужен пароль DSRM?
6. Как восстановить пароль DSRM, если он был утерян после установки?
7. Зачем нужно имя домена NetBIOS?
8. Какие группы пользователей создаются в AD автоматически? Опишите минимум 10 из них.

9. Какие записи в DNS создаются специально для AD? Перечислите их, укажете их назначение.

Артефакты:

1. Приведите скриншоты групповых политик AD из части 4.
2. Приведите скрипт из части 5.
3. Как с помощью Powershell восстановить удаленный объект AD?
4. Приведите конвейер команд из ч.6 п.3
5. Приведите конвейер команд из ч.6 п.4

Отчет выслать в течении 2-х недель на адрес edu-net@yandex.ru.

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 4)