Практическая работа №10

Основы работы с Active Directory

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

Необходимо:

1) компьютер с установленной системой VirtualBox,
2) установленная в VirtualBox операционная система Windows 2003 Standard или старше,
3) учетная запись пользователя с правами администратора,
4) справочная система MS Windows,
5) дистрибутив установленной ОС Windows Server.

Краткие теоретические сведения

Для централизованного управления ресурсами сети среди прочих применяют распределенные системы – службы каталогов. Эти системы позволяют хранить данные о 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 объектов.

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 для ассоциированных с ними объектами. 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 консольные утилиты dsquery, dsmod, dsadd, dsrm, dsget идр.

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. В качеств источников SID для ACL может выступать AD. В MS Windows реализованы две отдельных схемы контроля доступа к файлам и каталогам:

- контроль доступа к файлам и каталогам на уровне файловой системы

- контроль доступа к каталогам по сети (sharing).

В первом случае контроль осуществляется системой на основе записей в ACL (Access Control List) привязанных к файлам и каталогам. Права назначаются в Explorer (контекстное меню – Общий доступ и безопасность… закладка Безопасность). Существует возможность назначить сгруппированные права (они перечислены в закладке Безопасность) и подробные права (список доступен через кнопку Дополнительно).

Права, по умолчанию, наследуются от родительского каталога к вложенным файлам и к каталогам. Наследование можно отключать. По каждому праву можно установить разрешение и прямой запрет.

Подробное описание прав можно найти в справке Windows.

Существуют консольные утилиты управления сетевым доступом и ACL NTFS (net share, cacls, xcacls из пакета support tools и д.р.).

Пакетное управление объектами AD и правами доступа к файловым объектам реализуется так же с помощью PowerShell.

Порядок выполнения работы:

1) Создать две копии виртуальной машины с Windows Server – ADServ и ADClient.
2) Для виртуальной машины «ADServ» следует использовать IP 11.0.0.1 и MASK 255.255.255.0 и имя компьютера ADServ. В качестве типа подключения сетевого адаптера виртуальной машины использовать режим «Внутренняя сеть».
3) В виртуальной машине «ADClient» конфигурацию IP получать автоматически. Задать имя компьютера ADClient. В качестве типа подключения сетевого адаптера виртуальной машины использовать режим «Внутренняя сеть»
4) Если одна виртуальная машина является копией другой, или они обе являются копией третьей машины, то из-за совпадения SID компьютров использовать их в пределах одного домена будет невозможно. Для изменения SID машины ADClient используйте или утилиту sysprep или утилиту new_sid.
5) Сделайте снимки виртуальных машин.
6) Подготовьте компьютер «ADServ» к развертыванию AD (новый домен, новый лес) с установкой DNS на «ADServ». С помощью мастера установки AD (dcpromo.exe) развернуть домен с именем: «ваша_фамилия».local. После установки перезагрузить компьютер.
7) Установить DHCP-сервер и произвести его настройку (использовать адресный пул 11.0.0.100-11.0.0.110, обеспечьте получение клиентами адреса DNS и шлюза равных адресу сервера). Проведите авторизацию DHCP сервера. После установки перезагрузить компьютер.
8) Используя административную оснастку «Active Directory Users and Computers», создать в новом домене 2 подразделения (Organization Unit): ouSellers, ouManagers. В каждом подразделении создать пользователя: uSeller1, uManager1 и группы gSellers и uManagers.
9) На сервере на диске C:\ создать каталог «AllUsers» и дать всем пользователям домена право на чтение этого каталога. В нем создать каталоги Sellers и Managers, дать 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. Создать каталог AllUsers\BlackHole, в который пользователи созданных групп смогли бы копировать файлы "drag-and-drop", но не просматривать содержимое. Создать каталог AllUsers\Common, в который все пользователи домена смогли бы писать файлы, но удалять смогли бы только свои. Открыть общий доступ к каталогу AllUsers с необходимыми разрешениями и назначить сетевое имя AllUsersCom.

10) На диске C: сервера создайте папку UsersHome. Для каждого созданного в п. 8 пользователя создайте домашнюю папку c:\UsersHome\"имя пользователя". Обеспечите 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.
11) В свойствах каждого пользователя задать подключение домашней папки на диск X: и место хранения перемещаемого профиля. Обратите внимание, что надо использовать сетевые пути UNC.
12) Включите машину «ADClient», убедитесь, что получены параметры IP и подключить компьютер к созданному домену
13) Используя машину «ADClient», авторизоваться в системе под пользователем uSeller1, перегрузить клиентский компьютер, выполнить повторную аутентификацию и изучить данные в каталоге x:_profile.
14) Измените групповую политику домена, так чтобы пароли могли быть длиной 6 символов без контроля сложности. Для удобства управления групповыми политиками можно установить консоль GPMC.
15) Создать групповую политику для контейнера ouSellers, с помощью которой будет:
    - Запрещен доступ к Панели управления,
    - Установлена блокировка экрана при периоде неактивности 1 минута, с отключением возможности менять этот параметр.
    - Запретить пользователю редактировать реестр
    - Скрыть в проводнике диск C:

    Примечание: После создания необходимо принудительно обновить групповую политику командой gpupdate.
16) Создать групповую политику в контейнере ouManagers, которая будет определять приложения, которые может запускать пользователь:
    - Paint;
    - IE;
    - Notepad.
17) Создать контейнер для объектов – компьютеров и создать в нем групповую политику, которая:
    - отключает сбор и передачу в Microsoft сообщений об ошибках,
    - отключит локальные учетные записи Администратор (Administrator)
    - запретит пользователю пользоваться механизмом Offline Files
    - установит на клиентских компьютерах для всех файловых объектов на диске C:\ следующий ACL (Администраторы, Система – полный доступ, Пользователи домена – чтение, просмотр каталогов, выполнение файлов).

18) Создайте отдельную групповую политику с помощью которой разверните на клиентском компьютере программу 7-zip (инсталлятор MSI).
19) Произвести архивацию базы данных AD.
20) Напишите скрипт, получающий в качестве параметров имя пользователя, пароль и признак целевого контейнера (например «M» для ouManagers) и выполняющий следующие действия:
    - Создает пользователя в соответствующем контейнере,
    - Создает на контроллере домена в папке C:\ UsersHome каталог с именем равным имени пользователя (будущий домашний каталог),
    - Дает пользователю права NTFS на его каталог кроме права изменения прав
    - Открывает доступ пользователю к этому каталогу через сеть (протокол SMB) с скрытым именем общей папки,

- Настраивает подключение домашнего каталога пользователя на диск W:
- Настраивает хранение профиля пользователя в его домашнем каталоге в папке _profile
- Требует от пользователя смены пароля при первом входе в систему
- Включает пользователя в группу gSellers или gManagers (согласно выбранному контейнеру)

В отчет:

В отчет представить

1) Скрипт из задания 20.
2) Перечень установленных групповых политик в виде скриншотов окон консолей конфигурации.
3) Консольный вывод команды xcacls для подкаталогов каталога AllUsers.

Ответы на вопросы:

4) раскройте смысл терминов дерево доменов, лес и схема Active Directory?
5) перечислите роли контроллера домена и их назначение.
6) как с помощью команды DSMOD изменить пароль пользователю?
7) где на контроллере домена хранятся файлы, содержащие групповые политики домена?
8) где на контроллере домена хранится данные об объектах Active Directory в виде файлов?
9) какие виды групп в Active Directory существуют?
10) в чем отличие групп от контейнеров?
11) что такое авторизация DHCP сервера? Для чего она выполняется?

Отчет выслать в течении 2-х недель после выполнения работы. Еще одна неделя отводится на ответы на возможные вопросы и исправления.