ПРАКТИЧЕСКАЯ РАБОТА №2

# 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 R2/2016/2019.**
* 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 сроиться 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](https://info.microsoft.com/ww-landing-windows-10-enterprise.html).
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](http://slusar.su/nastroyka-seti-mezhdu-virtualnymi-ma/). Для сервера сделайте ip адрес сети 10.0.0.0/8 (маска длины 8 -> 11111111.00000000. 00000000. 00000000 –> 255.0.0.0).
5. В качестве DNS сервера (обоих) установите адрес самого сервера.

**Часть 2. Развертывание Active Directory**

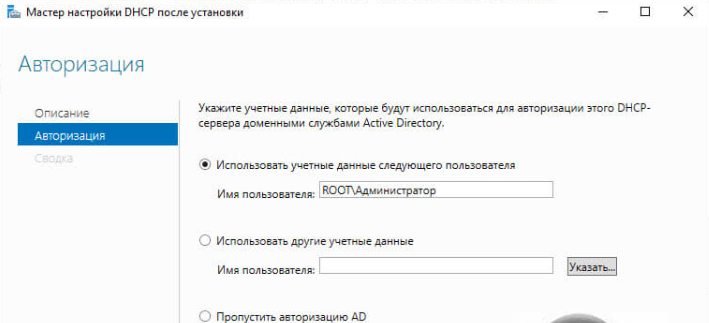
1. Подготовьте компьютер «AD-Srv» к развертыванию AD (новый домен, новый лес) с установкой DNS на «Ad-srv». С помощью мастера добавления ролей и компонентов и диспетчера серверов развернуть домен с именем: «ваши\_FIO».local. Автоматически установите и настройте DNS.

* Диспетчер серверов (приложение с чемоданом около пуска)
* (справа сверху) Управление
* Добавить роли и компоненты
* Перед началом работы – далее
* Установка ролей или компонентов
* Выбор сервера – у нас он 1 – далее
* Доменные службы AD, там предложит установить и дополнения, ставим и их тоже
* Компоненты – ничего не надо – далее
* Подтверждаем и устанавливаем
* там справа сверху флажочек
* Поднять роль этого сервера до контроллера доменов
* Создать новый лес, имя домена = «ваши\_FIO».local - далее
* Пишем пароль для восстановления, на всякий случай запоминаем его
* DNS – далее (там предупреждение будет, ничего страшного)
* NetBIOS – это чисто для обратной совместимости с динозаврами, просто оставляем как есть
* Пути, на всякий, не трогаем, далее
* Подтверждаем, устанавливаем

1. После установки перезагрузить компьютер.
2. Автоматически установите и настройте [DNS](https://info-comp.ru/sisadminst/411-dns-server-win-2012-r2.html).

* справа сверху управление
* добавить роли и компоненты
* Роли - DNS

1. Установить [DHCP-сервер](https://info-comp.ru/sisadminst/408-dhcp-win-server-2012-r2.html) 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



(**Если вы устанавливаете роль DHCP на контроллере домена, сервер автоматически авторизуется. Если вы устанавливаете его на рядовой сервер, вам нужно будет вручную выполнить процесс авторизации одним из способов в ссылке**).

После установки перезагрузить компьютер.

1. Убедитесь, что компьютер ad-client получил необходимую конфигурацию ip ([powershell] ipconfig /all, там адрес должен быть в диапазоне).

Подключите компьютер ad-client к домену.

* Настройки
* Система
* О программе (вниз)
* Переименовать ПК
* Изменить
* Является членом домена (ваше имя домена)
* Вводим имя пароль уполномоченного сервера! (Администратор, пароль\_от\_него) (п6)
* Перезагружаем комп

1. Войдите на ad-client с учетной записью администратора домена.
2. 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 С:\ создайте каталог «AllUsers» и дайте всем пользователям домена [право](https://windowsnotes.ru/other/nastrojka-razreshenij-fajlovoj-sistemy-ntfs/) на чтение этого каталога.

(По идее, по умолчанию, но я создал еще OU и Групповую политику для него, в которой можно открывать этот файл)

* ПКМ на папку
* Свойства
* Безопасность
* Дополнительно
* Тут уже лазийим и добавляем что надо

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.

Например:

* Добавить
* Выберите субъект
* gManagers
* Только для этой папки
* Содержимое, Чтение, чт и выполнение, Запись
* Ок
* Добавить
* gManagers
* Только для подпапок и файлов
* Изменение
* Ок

Создайте каталог AllUsers\BlackHole, в который пользователи созданных групп смогли бы копировать файлы "drag-and-drop", но не просматривать содержимое.

* (если не создавать группу, а прям пользователям домена, то выключить сначала наследование от C:\AllUsers, потом уже изменить)
* Create files / write data (Создание файлов / запись данных)

*Create files / write data (Создание файлов / запись данных) — это разрешение дает пользователю право создавать файлы в папке, не имея прав доступа к самой папке. Т.е. можно копировать в папку файлы и создавать новые, но нельзя просматривать содержимое папки и открывать\изменять уже имеющиеся файлы. После добавления пользователь уже не сможет изменить файл, даже будучи его владельцем;*

Создайте каталог AllUsers\Common, в который все пользователи домена смогли бы писать файлы, но удалять смогли бы только свои.

* Пользователям можно писать
* СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ может удалять (ну там по умолчанию полный доступ, так что я просто его убрал, оставив только изменение)

Открыть общий доступ через сеть к каталогу AllUsers с необходимыми разрешениями и назначить сетевое имя AllUsersCom.

* AllUsers ПКМ
* Настроить папку или свойства
* Безопасность – выставляем права
* Доступ – расширенная настройка
* имя AllUsersCom, выставляем разрешения

1. 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.

* **Пока под вопросом, я не уверен**
* c:\UsersHome\uSeller1$ (имя папки нужно заканчивать $, чтобы она не была видна в сетевых папках, но чел ее видит)
* Свойства
* Безопасность – выставляем [права](#Права_на_изм_подпапок_запись_текущей), чтобы он мог писать в папку, но не удалять, изменять подпапки и файлы
* Открываем доступ
* Проверяем права, вдруг изменились

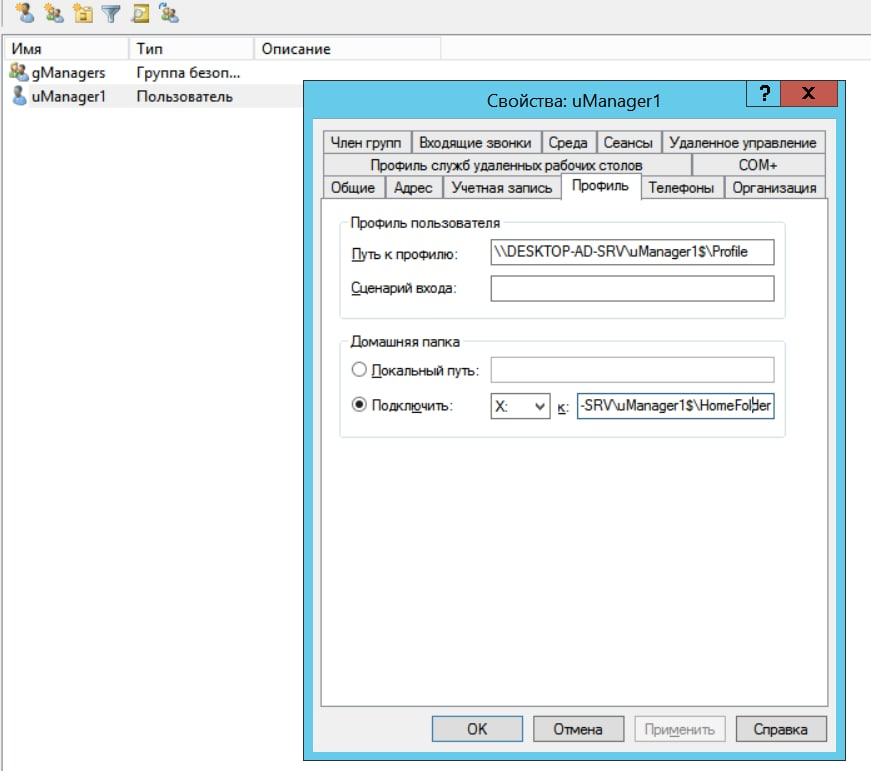
1. В свойствах каждого пользователя задайте подключение домашней папки на диск X:

* Свойства пользователя
* Профиль
* Домашняя папка, подключить X: в нужное место, я выбрал [\\SRV/uSeller1/HomeFolder](file:///\\SRV/uSeller1/HomeFolder)

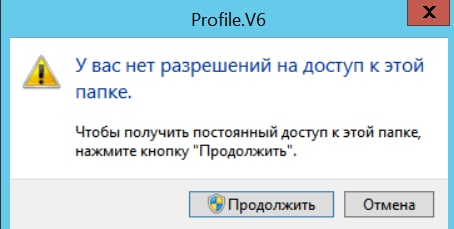
и [место хранения](https://www.youtube.com/watch?v=BjDJrxtSkQE) перемещаемого профиля:

* АААА, я смог, bitch!
* Свойства пользователя
* Профиль
* Путь к профилю, тут указываем где создастся папка с его профилем, когда он первый раз выйдет из системы, там будут все его файлы. Я использовал

[\\SRV\uSeller1\profile](file:///\\SRV\uSeller1\profile)



* Теперь заходим под этим пользователем, создаем че-нить рабочем столе, выходим из системы
* И вот теперь на сервере в папке появился profile.V6 (V6, как я понял, это использующий протокол SMB 6 версии, так надо)
* Попытаемся зайти в него, нам откажут в доступе, ну оно и правильно



* Продолжить
* Безопасность
* Дополнительно
* Владелец – изменить, ставим Администратор - применить
* Закрываем
* Снова открываем профиль, видим его папки)
* Может снова попросить поменять безопасность для рабочего стола, но в итоге все видим)

Обратите внимание на то, что необходимо использовать [сетевые пути UNC](https://learn.microsoft.com/ru-ru/dotnet/standard/io/file-path-formats).

1. Используя машину «Ad-client», авторизуйтесь в системе под пользователем uSeller1, перегрузить клиентский компьютер, выполнить повторную аутентификацию и изучить данные в каталоге x:\\_profile.

* Ну мы это только что делали, см предыдущий пункт

**Часть 4. Работа с групповыми политиками.**

1. С помощью консоли Управление групповой политикой измените [групповую политику](https://winitpro.ru/index.php/2018/10/26/politika-parolej-uchetnyx-zapisej-v-active-directory/) домена, так чтобы пароли могли быть длиной 6 символов без контроля сложности.

*Примечание: после создания политики она применяется не мгновенно, а согласно периоду обновления, заданному политикой домена. Для принудительного обновления политики можно использовать команду gpupdate.*

1. Создайте групповую политику для контейнера ouSellers, с помощью которой будет:
   1. Запрещен [доступ к Панели управления](https://windows-school.ru/blog/kak_zapretit_dostup_k_nastrojkam/2019-05-07-383),
   2. Установлена [блокировка экрана](https://winitpro.ru/index.php/2020/09/10/blokirovka-ekrana-pri-neaktivnosti-gpo/) при периоде неактивности 1 минута, с отключением возможности менять этот параметр.
   3. Запретить пользователю редактировать [реестр](https://windows-school.ru/blog/kak_zakryt_dostup/2019-04-19-362)
   4. [Скрыть](https://windows-school.ru/blog/kak_skryt_disk_v_windows_nevidimyj_razdel/2013-03-14-55) в проводнике диск C:
2. Создайте групповую политику в контейнере ouManagers, которая будет определять [приложения](https://geekteam.pro/kak-razreshit-zapusk-tolko-opredelennyih-programm-v-windows-10-8-1-8-7/), которые может запускать пользователь:
   1. Paint;
   2. calc;
   3. Notepad.
3. Создайте контейнер для объектов – компьютеров и создайте в нем групповую политику, которая:
   1. [отключает](https://dzen.ru/media/nastroyka1c/kak-otkliuchit-funkcii-sbora-i-otpravki-otchetov-os-windows-5e7aeb5e4432af1a9b9433a2) сбор и передачу в Microsoft сообщений об ошибках,
   2. отключит локальные учетные записи [Администратор](http://pyatilistnik.org/kak-otklyuchit-vstroennuyu-uchetnuyu-zapis-administrator-s-pomoshhyu-gruppovoy-politiki-gpo-v-windows-server-2008r2-2012r2/) (Administrator)
   3. запретит пользователю пользоваться механизмом Offline Files
   * Конфигурация компьютера
   * Политики
   * Шаблоны
   * Сеть
   * Автономные файлы
   * Разрешить или запретить использование автономных файлов – отключить
   1. [установит](https://system-administrators.info/?p=1430) на клиентских компьютерах для всех файловых объектов на диске C:\ следующий ACL (Администраторы, Система – полный доступ, Пользователи домена – чтение, просмотр каталогов, выполнение файлов).
      * Конфигурация компьютера
      * Политики
      * Конфигурация Windows
      * Параметры безопасности
      * Файловая система – ПКМ – добавить файл
      * Указываем путь (у нас просто диск С: )
      * Настраиваем права
      * (Там, по идее, по умолчанию и так все подходит, поэтому я просто удалил лишнее)
4. [Создайте](https://winitpro.ru/index.php/2011/10/21/ustanovka-programm-s-pomoshhyu-gruppovyx-politik/) отдельную [групповую](http://forum.oszone.net/post-1931091.html) политику с помощью, которой разверните на клиентском компьютере программу 7-zip (инсталлятор MSI).

* Конфигурация компа
* Конфигурация программ
* Установка программ
* Пкм – создать – пакет
* Ищем скачанный msi программы (<https://www.7-zip.org/a/7z2201-x64.msi>)
* (Надо положить msi установщик туда, где у всех будет сетевой доступ, я положил в [\\SRV\AllUsersCom\Common](file:///\\SRV\AllUsersCom\Common))
* Развертывание = Особый
* Пишем название ( у меня «7-Zip client (x64 edition)» )
* Во вкладке «Развертывание» жмем «дополнительно – Не использовать языковые установки» (это позволит игнорировать язык Windows на компьютерах клиентов)
* (на всякий случай)
* Конфигурация компа
* Конфигурация винды
* Сценарии
* Автозагрузка
* Показать файлы
* Создаем cmd файл со строкой:

REG DELETE "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\7-zip" /f

(это, по идее, для того, чтобы убирать [старую версию](http://forum.oszone.net/post-1931091.html) программы, если она уже была скачана, например, вручную, но это не точно)

1. Проверьте функционирование политик.

**Часть 5. Автоматизация работы с объектами AD**

1. Напишите [скрипт на PowerShell](https://github.com/TungFram/Winda-lab-2/blob/main/script51.ps1), получающий в качестве параметра путь к CSV файлу, содержащему:

([Значения атрибутов](https://notessysadmin.com/main-attributes-active-directory), помогло немного)

* 1. ФИО пользователя,
  2. Должность
  3. Название отдела
  4. E-mail
  5. Телефон
  6. Логин
  7. Пароль
  8. Имя контейнера, в который надо поместить пользователя
  9. Список групп, в которые нужно поместить пользователя
  10. Путь до домашней папки (подключается на диск X:).
  11. Путь до перемещаемого профиля.

1. Скрипт читает файл и создает необходимые объекты.
2. Существование групп и контейнеров необходимо проверять и создавать их в случае отсутствия.
3. Скрипт создает все необходимые каталоги, в случае их отсутствия, назначает [необходимые](https://activedirectoryfaq.com/2017/09/powershell-create-home-directory-grant-permissions/) [права NTFS](https://winitpro.ru/index.php/2019/04/22/ntfs-razresheniya-na-papki-powershell/) и включает сетевой доступ
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).

* Enable-ADOptionalFeature ′Recycle Bin Feature′ -Scope ForestOrConfigurationSet -Target ′корневой домен леса′

где, Target - это корневой домен леса

* Действие это необратимо, но нам насрать, подтверждаем

1. С помощью скрипта из части 5 создайте 5 пользователей в контейнере unit-for-delete.
2. С помощью команд dsquery и dsrm удалите всех пользователей в контейнере unit-for-delete.

* dsquery user "OU=unit-for-delete,DC=ad-training,DC=loc" | dsrm –noprompt

**[Выполнять в повершеле от имени админа!!]**

1. С помощью PowerShell восстановите всех удаленных пользователей в контейнере unit-for-delete.

* Get-ADObject -SearchBase 'CN=Deleted Objects,DC=ad-training,DC=loc' -Filter {isDeleted -eq $True -and lastKnownParent -eq 'OU=unit-for-delete,DC=ad-training,DC=loc'} -IncludeDeletedObjects | Restore-ADObject

**[Выполнять в повершеле от имени админа!!]**

**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?

* Дерево доменов – это пространство имен, которое формируется за счет нескольких доменов, использующих общую схему и конфигурацию Лес - это набор ссылочных объектов, который не формирует пространство имен, но содержит в себе несколько деревьев домена (или одно дерево) Схема AD - набор определений для классов, атрибутов и других объектов, которые могут существовать в лесу AD

1. Где на контроллере домена хранится данные об объектах Active Directory в виде файлов? Какие файлы за что отвечают?

* База данных Active Directory хранится в файле по имени Ntds.dit, который по умолчанию расположен в папке %systemroot %\NTDS. Эта папка содержит также следующие файлы. Edb.chk- файл контрольных точек, который указывает, какие транзакции из журналов регистрации были записаны в базу данных Active Directory.
* Edb.log- журнал регистрации текущих транзакций. Имеет фиксированную длину - 10 Мб.
* Edbxxxxx.log. После того как Active Directory проработала некоторое время, могут появиться один или более журналов, у которых часть имени файла, обозначенная как ххххх, представляется собой увеличивающийся шестнадцатеричный порядковый номер. Эти журналы являются предшествующими журналами; всякий раз, когда текущий журнал заполнен, он переименовывается в следующий предшествующий журнал, и создается новый журнал Edb.log. Старые журналы автоматически удаляются по мере того, как изменения, представленные в журналах, переносятся в базу данных Active Directory. Каждый из этих журналов также занимает 10 Мб.
* Edbtemp.log- временный журнал, который используется тогда, когда заполнен текущий журнал (Edb.log). Новый журнал создается под именем Edbtemp.log, в нем хранятся все транзакции, а затем журнал Edb.log переименовывается в следующий предшествующий журнал. Далее журнал Edbtemp.log переименовывается в журнал Edb.log.
* Resl.log и Res2.log— резервные журналы, которые используются только в ситуации, когда на жестком диске заканчивается свободное пространство. Если текущий журнал заполнен, а сервер не может создать новый журнал, потому что на жестком диске нет свободного пространства, сервер подавит любые транзакции Active Directory, находящиеся в настоящее время в памяти, использует место для резервных журналов, а затем завершит работу Active Directory. Размер каждого из этих журналов также 10 Мб.

1. Где на контроллере домена хранятся файлы, содержащие групповые политики домена?

* GP Container (контейнер в AD), GP Template (domain\Policies\SysVol)

1. Какие компоненты автоматически устанавливаются мастером при добавлении ролей Active Directory?

* Только один тип раздела приложений каталога создается в Active Directory по умолчанию — это раздел, предназначенный для службы сервера доменной системы имен (DNS - Domain Name System). При установке первой интегрированной (integrated) зоны Active Directory создаются прикладные разделы каталога ForestDnsZones и DomainDnsZones. Раздел приложений каталога может хранить любой тип объекта Active Directory, кроме участников безопасности. Кроме того, разделы приложений каталога создаются для управления процессом репликации данных, и ни один из объектов раздела приложений каталога не может реплицироваться в раздел GC.

1. Для чего нужен пароль DSRM?

* DSRM позволяет администратору AD чинить или восстанавливать базу данных при необходимости, а пароль к DSRM позволяет иметь доступ/бэкдор к базе данных в случае поломок, но не дает доступ к домену или службам

1. Как восстановить пароль DSRM, если он был утерян после установки?

* С помощью утилиты ntdsutil (start->run->ntdsutil, пишем set dsrm password). В DSMR пишем reset password on server servername (null для локального компьютера)

1. Зачем нужно имя домена NetBIOS?

* Это сабдомен домена, например test в test.com, NetBIOS нужен для избежания конфликтов имен и для сохранения обратной совместимости со старыми версиями

1. Какие группы пользователей создаются в AD автоматически? Опишите минимум 5 из них.

* Administrators - полный доступ к компьютеру без запрещений
* Guests - почти то же, что и Users, но больше ограничений, при выходе из профиля, данные о нем удаляются
* Users - члены этой группы не могут делать изменения с системой, могут запускать большинство
* DHCP Administrators - члены этой группы могут создавать, удалять и управлять разными областями scope’а сервера, включая права на восстановление и бэкап Dynamic Host Configuration Protocol
* Domain Controller - включает в себя все контроллеры домена в домене, новые контроллеры добавляются сюда автоматически

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

* A(Host)
* CNAME(alias)
* SRV(service location)

Артефакты:

1. Приведите скриншоты групповых политик AD из части 4.

* Управление групповой политикой
* Выбираем нужную
* Справа выбираем «Параметры», там все изменения
* Раскрываем значения
* Скриним

1. Приведите скрипт из части 5.
2. Как с помощью Powershell восстановить удаленный объект AD?

* Надо каким-либо способом выбрать нужный объект
* Восстанавливаем с помощью Restore-ADObject

1. Приведите конвейер команд из ч.6 п.3
2. Приведите конвейер команд из ч.6 п.4

Отчет выслать в течение 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 2)