

**МИНИСТЕРСТВО НАУКИ ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего
образования Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики**

Мегафакультет трансляционных информационных технологий

Факультет информационных технологий и программирования

Лабораторная работа №2

По дисциплине «Администрирование в ОС Windows Server»

**Выполнили студенты группы
М33081:**

Найман Егор

Кузнецова Алика

Мещеряков Никита

Проверил:

Папикян С. С.

САНКТ-ПЕТЕРБУРГ

2022

Ответы на вопросы:

1. Раскройте смысл терминов дерево доменов, лес и схема Active Directory?

Дерево домена - состоит из нескольких доменов, которые совместно используют общую схему и конфигурацию, формируя непрерывное пространство имен.

Active Directory — это набор из одного или нескольких деревьев.

Схема *Active Directory* используется совместно всеми доменами в пределах леса. *Схема* — это конфигурационная информация, которая управляет структурой и содержимым каталога.

Лес — это высший уровень логической иерархии *Active Directory*. Это полностью самостоятельную организацию *Active Directory*, которая имеет определенный набор атрибутов и является периметром безопасности организации. В состав леса могут входить как один, так и несколько доменов.

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

База данных Active Directory хранится на контроллере домена в файле NTFS. DIT, который находится в папке %SYSTEMROOT%\NTDS.

Название файла	Описание
NTDS.DIT	База данных Active Directory
EDD.CHK	Проверочный (checkpoint) файл
EDB.LOG	Журнал транзакций (событий). Все изменения, происходящие с каталогом Active Directory, содержатся в этом файле. Размер файла ограничивается 10 Мб.
EDBxxxx.LOG	Вспомогательные журналы событий, которые создаются, когда файл EDB.LOG уже достиг 10 Мб, а данные еще не выгружены в файл NTDS.DIT. Соответственно каждый файл занимает не более 10 Мб дискового пространства
RES1.LOG	Резервный файл журнала событий
RES2.LOG	Резервный файл журнала событий
TEMP.EDB	Временный журнал, который содержит информацию о событиях, происходящих в настоящий момент
HEMA.INI	Необязательный файл, используемый для инициализации файла NTDS.DIT во время загрузки контроллера домена

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

Файлы, которые содержат параметры политики («Шаблон групповой политики») расположены по пути C:\Windows\SYSTEM32\Policy\ на контроллере домена. Используя PowerShell Active Directory Get-ADObject , можно проверить наличие объекта групповой политики и его ключевые поля

4. 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.

5. Для чего нужен пароль DSRM?

Пароль DSRM требуется для входа на контроллер домена, если служба AD DS (Active Directory Domain Services) не запущена, либо потому что она была остановлена, либо потому что контроллер домена был запущен в режиме DSRM.

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

Восстановить пароль DSRM можно:

Зайдите в систему как администратор домена.

Нажмите Start, Run, затем наберите ntdsutil.

Вы увидите приглашение “ntdsutil:”.

Наберите “set dsrm password” и нажмите Ввод.

Программа выдаст “Reset DSRM Administrator Password:”.

Теперь наберите “reset password on server null“. Слово “null” означает, что сброс пароля будет производиться на локальном сервере.

После нажатия «Ввод» вы получите приглашение для ввода пароля, а затем — для его повторения.

Для выхода из ntdsutil после смены пароля администратора дважды введите «q».

Теперь вы можете перегрузить сервер и зайти в консоль восстановления или в режим восстановления Directory Services с новым паролем.

7. Зачем нужно имя домена NetBIOS?

Имя домена netbios нужно для обнаружения компьютеров в сети, построенной на базе TCP/IP и избежания конфликтов имён. Имя NetBIOS представляет собой 16-байтовый адрес, используемый для идентификации в сети ресурса NetBIOS.

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

Группы по умолчанию, такие как группа "Администраторы домена", — это группы безопасности, которые создаются автоматически при создании домена Active Directory.

Администраторы - Члены группы администраторов имеют полный и неограниченный доступ к компьютеру.

Издатели сертификатов - Члены группы издателей сертификатов имеют право публиковать сертификаты для объектов пользователей в Active Directory.

Администраторы домена - имеют право администрировать домен. По умолчанию группа "Администраторы домена" входит в группу "Администраторы" на всех компьютерах, присоединенных к домену, включая контроллеры домена. По умолчанию является владельцем любого объекта, созданного в Active Directory для домена любым участником группы. Если члены группы создают другие объекты, такие как файлы, владелец по умолчанию — это группа "Администраторы". Управляет доступом ко всем контроллерам домена в домене и может изменять членство всех административных учетных записей в домене.

Гости домена - включает встроенную гостевую учетную запись домена. Когда члены этой группы входят в систему как локальные гости на компьютере, присоединенном к домену, на локальном компьютере создается профиль домена.

Пользователи домена - включает все учетные записи пользователей в домене. При создании учетной записи пользователя в домене она автоматически добавляется в эту группу.

Гости - имеют тот же доступ, что и члены группы "Пользователи" по умолчанию, за исключением того, что у гостевой учетной записи есть дополнительные ограничения. По умолчанию единственным членом является гостевая учетная запись. Группа гостей позволяет случайным или

одноразовым пользователям входить с ограниченными привилегиями во встроенную гостевую учетную запись компьютера.

Пользователи - не могут вносить случайные или преднамеренные системные изменения. Члены этой группы могут запускать большинство приложений. После первоначальной установки операционной системы единственным членом является группа прошедших проверку подлинности пользователей. Когда компьютер присоединяется к домену, группа "Пользователи домена" добавляется в группу "Пользователи" на компьютере.

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

В AD и интегрированном DNS все устройства будут иметь некую запись A или AAAA

A-запись (Address record) - указывает на конкретный IP-адрес домена. Без нее сайт работать не будет. По этой записи система определяет к какому серверу обращаться за получением информации, когда пользователь вводит название сайта в адресную строку веб-браузера.

AAAA-запись (Address record to IPv6) — аналог предыдущей A-записи. В значении указывается внешний IP-адрес в формате IPv6.

CNAME(alias) - это тип записи DNS, которая привязывает псевдоним к действительному (каноническому) доменному имени.

SRV(service location) - стандарт в DNS, определяющий местоположение, то есть имя хоста и номер порта серверов для определённых служб.

Артефакты:

3. ouManagersPolicy

ouManagersPolicy
Данные собраны: 29.10.2022 8:45:05 показать все

Область Сведения **Параметры** Делегирование

Общие скрыть

Подробности показать

Ссылки показать

Фильтрация ограничений безопасности показать

Делегирование показать

Конфигурация компьютера (включено) скрыть

Параметры не заданы.

Конфигурация пользователя (включено) скрыть

Политики скрыть

Административные шаблоны скрыть

Определения политик (ADMX-файлы) получены с локального компьютера.

Система скрыть

Политика	Параметр	Примечание
Выполнять только указанные приложения Windows	Включено	
<div> <div>Список разрешенных приложений</div> <div> Paint Notepad calc </div> </div>		

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

4. pcsPolicy

pcsPolicy

Область Сведения **Параметры** Делегирование

Конфигурация компьютера (включено) скрыть

Политики скрыть

Конфигурация Windows скрыть

Параметры безопасности скрыть

Локальные политики/Параметры безопасности скрыть

Учетные записи скрыть

Политика	Параметр
Учетные записи: Состояние учетной записи 'Администратор'	Отключено

Файловая система скрыть

%SystemDrive% скрыть

Настройка этого файла или папки и распространение наследуемых разрешений на все вложенные папки и файлы

Владелец

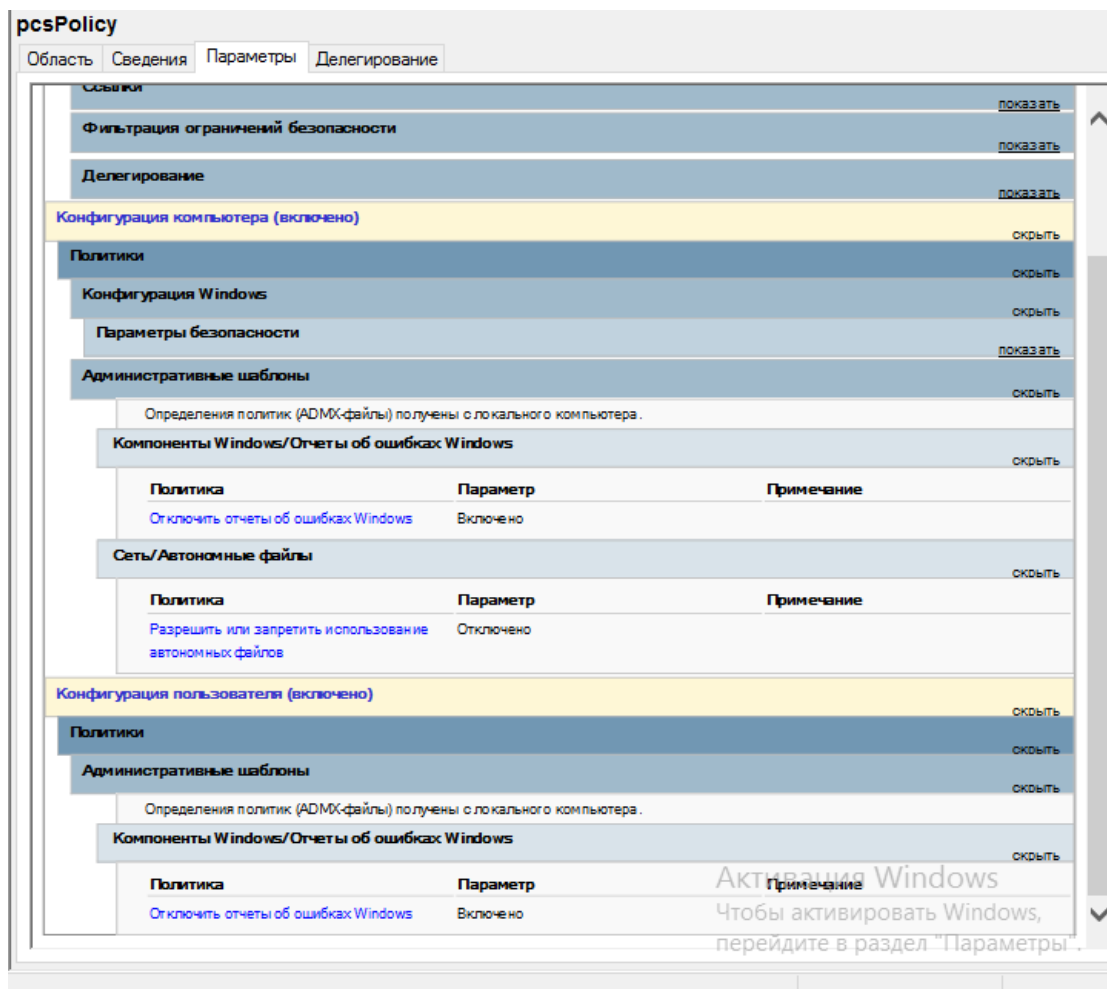
Разрешения

Тип	Имя	Разрешение	Применять к
Разрешить	ЦЕНТР ПАКЕТОВ ПРИЛОЖЕНИЙ\ВСЕ ПАКЕТЫ ПРИЛОЖЕНИЙ	Чтение и выполнение	Для этой папки, вложенных папок и файлов
Разрешить	СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ	Полный доступ	Для этой папки, вложенных папок и файлов
Разрешить	NT AUTHORITY\СИСТЕМА	Полный доступ	Для этой папки, вложенных папок и файлов
Разрешить	BUILTIN\Администраторы	Полный доступ	Для этой папки, вложенных папок и файлов
Разрешить	BUILTIN\Пользователи	Чтение и выполнение	Для этой папки, вложенных папок и файлов

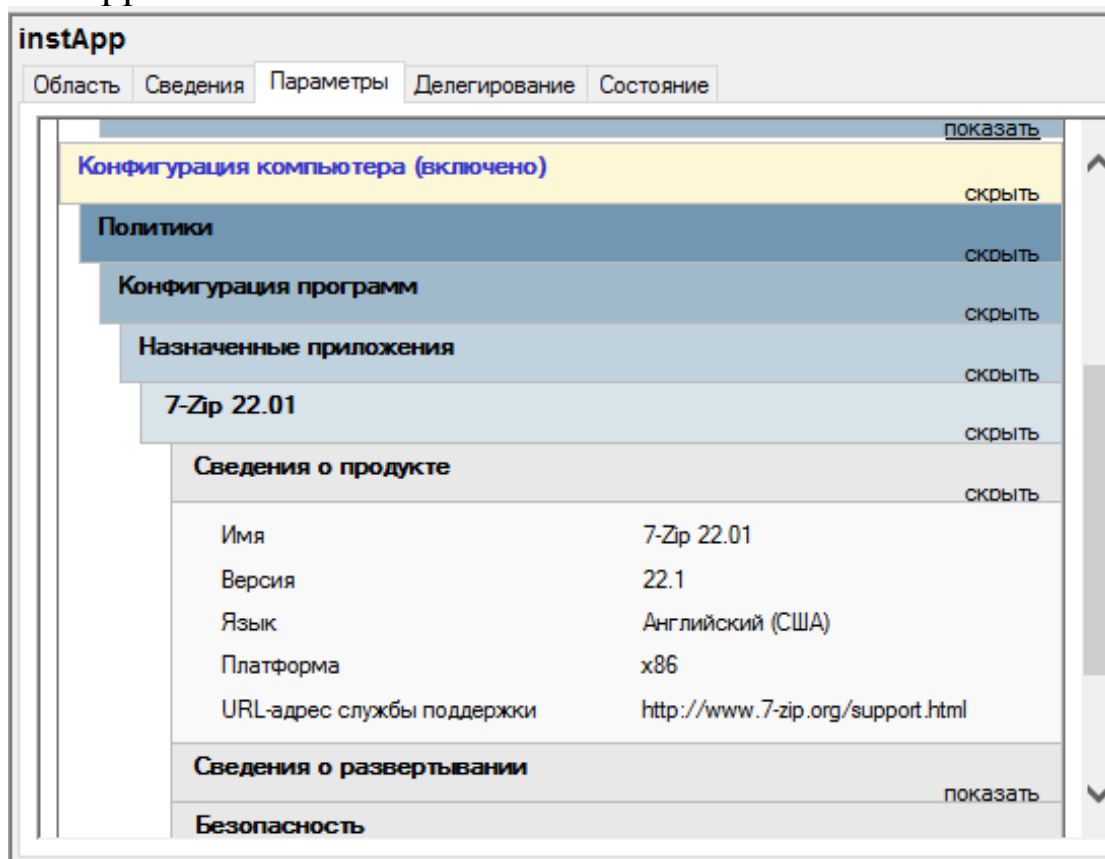
Переносить наследуемые от родительского объекта разрешения на этот объект и все его дочерние объекты Отключено

Аудит
Параметры аудита не указаны

Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".



5. instApp



1. Скрипт

```
$GroupsCount = 0
$ContainersCount = 0
$UsersCount = 0
$str = ""

$Path = Read-Host "Enter path to csv"
$Csv = Get-Content $Path

$GroupList = New-Object Collections.Generic.List[String]
$ContainerList = New-Object Collections.Generic.List[String]
$UserList = New-Object Collections.Generic.List[String]

foreach ($Line in $Csv) {
    $LineArray = $Line.Split(',')

    $Name = $LineArray[0]
    $Occupation = $LineArray[1]
    $Department = $LineArray[2]
    $Email = $LineArray[3]
    $Phone = $LineArray[4]
    $Login = $LineArray[5]
    $Password = $LineArray[6]
    $Container = "OU=" + $LineArray[7] + "DC=NEB,DC=local"
    $Group = $LineArray[8]
    $Homedir = $LineArray[9]
    $ProfilePath = "\\AD-SRV\UsersHome$\\" + $LineArray[10]

    $Groupobj = Get-ADGroup -Identity $Group

    if ($null -eq $Groupobj) {
        New-ADGroup -Name $Group -GroupScope Global
        $GroupsCount = $GroupsCount + 1
        $GroupList.Add($Group)
        $str = $str + "CreatedGroup: " + $Group + "`n"
    }
    try {
        Get-ADOrganizationalUnit -Identity $Container
    } catch {
        New-ADOrganizationalUnit -Name $LineArray[7] -Path "DC=NEB,DC=local"
        $ContainersCount = $ContainersCount + 1
        $ContainerList.Add($LineArray[7])
        $str = $str + "CreatedContainer: " + $LineArray[7] + "`n"
    }
    try {
        New-ADUser -DisplayName $Name -Name $Login -SamAccountName $Login -
        Accountpassword (ConvertTo-SecureString $Password -AsPlainText -Force) -
        OfficePhone $Phone -Title $Occupation -Department $Department -EmailAddress
```

```

$Email -Path $Container -HomeDirectory $Homedir -ProfilePath $ProfilePath -
Enabled $true
    $UsersCount = $UsersCount + 1
    $UserList.Add($Login)
    $str = $str + "CreatedUser: " + $Login+ "`n"
} catch {
    Write-Host "error: user already exists"
}

    Add-ADGroupMember -Identity $Group -Members $Login
}

$html = "<html>" + $str + "usersCreated : " + $UsersCount + "groupsCreated:"
+$GroupsCount +"containersCreated: " + $ContainersCount+ "<html>" | Set-Content -
Path test.html -Value $html

```

**2. Проверяем корзину AD, если не подключена,
подключаем, далее с помощью корзины
восстанавливаем объект.**

3. Конвейер команд из ч. 6 п. 3

```
dsquery user "OU=unit-for-delete,DC=aababich,DC=local" | dsrm -noprompt
```

4. Конвейер команд из ч. 6 п. 3

```

(Get-ADObject -SearchBase (get-addomain).deletedobjectscontainer -IncludeDeletedObjects
-Filter "samaccountname -eq 'petr1'") | Restore-ADObject

```