

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
(БГТУ им. В.Г.Шухова)**

Лабораторная работа №4
дисциплина «Администрирование распределенных вычислительных сетей»
по теме «Группы. Настройка политик и событий»

Выполнил: студент группы ВТ-41
Проверил:

Макаров Д.С.
Федотов Е.А.

Белгород 2020

Лабораторная работа №4

«Группы. Настройка политик и событий»

Цель работы: получить навыки создания групп и работы с ними при помощи сценариев и команды LDIFDE, а также настройки политик и событий.

Ход работы

1. Создание группы.

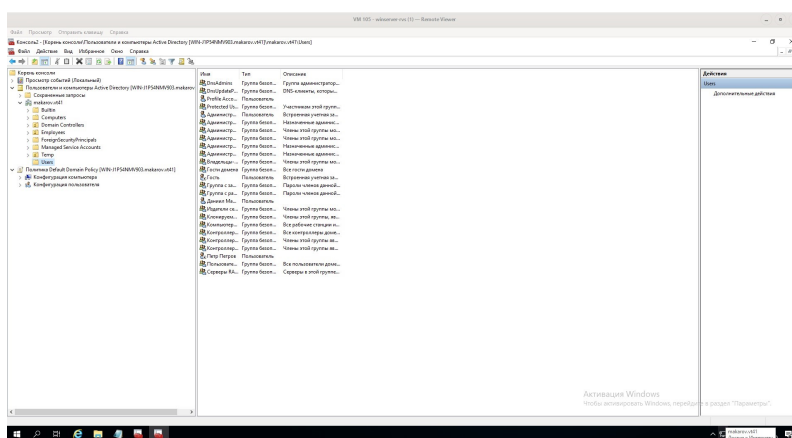


Рис. 1: Создание группы

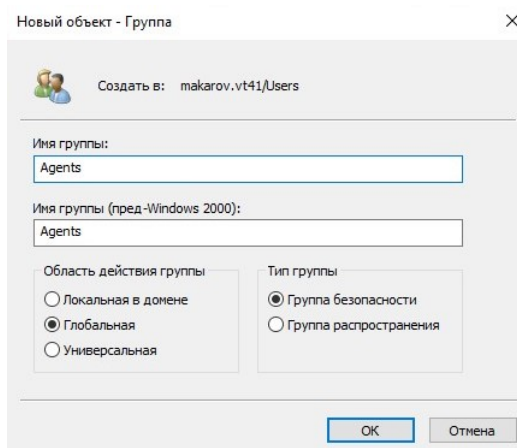


Рис. 2: Диалоговое окно

В созданной группе, можно изменить область действия группы.

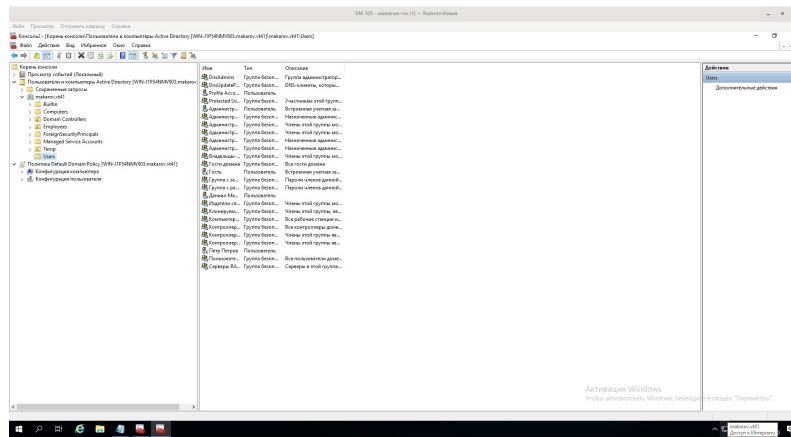


Рис. 3: Свойства группы

2. Для выполнения указанных операций был написан скрипт на языке Powershell.

```
New-ADGroup -GroupScope DomainLocal -Name Group1
New-ADGroup -GroupScope DomainLocal -Name Group2
New-ADGroup -GroupScope DomainLocal -Name Group3
Get-ADGroup -Filter 'name -like "Group*"' | Set-ADGroup -GroupScope Universal
Get-ADGroup -Filter 'name -like "Group*"' | Set-ADGroup -GroupScope Global
New-ADUser -Name User1
New-ADUser -Name User2
New-ADUser -Name User3
Add-ADGroupMember -Identity Group1 -Members User1,User2,User3
Get-ADGroupMember -Identity Group1
Get-ADGroupMember Group1 | ForEach-Object {
    Add-ADGroupMember -Identity Group2 -Members $_
    Remove-ADGroupMember -Identity Group1 -Members $_
}
Get-ADGroupMember -Identity Group1
```

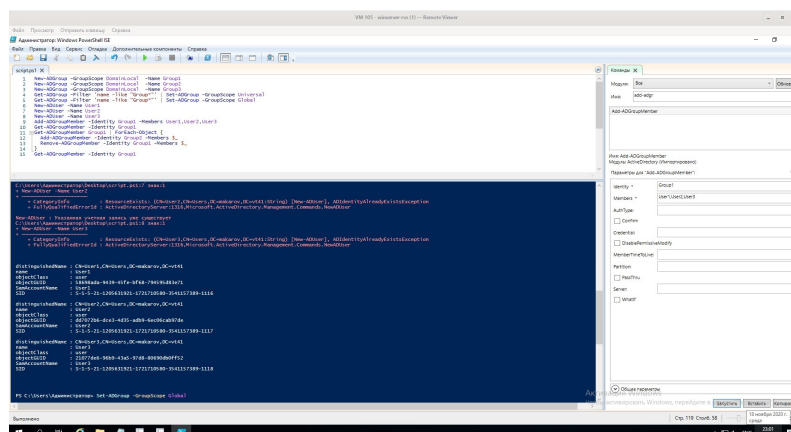


Рис. 4: Результат выполнения скрипта

3. Работа с LDIFDE

```
Администратор: Windows PowerShell
PS C:\Users\Администратор> ldifde

Обмен каталогов LDIF

Общие параметры
=====
-i          Включение режима импорта (по умолчанию режим экспорта)
-f имя_файла  Имя входного или выходного файла.
-s имя_сервера  Сервер для связи (по умолчанию контроллер домена компьютера)
-c FromDN ToDN  Замена входящих FromDN на ToDN
                Если FromDN или ToDN заканчивается атрибутом #имя_атрибута,
                будет выполнен поиск значения атрибута в rootDSE,
                и оно будет использовано для замещения элемента #имя_атрибута. Пример для "Макрорасширение
                в DN".
-v          Включение подробного режима
-j путь       Расположение файла журнала
-t порт       Номер порта (по умолчанию 389)
-u          Использование Юникода
-w время_ожидания  Прекращение выполнения, если сервер не отвечает
                на операцию в течение указанного времени
                (по умолчанию время ожидания не задано)
-h          Включение подписывания и шифрования уровня SASL
-?          Справка

Параметры экспорта
=====
-d DN_хвоя    Корень поиска LDAP (по умолчанию контекст именования)
-r фильтр     Фильтр поиска LDAP (по умолчанию "(objectClass=*)")
-o область_поиска  Область поиска (Base/OneLevel/Subtree)
-l список     Список атрибутов (через запятую), для которых
                выполняется поиск LDAP
-o список     Список исключаемых атрибутов (через запятую)

-g          Отключение страничного поиска
-m          Включение логики SAM для экспорта
-n          Запрет экспорта двоичных значений
-x          Включение удаленных значений ("мемориалов")
-l          Сохранение только важных repPropertyMetadata

Импорт
=====
-k          Будут игнорироваться ошибки "Нарушение ограничения"
                и "Объект уже существует"
-y          Использование режима Lazy Commit для повышения
                производительности (включено по умолчанию)
-e          Отключение режима Lazy Commit
-q threads    Использование указанного числа потоков
                (по умолчанию 1)
-z          Продолжение импорта даже при наличии ошибок.
-x          Включение возможности восстановления "мемориалов" (передает управление
                объектами с запросами изменения LDAP)

Задание учетных данных
=====
Обратите внимание, что если учетные данные не указаны, то LDIFDE будет подключен
как текущий пользователь с помощью SSPI.

-a DN_пользователя [пароль | *]    Простая проверка подлинности
-b имя_пользователя домен [пароль | *]  Метод связывания SSPI

Пример: простой импорт текущего домена
ldifde -i -f INPUT.LDF
```

Рис. 5: Вывод доступных параметров LDIFDE

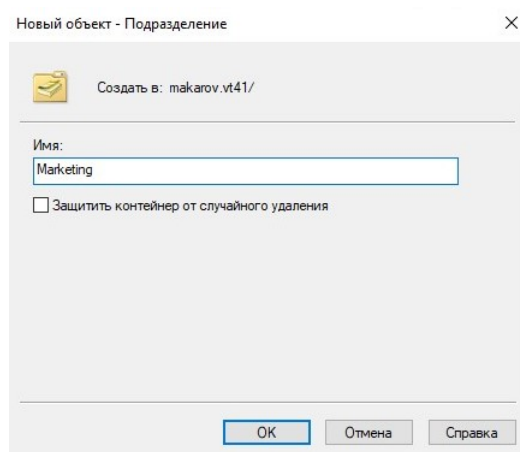
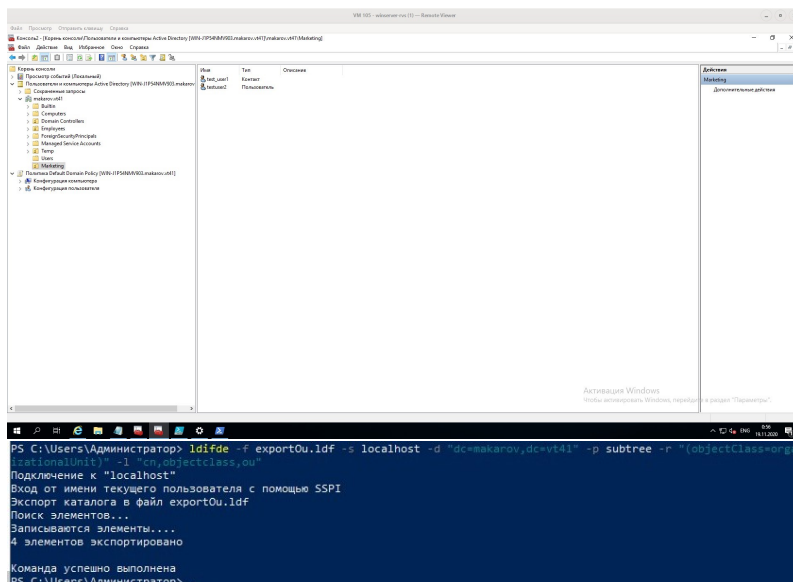


Рис. 6: Экспорт при помощи данных LDIFDE



```
PS C:\Users\Администратор\Desktop> ldifde -i -f gc.txt -s localhost
Подключение к "localhost"
Вход от имени текущего пользователя с помощью SSPI
Импортирование каталога из файла "gc.txt"
Загружаются элементы..
1 элемент успешно изменен.

Команда успешно выполнена
PS C:\Users\Администратор\Desktop>
```

Рис. 7: Создание группы при помощи LDIFDE

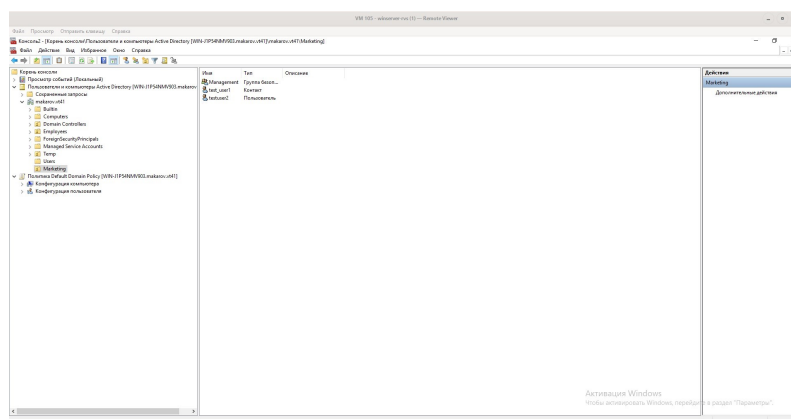


Рис. 8: Результат работы утилиты

4. Настройка политик Active Directory

Контрольные вопросы

1. Что такое группы Active Directory? Типы групп.

Группа Active Directory - это совокупность объектов в Active Directory. В группу могут входить пользователи, компьютеры, другие группы и другие объекты AD.

Существует 2 типа групп: * группы безопасности * группы распространения
Так же группы подразделяются по области действия

- универсальные
- глобальные
- локальные

2. Перечислите политики паролей. Что они определяют?

- Вести журнал паролей
- Максимальный срок действия пароля
- Минимальный срок жизни пароля
- Минимальная длина пароля
- Пароль должен отвечать требованию сложности
- Хранить пароли, используя обратимое шифрование

3. Перечислите политики блокировки учетной записи. Что они определяют?

- Время до сброса счетчиков блокировки.
- Пороговое значение блокировки.
- Продолжительность блокировки учетной записи.

4. Что такое аудит? Перечислите политики аудита.

Аудит - журналирование событий.

- аудит проверки учетных данных
- отслеживание изменений в учетных записях пользователей и компьютеров
- аудит активности индивидуальных приложений
- аудит изменений в объектах службы Active Directory Domain Services
- аудит интерактивных и сетевых попыток входа на компьютеры и сервера домена
- аудит доступа к различным объектам
- аудит изменений в групповых политиках
- аудит прав доступа к различным категориям данных
- изменения в настройках компьютеров, потенциально критичных с точки зрения безопасности

5. Что содержит журнал событий безопасности?

Список записей о событиях, с различными фильтрами.

Приложение

Содержимое файла p2.ps1

```
New-ADGroup -GroupScope DomainLocal -Name Group1
New-ADGroup -GroupScope DomainLocal -Name Group2
New-ADGroup -GroupScope DomainLocal -Name Group3
Get-ADGroup -Filter 'name -like "Group*"' | Set-ADGroup -GroupScope Universal
Get-ADGroup -Filter 'name -like "Group*"' | Set-ADGroup -GroupScope Global
New-ADUser -Name User1
New-ADUser -Name User2
New-ADUser -Name User3
Add-ADGroupMember -Identity Group1 -Members User1,User2,User3
Get-ADGroupMember -Identity Group1
Get-ADGroupMember Group1 | ForEach-Object {
    Add-ADGroupMember -Identity Group2 -Members $_
    Remove-ADGroupMember -Identity Group1 -Members $_
}
Get-ADGroupMember -Identity Group1
```