ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»

(БГТУ им. В.Г.Шухова)

**Лабораторная работа №4**

**Группы. Настройка политик и событий**

Выполнил:

студент группы ВТ-41

Сидорова А.С.

Проверил:

Федотов Е.А.

Белгород 2020

**Цель работы:** получить навыки создания групп и работы с ними

при помощи сценариев и команды LDIFDE, а также настройки

политик и событий.

**Задания к работе**

1. Создание и изменение группы.
2. Напишите сценарии, которые позволят выполнить операции
3. Управление учетными записями групп с помощью команды

LDIFDE

3.1. Вывести список доступных параметров команды

LDIFDE

* 1. Экспорт сведений о пользователях из одного ОП.
  2. Создание группы командой LDIFDE

1. Работа с политиками

4.1. Настройка политик

4.2. Генерация событий входа в систему

4.3. Генерация событий управления учетными записями

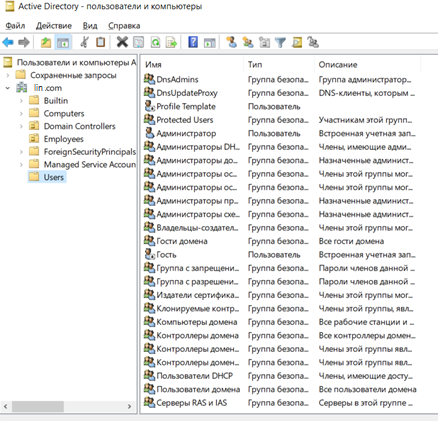
4.4. Анализ событий безопасности, сгенерированных проверкой

подлинности

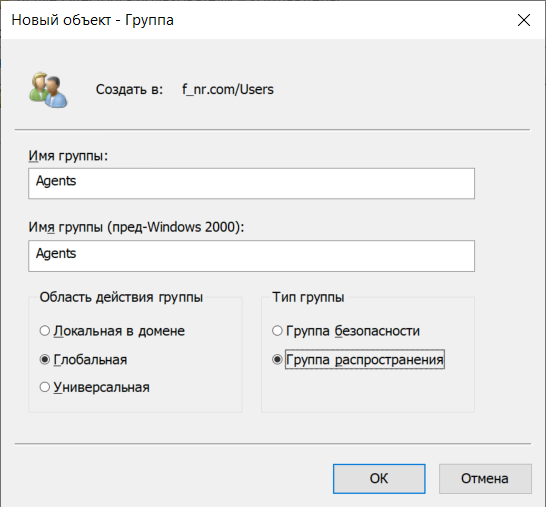
**Выполнение**

1. Создание и изменение группы.

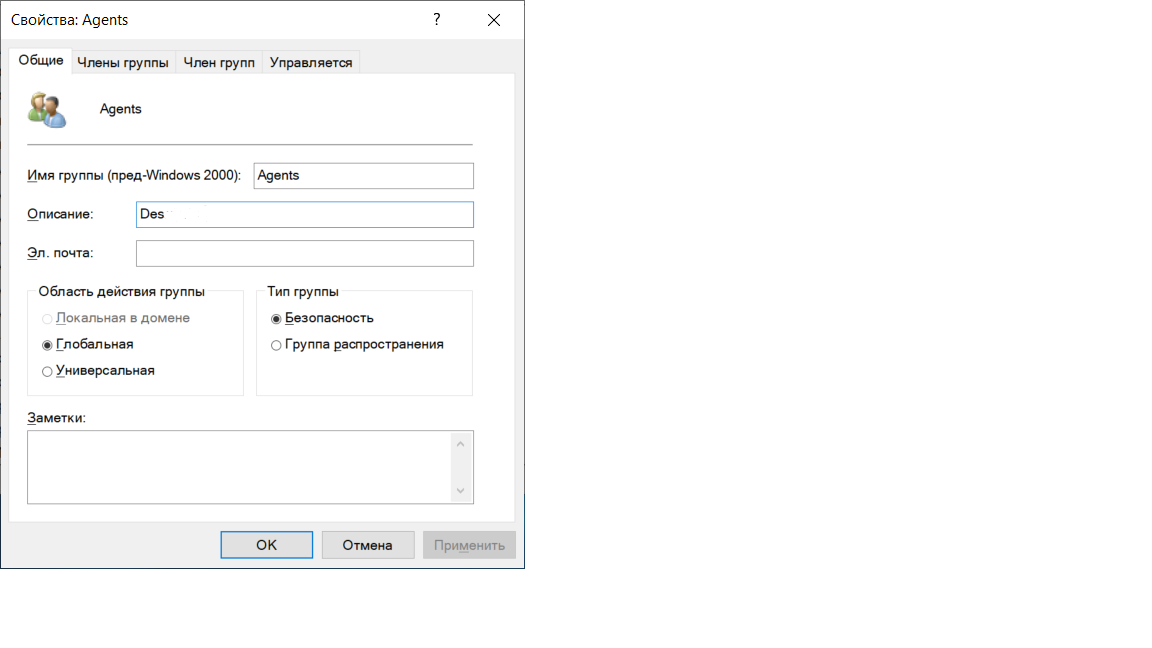
Откроем консоль Active Directory

****

В контейнере Users и создадим глобальную группу распространения Agents



Зайдём в свойства данного объекта и попробуем изменить:



Свойства объекта изменились:



Значит, сервер работает качественно.

1. Напишите сценарии, которые позволят выполнить операции

Описала 5 видов сценариев:

1. Создание трех локальных групп в ОП Groups: Group1, Group2 и Group3.

New-ADGroup "Group1" -GroupScope 0 -PassThru -Verbose

New-ADGroup "Group2" -GroupScope 0 -PassThru -Verbose

New-ADGroup "Group3" -GroupScope 0 -PassThru -Verbose

1. Изменение области действия созданных групп на глобальную (сначала на универсальную, а затем на глобальную).

Set-ADGroup -Identity "Group1" -GroupScope 1 -Verbose

Set-ADGroup -Identity "Group2" -GroupScope 1 -Verbose

Set-ADGroup -Identity "Group3" -GroupScope 1 -Verbose

Set-ADGroup -Identity "Group1" -GroupScope 2 -Verbose

Set-ADGroup -Identity "Group2" -GroupScope 2 -Verbose

Set-ADGroup -Identity "Group3" -GroupScope 2 -Verbose

1. Создание трех учетных записей пользователей: User1, User2 и User3.

New-ADUser "User1" -Verbose

New-ADUser "User2" -Verbose

New-ADUser "User3" -Verbose

1. Добавление User1, User2 и User3 в группу Group1

Add-ADGroupMember -Identity group1 -Members User1, User2, User3 -Verbose

1. Перемещение Group1 в группу Group2.

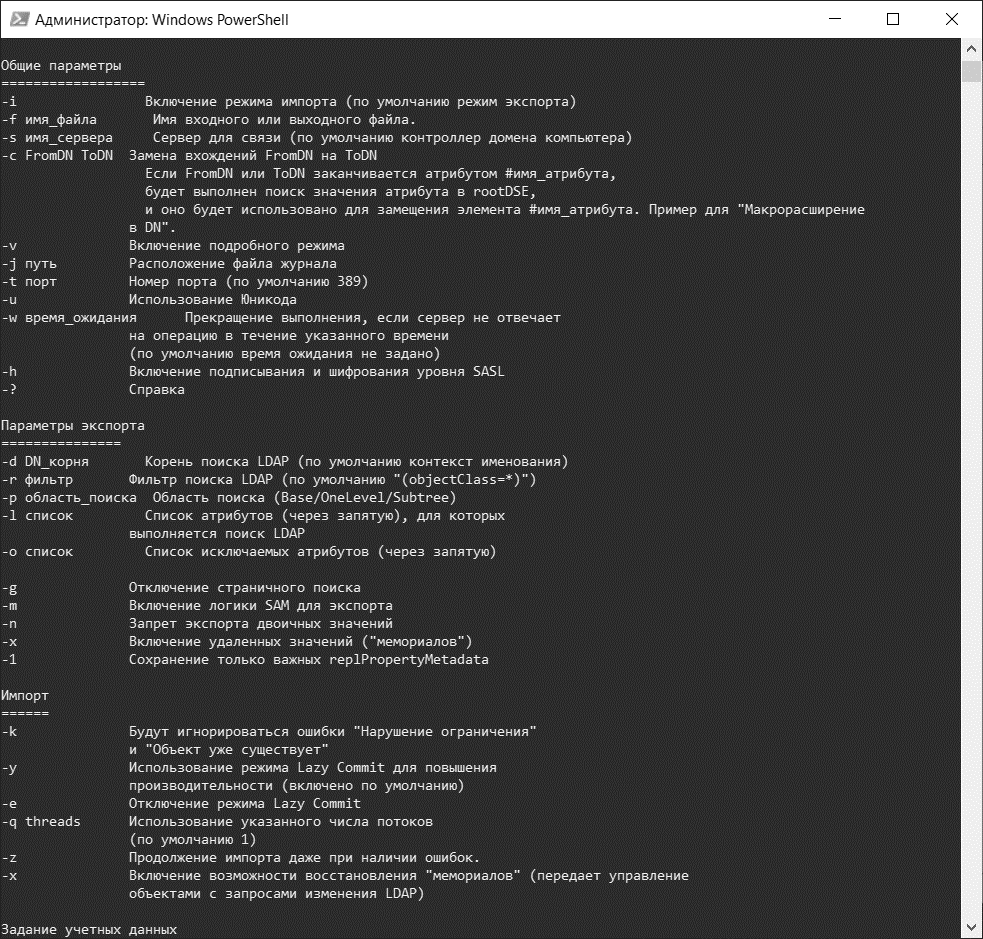
Move-ADObject -Identity group1 -TargetPath "OU=groups,OU=Group2, DC=f\_nr, DC=com" -verbose

1. Управление учетными записями групп с помощью команды

LDIFDE

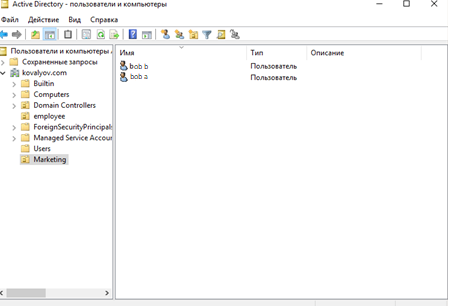
3.1. Вывести список доступных параметров команды

LDIFDE

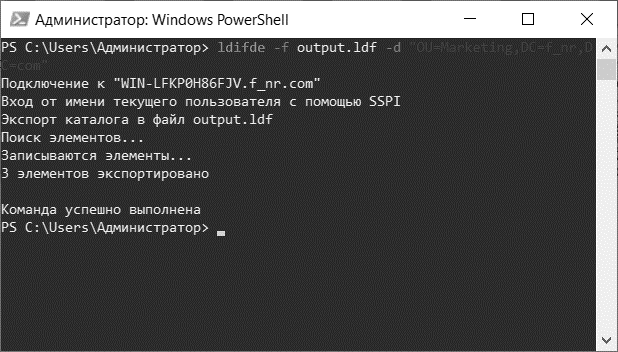


3.2.Экспорт сведений о пользователях из одного ОП.

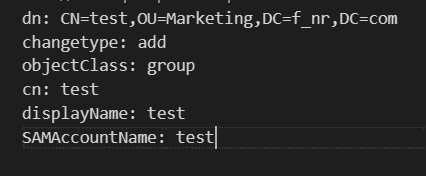
В домене был создан ОП Marketing, в него добавлены 2 пользователя:



Выполним экспорт:

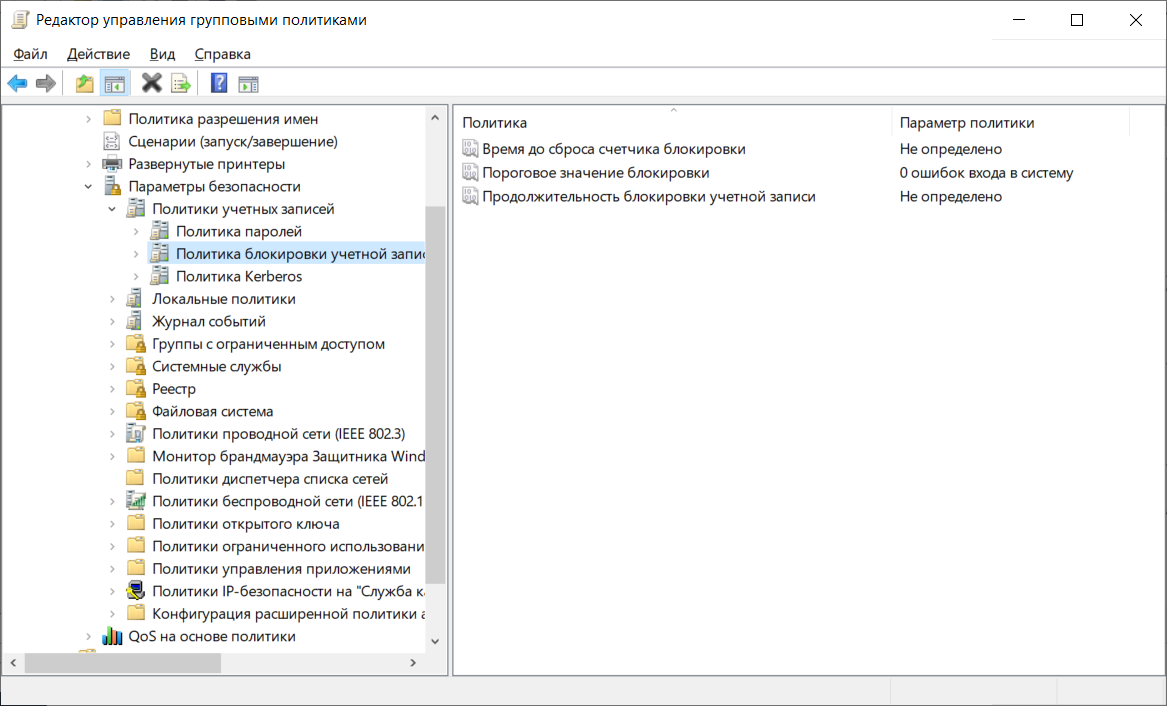


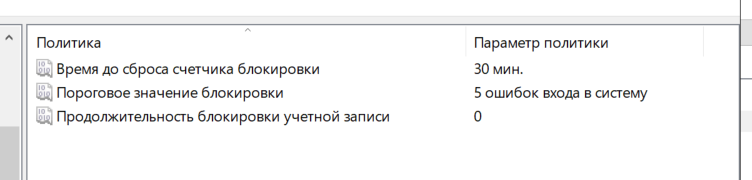
3.3.Создание группы командой LDIFDE



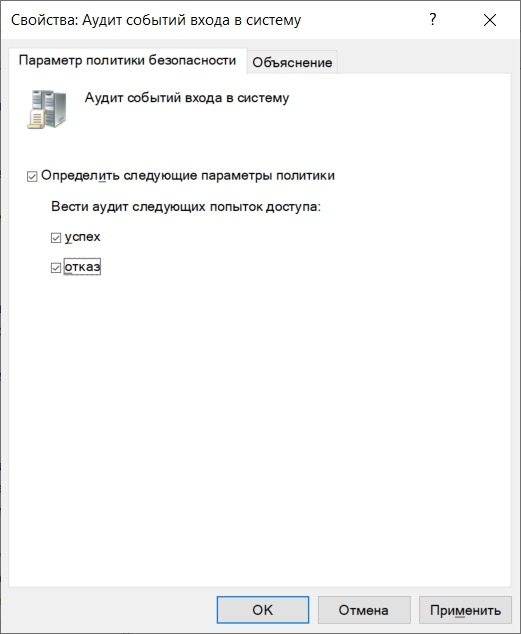
4.Работа с политиками

4.1. Настройка политик

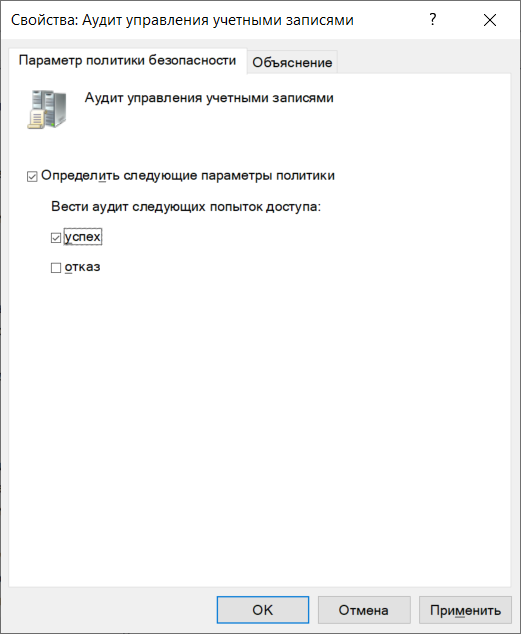
В консоли Active Directory — пользователи и компьютеры щелкнем узел домена lin.com и выберем его свойства. Находим раздел Политика блокировки учетной записи.  




Настроим политику Аудит событий входа в систему:



Настроим Аудит управления учетными записями:

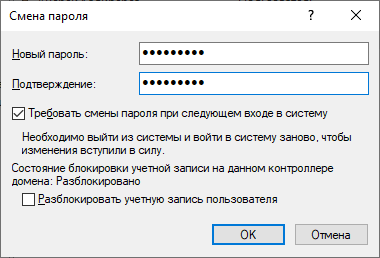


* 1. Генерация событий входа в систему

Сгенерируем два события неудачного входа в систему, введя неверный пароль у пользователя, а затем введём верный пароль.

* 1. Генерация событий управления учетными записями

В панели управления Active Directory создадим новый пароль пользователю.



4.4. Анализ событий безопасности, сгенерированных проверкой

подлинности

Откроем консоль Управление компьютером из группы Администрирование. В разделе «Просмотр событий» откроем журнал безопасности Windows. Найдём список относящиеся к сгенерированным событиям удачных и неудачных входов и смены пароля.

**Вывод**

В лабораторной работе мы изучили этапы создания групп в Active Directory и работы с ними при помощи сценариев и команды LDIFDE, а также настройку политику и событий, которые возникали внутри домена.

**Контрольные вопросы**

1. **Что такое группы Active Directory? Типы групп.**

**Группа Active Directory** – это совокупность объектов в Active Directory.

Существует два типа групп -**безопасности** и **распространения**.

**Группа распространения** - применяется для создания групп почтовых рассылок. Письмо отправленное на группу распространения дойдет всем пользователям группы. Это группа не предназначена для работы с предоставлением доступа на ресурсы.

**Группа безопасности** - применяется для управления безопасности доступа к ресурсам. Т.е. если вы хотите для сетевой папки создать группу, для этого необходимо создать группу безопасности. Так же с помощью группы безопасности можно сделать почтовую рассылку, но это не рекомендуется делать поскольку для этого есть группа распространения.

1. **Перечислите политики паролей. Что они определяют?**

|  |  |  |
| --- | --- | --- |
| **Политика** | **Краткое пояснение** | **Возможные значения** |
| Вести журнал паролей/ Enforce password history | Определяет число новых уникальных паролей | 0-24 |
| Максимальный срок действия пароля/ Maximum password age | Определяет период времени (в днях), в течении которого можно использовать пароль, пока система не потребует сменить его. | 1-999 |
| Минимальная длина пароля / Minimum password lenght | Параметр определяет минимальное количество знаков, которое должно содержаться в пароле | 0- без пароля  1-14 |
| Минимальный срок действия пароля/ Minimum password age | Параметр определяет период времени (в днях)?в течении которого пользователь должен использовать пароль, прежде чем его можно будет изменить. | 0-998 |
| Пароль должен отвечать требованиям сложности / Password must meet complexity requirements | Параметр определяет должен ли пароль отвечать сложности:  -не содержать имени учетной записи  - длина не менее 6 знаков  - содержать заглавные буквы (F, G,R)  - содержать строчные буквы (f,y,x)  - содержать цифры  - содержать спец знаки (#,@,$) | Включена/ Отключена |
| Хранить пароли, используя обратимое шифрование / Store passwords using reversible encryption | Параметр указывает использовать ли операционной системой для хранения паролей обратимое шифрование. | Включена/ Отключена |

**3. Перечислите политики блокировки учетной записи. Что они**

**определяют?**

* Блокировка ввода пароля на определенное время
* Восстановление счетчика блокировки

Данные политики применяются для защиты учетной записи пользователя от злоумышленника, который не придумал ничего лучше, чем перебирать все пароли.

1. **Что такое аудит? Перечислите политики аудита.**

Аудит – процесс отслеживания различных действий, выполняемых ОС.

1. Аудит событий входа в систему
2. Аудит управления учетными записями
3. Аудит доступа к службе каталогов
4. Аудит события входа
5. Аудит доступа к объектам
6. Аудит изменения политики
7. Аудит использования привилегий
8. Аудит отслеживания процессов
9. Аудит системных событий
10. **Что содержит журнал событий безопасности?**

В журнале безопасности записываются все события, определенные политиками аудита, заданными для каждого объекта.