Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет информационных технологий и программирования

Администрирование в ОС Windows Server

Лабораторная работа №2

Основы работы с Active Directory в Windows Server

Выполнили студенты группы № M33091

Фисенко Никита Данилович

Рустамов Марк Самирович

Санкт-Петербург 2023

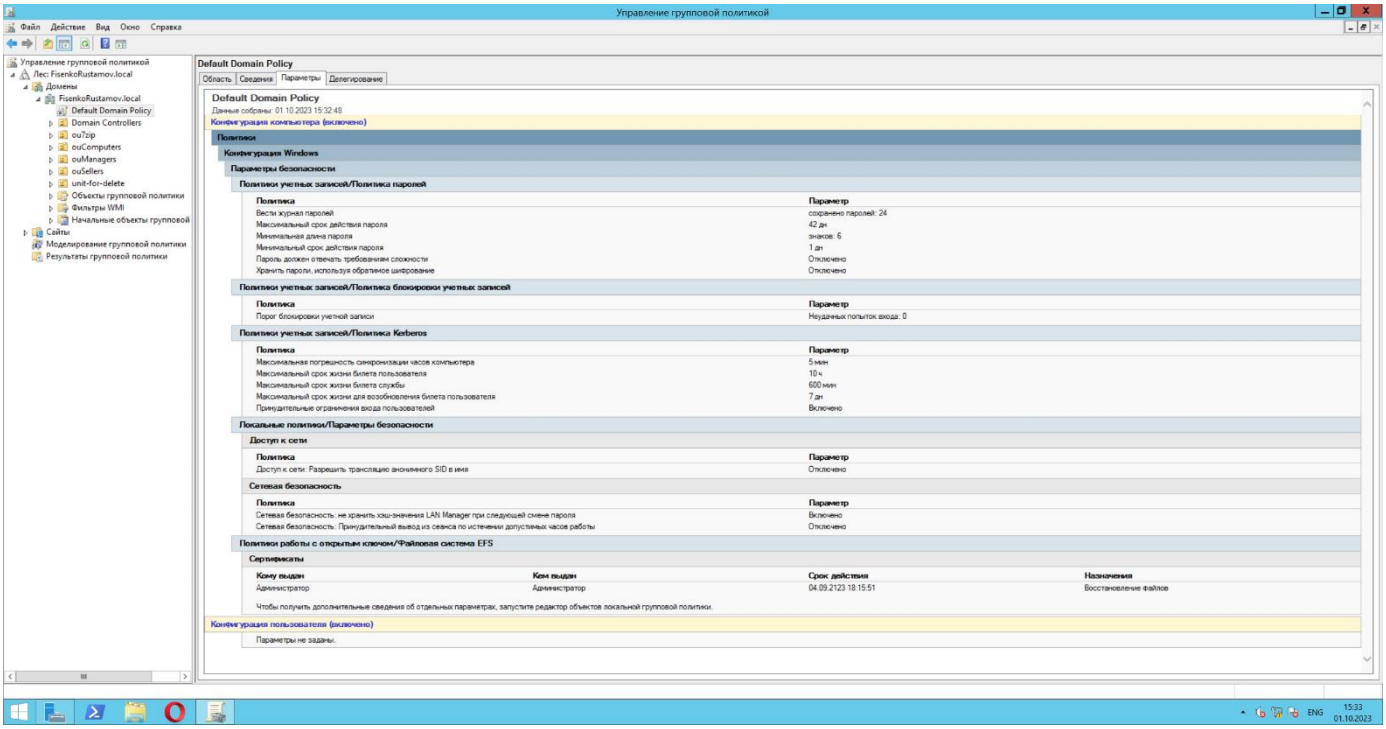
Цель работы:

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

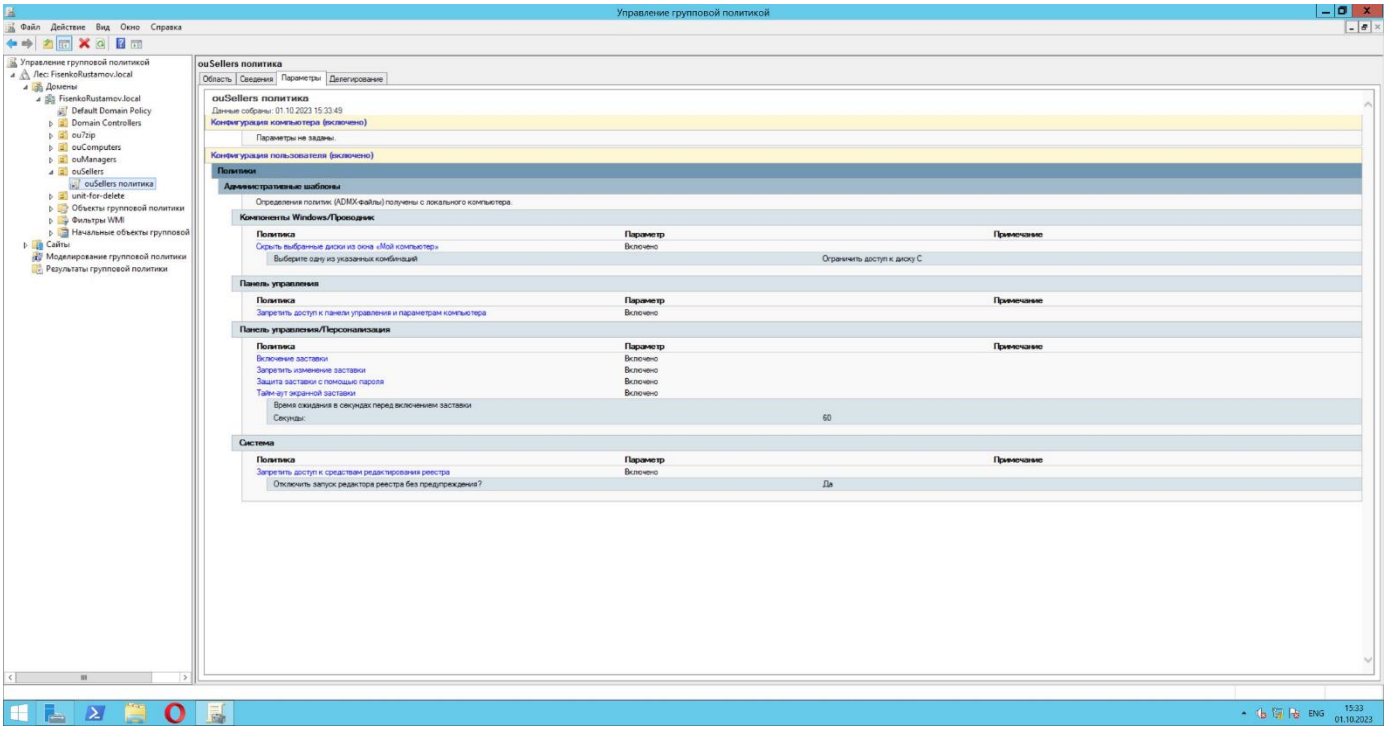
Артефакты:

1. Групповые политики Active Directory:

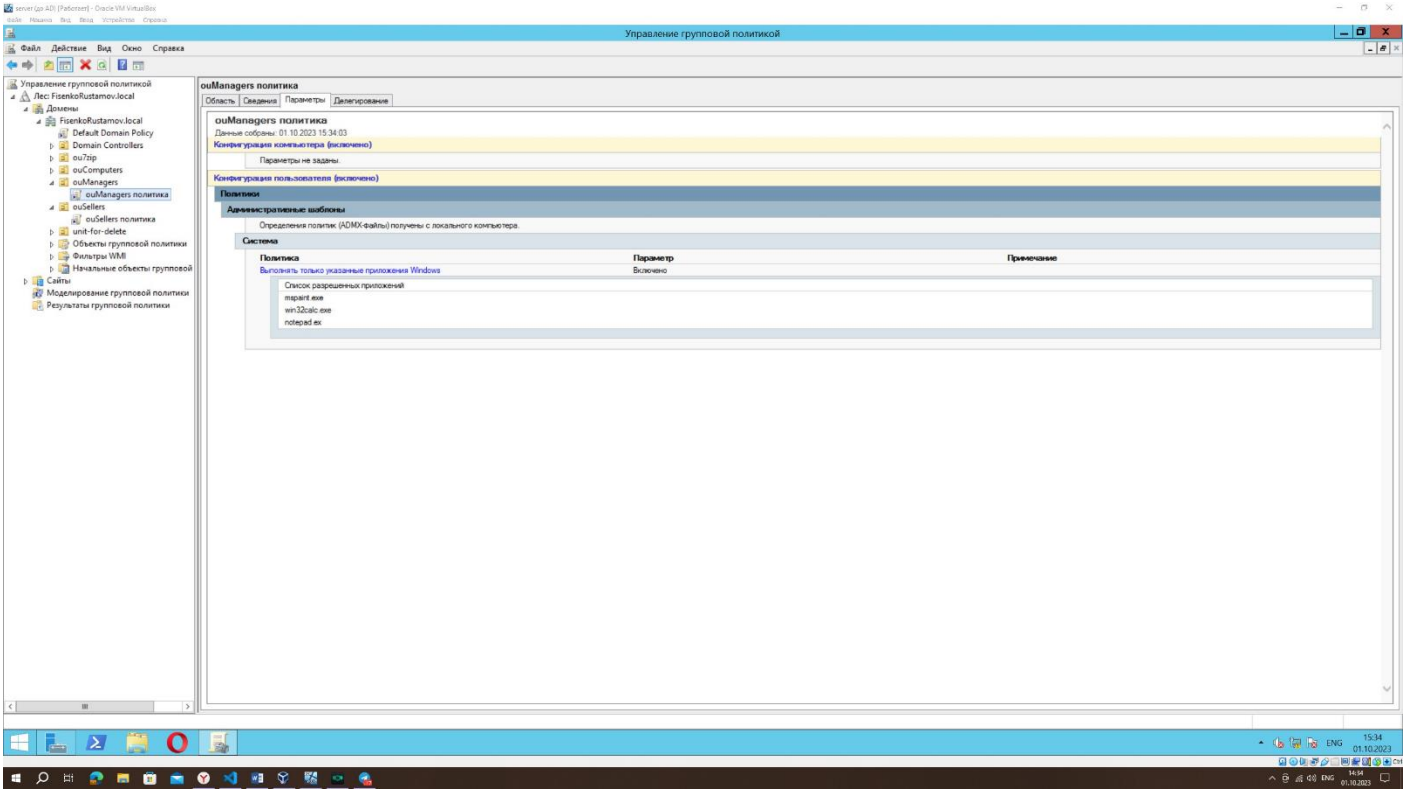
Default Domain Policy



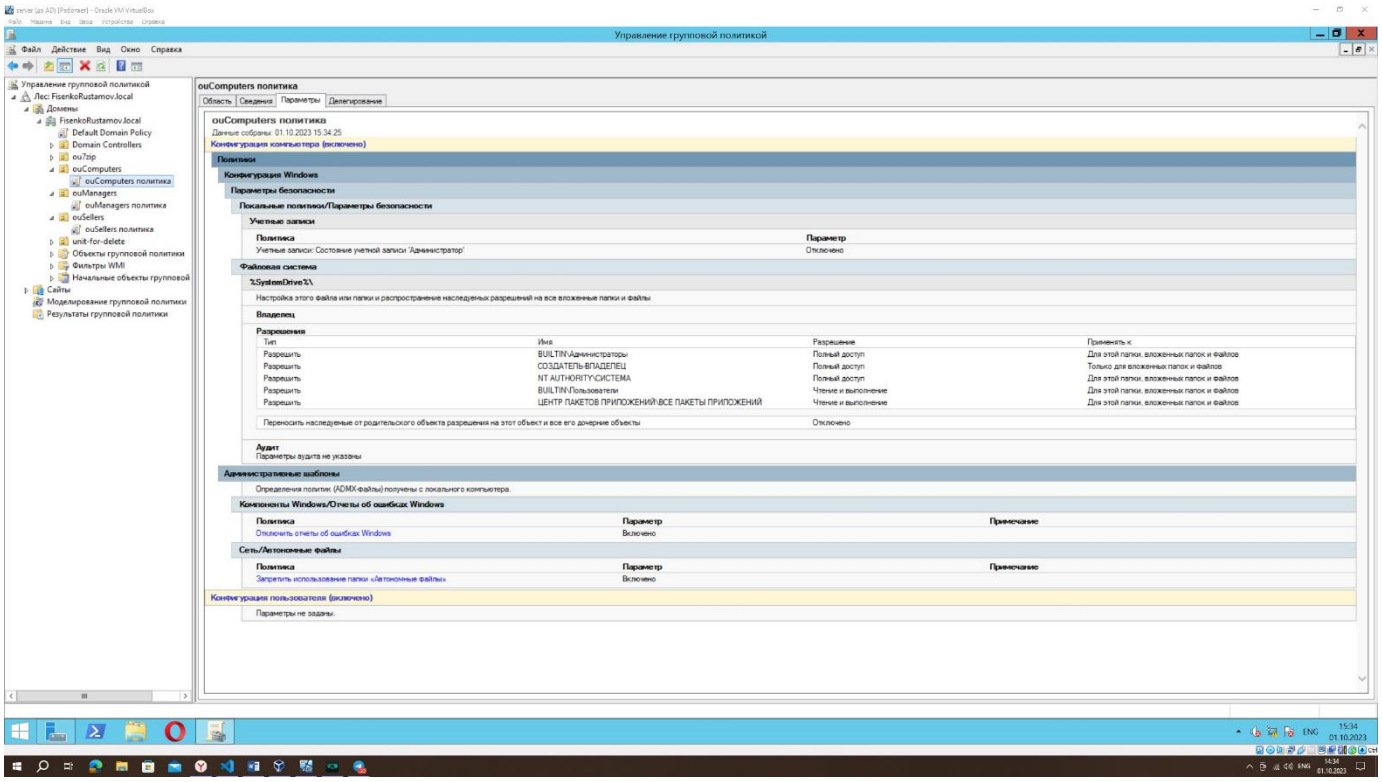
ouSellers Policy



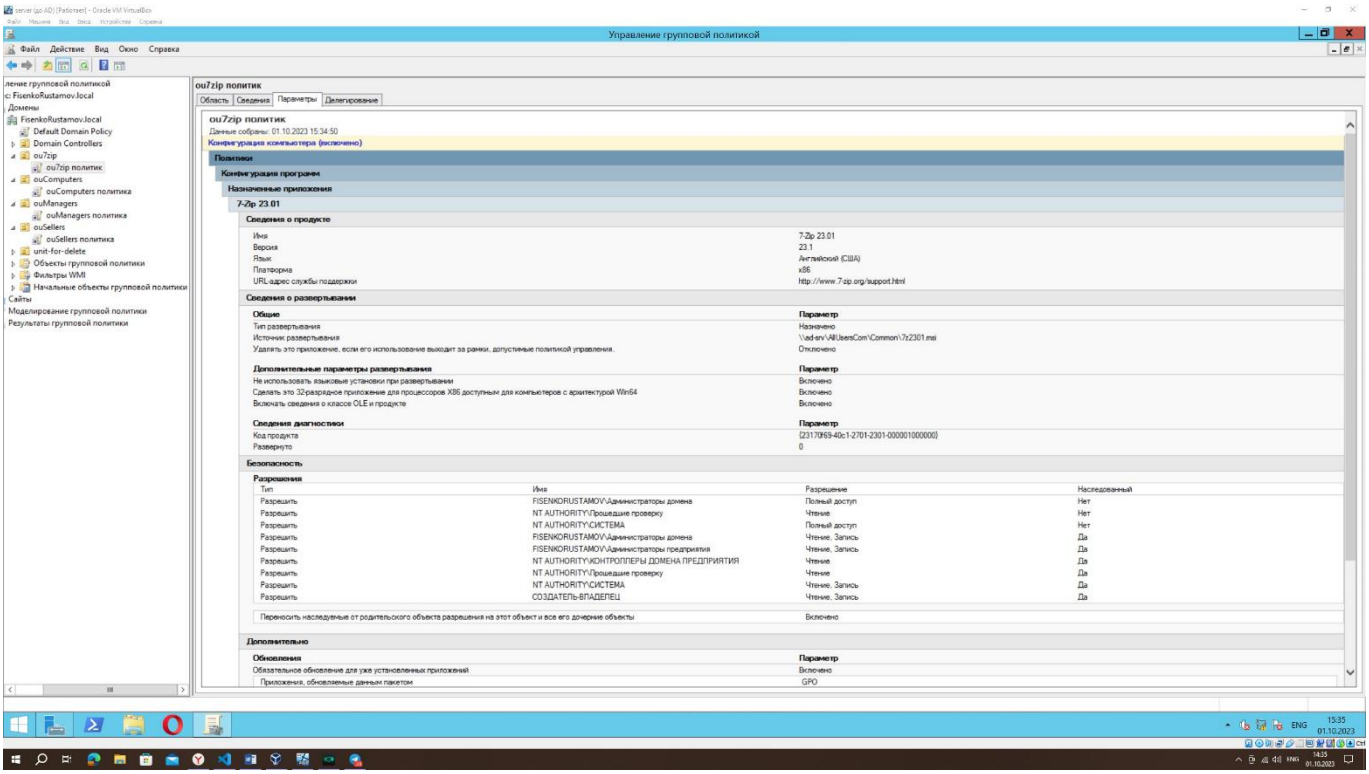
ouManagers Policy



ouComputers Policy



ou7zip Policy

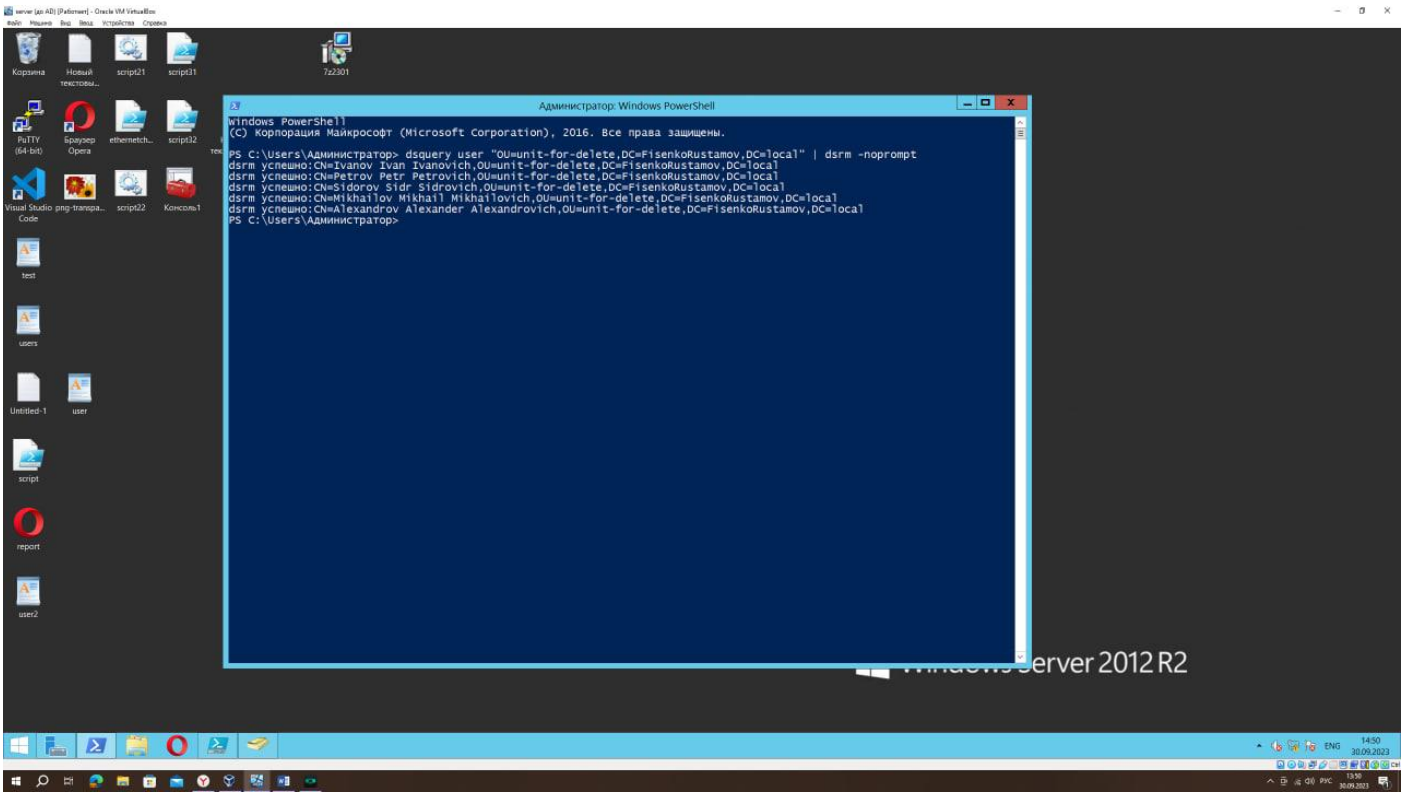


2. Скрипт создания пользователей

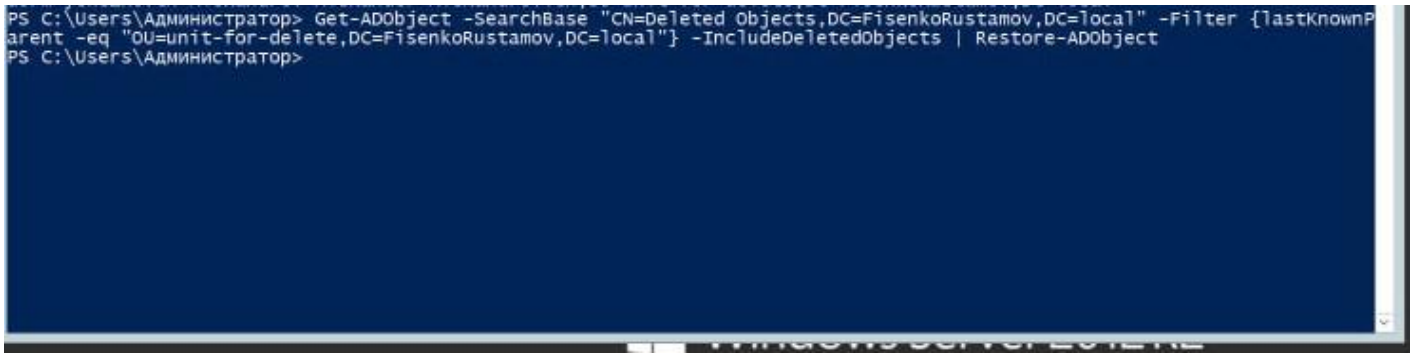
```
Import-Module ActiveDirectory

$ADUsers = Import-CSV -path $args[0] -Delimiter ";"
$log = @()

$ADUsers | ForEach-Object {
    $password = ConvertTo-SecureString $_.Password -AsPlainText -Force
    $ouName = $_.Container
    $ouExists = Get-ADOrganizationalUnit -Filter {Name -eq $ouName}
    if (!$ouExists) {
        New-ADOrganizationalUnit -Name $ouName -PassThru -
ProtectedFromAccidentalDeletion $false
        $log += ("OU: " + $ouName)
    }
    $ouPath = Get-ADOrganizationalUnit -Filter {Name -eq $ouName}
    $groups = $_.Groups
    $groups | ForEach-Object -Process {
        if ($null -eq (Get-ADGroup -Filter { Name -Like $_ })) {
            New-ADGroup -Name $_ -SamAccountName $_ -GroupCategory Security -
GroupScope Global -DisplayName $_
            $log += ("Group: " + $_)
        }
```

```
    }
    $fiostr = $_.FIO  -Split " "
    New-ADUser -Name $_.Login -SamAccountName $_.Login -GivenName $fiostr[1] -Surname $fiostr[0] -Title $_.JobTitle -Department $_.UnitName -EmailAddress $_.EMail -MobilePhone $_.Phone -AccountPassword $password -Path $ouPath -ProfilePath $_.Profile -HomeDirectory $_.HomePath -HomeDrive "X:" -Enable $true
    $userHomePath = "C:\UsersHome\$($_.Login)"
    if (!(Test-Path -Path $userHomePath -PathType Container)) {
        New-Item -Path $userHomePath -ItemType Directory
    }
    $log += ("Directory: " + $userHomePath)
    $shareName = $_.Login
    $userToGrantAccess = $_.Login
    New-SmbShare -Name $shareName -Path $userHomePath -FullAccess $userToGrantAccess
    icacls $userHomePath /grant "$($userToGrantAccess):(OI)(CI)(M,DC,WD,AD)"

    Add-ADGroupMember -Identity $groups -Members $_.Login
    $log += ("User: " + $_.Login)
}

$log | ConvertTo-Html -Property @{l='New Objects:'; e={$_}} | Out-File "C:\log.html"
echo $log
Read-Host
```

3. Конвейер команд (ч. 6.3)



4. Конвейер команд (ч. 6.4)



Ответы на вопросы:

1. Дерево доменов: состоит из нескольких доменов, которые совместно используют общую схему и конфигурацию, образуя непрерывное пространство имен. Лес (Forest): набор доменов, который имеет общий каталог, глобальный каталог, и общую схему, а также общую конфигурацию. Схема Active Directory: определяет объекты и атрибуты, которые могут быть созданы или включены в AD. Она описывает типы данных, которые могут быть сохранены, и определяет структуру AD. Диалог в скриптах PowerShell намного удобнее, чем CMD. В PowerShell существует множество команд (такие как Contains, Length) и другие, которые упрощают разработку скриптов.
2. База данных Active Directory хранится на контроллере домена в файле NTFS.DIT, который находится в папке %SYSTEMROOT%\NTDS. ntds.dit: Основной файл данных, содержащий все объекты и их атрибуты. edb.log: Журнал транзакций, который содержит все изменения, производимые с данными, прежде чем они будут применены к файлу ntds.dit. res.log: Файлы журнала резерва. temp.edb: Временный файл, используемый для хранения данных во время выполнения задач обслуживания, таких как сжатие.

3. Эти файлы находятся в каталоге C:\Windows\SYSVOL\[domain]\Policies\ на контроллере домена
4. Такие компоненты, как ADFS, для которых нужно установить сертификат, или DNS, для которого следует указать полное доменное имя FQDN.
5. Для предотвращения несанкционированного доступа к данным и для входа на контроллер домена, если служба AD DS не запущена или контроллер домена запущен в режиме DSRM.
6. С помощью инструмента ntdsutil.exe, можно сбросить пароль DSRM.
7. Имя NetBIOS используется для обратной совместимости со старыми системами и приложениями, которые не понимают DNS-имена.
8. Администраторы: локальная группа, предоставляющая полный административный доступ. Администраторы домена: глобальная группа для администрирования всех компьютеров в домене. Администраторы предприятия: глобальная группа для администрирования всех компьютеров в дереве или лесу. Все: все интерактивные, сетевые, коммутируемые и прошедшие проверку пользователи. Создатель-владелец: пользователь, создавший данный файл или папку.
9. A: Адресная запись, соответствие между именем и IP-адресом. CNAME: Каноническое имя для псевдонима. SRV: Указание на местоположение серверов для сервисов. NS: определяет серверы, авторитетные для этой зоны. PTR: используется для обратного поиска DNS. MX: указывает на почтовые серверы для домена.

Вывод: в результате выполнения лабораторной работы мы получили базовые навыки развертывания службы каталогов Active Directory на основе Windows Server, также попробовали управлять объектами AD и правами на NTFS и SMB, создавали групповые политики и изучили механизм восстановления удаленных объектов.