МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет

ИТМО»

Факультет информационных технологий и программирования

Кафедра информационных систем

**Практическая работа 4:**

**Основы работы с Active Directory в Windows Server.**

Выполнил студент группы М32051:

Никитин Александр Юрьевич

САНКТ-ПЕТЕРБУРГ

2020

**Ход работы:**

**Вопросы:**

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

* Дерево доменов - иерархическая система доменов, имеющая единый корень (корневой домен)
* Лес - множество деревьев доменов, находящихся в различных формах доверительных отношений
* Схема - по умолчанию содержит все определения и описания объектов, которые необходимы для корректной работы Active Directory

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

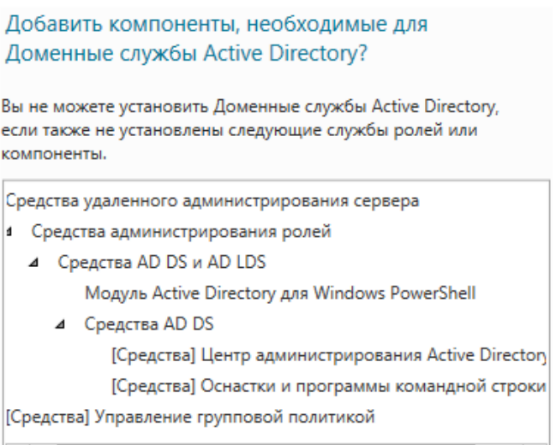
База данных Active Directory хранится на контроллере домена в файле NTFS.DIT, который находится в папке %SYSTEMROOT%\NTDS. Кроме файла NTDS.DIT в каталоге %SystemRoot%\NTDS находятся вспомогательные файлы.

|  |  |
| --- | --- |
| **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. |
| EDBхххх.LOG | Вспомогательные журналы событий, которые создаются, когда файл EBD.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 |
| SHEMA.INI | Необязательный файл, используемый для инициализации файла NTDS.DIT во время загрузки контроллера домена |

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

Локальный объект групповой политики хранится в %SystemRoot%\System32\GroupPolicy.

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



1. Для чего нужен пароль DSRM?

Пароль режима восстановления служб каталога (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.

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

Можно сбросить старый пароль и установить новый.

ntdsutil  
set dsrm password  
reset password on server NULL  
[новый\_пароль\_dsrm]  
[подтверждение\_нового\_пароля]  
quit  
quit

1. Зачем нужно имя домена NetBIOS?

NetBIOS - сетевой протокол. Нужен для обнаружения компьютеров в сети, построенной на базе TCP/IP. Не обязателен — если его отключить, сеть будет работать, но в сетевом окружении пропадет список узлов.

1. Какие группы пользователей создаются в AD автоматически? Опишите минимум 10 из них.

Группы по умолчанию, например группа «Администраторы домена», являются группами безопасности, которые автоматически создаются при создании домена Active Directory.

* Администраторы - члены группы администраторов получают полные и неограниченные права на доступ к компьютеру, а также повышенный уровень доступа пользователей к домену.
* Гости - По умолчанию единственным участником является Гостевая учетная запись. Участники группы не могут вносить случайные или преднамеренные изменения на уровне системы и запускать большинство приложений.
* Администраторы предприятий - участники этой группы имеют право вносить изменения в масштабе леса в ActiveDirectory.
* Пользователи домена - группа включает в себя все учетные записи пользователей домена. Когда вы создаете учетную запись пользователя в домене, она автоматически добавляется в эту группу.
* Операторы настройки сети - члены группы могут обладать следующими правами администратора для управления настройкой сетевых функций.
  + Измените свойства протоколов управления передачей и протокола IP (TCP/IP) для подключения через локальную сеть, в том числе IP-адреса, маски подсети, шлюза по умолчанию и серверов доменных имен.
  + Переименуйте подключения к локальной сети или подключения удаленного доступа, доступные всем пользователям.
  + Включение и отключение подключения к локальной сети.
  + Измените свойства всех подключений удаленного доступа пользователей.
  + Удалите все подключения удаленного доступа пользователей.
  + Переименование всех подключений удаленного доступа пользователей.
  + Выдайте команды **ipconfig**, **ipconfig/release**или **ipconfig/renew** .
  + Введите ключ PINunblock (PUK-код) для устройств мобильной широкополосной связи, поддерживающих SIM-карту.
* Защищенные пользователи - участники группы могут обеспечить дополнительную защиту от раскрытия учетных данных во время проверки подлинности.
* Пользователи удаленного управления - члены группы могут получать доступ к ресурсам WMI через протоколы управления.
* Операторы архива - участники группы могут архивировать и восстанавливать все файлы на компьютере независимо от разрешений, защищающих эти файлы. Операторы архивации также могут войти в систему и завершить работу компьютера. Эту группу невозможно переименовать, удалить или переместить.
* Криптографические операторы - участники этой группы авторизованы для выполнения криптографических операций.
* Операторы для учетных записей - предоставляет пользователю ограниченные полномочия на создание учетной записи. Участники этой группы могут создавать и изменять большинство типов учетных записей, в том числе пользователей, локальных групп и глобальных групп, а также входить в локальную систему на контроллерах домена.

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

* **SOA (start of authority)** создаётся при создании какой- то зоны в самый первый раз. Эта запись предоставляет множество общих сведений для имеющихся зон DNS.
* Записи хоста используются для установки соответствия некого FQDN (fully qualified domain name) какому- то IP адресу.
* Записи **NS** применяются для перечисления авторизованных DNS серверов данной зоны.
* Записи **MX** (**Mail exchanger**) определяют основной сервер MX для некого домена. Значением MX может быть любой сервер электронной почты.
* Записи **CNAME** (**Canonical name**) являются псевдонимами, короткими именами для FQDN.
* Записи **PTR** (**Pointer**) применяются для установления соответствия IP адреса с FQDN.
* Записи **SRV** используются для определения значения местоположения некой службы внутри инфраструктуры.

**Артефакты:**

1. Приведите скриншоты групповых политик AD из части 4.

Политика для контейнера ouSellers:

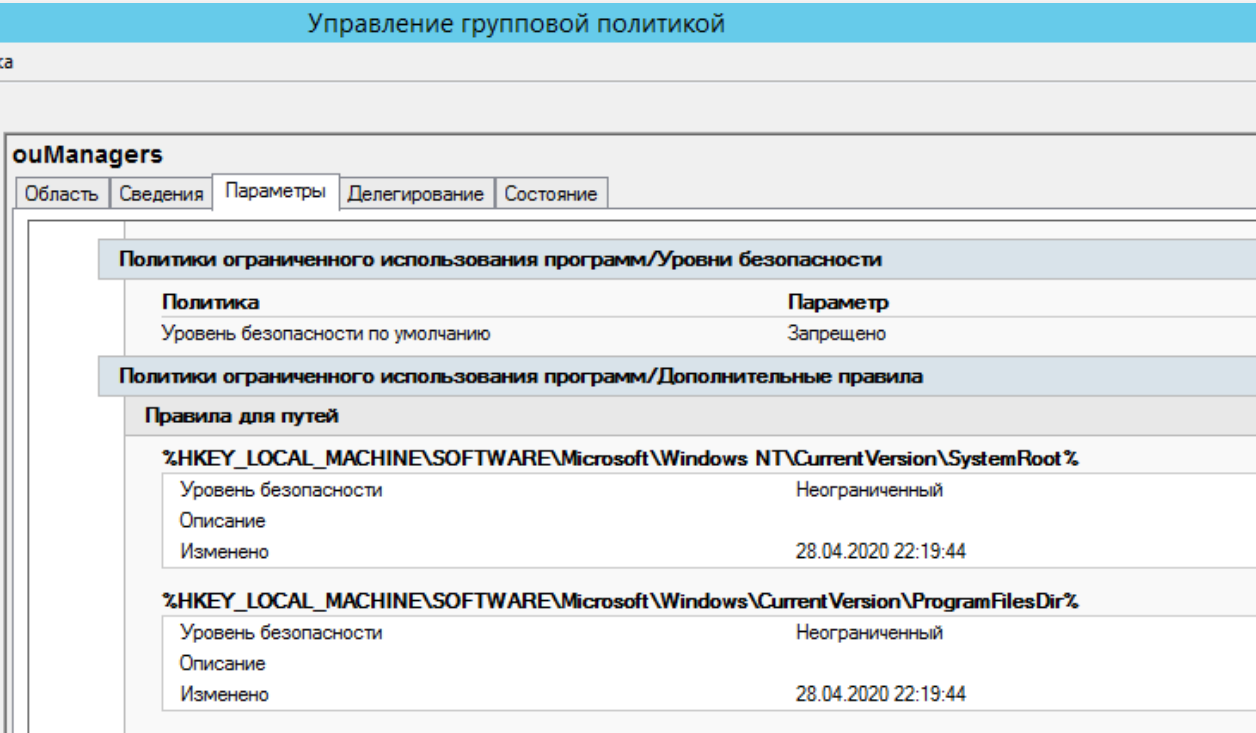
Изображение выглядит как снимок экрана

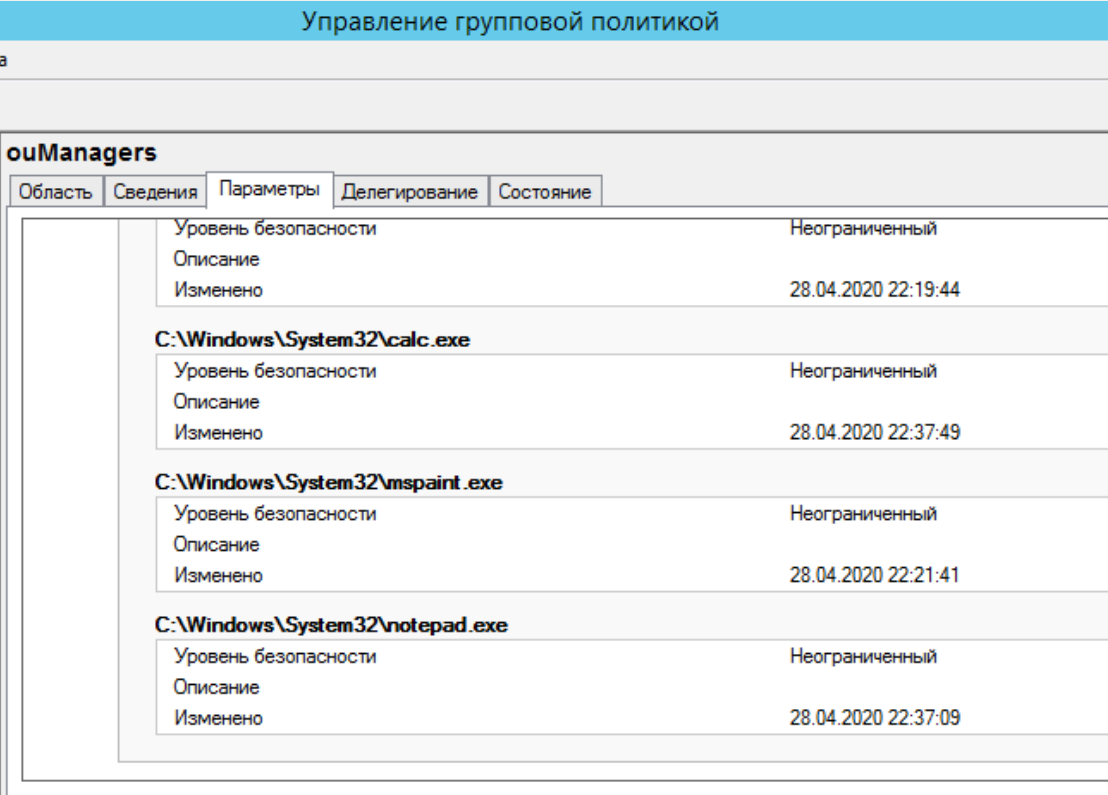
Автоматически созданное описание

Изображение выглядит как снимок экрана

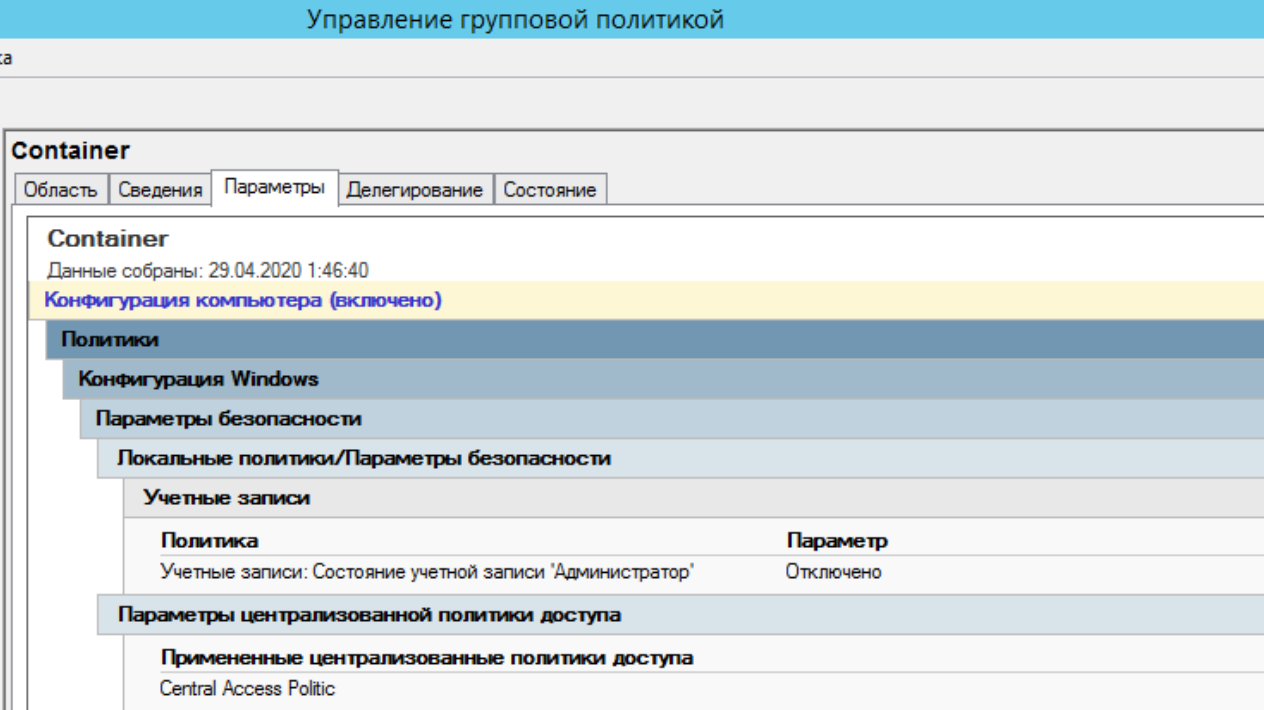
Автоматически созданное описание

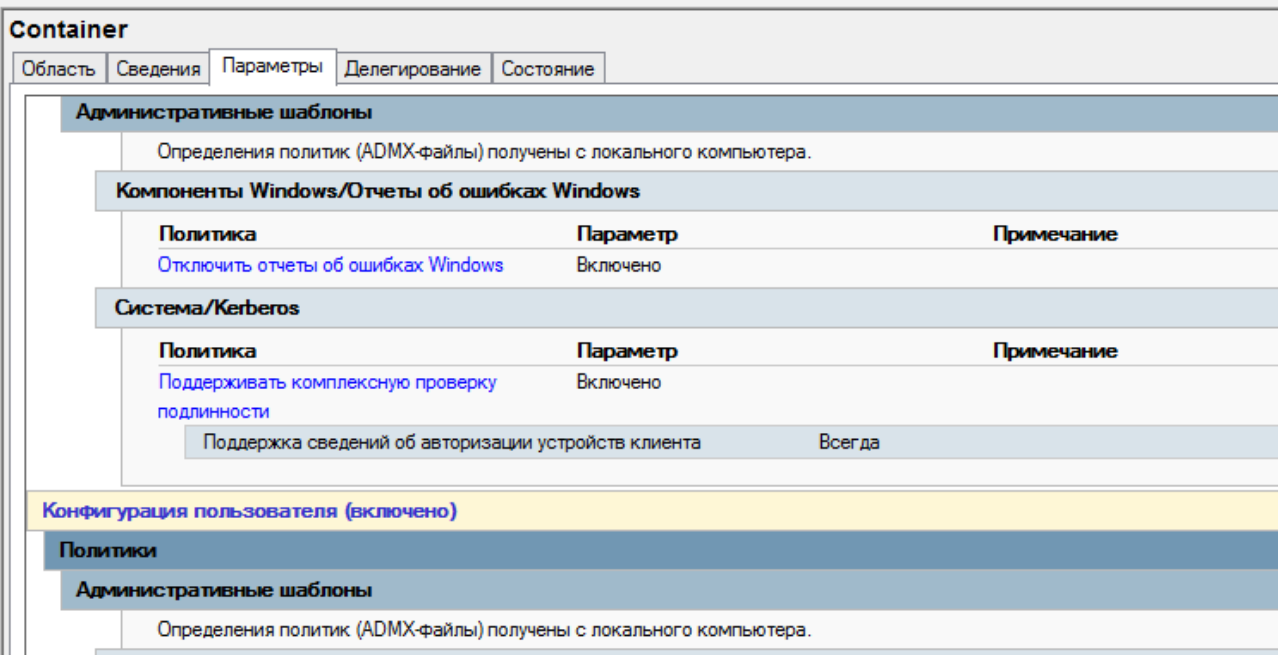
Политика в контейнере ouManagers:

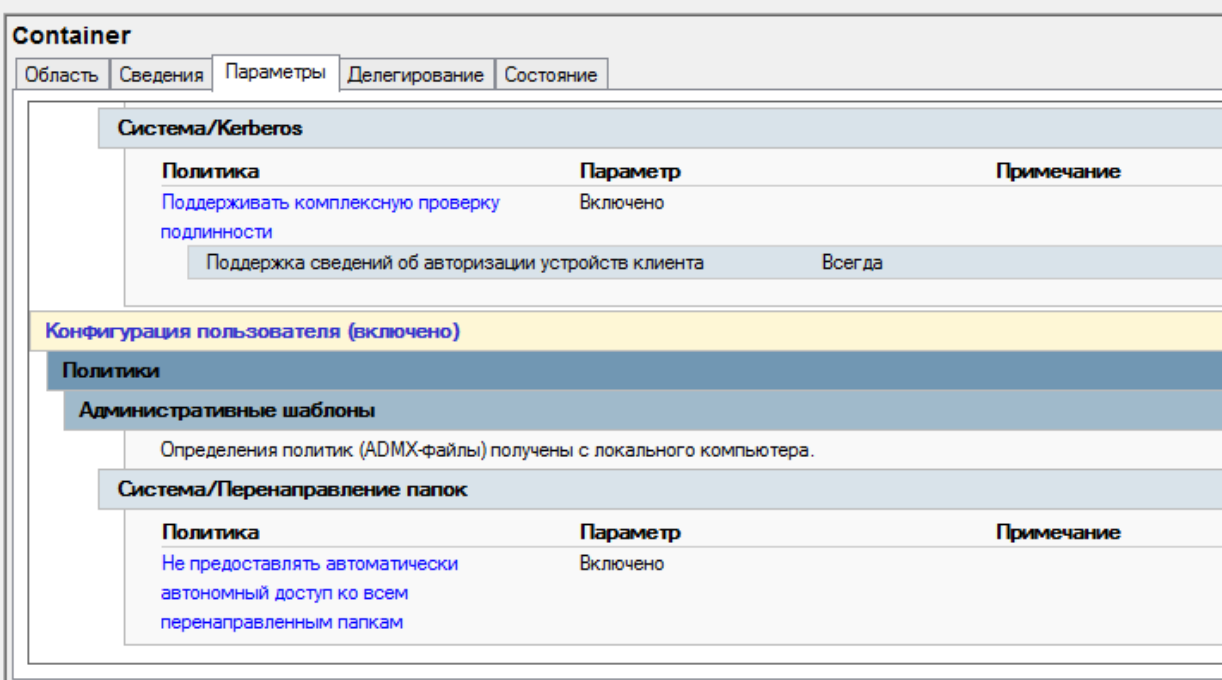




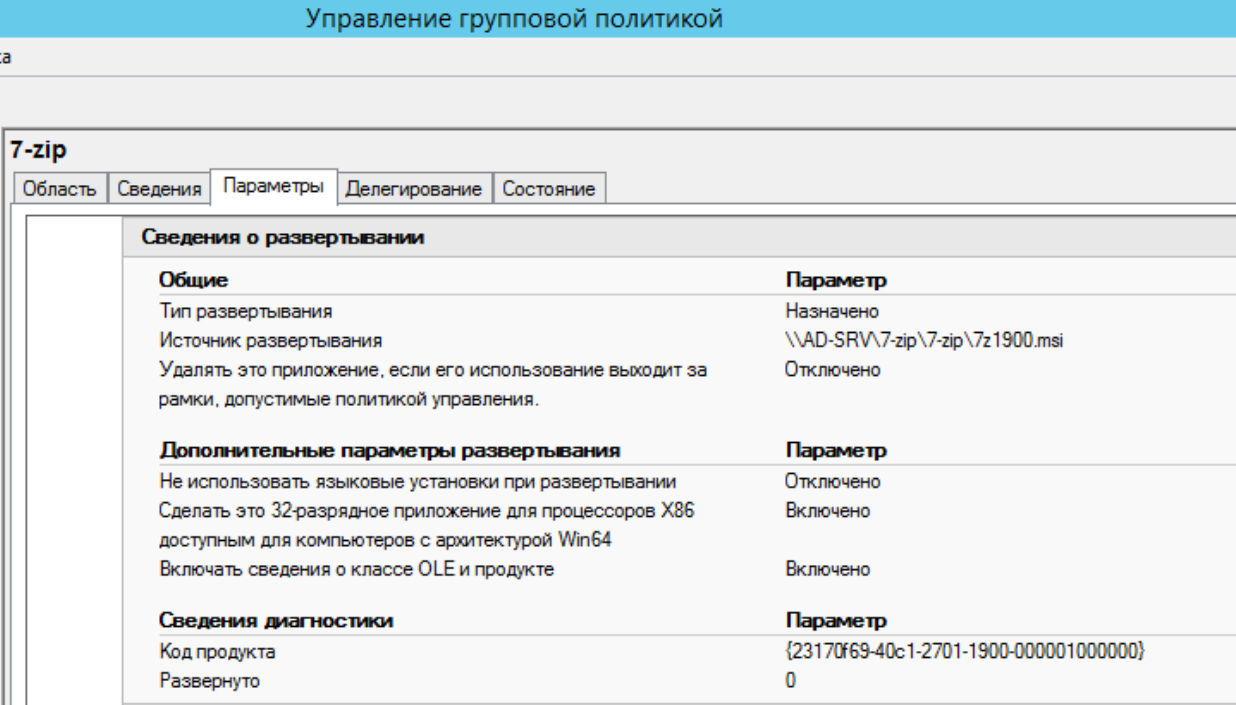
Контейнер для объектов – компьютеров и в нем групповая политика:



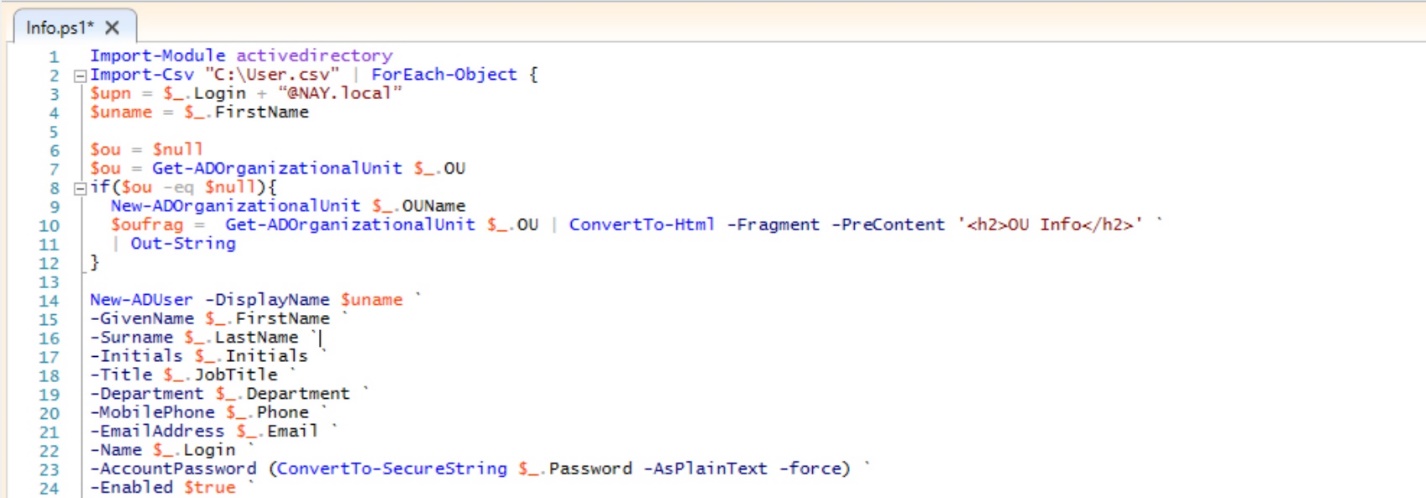


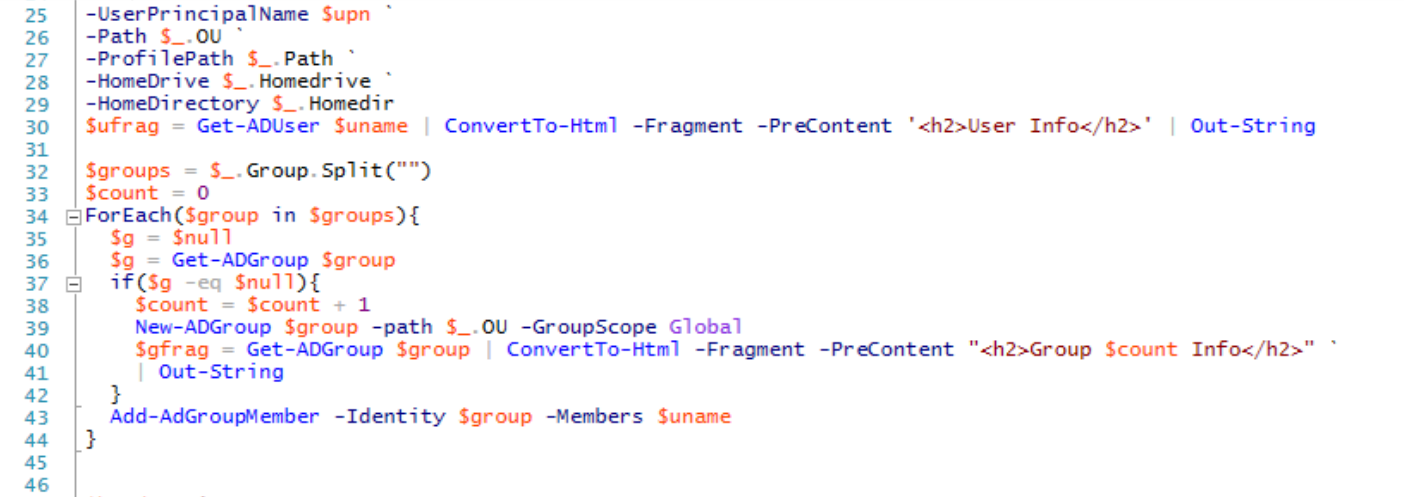


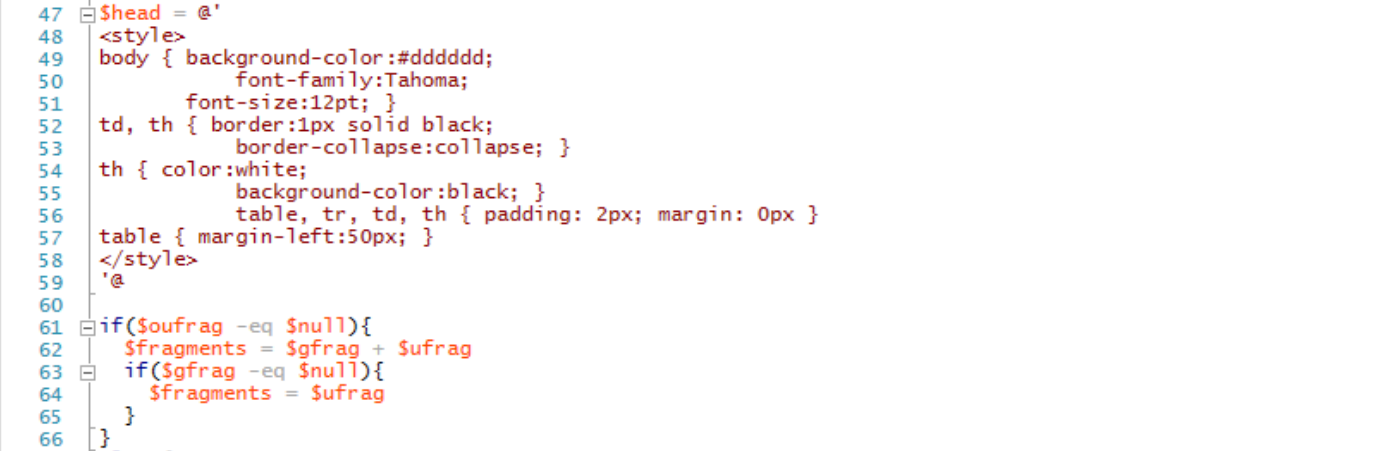
Групповая политика, с помощью которой установится на клиентском компьютере программа 7-zip:

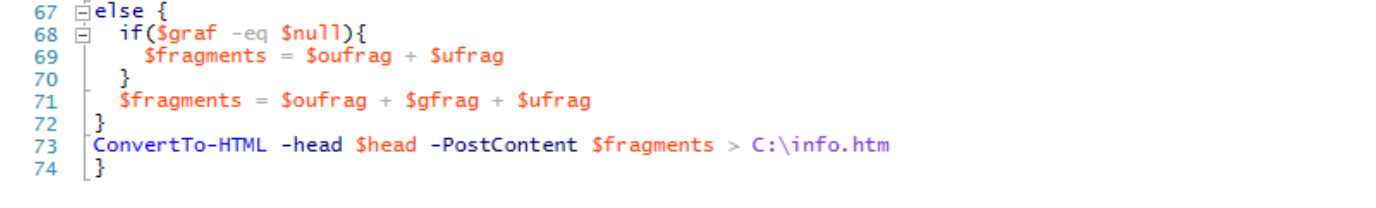


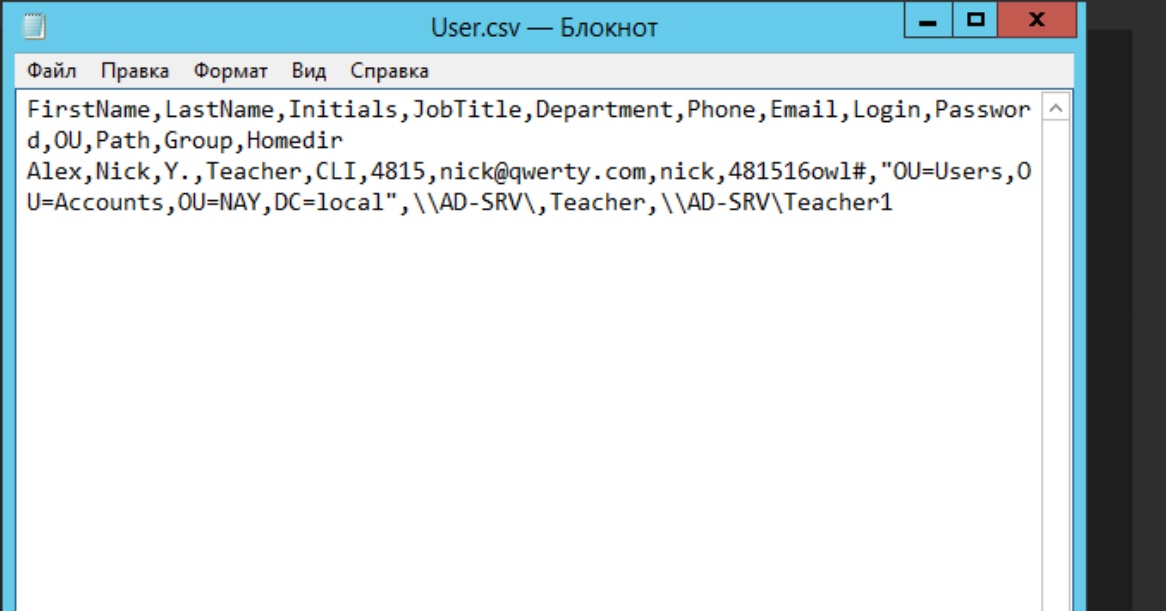
1. Приведите скрипт из части 5.











1. Как с помощью Powershell восстановить удаленный объект AD?

Восстановление объекта происходит с помощью Powershell командлетов Get-ADObject и Restore-ADObject.

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

dsquery user “OU=unit-for-delete,DC=NAY,DC=local” | dsrm -nopromt

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

Get-ADObject -Filter{lastKnownParent -eq “OU=unit-for-delete,DC=NAY,DC=local” -IncludeDeletedObjects | Restore-ADObject