

POCATOM ALD PRO

Предисловие:

ALD Pro ебать как на приколе работает. Если что-то не работает, вероятность что виноват ald pro реальная. Нормальная практика, повторять какие-то действия несколько раз, пока не сработает.

Памятка по сети:

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 172.25.2.37
    netmask 255.255.255.0
    gateway 172.25.2.1
```

(плюс маскирование сервиса Network Manager)

```
sudo systemctl stop NetworkManager
sudo systemctl disable NetworkManager
sudo systemctl mask NetworkManager
```

Установка ALD Pro на тачку CR-SRV

1. Мы учитываем что на astra выставлен уровень защищенности "Смоленск", использован весь диск и настроен LVM.(настраивается при установке astra)
2. Необходимо внести (желательно frozen) репозитории astra и отдельно ald pro

/etc/apt/sources.list:

```
deb http://172.26.72.149/astra/frozen/1.7_x86-64/1.7.5/repository-base/
1.7_x86-64 main non-free contrib
deb http://172.26.72.149/astra/frozen/1.7_x86-64/1.7.5/repository-extended/
1.7_x86-64 main contrib non-free
```

```
/etc/apt/sources.list.d/aldpro.list:
```

```
deb http://172.26.72.149/aldpro/frozen/01/2.4.0/ 1.7_x86-64 main base
```

3. Файл Hosts

Файл должен иметь формат:

```
127.0.0.1 localhost.localdomain localhost
<'IP CR-SRV'> <'Full FQDN'> <'Short FQDN'>
```

```
127.0.0.1      localhost.localdomain localhost
#127.0.1.1     alse-vanilla-gui
172.25.2.37    dc1.aldpro.izpo.me dc1
# The following lines are desirable for IPv6 capable hosts
::1           localhost ip6-localhost ip6-loopback
ff02::1       ip6-allnodes
ff02::2       ip6-allrouters
```

4. Проверить приоритет пакетов:

```
sudo cat /etc/apt/preferences.d/smolensk Ожидаемый вывод: ![[Pasted image
```

```
20241216153822.png]] 5. Обновление системы sudo apt update
```

```
sudo apt list --upgradable -a
```

```
sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew 6. Установка ALD Pro
```

```
sudo DEBIAN_FRONTEND=noninteractive apt-get install -q -y aldpro-mp aldpro-gc aldpro-
syncer sudo aldpro-server-install -d домен -n имя -p 'пароль' --ip айпи --no-reboot --
setup_syncer --setup_gc`
```

```
==ПРИ НАЛИЧИИ ОШИБОК ПОПРОБОВАТЬ ЗАПУСТИТЬ КОМАНДУ ВЫШЕ 2-3 РАЗА==
```

```
![[Pasted image 20241216154658.png]]
```

7. Проверка работы. Если эти пункты выполняются, то все работает

- После установки попробовать зайти в домен под записью admin+пароль, заданный в команде
- Зайти в браузер, должен открыться портал управления

Добавление тачек в домен

(Даже при добавлении модуля, сначала скачиваем это, а потом в веб морде добавляем куда нужно, он сам потом догружает что нужно, как в zvirt ноду добавлять)

- Выключить NetworkManager
- Настроить файл /etc/network/interfaces

- search доменная зона в /etc/resolve.conf
- Добавить репозитории в файл /etc/apt/sources.list
- Добавить репозитории ALD Pro в файл /etc/apt/sources.list.d/aldpro.list
- Запись в /etc/hosts: "127.0.0.1 localhost localhost.localdomain"
- Проверить пакеты и выполнить изменения командой: `sudo apt dist-upgrade -y -o Dpkg::Options::=--force-confnew`
- Установить ALD Pro клиент командой:
`sudo DEBIAN_FRONTEND=noninteractive apt-get install -y -q aldpro-client`
- Ввести машину в домен: `sudo /opt/rbta/aldpro/client/bin/aldpro-client-installer --domain домен --account admin --password 'пароль' --host "имя хоста" --gui --force`

Проработка заданий

1. Миграция пользователей с MS AD:

1. Подготовка:

Настройка ALD Pro

Добавление зоны перенаправления можно сделать из графического интерфейса «Роли и службы сайта Служба разрешения имен Перенаправление запросов».

1. Имя зоны = имя домена MS AD
2. Глобальные перенаправители = IP-адрес контроллера домена MS AD, с которым устанавливаются доверительные отношения
3. Остальные поля и параметры оставить без изменений После на каждом контроллере домена необходимо выполнить команды:

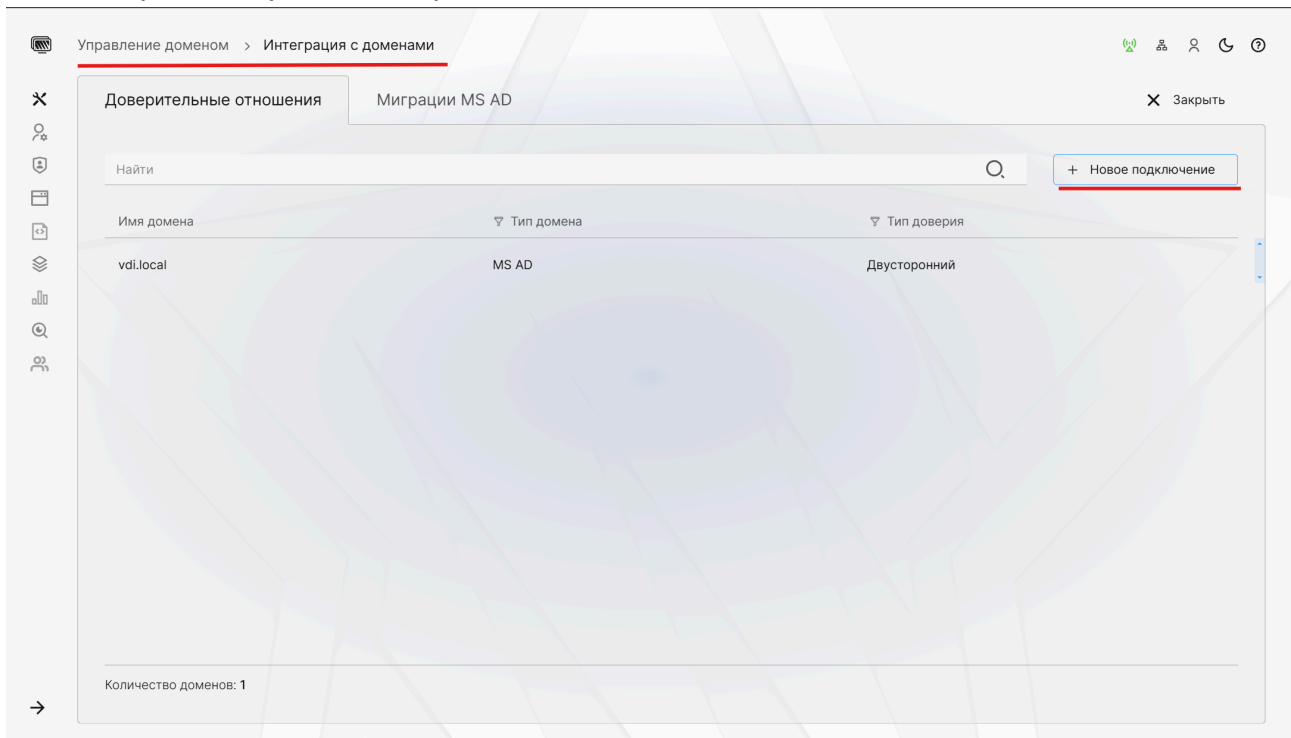
```
sudo net conf setparm global "restrict anonymous" "0" sudo aldproctl restart -i
```

Настройка MS AD

Настройка контроллера домена MS AD осуществляется согласно официальным инструкциям к MS AD. (Пуск -> Оснастка "DNS"):

4. Контекстное меню к "Серверы условной пересылки" -> Создать сервер условной пересылки.
5. В поле "DNS-домен" ввести имя домена ALD Pro.
6. Добавить IP-адрес контроллера домена ALD Pro в блоке "IP-адреса основных серверов:"

2. В веб-морде настроить доверительные отношения с AD:



Новое подключение

Настройки доверенного домена

Имя домена Поле является обязательным

Тип домена

☐ ALD Pro

☒ Active Directory

Учетная запись Поле является обязательным

Учетная запись должна обладать правами создания доверительных отношений

Пароль Поле является обязательным

Подтверждение пароля Поле является обязательным

+ Добавить


Настройки доверия

Тип доверия

☒ Двусторонние

☐ Исходящие

3. Создание миграции из MS AD



Новая миграция

✕

Настройки домена MS AD

Имя домена

обязательно

Введите значение

Контроллер домена

обязательно

Введите значение

Формат вводимых данных: {протокол}/{имя.контроллера.домена}:
{порт}, где протокол = ldap или ldaps

Базовое уникальное имя (base DN)

обязательно

Введите значение

☐ Игнорировать ошибки SSL

Настройки учетной записи MS AD

Учетная запись для миграции

обязательно

Введите значение

Учетная запись должна обладать правами администратора

Пароль

обязательно

Введите значение

Подтверждение пароля

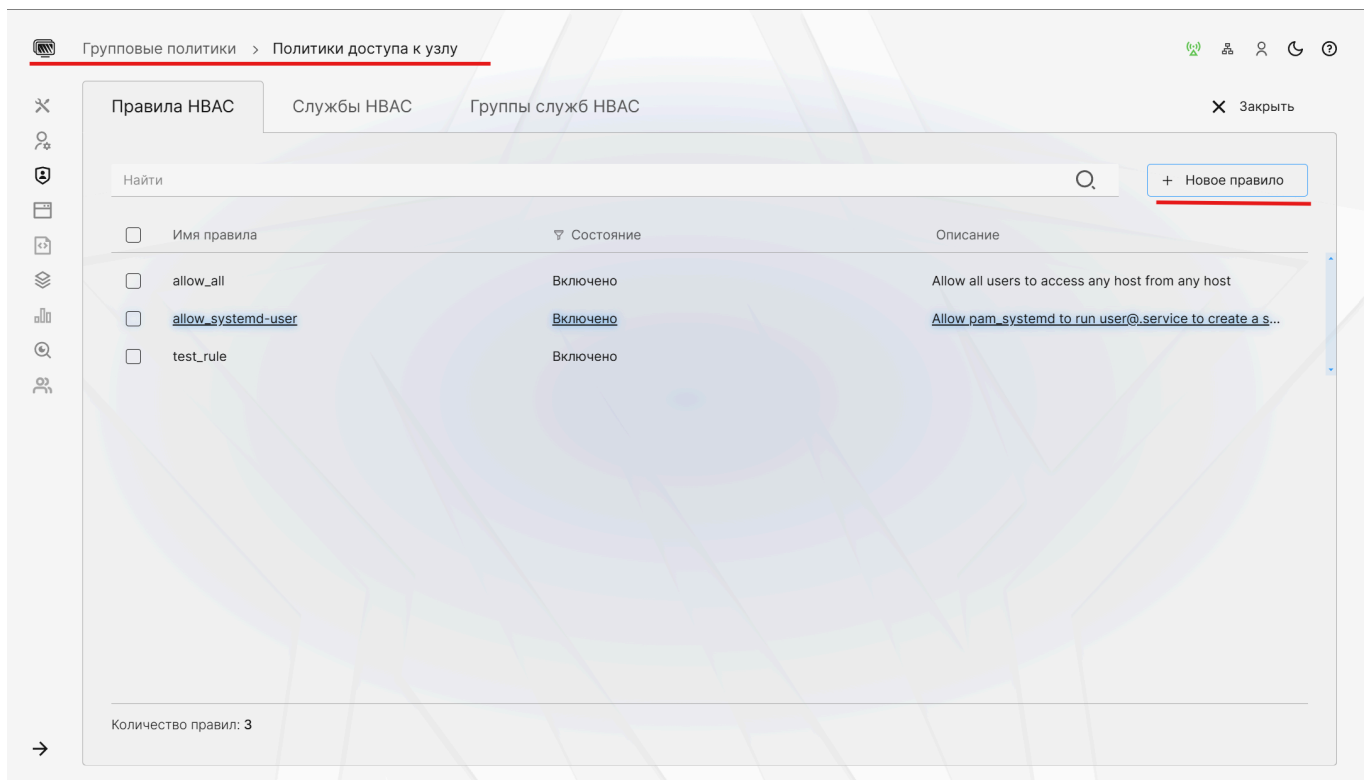
обязательно

Введите значение

+ Добавить

(Базовое DN это условное путь до группы объектов, с которой ворует все вложенные объекты. Как в запросах ldapsearch)

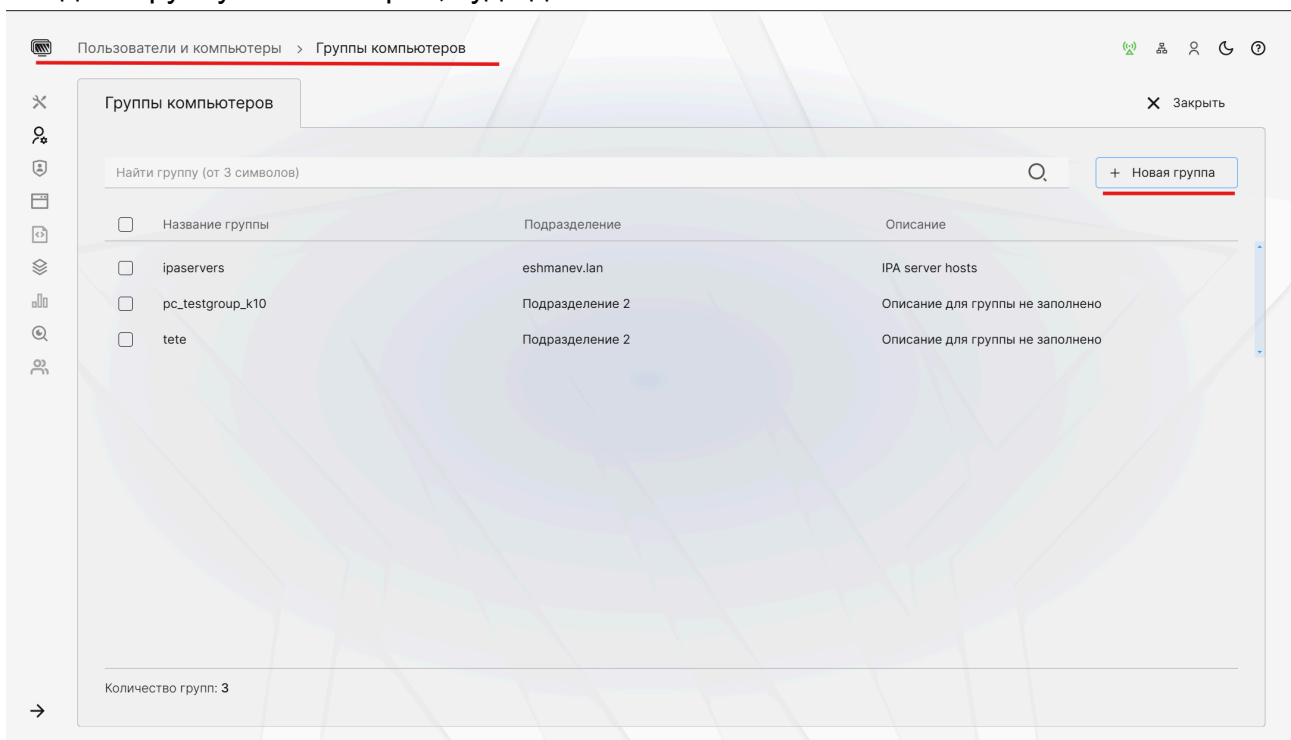
2. На BR-CLI могут аутентифицироваться только пользователи группы `branch` и локальные пользователи.



В правиле в меню "Пользователи" добавить группу branch, а в меню "Компьютеры" добавить BR-CLI

3. Пользователи группы **main** имеют право аутентифицироваться на **любом** клиентском ПК.

1. Создать группу компьютеров, куда добавить все клиентские компы

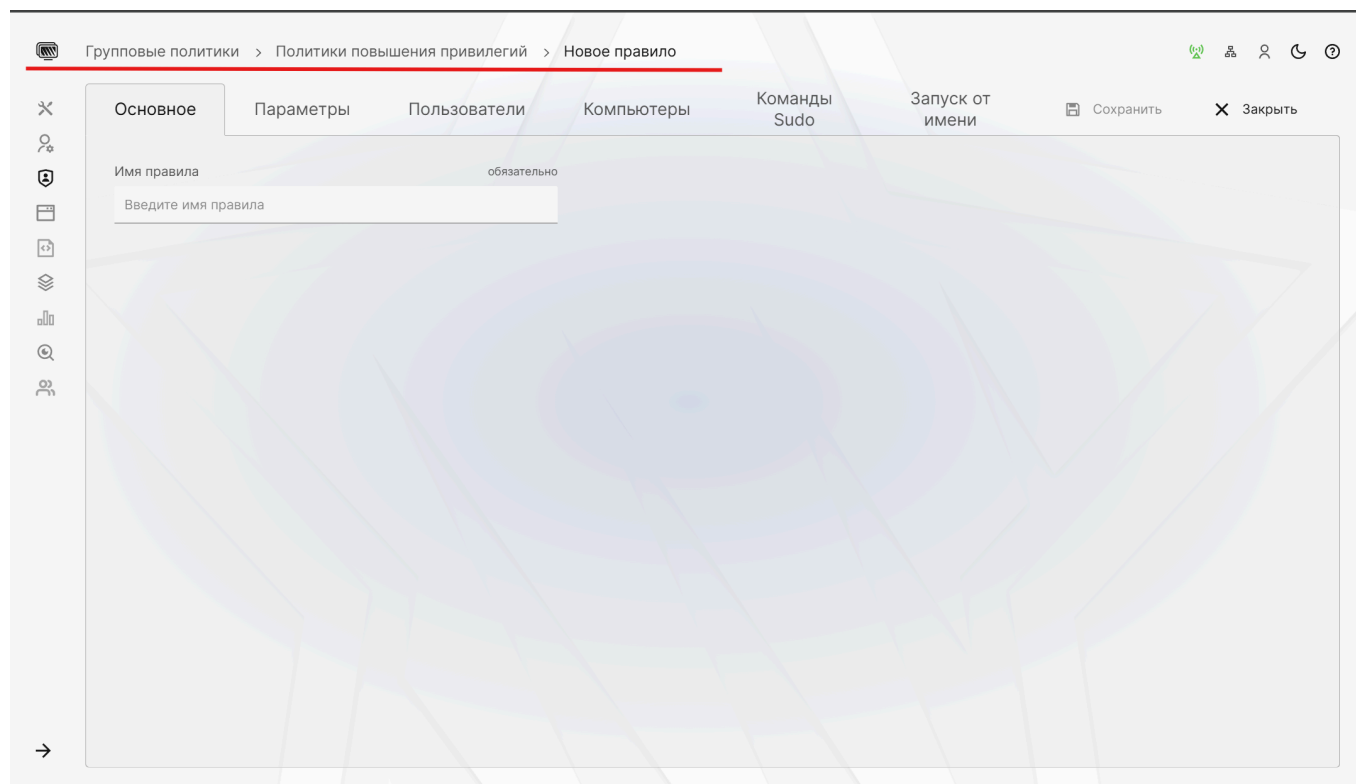


2. Аналогично создать Правило HBAC, но добавить группу компов

4. На OUT-CLI имеют право аутентифицироваться **только** пользователи группы **remotes** и локальные пользователи

Аналогично

5. Пользователи группы **main** должны иметь возможность повышать привилегии с использованием **sudo**. У других **доменных** пользователей такой возможности быть **не должно**.



Основное - Имя

Параметры - скип

Пользователи - Группа main

Компьютеры - Все компы

Команды sudo - любая команда

Запуск от имени - Ниже прокрутить и выбрать локального пользока *root*

6. Пользователи группы **branch** должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: **cat, grep, head, tail, id**.

1. Залетаем сюда и в "Команда Sudo" прописываем полный путь до команды(/usr/bin/....)

Групповые политики > Политики повышения привилегий > Новая команда

Основное Группы

Сохранить Закрыть

Команда Sudo Поле является обязательным

Введите команду Sudo

Описание

Введите описание

2. Создаем из этих команд группу

Групповые политики > Политики повышения привилегий > Новая группа

Основное Команды

Сохранить Закрыть

Имя группы Поле является обязательным

Введите имя группы

Описание

Введите описание

3. Аналогично создаем правило, но в меню команды sudo выбираем нашу группу команд

7. Все пользователи, которым разрешен доступ к sudo должны иметь возможность выполнения команд с повышенными привилегиями без ввода пароля.

По хорошему нужно создать новую политику повышения привилегий, с наивысшим приоритетом(или наименьшим)

Групповые политики > Политики повышения привилегий > Правило Sudo: sudo_2

Основное

Параметры

Пользователи

Компьютеры

Команды Sudo

Запуск от имени

Закрыть

Найти

+

Новый параметр

Параметр Sudo

Данные отсутствуют

Количество параметров: 0

Параметр Sudo

обязательно

Сохранить

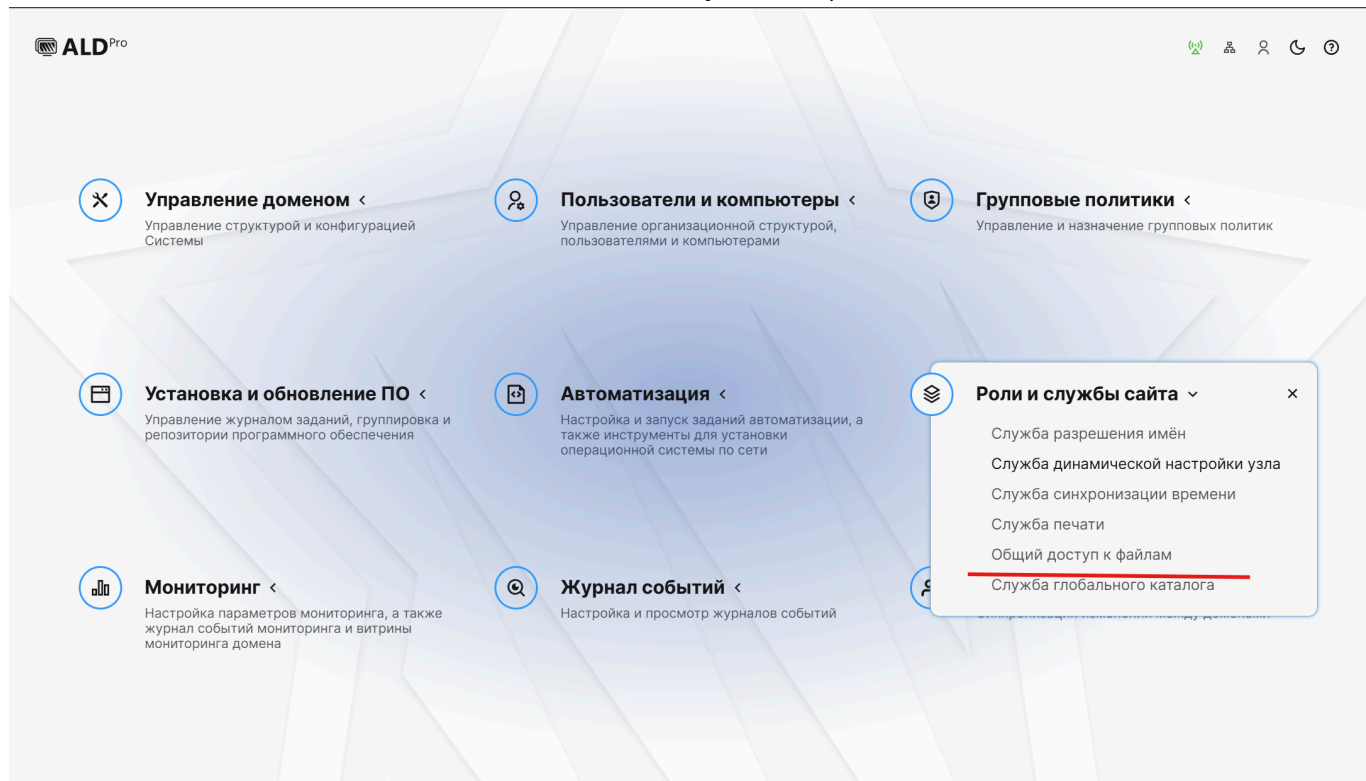
Закрыть

Введите значение

И в параметре написать "!authenticate", что отключает запрос пароля
В пользаков добавить все группы из прошлых заданий из sudo, и группы admins ald trust admin

8. Для всех пользователей домена должны быть реализованы общие каталоги.

(Вообще про сетевые каталоги хз, по идее нужно присоединить отдельный модуль для этого, но в задании я этого не нашел, так что хуй знает)



Вот тут добавляется, по идее все остальное интуитивно должно быть