

Задание 1. Подготовка доменов

Контекст

В «песочнице» развёрнуты два контроллера домена: **demo.lab** (Active Directory) и **aldpro.lab** (ALD Pro). Необходимо подготовить оба домена к дальнейшей работе: создать подразделения, добавить пользователей, настроить доверие между доменами и выполнить миграцию сотрудников отдела HR.

Задача

1. Создать в AD подразделение `FinalOfficeAD2026` с каталогами `Users` и `Computers`, добавить пользователей.
2. Создать в ALD Pro подразделение `FinalOfficeALD2026`, добавить пользователей.
3. Настроить отношение доверия между ALD Pro и Active Directory.
4. Ввести машину `IW-CLI` в домен ALD Pro, авторизоваться под пользователем `ad-user` из AD через доверие.
5. Ввести машину `IW-CLI-open` в домен ALD Pro.
6. Мигрировать группы и пользователей отдела HR из AD в ALD Pro.

Термины

Термин	Пояснение
AD	Active Directory — служба каталогов Microsoft для управления пользователями и компьютерами в домене
ALD Pro	Astra Linux Directory Pro — российская служба каталогов, аналог AD, для инфраструктуры на Astra Linux

Термин	Пояснение
OU	Organization Unit — организационная единица в каталоге (папка для группировки объектов)
Domain Controller	Контроллер домена — сервер, на котором работает служба каталогов (AD или ALD Pro)
LDAP	Lightweight Directory Access Protocol — протокол доступа к службам каталогов. Через него системы (например, IWTM) получают список пользователей и групп из AD или ALD Pro
LDAP-синхронизация	Автоматическое сопоставление пользователей и групп между службой каталогов и внешней системой через протокол LDAP
Доверие доменов	Trust Relationship — отношение между двумя доменами, позволяющее пользователям одного домена авторизоваться в другом
Миграция	Перенос пользователей, групп и других объектов из одного домена в другой с сохранением прав и связей

Параметры

Параметр	Значение
Домен AD	demo.lab
Домен ALD Pro	aldpro.lab
OU в AD	FinalOfficeAD2026
OU в ALD Pro	FinalOfficeALD2026
Пароль всех пользователей	xxXX4321

Пользователи AD

Логин	Права
admin-dm	Доменный администратор
admin-db	Доменный администратор
ad-user	Пользователь домена
ldapuser	Пользователь домена (для LDAP-синхронизации)
tmofficer	Пользователь домена (для входа в веб-консоль)

Пользователи ALD Pro

Логин	Права
ald-offadm	Доменный администратор
ald-offuser	Пользователь домена

Решение

Шаг 1. Создание OU в AD

Что нужно сделать

Создать в Active Directory подразделение `FinalOfficeAD2026` с двумя вложенными папками — `Users` и `Computers`. В `Users` добавить пять пользователей с паролем `xxXX4321`.

Ход работы

1. Открываем оснастку

Пуск → Администрирование → Active Directory — пользователи и компьютеры.

Открытая оснастка ADUC

2. Создаём OU FinalOfficeAD2026

Правой кнопкой по домену `demo.lab` → Создать → Подразделение. Вводим имя `FinalOfficeAD2026`, нажимаем ОК.

Создание OU

3. Создаём вложенные OU Users и Computers

Правой кнопкой по `FinalOfficeAD2026` → Создать → Подразделение. Вводим `Users`, ОК. Повторяем для `Computers`.

Должно получиться так:

demo.lab └─ FinalOfficeAD2026 └─ Users └─ Computers

4. Добавляем пользователей

Правой кнопкой по Users → Создать → Пользователь.

Для каждого из пяти пользователей:

Логин	Пароль
admin-dm	xxXX4321
admin-db	xxXX4321
ad-user	xxXX4321
ldapuser	xxXX4321
tmofficer	xxXX4321

При создании снимаем галочку «Требовать смену пароля» и ставим «Срок действия пароля не ограничен».

Создание пользователя

5. Назначаем права администратора

Правой кнопкой по admin-dm → Добавить в группу → пишем Domain Admins → Проверить имена → ОК.

Повторяем для admin-db.

Добавление в Domain Admins

Как проверить

- ☐ OU FinalOfficeAD2026 создано
- ☐ Внутри есть Users и Computers
- ☐ В Users — пять пользователей
- ☐ admin-dm и admin-db в группе Domain Admins

Если что-то не работает

Проблема	Что делать
Не открывается оснастка	Запустить dsa.msc из командной строки

Проблема	Что делать
Пароль не принимается	Проверить политику паролей домена
Не добавляется в Domain Admins	Убедиться, что вы вошли как администратор

Шаг 2. Создание OU в ALD Pro

Что нужно сделать

Подготовить виртуальную машину ALD Pro к работе: сменить пароль администратора, настроить DNS-резолвинг на контроллер demo.lab, перенести файл hosts с ВМ demo.lab на ALD Pro. Затем создать подразделение FinalOfficeALD2026 и добавить в него двух пользователей: ald-offadm (доменный администратор) и ald-offuser (пользователь домена). Для обоих задать пароль xxXX4321.

Ход работы

1. Первичный вход в ВМ ALD Pro

Запустите виртуальную машину ALD Pro. При первом входе используйте учётные данные по умолчанию:

Логин	Пароль
admin	Aa12345678

Система предложит **сменить пароль администратора** — задайте новый пароль и запишите его (он понадобится для входа на портал управления и для WinSCP).

“ ⚠ **Если смена пароля не предлагается** — откройте терминал и выполните команду принудительной смены:

```
kinit admin
```

Система запросит текущий пароль (Aa12345678), затем новый — введите и подтвердите.

Смена пароля администратора

2. Настраиваем DNS-резолвинг на demo.lab

Чтобы ALD Pro мог обращаться к контроллеру AD `demo.lab`, нужно указать его IP-адрес в настройках DNS.

Откройте файл:

```
nano /etc/resolv.conf
```

В строке `nameserver` укажите IP-адрес `demo.lab`:

```
nameserver 192.168.88.100
```

“ ” Как сохранить и выйти из nano:

- Сохранить изменения: `Ctrl + O`, затем `Enter`
- Выйти из редактора: `Ctrl + X`

Настройка `resolv.conf`

3. Создаём шаблон файла `hosts` на рабочем столе `demo.lab`

Файл `hosts` создаётся **один раз** как шаблон и потом раскидывается на все Linux-машины стенда — чтобы не заполнять его вручную на каждой VM.

На контроллере `demo.lab` (Windows) откройте **Блокнот** и создайте новый файл. Сохраните его на **рабочий стол** под именем `hosts` (без расширения `.txt`).

“ ” Как сохранить без расширения:

- В Блокноте: **Файл → Сохранить как**
- Тип файла: **Все файлы (*.*)**
- Имя файла: `hosts` (в кавычках, чтобы Блокнот не добавил `.txt`)
- Папка: **Рабочий стол**

Заполните файл согласно образцу на скриншоте:

Содержимое файла `hosts`

“ ” Как сохранить в Блокноте:

- Сохранить изменения: `Ctrl + S`

- **Выйти:** `Alt + F4` или закрыть окно

“ **Важно:** Сохраняйте файл **именно на рабочем столе** — это шаблон для распространения. В системную папку `C:\Windows\System32\drivers\etc\` его класть не нужно.

4. Подключаемся к ALD Pro через WinSCP

Откройте WinSCP и подключитесь к VM ALD Pro:

Параметр	Значение
Имя хоста	<code>192.168.88.30</code>
Пользователь	<code>admin</code>
Пароль	новый пароль администратора (из шага 1)
Порт	<code>22</code> (SSH)

Подключение WinSCP

“ **Важно:** WinSCP подключается по **SFTP** (через SSH). Убедитесь, что на ALD Pro запущена служба SSH.

5. Копируем файл `hosts` в домашнюю директорию `admin`

Напрямую в `/etc/` через WinSCP файл положить не получится — нужны права `root`, а пользователь `admin` их не имеет. Поэтому сначала копируем файл в домашнюю директорию.

1. В **левой панели** WinSCP откройте рабочий стол `demo.lab` — там лежит файл `hosts`
2. В **правой панели** перейдите в домашнюю директорию пользователя `admin` — обычно это `/home/admin/`
3. **Перетащите** файл `hosts` из левой панели в правую

Копирование `hosts` в `/home/admin`

6. Переносим файл `hosts` в `/etc/` через терминал

Теперь из терминала ALD Pro скопируем файл из домашней директории в `/etc/`.

Откройте терминал на ALD Pro и выполните:

```
cp /home/admin/hosts /etc/hosts
```

“  **Если скопировать не получается** — сначала переключитесь на root:

```
su -  
cp /home/admin/hosts /etc/hosts
```

Проверьте, что файл на месте:

```
cat /etc/hosts
```

Вы должны увидеть содержимое вашего шаблона.

Копирование в /etc через терминал

7. Заходим на портал управления ALD Pro

Откройте браузер и перейдите по адресу:

```
https://dc.aldpro.lab
```

Авторизуйтесь под учётной записью администратора, пароль которой вы задали на шаге 1.

“  **Если браузер ругается на сертификат** — примите исключение (для тестового стенда это допустимо).

Вход на портал ALD Pro

8. Переходим в раздел организационной структуры

В веб-интерфейсе администрирования пройдите путь: «**Пользователи и компьютеры**» → «**Организационная структура**» → выберите корневое подразделение вашего домена `aldpro.lab`.

Если выбран корень, доступны кнопки создания объектов, включая «+ **Подразделение**».

Раздел организационной структуры

9. Создаём подразделение FinalOfficeALD2026

Нажмите кнопку «+ **Подразделение**», введите название `FinalOfficeALD2026` и сохраните изменения. Кнопка «Сохранить» находится в правом верхнем углу.

Создание подразделения

Должно получиться так:

aldpro.lab

└─ FinalOfficeALD2026

Структура после создания OU

10. Добавляем пользователей

В созданном подразделении FinalOfficeALD2026 нажмите кнопку «+ Пользователь». Откроется карточка нового пользователя.

Создайте последовательно двух пользователей:

Логин	Пароль	Права
ald-offadm	xxXX4321	Доменный администратор
ald-offuser	xxXX4321	Пользователь домена

Для каждого: на вкладке «Основное» заполните обязательные поля (логин, пароль), нажмите сохранить.

“ ⚠ **Важно:** Пароль xxXX4321 должен соответствовать политике паролей ALD Pro. Если система выдаст ошибку «Пароль не соответствует требованиям политики», используйте более сложный пароль и запишите его.

Создание пользователя в ALD Pro

Список пользователей в подразделении

11. Назначаем права администратора для ald-offadm

Откройте карточку пользователя ald-offadm → перейдите на вкладку «Роли». В списке «Все роли» отметьте тип администратора, которым нужно наделить пользователя, и перенесите его в список «Выбранные роли» кнопкой [< -].

Сохраните изменения.

Назначение роли администратора

Как проверить

- ☐ Пароль администратора ALD Pro сменён
- ☐ В `/etc/resolv.conf` указан `nameserver 192.168.88.100`
- ☐ Файл `hosts` создан на рабочем столе `demo.lab` как шаблон
- ☐ Файл `hosts` скопирован через WinSCP в `/home/admin/`
- ☐ Файл `hosts` перенесён в `/etc/` командой `cp`
- ☐ Открывается портал `https://dc.aldpro.lab`
- ☐ Подразделение `Final0fficeALD2026` создано
- ☐ В подразделении есть пользователи `ald-offadm` и `ald-offuser`
- ☐ `ald-offadm` наделён ролью администратора

Если что-то не работает

Проблема	Что делать
Не предлагает сменить пароль	Выполнить <code>kinit admin</code> в терминале
Блокнот добавляет <code>.txt</code> к файлу	Сохранять через Файл → Сохранить как , тип «Все файлы», имя в кавычках: <code>"hosts"</code>
WinSCP не даёт положить файл в <code>/etc/</code>	Это нормально — копируйте в <code>/home/admin/</code> , потом через <code>cp</code> в <code>/etc/</code>
<code>cp</code> выдаёт <code>Permission denied</code>	Использовать <code>sudo cp</code> или работать от root
Не открывается <code>https://dc.aldpro.lab</code>	Принять сертификат в браузере, проверить доступность контроллера
Пароль не принимается	Использовать более сложный пароль, соответствующий политике ALD Pro

Шаг 3. Настройка доверия между доменами

Скриншоты и команды добавьте сюда.

Шаг 4. Ввод IW-CLI в домен ALD Pro

Скриншоты и команды добавьте сюда.

Шаг 5. Ввод IW-CLI-Open в домен ALD Pro

Скриншоты и команды добавьте сюда.

Шаг 6. Миграция отдела HR

Не делаем.

Revision #3

Created 2026-10-11 10:17:17 UTC by Admin

Updated 2026-10-11 13:15:53 UTC by Admin