

Инструкция по использованию графической утилиты aldpro-join

ALD Pro

Содержание

1. Общая информация об утилите aldpro-join.....	3
2. Установка пакетов.....	4
3. Привилегии, необходимые для использования утилиты.....	5
4. Использование утилиты.....	7
4.1. Запуск.....	7
4.1.1. В режиме графического интерфейса.....	7
4.1.2. В режиме командной строки.....	7
4.2. Основные параметры.....	7
5. Ввод компьютера в домен.....	9
6. Вывод компьютера из домена.....	12
7. Проверка наличия доверия с доменом.....	13
8. Обновление пароля компьютера и восстановление доверия с доменом.....	14

1. Общая информация об утилите aldpro-join

Для удобства присоединения компьютеров Astra Linux к домену ALD Pro была разработана дополнительная графическая утилита aldpro-join, которая предоставляет Windows - администраторам знакомый интерфейс и дополнительные преимущества, в том числе возможность присоединения компьютера в заданное структурное подразделение. Утилита распространяется в виде deb-пакета, который доступен для скачивания в личном кабинете. Утилита позволяет выполнять ввод компьютера с установленной ОС Astra Linux в домен ALD Pro. Версии Astra Linux поддерживаются в соответствии с матрицей совместимости.

2. Установка пакетов

1. Для корректной работы утилиты в системе должны быть предварительно установлены следующие пакеты. Их можно скачать из официальных репозиторий ALSE и ALD Pro.

```
sudo apt install aldpro-client python3-tk python3-requests  
python3-dnspython python3-psutil python3-systemd
```

2. Скачайте zip-архив aldpro-join_3.0.0.zip из личного кабинета <https://lk.astra.ru/>. Архив содержит deb-пакет, который необходимо извлечь.

3. Для установки deb-пакета на рабочей станции используйте команду:

```
sudo DEBIAN_FRONTEND=noninteractive apt-get install  
-y -q ./aldpro-join_2.0-2_amd64.deb
```

3. Привилегии, необходимые для использования утилиты

Для корректной работы утилиты aldpro-join пользователь должен иметь необходимые привилегии на ввод и вывод компьютеров из домена, включая связанные привилегии. Для делегирования необходимых привилегий необходимо выполнить следующие шаги:

1. На портале создать и назначить на пользователя роль, содержащую следующие привилегии ALD Pro:

1. DNS Zones - Manage
2. Computers - Read
3. Domain Info - Read
4. Organization Units - Read
5. Computers – Delete

2. Создать привилегию в составе которой должны быть следующие разрешения:

1. 'System: Add Hosts'
2. 'System: Add krbPrincipalName to a Host'
3. 'System: Enroll a Host'
4. 'System: Manage Host Certificates'
5. 'System: Manage Host Enrollment Password'
6. 'System: Manage Host Keytab'
7. 'System: Manage Host Principals'

Привилегию можно создать следующим образом:

```
ipa privilege-add 'наименование привилегии'
```

Добавить в созданную привилегию необходимые разрешения:

```
ipa privilege-add-permission 'наименование привилегии' \
--permissions='System: Add Hosts' \
--permissions='System: Add krbPrincipalName to a Host' \
--permissions='System: Enroll a Host' \
--permissions='System: Manage Host Certificates' \
--permissions='System: Manage Host Enrollment Password' \
--permissions='System: Manage Host Keytab' \
--permissions='System: Manage Host Principals'
```

3. Добавить новую привилегию к роли, созданной на шаге 1:

```
ipa role-add-privilege 'наименование роли'  
--privileges='наименование привилегии'
```

4. Активировать роль, назначенную на пользователя на шаге 1.

4. Использование утилиты

4.1. Запуск

4.1.1. В режиме графического интерфейса

Для запуска утилиты в графическом режиме необходимо выполнить команду:

```
aldpro-join --gui
```

Также утилиту можно запустить через меню **Пуск ► ALD Pro** ярлык **"Ввод компьютера в домен ALD Pro v2.0"** (рисунок 1).

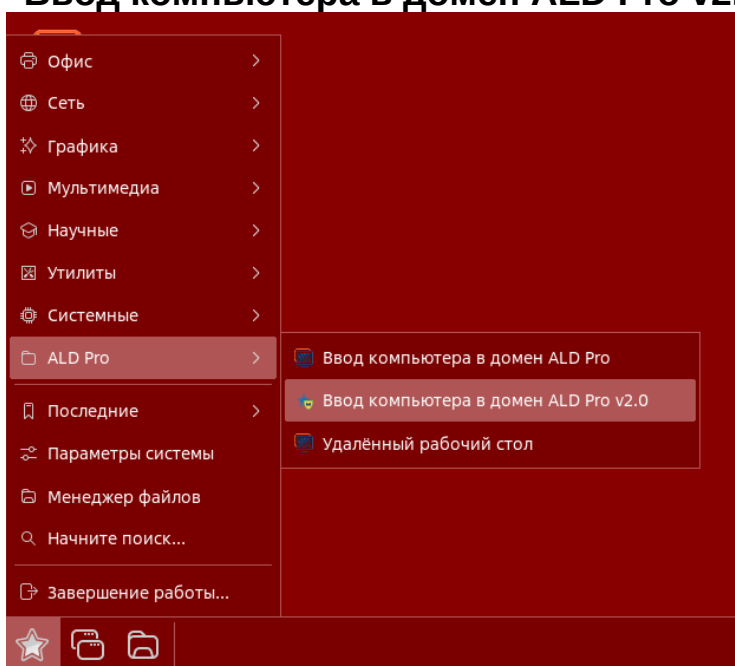


Рисунок 1. Запуск приложения для присоединения к домену v2.0

4.1.2. В режиме командной строки

Утилиту можно использовать в режиме командной строки для автоматизации ввода компьютеров в домен. Для автоматизации утилита должна быть запущена без указания ключа `--gui`:

```
sudo aldpro-join
```

4.2. Основные параметры

Синтаксис команды aldpro-join:

```
aldpro-join [-h] [-i] [-r] [-f] [-c DOMAIN] [-u ACCOUNT]
```

`[-o ORGANIZATION] [-d HOST] [-R] [-p PASSWORD]`

Примечание: Параметры утилиты доступны на её map-странице.

Параметр	Полная форма	Описание
-h	--help	Показать описание основных параметров
-i	--gui	Запуск утилиты в графическом режиме
-r	--reboot	Перезагрузить систему после выполнения команд в режиме консоли
-f	--force	Ввести в домен принудительно
-c DOMAIN	--domain DOMAIN	Домен
-u ACCOUNT	--account ACCOUNT	Учетная запись привилегированного пользователя с правами на ввод в домен
-o ORGANIZATION	-ou ORGANIZATION, --organization ORGANIZATION, --orgunits ORGANIZATION	Организационное подразделение
-d HOST	--host HOST	Имя хоста
-R	--remove	Вывод из домена
-p PASSWORD	--password PASSWORD	Пароль учетной записи привилегированного пользователя с правами на ввод в домен

5. Ввод компьютера в домен

Для присоединения компьютера к домену с помощью графической утилиты все предыдущие этапы по подготовке виртуальной машины должны быть точно такими же, включая настройку сетевого интерфейса и добавление репозитория продукта.

1. Запустите утилиту любым из указанных в п. 4.1 способом.

Положение переключателя «Состояние» указывает на то, является ли компьютер участником домена на момент запуска утилиты. Если компьютер введен в домен ранее — поле «Участник домена» будет заполнено.

2. Чтобы изменить имя компьютера, нажмите кнопку **Изменить...** напротив имени компьютера и установите желаемое значение, например, pc-14 (рисунок 2).

Обратите внимание, что после изменения имени компьютера вы сможете продолжить работу с графической утилитой, но если вы закроете ее, то повторный запуск приложения будет возможен только после перезапуска графической оболочки. Для этого необходим выход из сессии и повторный вход в систему.

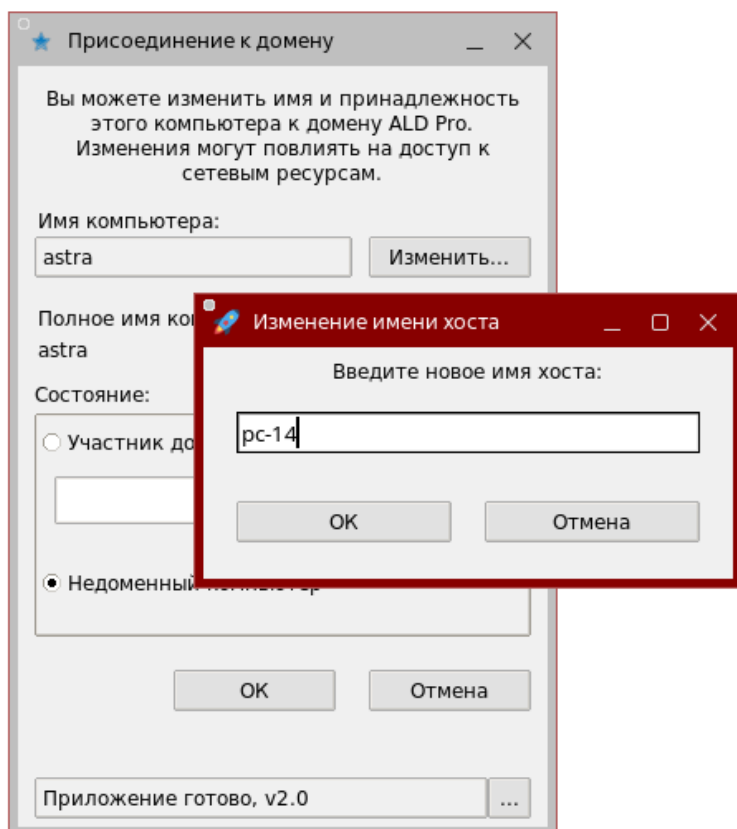


Рисунок 2. Изменение имени компьютера

3. Установите переключатель в положение **Участник домена ALD Pro** и введите имя домена, например, **ald.company.lan**. Нажмите кнопку **ОК**, чтобы начать присоединение компьютера к домену.

4. В окне аутентификации (рисунок 3) введите учетные данные доменного администратора. Это может быть пользователь admin, но можно создать отдельную учетную запись, которой будет назначена роль, содержащая необходимые привилегии (см. раздел 3).

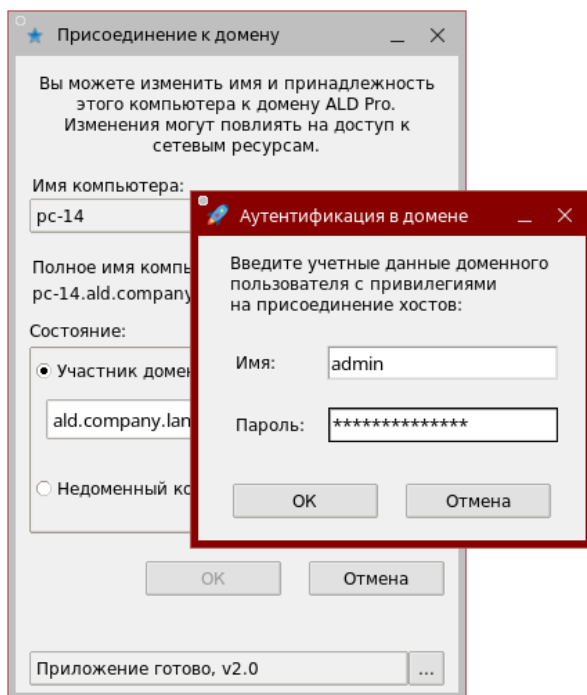


Рисунок 3. Ввод имени администратора домена для присоединения компьютера

5. Выберите организационное подразделение, в котором требуется создать учетную запись компьютера (рисунок 4).

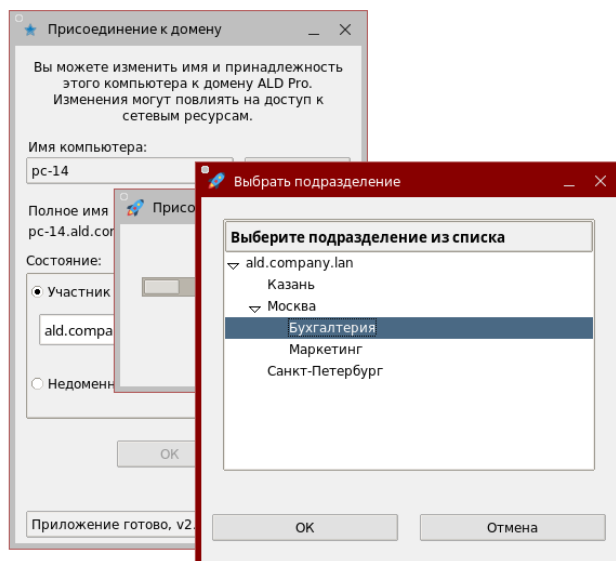
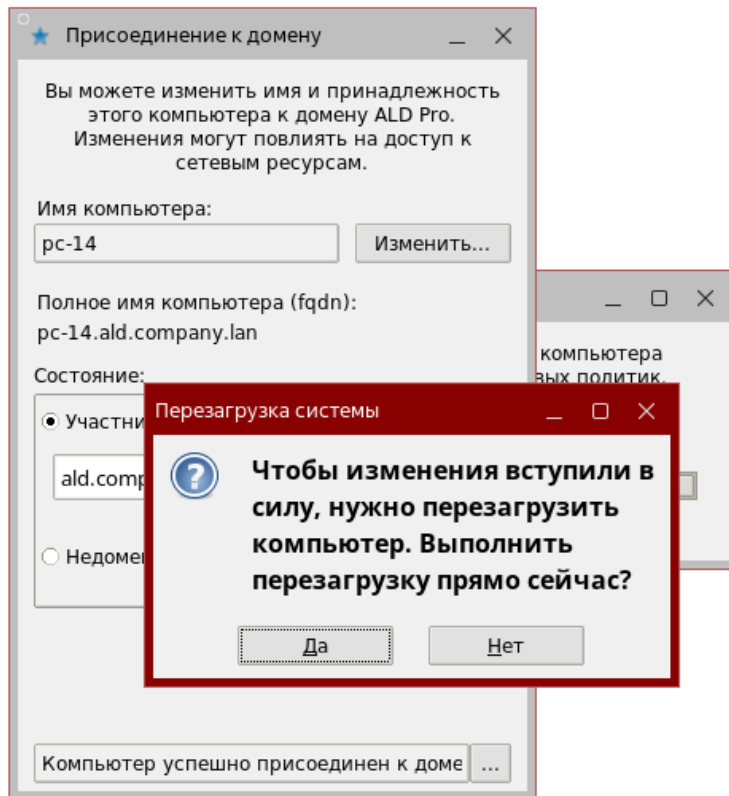


Рисунок 4. Выбор организационного подразделения

6. Если процедура присоединения компьютера ALSE к домену прошла успешно, вы увидите соответствующее уведомление. Обратите внимание, что утилита сразу применяет групповые политики, политики ПО и задания автоматизации, поэтому процедура может занять некоторое время (рисунок 5).

*Рисунок 5. Выполните перезагрузку системы*

Журнал событий вы сможете посмотреть в файле `/var/log/aldpro-join.log`. После перезагрузки компьютера вам станет доступен вход в систему доменным пользователем.

6. Вывод компьютера из домена

При выводе компьютера из домена необходимо повторно запустить приложение из-под локального администратора localadmin, установить переключатель в положение **Недоменный компьютер** и нажать кнопку **ОК**. Учетная запись компьютера и его DNS-записи будут удалены из домена.

После вывода машины из домена рекомендуется сразу выполнить перезагрузку.

7. Проверка наличия доверия с доменом

При вводе компьютера в домен для него создается учетная запись, пароль которой сохраняется в файле /etc/krb5.keytab. Если компьютер располагает актуальным паролем от своей учетной записи в домене, это означает, что между компьютером и доменом установлены «доверительные отношения» или «доверие с доменом».

При восстановлении компьютера из старой резервной копии либо по истечении срока действия пароля хоста вы можете столкнуться с тем, что он потеряет доверие с доменом. В домене FreeIPA пароль компьютера автоматически не обновляется, но вы можете настроить доп. параметр групповой политики ALD Pro, с помощью которого реализовать автоматическое обновление, поэтому в утилиту aldpro-join встроен механизм для проверки и восстановления доверия с доменом.

Чтобы проверить актуальность пароля компьютера, нажмите кнопку **Проверить...** напротив имени домена. При наличии доверия с доменом в поле **Версия ключа и дата выдачи** будет отображаться значение в следующем формате: **<Версия пароля> <Дата изменения пароля> <Время изменения пароля>** (рисунок 6).

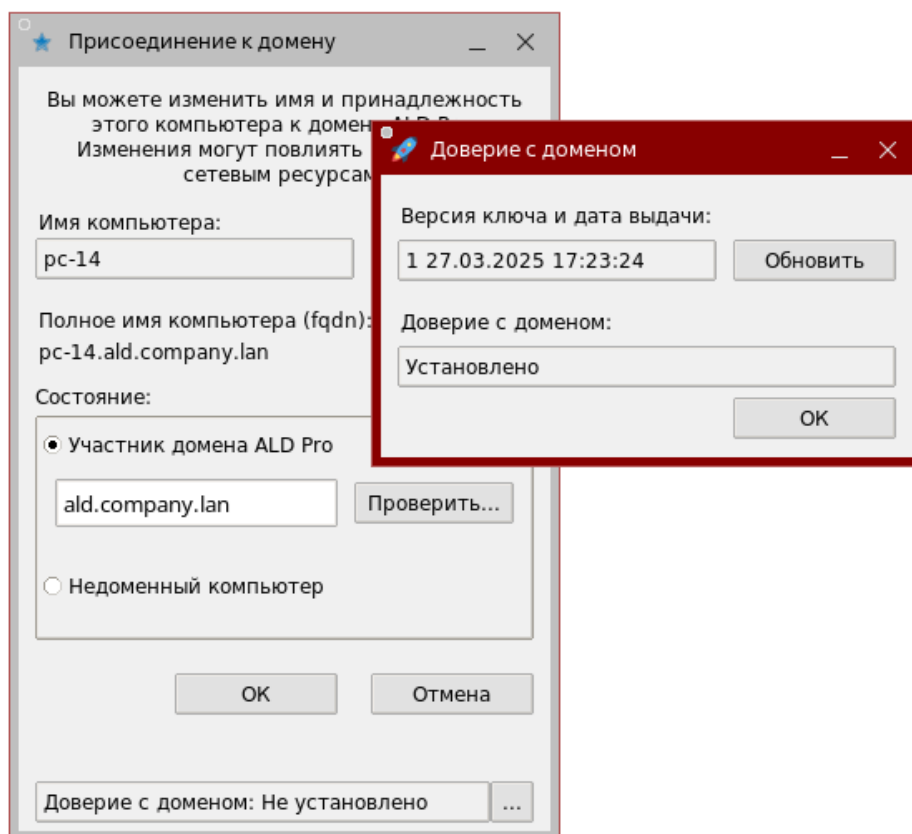


Рисунок 6. Проверка доверия с доменом

8. Обновление пароля компьютера и восстановление доверия с доменом

Если нажать кнопку **Обновить**, то приложение установит компьютеру новый пароль и сохранит его в файл `/etc/krb5.keytab` (рисунок 7).

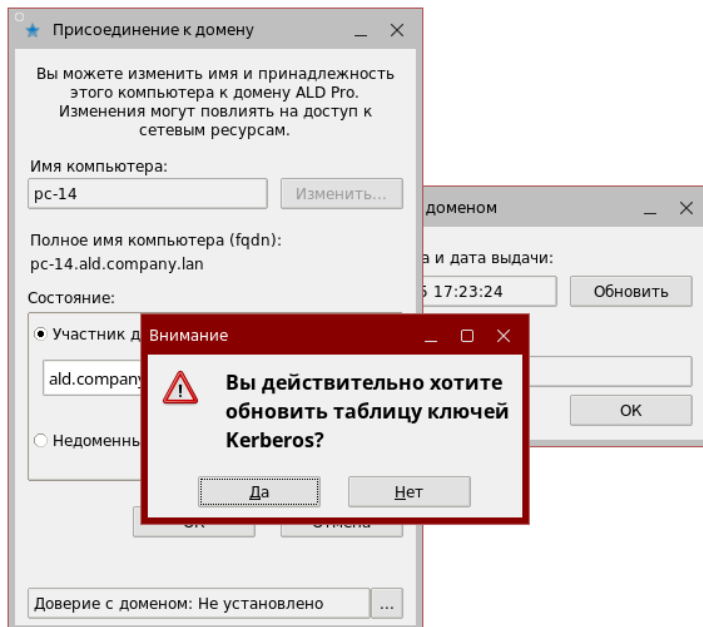


Рисунок 7. Обновление пароля компьютера

Если в момент обновления пароля у компьютера будет доверие с доменом, то пароль будет обновлен из-под учетной записи компьютера автоматически. Если компьютер не будет располагать актуальным паролем, то для восстановления доверия потребуется ввести учетные данные администратора домена или любого другого пользователя, который обладает достаточными привилегиями.