

Инструкция по установке контроллера домена ALD Pro

1 Подготовка к установке

Обратите внимание:

- Все необходимые пакеты и зависимости уже включены в образ.
- Имя пользователя может быть любым.
- Для облегчения запуска приложения, при входе пользователя по SSH реализован автоматический запуск приложения путем добавления соответствующего кода в `~/.bashrc`.

Минимальные системные требования:

- CPU: 8
- RAM: 16 Gb
- SSD: 50 Gb

2 Предварительная конфигурация установщика

2.1 Переменные для автоматической установки виртуальной машины в Яндекс Облаке можно передать с помощью графического интерфейса и через terraform.

Пример передачи параметров через веб-интерфейс:

Метаданные ▼ ?

! Настройки метаданных могут повлиять на работоспособность виртуальной машины.
Меняйте их только если вы точно знаете, что хотите сделать.

domainname	ald.company.lan	×
hostname	dc01	×
password	P@ssw0rd	×
Добавить поле		

Пример передачи параметров через terraform:

```
metadata = {
  serial-port-enable = 0
  user-data          = "${data.template_file.userdata-01.rendered}"

  domainname        = "ald.company.lan"
  hostname           = "dc01"
  password           = "P@ssw0rd"
}
```

2.2. Установщик ожидает следующие параметры, формат и регистр названий должен соответствовать списку:

- domainname
- hostname
- password

2.3 В момент передачи параметров установщик не валидирует значения переданных параметров, валидация значений произойдет позднее, на этапе проверки формы.

2.4 Возможно частичное заполнение параметров. Порядок заполнения может быть любым.

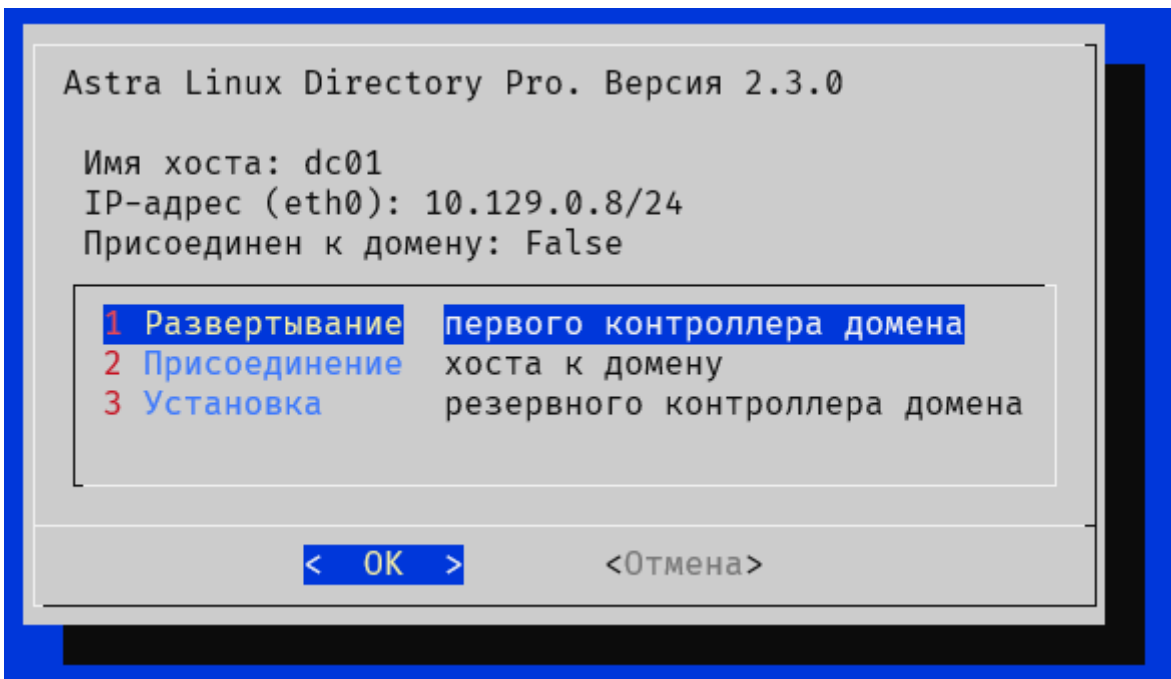
Важно: учитывайте следующие требования перед установкой:

- Права root
 - Скрипт установки ALDPro должен быть запущен с правами суперпользователя (root).
 - Если вы не вошли в систему как root, используйте команду `sudo` перед запуском скрипта.
 - Если у вас нет прав root, установка не начнется, и вы получите сообщение об ошибке.
 - Отсутствие установленного контроллера домена
 - Перед началом установки убедитесь, что на вашем сервере не установлен контроллер домена ALD Pro.
 - Если контроллер домена уже установлен, вы увидите сообщение: "Сервер уже сконфигурирован как контроллер домена", и установка будет прервана.
 - Предотвращение параллельного запуска
 - Скрипт использует механизм блокировки, чтобы предотвратить запуск нескольких экземпляров одновременно.
 - Если вы попытаетесь запустить второй экземпляр скрипта, пока первый все еще работает, второй экземпляр не запустится.
-

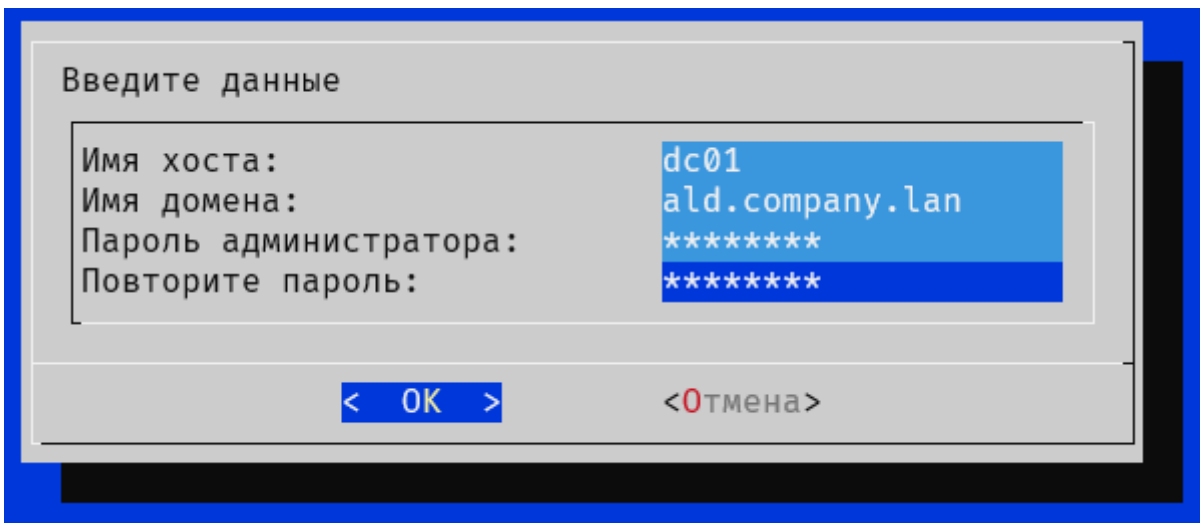
3 Запуск установщика и настройка первого контроллера домена

3.1. Для запуска установщика есть два варианта:

- Выйдите из системы и снова войдите по ssh. Установщик должен запуститься автоматически.
- Или выполните вручную команду `sudo python3 /usr/sbin/aldpro-dc-installer`



3.2. Выберите пункт меню «1 Развертывание первого контроллера домена». Появится форма для ввода данных:



Вам нужно будет указать следующую информацию:

- Имя хоста сервера
- Доменное имя
- Пароль администратора домена
- Подтверждение пароля администратора домена

Параметры будут предзаполнены, если соответствующие параметры были переданы при создании виртуальной машины.

3.3. Введите запрашиваемые данные, учитывая следующие требования.

3.3.1 Имя хоста должно быть валидным именем NetBIOS. Система использует следующее правило для проверки корректности NetBIOS имени:

```
netbios_regex = r'^[a-zA-Z0-9][a-zA-Z0-9\-\.]{0,14}[a-zA-Z0-9]$'
```

Учитываются следующие требования:

1. Общая длина: NetBIOS имя должно быть от 1 до 16 символов.
2. Допустимые символы:
 - a. Буквы латинского алфавита (a-z, A-Z)
 - b. Цифры (0-9)
 - c. Дефис (-) и точка (.)
3. Особые правила:
 - a. Имя должно начинаться с буквы или цифры
 - b. Имя должно заканчиваться буквой или цифрой
 - c. Дефисы и точки могут использоваться только внутри имени, не в начале и не в конце

Примеры допустимых NetBIOS имен:

- SERVER1
- DEV-MACHINE
- TEST.NODE
- A123456789012345 (максимальная длина в 16 символов)

Примеры недопустимых NetBIOS имен:

- SERVER_1 (содержит недопустимый символ '_')
- -TESTSERVER (начинается с дефиса)
- DEVELOPMENT.SERVER (превышает максимальную длину в 16 символов)
- TEST. (заканчивается точкой)

3.3.2 Доменное имя должно быть корректным.

Система использует следующее правило для проверки корректности имени домена:

```
domain_regex = r'^([a-z0-9]+(-[a-z0-9]+)*\.)+[a-z]{2,}$'
```

Учитываются следующие требования:

1. Имя домена должно состоять из одного или более слов, разделенных точками.
2. Каждое слово может содержать:
 - a. Строчные буквы латинского алфавита (a-z)
 - b. Цифры (0-9)
 - c. Дефисы (-), но не в начале или конце метки
3. Домен верхнего уровня (последняя часть после точки) должен состоять как минимум из двух букв.

Примеры допустимых имен доменов:

- ald.lan
- ald.company.lan
- sub-ald.company-site.com.lan

Примеры недопустимых имен доменов:

- EXAMPLE.COM (содержит заглавные буквы)
- example.c (домен верхнего уровня слишком короткий)
- -example.com (начинается с дефиса)
- example-.com (заканчивается дефисом перед точкой)

3.3.3 Пароль администратора должен быть достаточно сложным и длинным

Система использует следующее правило для проверки надежности пароля:

```
password_regex = r'^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[!@#$%^&*(){}|;:<>.,?]).{8,}$'
```

Учитываются следующие требования:

1. Минимальная длина: Пароль должен содержать не менее 8 символов.
2. Обязательные элементы (пароль должен содержать как минимум по одному символу из каждой категории):
 - a. Строчные буквы латинского алфавита (a-z)
 - b. Заглавные буквы латинского алфавита (A-Z)
 - c. Цифры (0-9)
 - d. Специальные символы (например, !@#\$%^&*()+{}|;:<>.,?) или подчеркивание

Примеры допустимых паролей:

- P@ssw0rd (минимальная длина, содержит все требуемые элементы)
- Str0ng!Password (более длинный пароль с всеми требуемыми элементами)
- C0mplex_P@ssword123 (сложный пароль, превышающий минимальные требования)

Примеры недопустимых паролей:

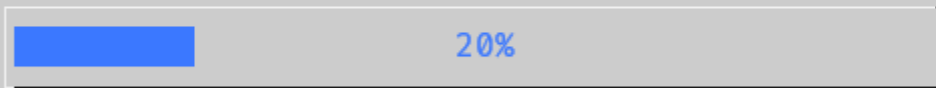
- password (нет заглавных букв, цифр и специальных символов)
- PASSWORD123 (нет строчных букв и специальных символов)
- Pass123! (менее 8 символов)
- StrongPass (нет цифр и специальных символов)

3.4. После ввода данных начнется процесс установки и настройки контроллера домена. Этот процесс состоит из нескольких этапов:

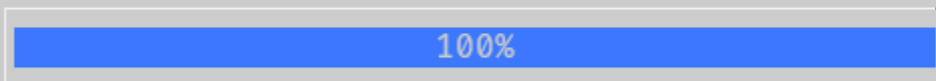
1. Конфигурация сервера
 - a. Настройка сетевых параметров
 - b. Настройка hostname
2. Установка необходимых пакетов, если они отсутствуют
 - a. Установка aldpro-mp, aldpro-gc, aldpro-synsger
3. Продвижение сервера до контроллера домена
 - a. Запуск скрипта aldpro-server-install
4. Конфигурация DNS
 - a. Настройка DNS-форвардера
 - b. Настройка дополнительных параметров BIND

3.5. Процесс установки может занять некоторое время. Прогресс установки будет отображаться в окне установщика.

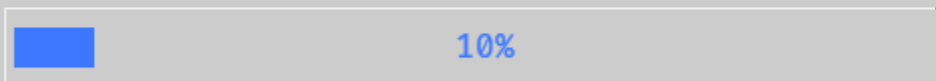
1/4 : Обновление списка пакетов



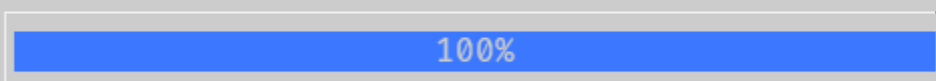
2/4 : Продвижение сервера успешно запущено.



3/4 : Запущен стейт
[event/software_installed]



4/4 : Конфигурация DNS



3.6. После завершения установки, система попросит перезагрузить компьютер.

Выполнено. Для применения настроек необходимо выполнить перезагрузку вручную.

3.7. В случае завершения установки с ошибкой, система укажет на лог файл с подробным описанием проделанных шагов.

Выполнение скрипта завершено с ошибкой. Подробности в /var/log/aldpro-role-installer.log

4 Проверка установки

4.1. После перезагрузки войдите в систему по ssh с учетными данными администратора домена.

После продвижения сервера до контроллера домена станет доступной возможность подключения к серверу по ssh с помощью пароля. В зависимости от производительности сервера, может потребоваться подождать некоторое количество времени до того, как загрузятся все необходимые доменные службы.

Возможность подключения с ключом и с именем пользователя указанным при создании виртуальной машины так же остается.

- Логин: admin
- Пароль: указанный на форме ввода при развертывании контроллера домена

4.2. Откройте терминал и выполните следующую команду для проверки статуса домена:

```
sudo ipactl status
```

Эта команда должна показать доступность доменных служб:

```
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
smb Service: RUNNING
winbind Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

Так же можно использовать специальную утилиту aldproctl:

```
sudo aldproctl status
```

Эта команда должна показать доступность доменных служб включая службы ALD Pro:

```
.....Сервисы ALD Pro.....
Сервис aldpro-mp-services: ЗАПУЩЕН
Сервис aldpro-canclient: ЗАПУЩЕН
Сервис ad-salt-canrunner: ЗАПУЩЕН
Сервис syncer: ОСТАНОВЛЕН
Сервис syncer.timer: ЗАПУЩЕН
Сервис globalcatalog: ЗАПУЩЕН
Сервис ipa-gcsyncd: ЗАПУЩЕН
.....Сервисы FreeIPA.....
Сервис Directory Service: ЗАПУЩЕН
Сервис krb5kdc: ЗАПУЩЕН
Сервис kadmin: ЗАПУЩЕН
```

Сервис named: ЗАПУЩЕН
Сервис httpd: ЗАПУЩЕН
Сервис ipa-custodia: ЗАПУЩЕН
Сервис smb: ЗАПУЩЕН
Сервис winbind: ЗАПУЩЕН
Сервис ipa-otpd: ЗАПУЩЕН
Сервис ipa-dnskeysyncd: ЗАПУЩЕН
.....Другие сервисы.....
Сервис celery: ЗАПУЩЕН
Сервис celerybeat: ЗАПУЩЕН

4.3. Проверьте работу DNS, выполнив команду:

```
host -t SOA имя_вашего_домена
```

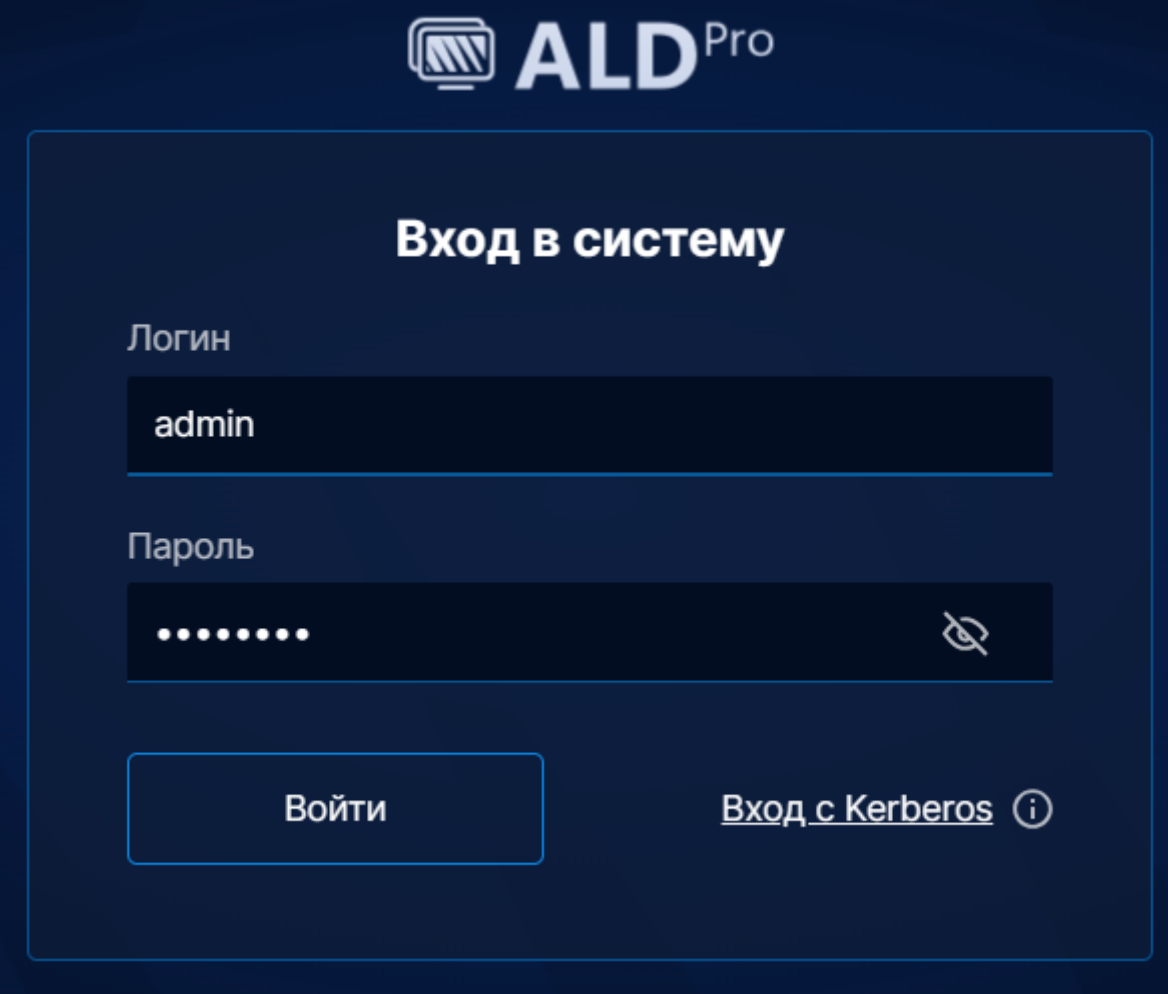
Команда должна вернуть SOA запись вашего домена с указанием на контроллер домена. Пример:

```
host -t SOA ald.company.lan
```

```
ald.company.lan has SOA record dc01.ald.company.lan. hostmaster.ald.company.lan.  
1729158002 3600 900 1209600 3600
```

4.4. Проверьте работу портала по пути https://<ip_address>/ad/ui

Должна быть доступна форма следующего вида:



ALD^{Pro}

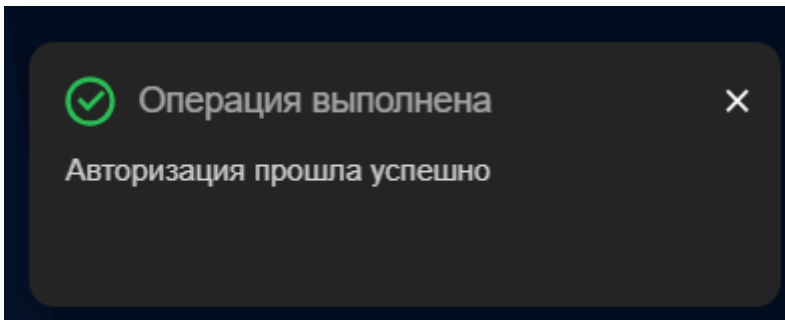
Вход в систему

Логин

Пароль

[Войти](#) [Вход с Kerberos](#) ⓘ

Аутентификация пользователя должна успешно проходить:

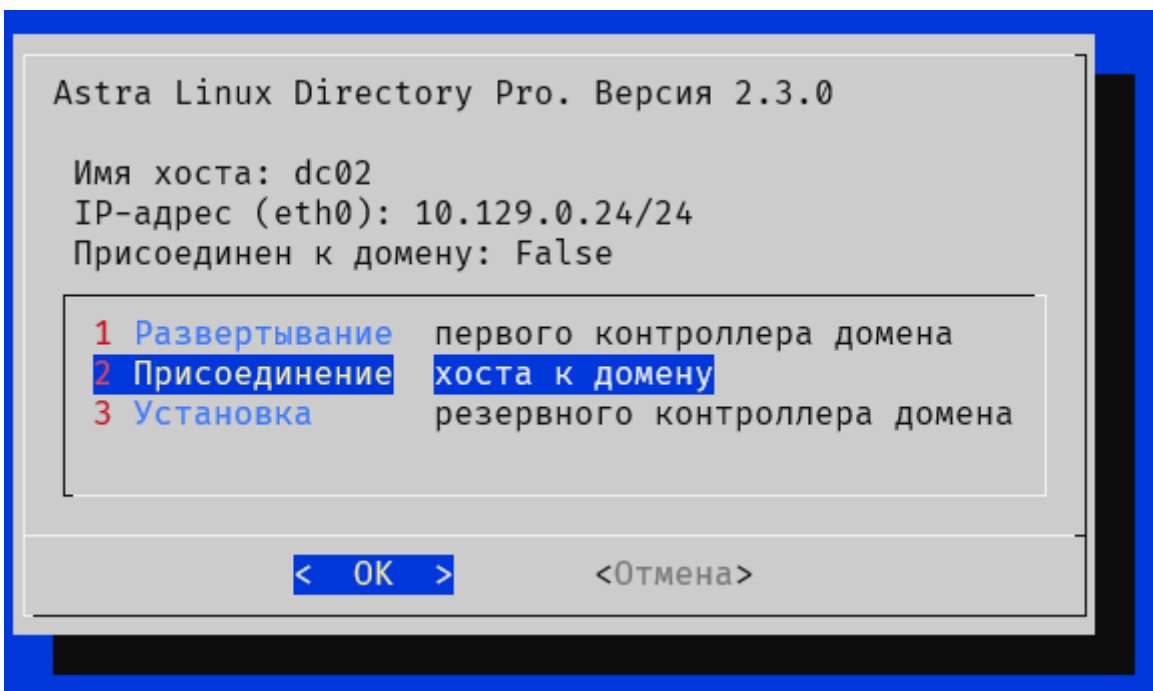


Если все шаги выполнены успешно, ваш первый контроллер домена должен быть установлен и настроен.

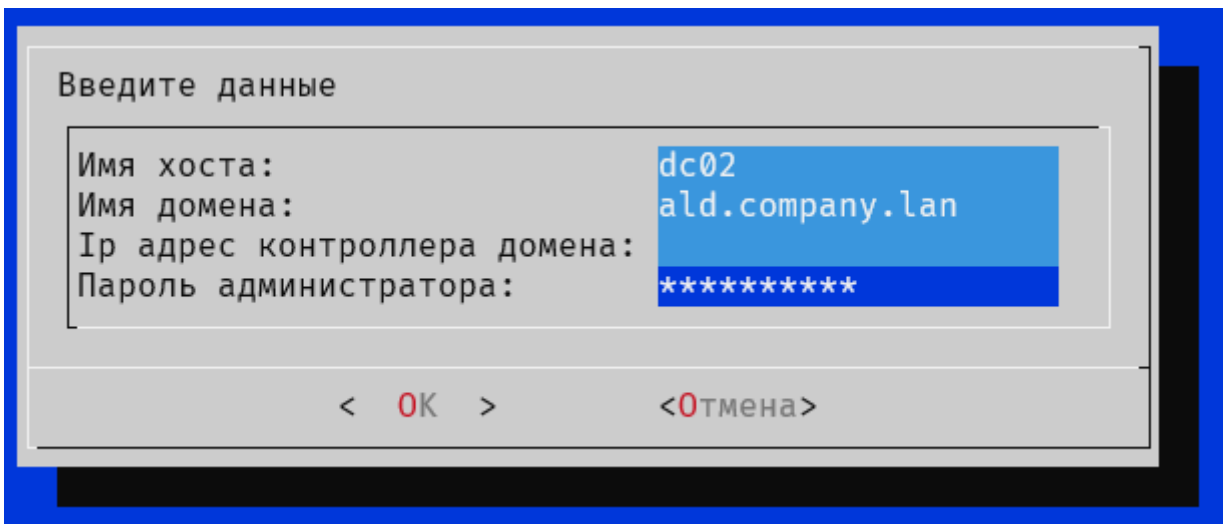
5 Настройка резервного контроллера домена

Для настройки резервного контроллера домена необходимо сначала присоединить сервер к домену.

5.1. Выберите «2 Присоединение хоста к домену».



Появится форма для ввода данных:



Вам нужно будет указать следующую информацию:

- Имя хоста сервера
- Доменное имя
- IP-адрес контроллера домена
- Пароль администратора домена

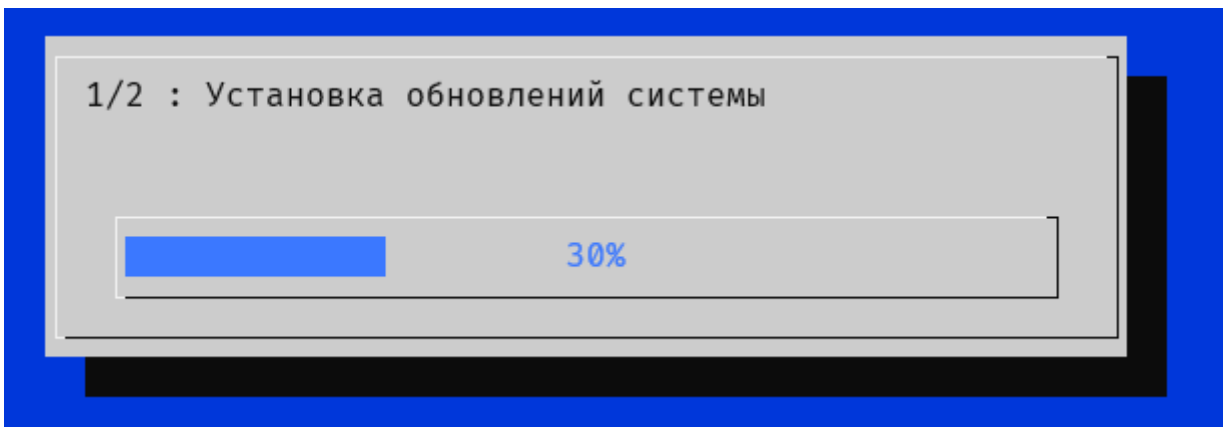
Параметры будут предзаполнены, если соответствующие параметры были переданы при создании виртуальной машины (Кроме поля "IP-адрес контроллера домена").

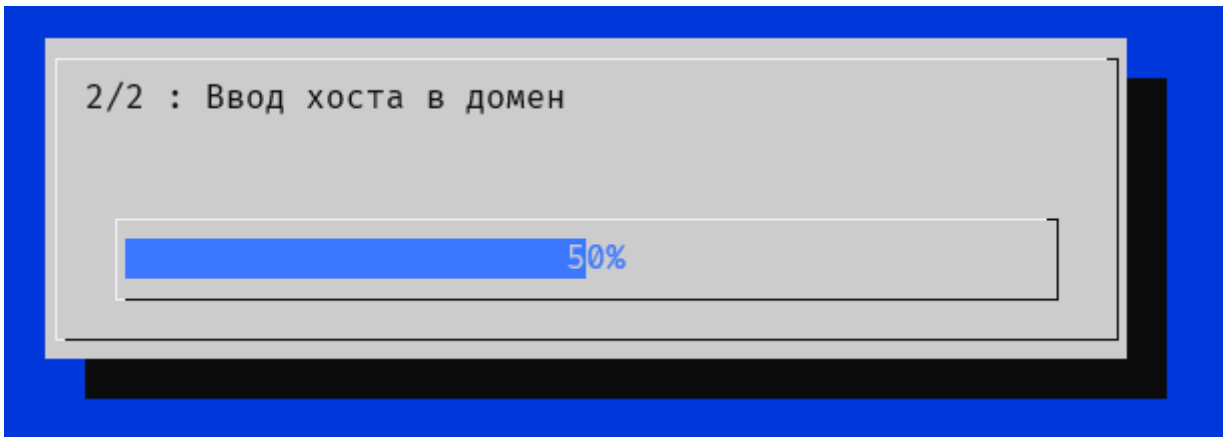
5.2. Введите запрашиваемые данные.

5.3. После ввода данных начнется процесс присоединения к домену. Этот процесс состоит из нескольких этапов:

1. Конфигурация сервера
 - a. Настройка сетевых параметров
 - b. Настройка hostname
2. Установка необходимых пакетов, если они отсутствуют
 - a. Установка aldpro-client
3. Присоединение сервера к домену
 - a. Запуск скрипта aldpro-client-installer

5.4. Процесс присоединения может занять некоторое время. Прогресс присоединения будет отображаться в окне установщика.





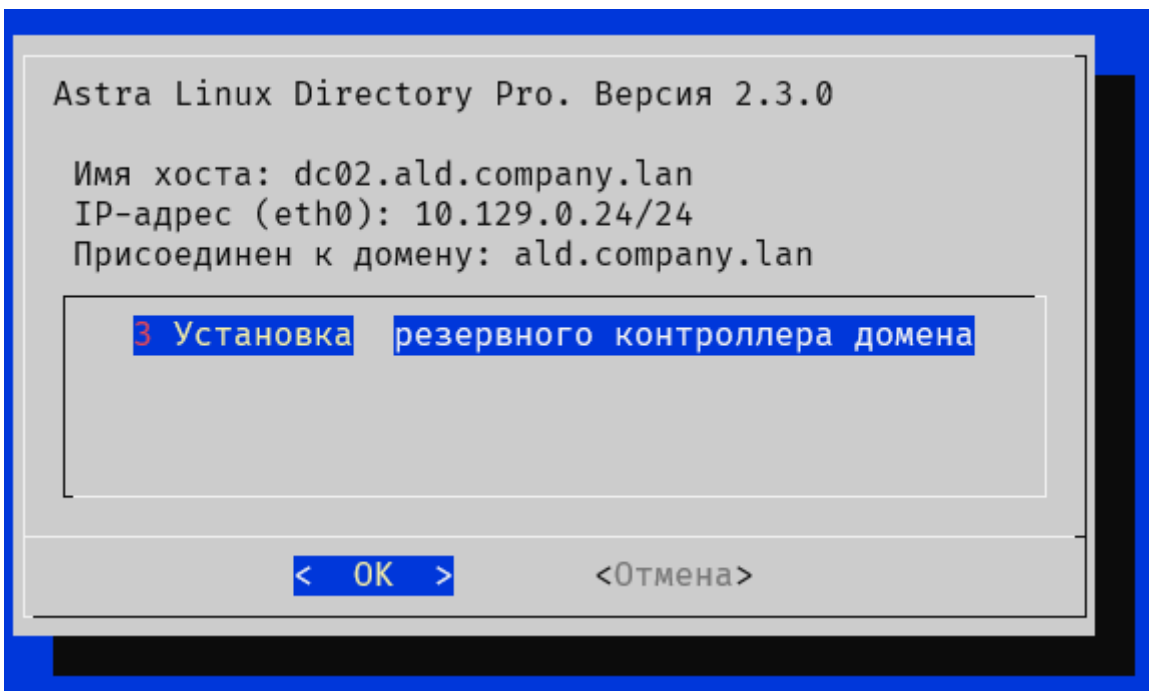
5.5. После завершения присоединения, система попросит перезагрузить компьютер.
Выполнено. Для применения настроек необходимо выполнить перезагрузку вручную.

5.6. В случае завершения установки с ошибкой, система укажет на лог файл с подробным описанием проделанных шагов.

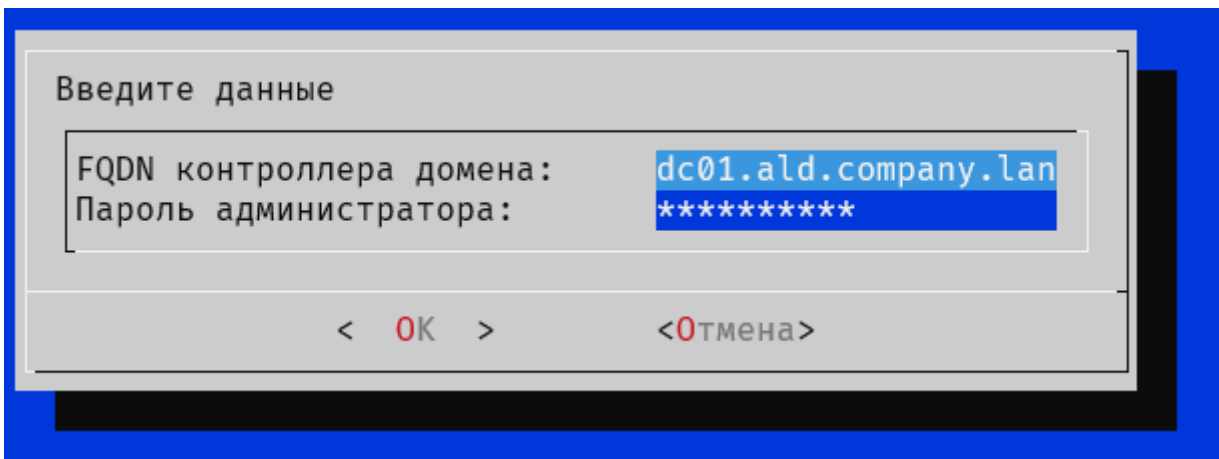
Выполнение скрипта завершено с ошибкой. Подробности в `/var/log/aldpro-role-installer.log`

5.7. После перезагрузки сервера, при входе пользователя по ssh, автоматически запустится установщик.

Выберите «3 Установка резервного контроллера домена».



5.8. Появится форма для ввода данных:



Вам нужно будет указать следующую информацию:

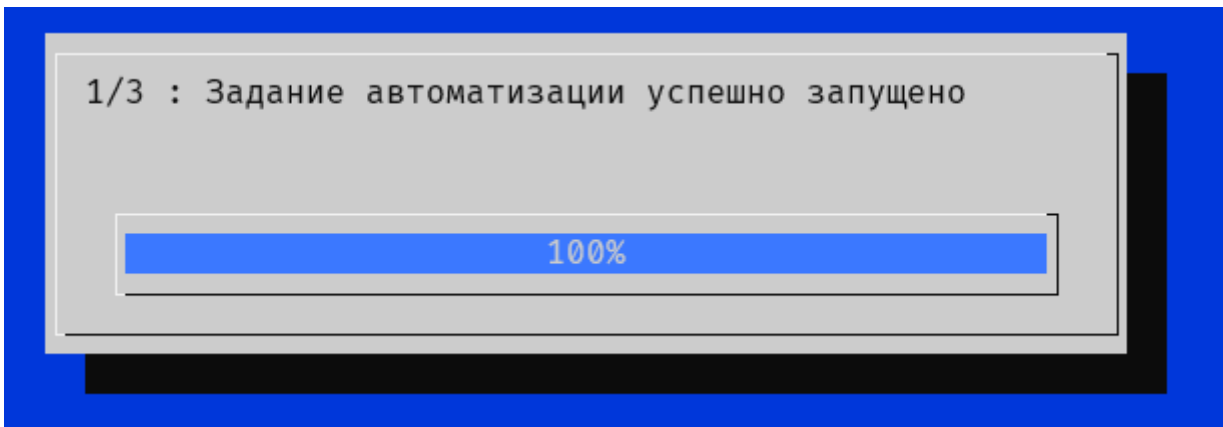
- FQDN контроллера домена
- Пароль администратора

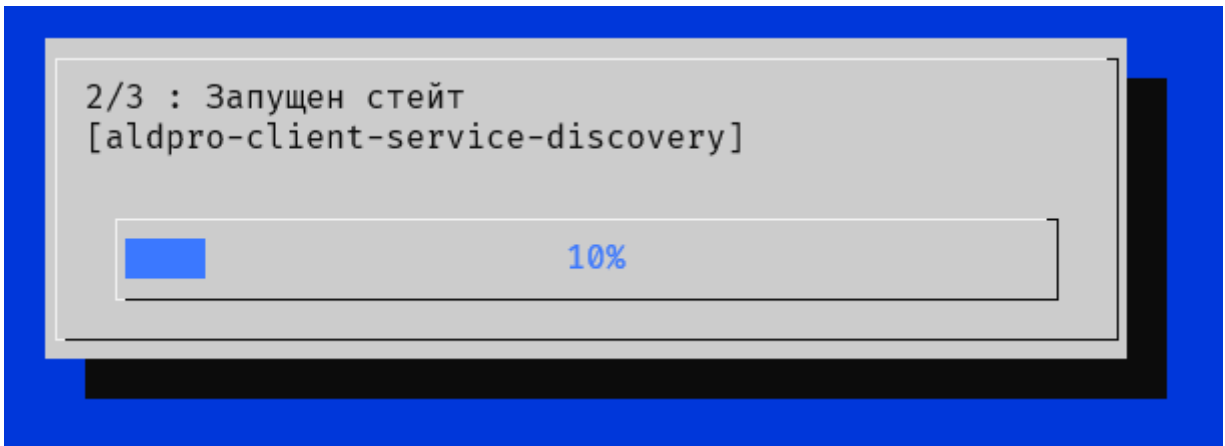
5.9. Введите запрашиваемые данные.

5.10. После ввода данных начнется процесс установки резервного контроллера домена. Этот процесс состоит из нескольких этапов:

1. Аутентификация на указанном контроллере домена
2. Запуск задания автоматизации
3. Конфигурация DNS

5.11. Процесс установки может занять некоторое время. Прогресс установки будет отображаться в окне установщика.





5.12. После завершения установки, система выведет следующее сообщение:
Выполнено. Отчет о выполнении задания можно получить на портале.

5.13. Выполните перезагрузку системы

5.14. Проверка установки

Зайдите на портал управления на первом контроллере домена и откройте "Задания автоматизации", задача replica_install должно быть в статусе "Успешно"

Автоматизация > Задания автоматизации

Журнал заданий Каталог заданий автоматизации

Найти задание

Дата запуска задания	Название задания	Инициатор	Статус
18/01/2024, 12:25:08 PM	replica_install	Administrator	Успешно

Более подробный отчет о выполнении задания автоматизации можно посмотреть внутри самого задания:

Основное

Параметры задания

Дата начала задания

10/21/2024, 12:35:08 PM

Дата завершения задания

10/21/2024, 12:43:03 PM

Инициатор запуска задания

Administrator

Узел

['dc02.ald.company.lan']

Отчет о выполнении задания

```
"loop_|-wait_for_salt_minion_on_dc01.ald.company.lan_|-
saltutil.runner_|-until_no_eval":
  "duration": 5810.705,
  "name": "saltutil.runner",
  "jid": null,
  "comment": "Call provided the expected results in 1 attempts"
```