ALD Pro Domain Controller Installation Manual

1 Preparing for Installation

Please notice:

- All necessary packages and dependencies are already included in the image.
- The username can be any name.
- When the user logs in via ssh, the application is automatically launched by adding the corresponding code to ~/.bashrc to facilitate the application launch.

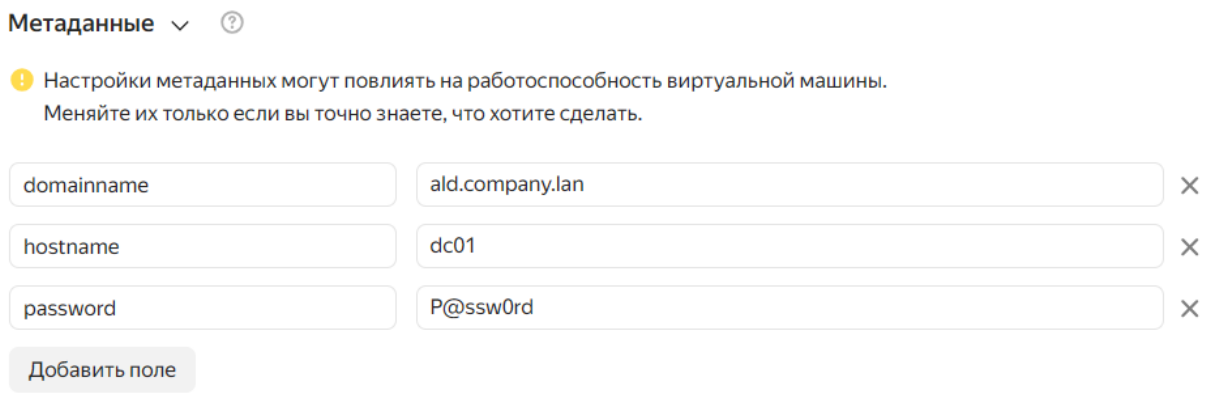
Minimum system requirements:

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

2 Preliminary configuration of the installer

2.1 It is possible to pass the parameters to the installer for autofill of the corresponding forms when creating a virtual machine in Yandex Cloud: using the graphical interface and Terraform.

Using the graphical interface:



Using Terraform, example:

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

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

2.2. The installer expects the following parameters; the format and case of the names must match the list::

- domainname
- hostname
- password

2.3 When the parameters are transferred, the installer does not validate the values of the transferred parameters; the values will be validated later, during the form verification stage.

2.4 It is possible to fill in the parameters partially. The filling order can be arbitrary.

Important: consider the following requirements before installation

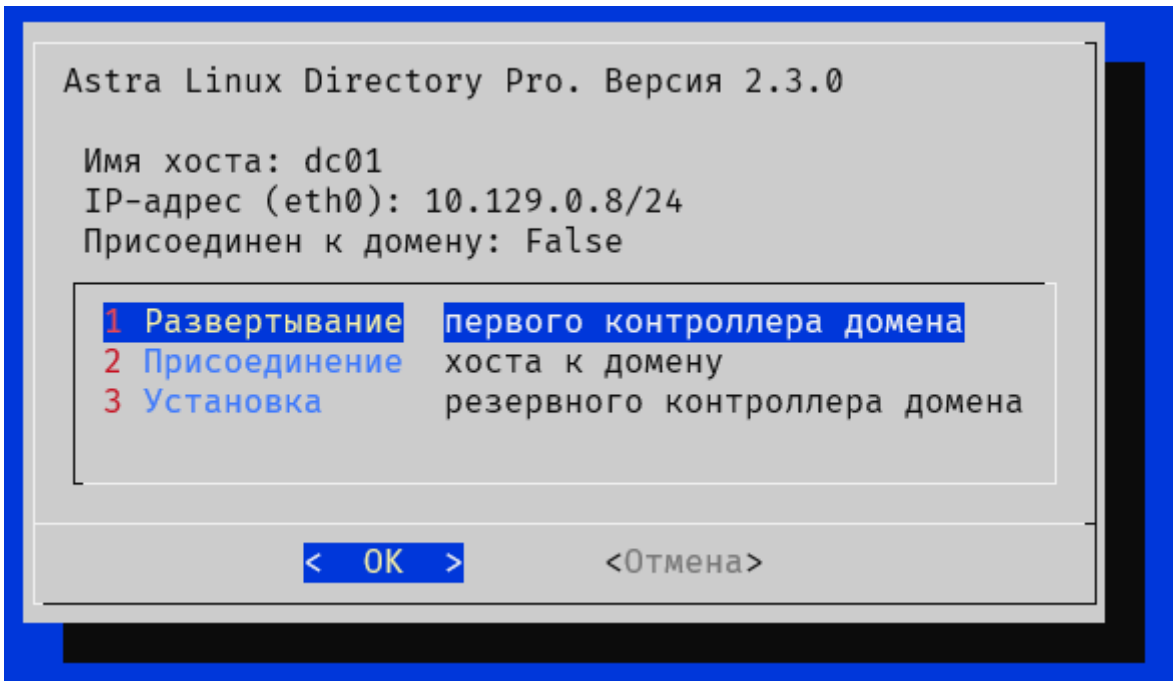
- Root privileges
  - The ALD Pro installation script must be run with superuser (root) privileges.
  - If you are not logged in as root, use the sudo command before running the script.
  - If you do not have root privileges, the installation will not start, and you will receive an error message.
- No domain controller installed
  - Before starting the installation, make sure that the ALD Pro domain controller is not installed on your server.
  - If the domain controller is already installed, you will see the message: "The server is already configured as a domain controller," and the installation will be aborted.
- Preventing parallel running
  - The script uses a locking mechanism to prevent multiple instances from running simultaneously.
  - If you attempt to run a second instance of the script while the first one is still running, the second instance will not start.

---

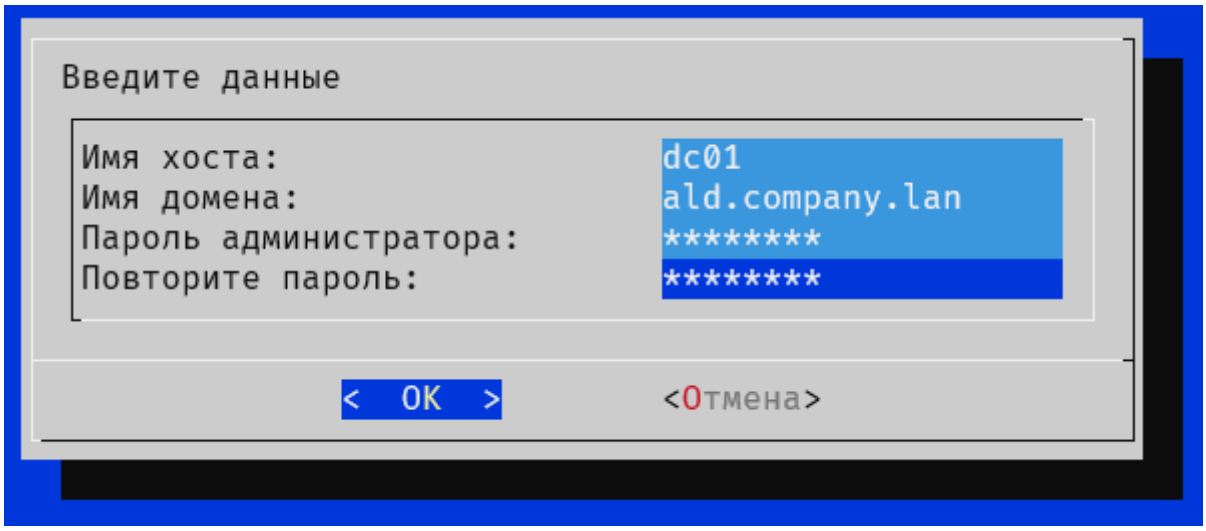
3 Running the installer and configuring the primary domain controller

3.1. There are two options to run the installer:

- Log out and log in again via ssh. The installer should start automatically.
- Or run the command manually: `sudo python3 /usr/sbin/aldpro-dc-installer`



3.2. Choose a menu item «1 Развертывание первого контроллера домена». A data entry form will appear:



You will need to provide the following information:

- Server hostname (Имя хоста сервера)
- Domain name (Доменное имя)
- Domain admin password (Пароль администратора домена)
- Domain admin password confirmation (Подтверждение пароля администратора домена)

The parameters will be pre-filled if the corresponding parameters were provided when creating the virtual machine.

3.3. Enter the requested information, considering the following requirements.

3.3.1 The hostname must be a valid NetBIOS name.

The system uses the following rule to validate the NetBIOS name:

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

The following requirements are taken into account:

1. Total length: The NetBIOS name must be between 1 and 16 characters.
2. Allowed characters:
    a. Latin letters (a-z, A-Z)
    b. Digits (0-9)
    c. Hyphen (-) and dot (.)
3. Special rules:
    a. The name must start with a letter or a digit.
    b. The name must end with a letter or a digit.
    c. Hyphens and dots can only be used within the name, not at the beginning or not at the end.

Examples of valid NetBIOS names:

- SERVER1
- DEV-MACHINE
- TEST.NODE
- A123456789012345 (maximum length of 16 characters)

Examples of invalid NetBIOS names:

- SERVER_1 (contains invalid character '_')
- -TESTSERVER (starts with a hyphen)
- DEVELOPMENT.SERVER (exceeds maximum length of 16 characters)
- TEST. (ends with a dot)

3.3.2 The domain name must be valid.

The system uses the following rule to validate the domain name:

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

The following requirements are taken into account:

1. The domain name must consist of one or more words separated by dots.
2. Each word may contain:
    a. Lowercase Latin letters (a-z)
    b. Digits (0-9)
    c. Hyphens (-), but not at the beginning or not at the end of the label.
3. The top-level domain (the last part after the dot) must consist of at least two letters.

Examples of valid domain names:

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

Examples of invalid domain names:

- EXAMPLE.COM (contains uppercase letters)
- example.c (top-level domain is too short)
- -example.com (starts with a hyphen)
- example-.com (ends with a hyphen before the dot)

3.3.3 The administrator password must be complex and long enough.

The system uses the following rule to verify password reliability:

```
password_regex = r'^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[\W_]).{8,}$'
```

The following requirements are taken into account:

1. Minimum length: The password must contain at least 8 characters.
2. Mandatory elements (the password must contain at least one character from each category):
    a. Lowercase Latin letters (a-z)
    b. Uppercase Latin letters (A-Z)
    c. Digits (0-9)
    d. Special characters (e.g., !@#$%^*()+{}[]|:;<>,.?) or underscore (_)

Examples of valid passwords:

- P@ssw0rd (minimum length, contains all required elements)
- Str0ng!Password (longer password with all required elements)
- C0mplex_P@ssword123 (complex password exceeding minimum requirements)

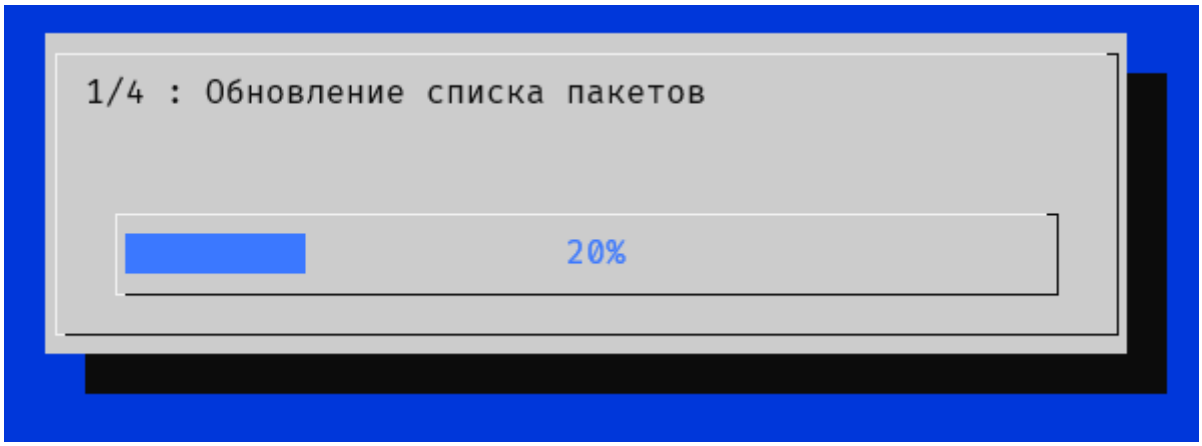
Examples of invalid passwords:

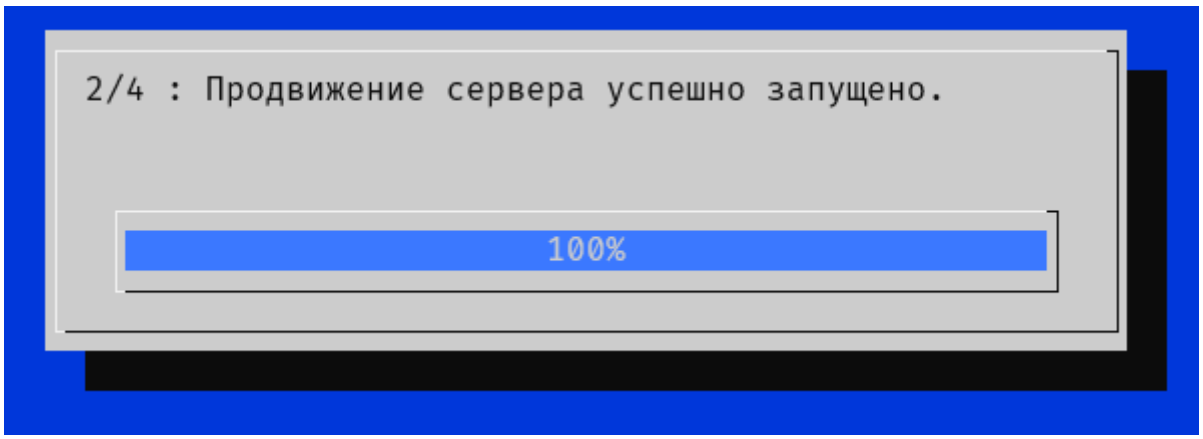
- password (no uppercase letters, digits, or special characters)
- PASSWORD123 (no lowercase letters or special characters)
- Pass123! (less than 8 characters)
- StrongPass (no digits or special characters)

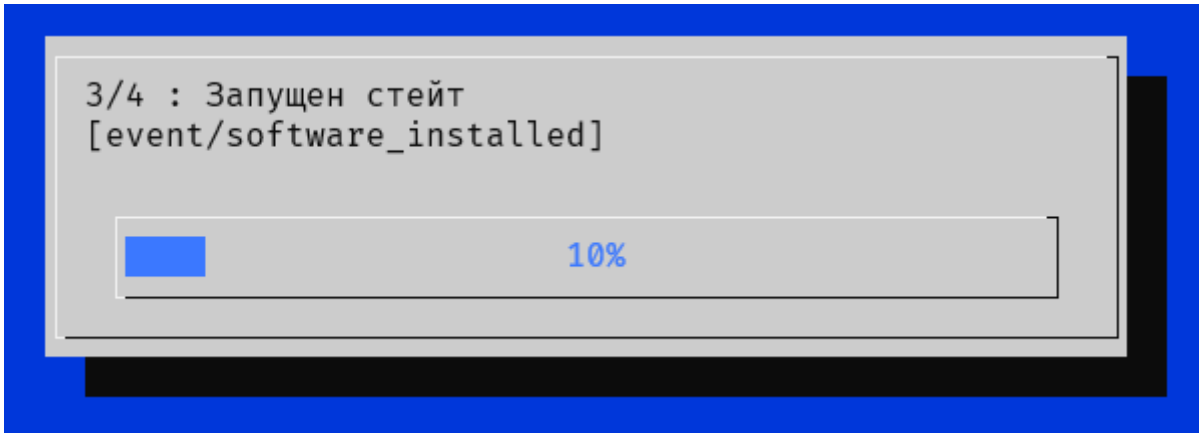
3.4. The installation and configuration of the domain controller will begin after entering the data. This process consists of several stages:

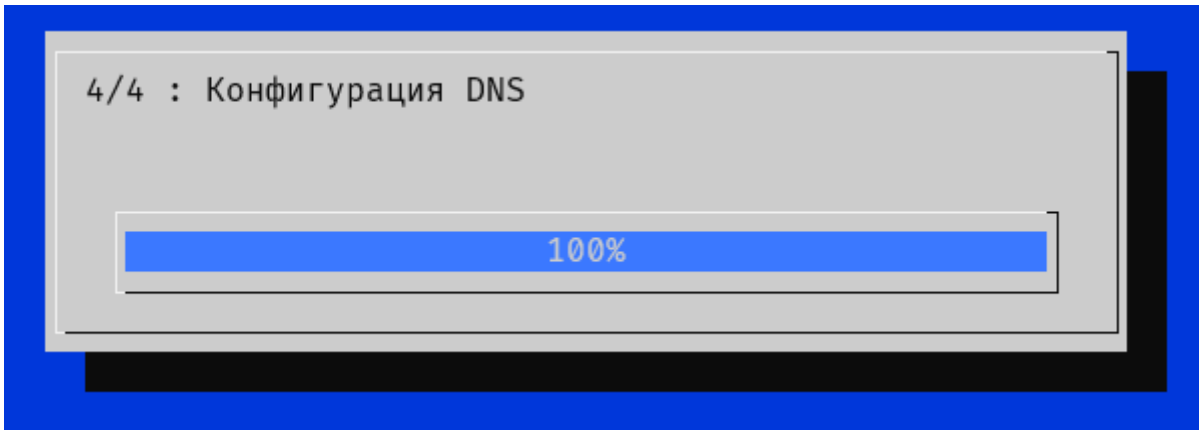
1. Server configuration
    a. Configuring network parameters
    b. Configuring the hostname
2. Installing the necessary packages, if they are not present
    a. Installing aldpro-mp, aldpro-gc, aldpro-syncer
3. Promoting the server to a domain controller
    a. Running the aldpro-server-install script
4. DNS Configuration
    a. Configuring the DNS forwarder
    b. Configuring additional BIND parameters

3.5. The installation process may take some time. The installation progress will be displayed in the installer window.









3.6. After the installation is complete, the system will ask you to reboot the computer.
Выполнено. Для применения настроек необходимо выполнить перезагрузку вручную.

3.7. If the installation completes with an error, the system will point to a log file with a detailed description of the steps taken.
Выполнение скрипта завершено с ошибкой. Подробности в /var/log/aldpro-role-installer.log

4 Installation Verification

4.1. After rebooting, log in via SSH using the domain administrator credentials.

After promoting the server to a domain controller, it will be possible to connect to the server via ssh using a password. Depending on the server performance, it may take some time for all the necessary domain services to load.

The option to connect with the key and with the username specified when creating the virtual machine also remains.

- Login: admin
- Password: as specified in the input form during the domain controller deployment.

4.2. Open a terminal and execute the following command to check the domain status:

```
sudo ipactl status
```

This command should show domain services availability:

```
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
```

You can also use the special utility aldproctl:

```
sudo aldproctl status
```

This command should show domain services availability including ALD Pro services:

```
.....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. Check DNS functionality by executing the command:

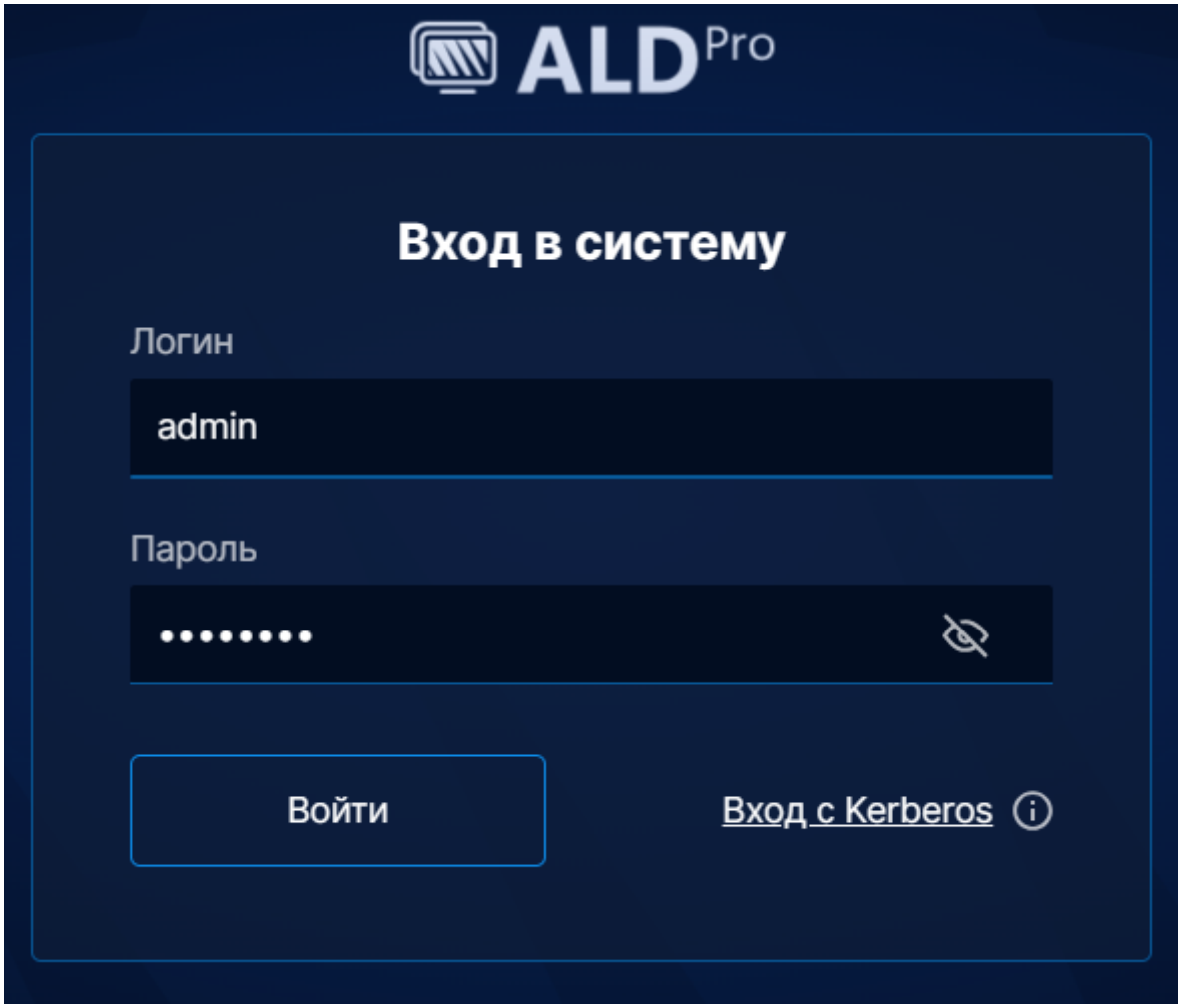
```
host -t SOA имя_вашего_домена
```

The command should return the SOA record of your domain with an indication of the domain controller.
Example:

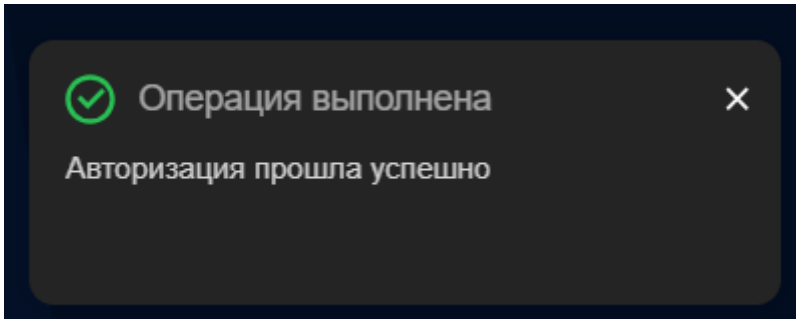
```
host -t SOA ald.company.lan

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

4.4. Check the portal functionality using the following path:https://<ip_address>/ad/ui

The following authorization form should be available:



User authentication should be successful:

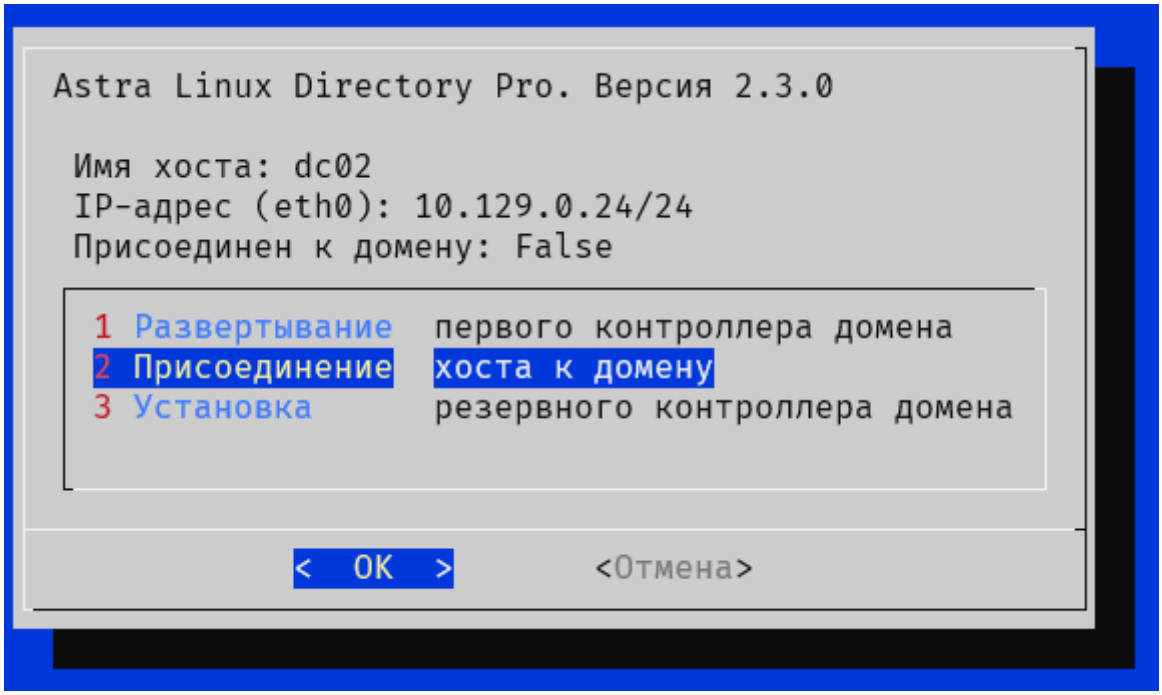


If all steps are completed successfully, your primary domain controller should be installed and configured.

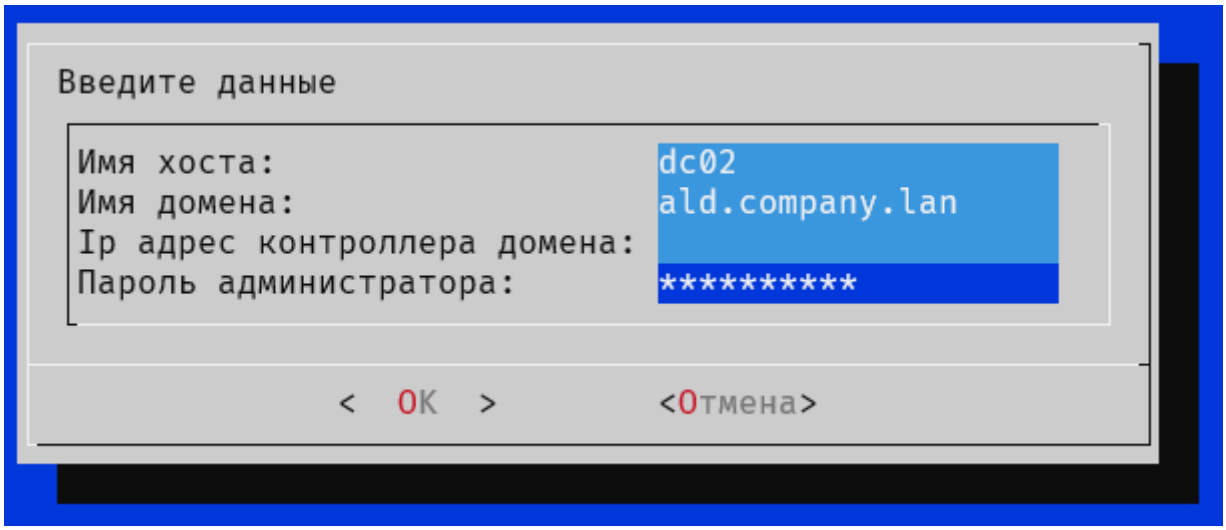
5 Configuring Backup Domain Controller

To configure the backup domain controller, you should join this server to the domain.

5.1. Choose a menu item «2 Присоединение хоста к домену».



A data entry form will appear:



You will need to provide the following information:

- Server hostname (Имя хоста сервера)
- Domain name (Доменное имя)
- IP address of the domain controller (IP-адрес контроллера домена)
- Domain admin password (Пароль администратора домена)

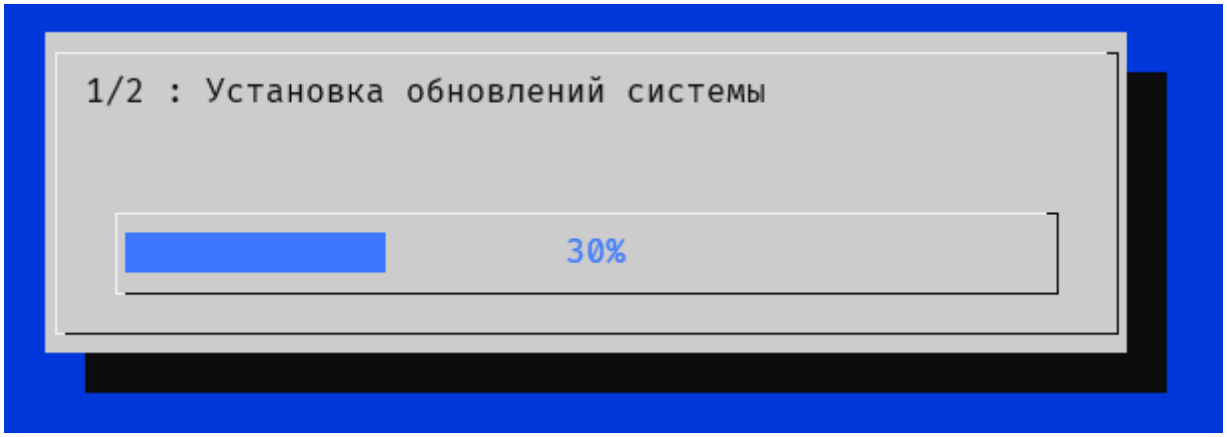
The parameters will be pre-filled if the corresponding parameters were provided when creating the virtual machine (except “IP address of the domain controller” value).

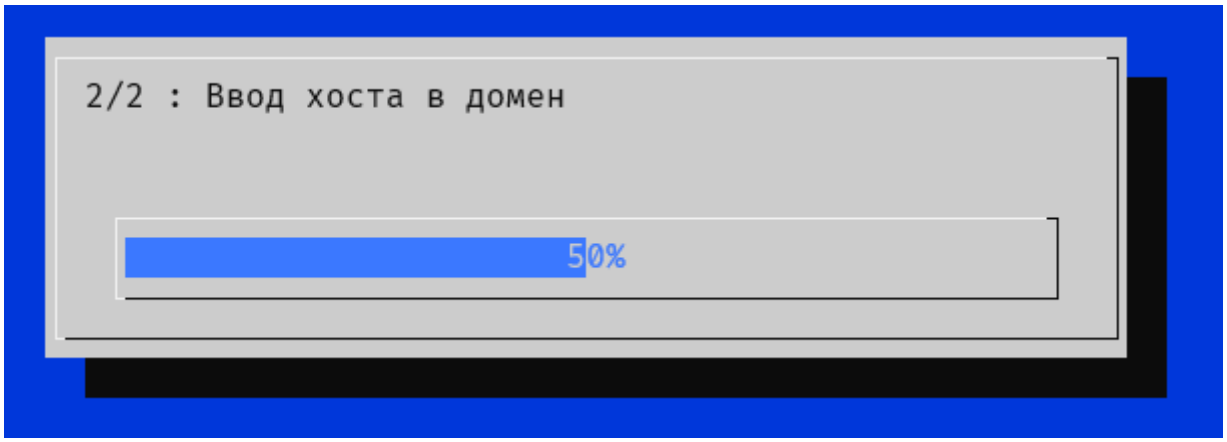
5.2. Enter the requested information.

5.3. After entering the data the system will initiate the domain joining process. This process consists of several stages:

1. Server configuration
    a. Configuring network parameters
    b. Configuring the hostname
2. Installing the necessary packages, if they are not present
    a. Installing aldpro-client
3. Joining the server to the domain
    a. Running the aldpro-client-installer script

5.4. The joining process may take some time. The joining progress will be displayed in the installer window.





5.5. After the joining is complete, the system will ask you to reboot the computer.

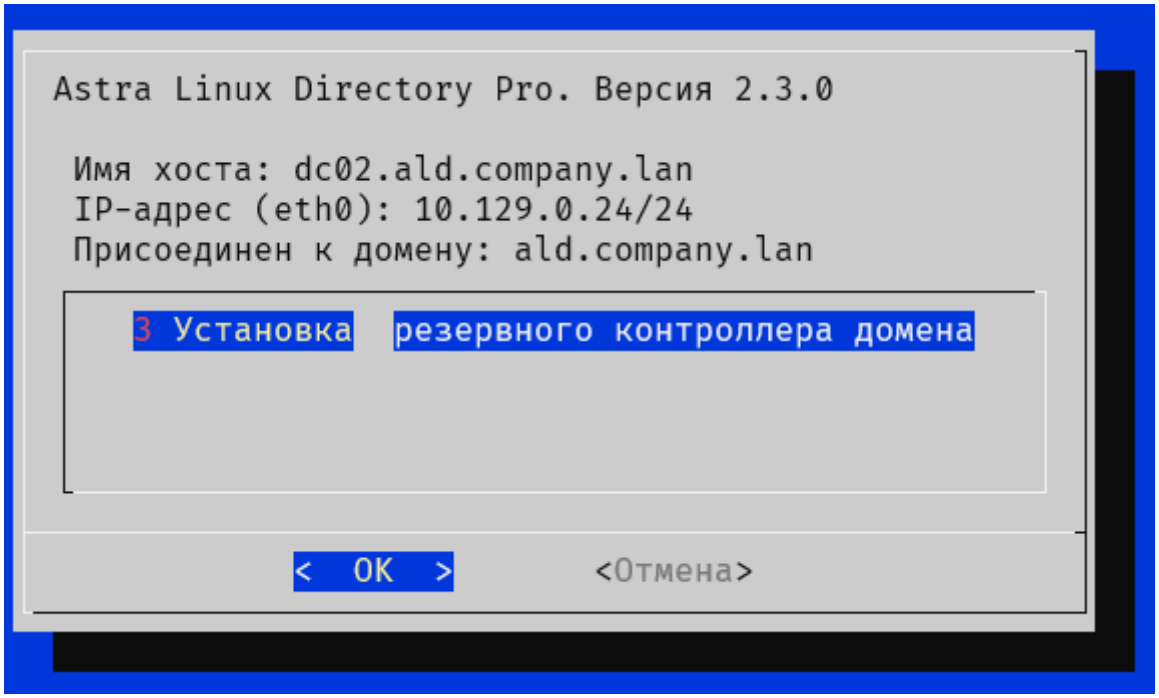
```
Выполнено. Для применения настроек необходимо выполнить перезагрузку вручную.
```

5.6. If the installation completes with an error, the system will point to a log file with a detailed description of the steps taken..

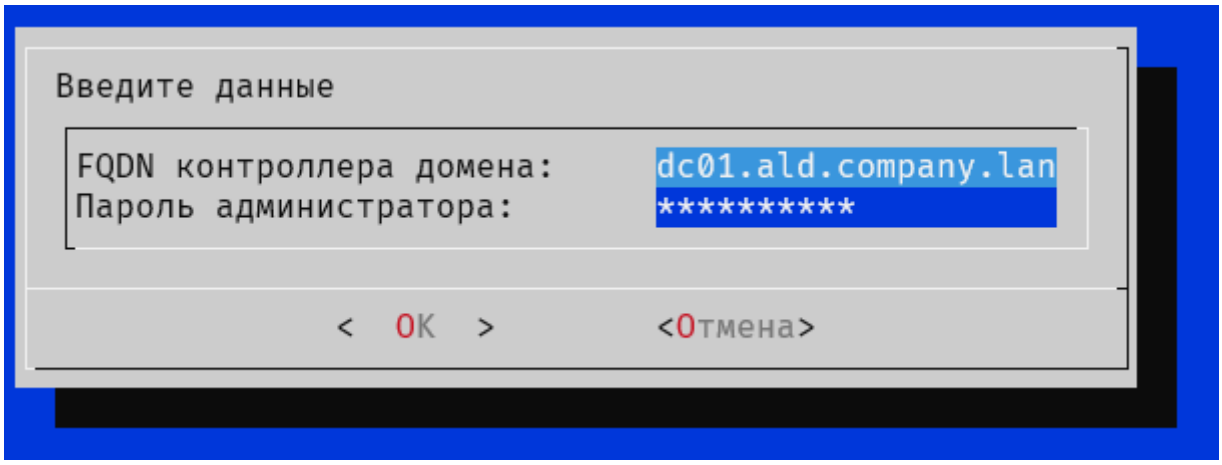
```
Выполнение скрипта завершено с ошибкой. Подробности в /var/log/aldpro-role-installer.log
```

5.7. After rebooting, log in via SSH. The installer should start automatically.

Choose a menu item «3 Установка резервного контроллера домена».



5.8. A data entry form will appear:



You will need to provide the following information:

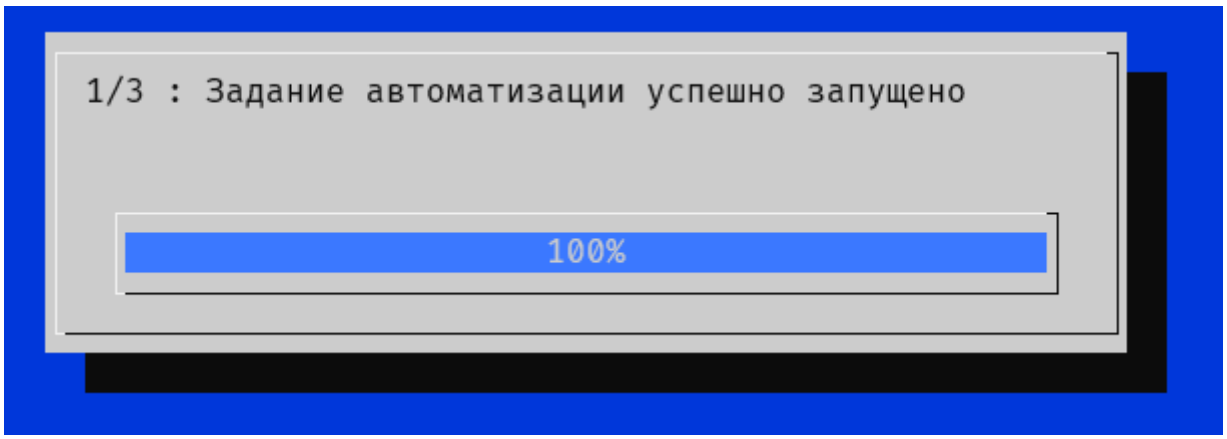
- Domain Controller FQLD (FQDN контроллера домена)
- Domain admin password (Пароль администратора домена)

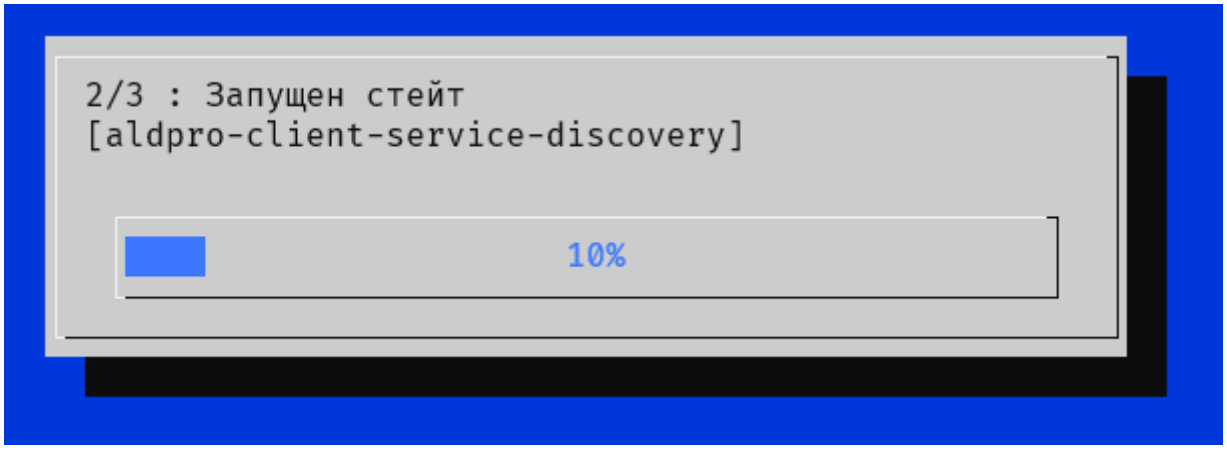
5.9. Enter the requested information.

5.10. The installation of the backup domain controller will begin after entering the data. This process consists of several stages:

1. Authentication on the specified domain controller
2. Launching the automation job
3. DNS configuration

5.11. The installation process may take some time. The installation progress will be displayed in the installer window.



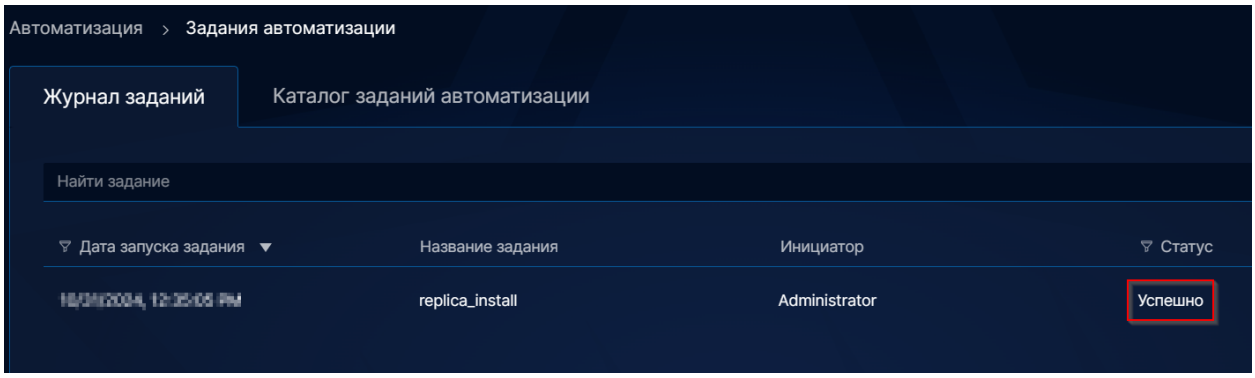


5.12. After the installation is complete, the system will display the following message:
Выполнено. Отчет о выполнении задания можно получить на портале.

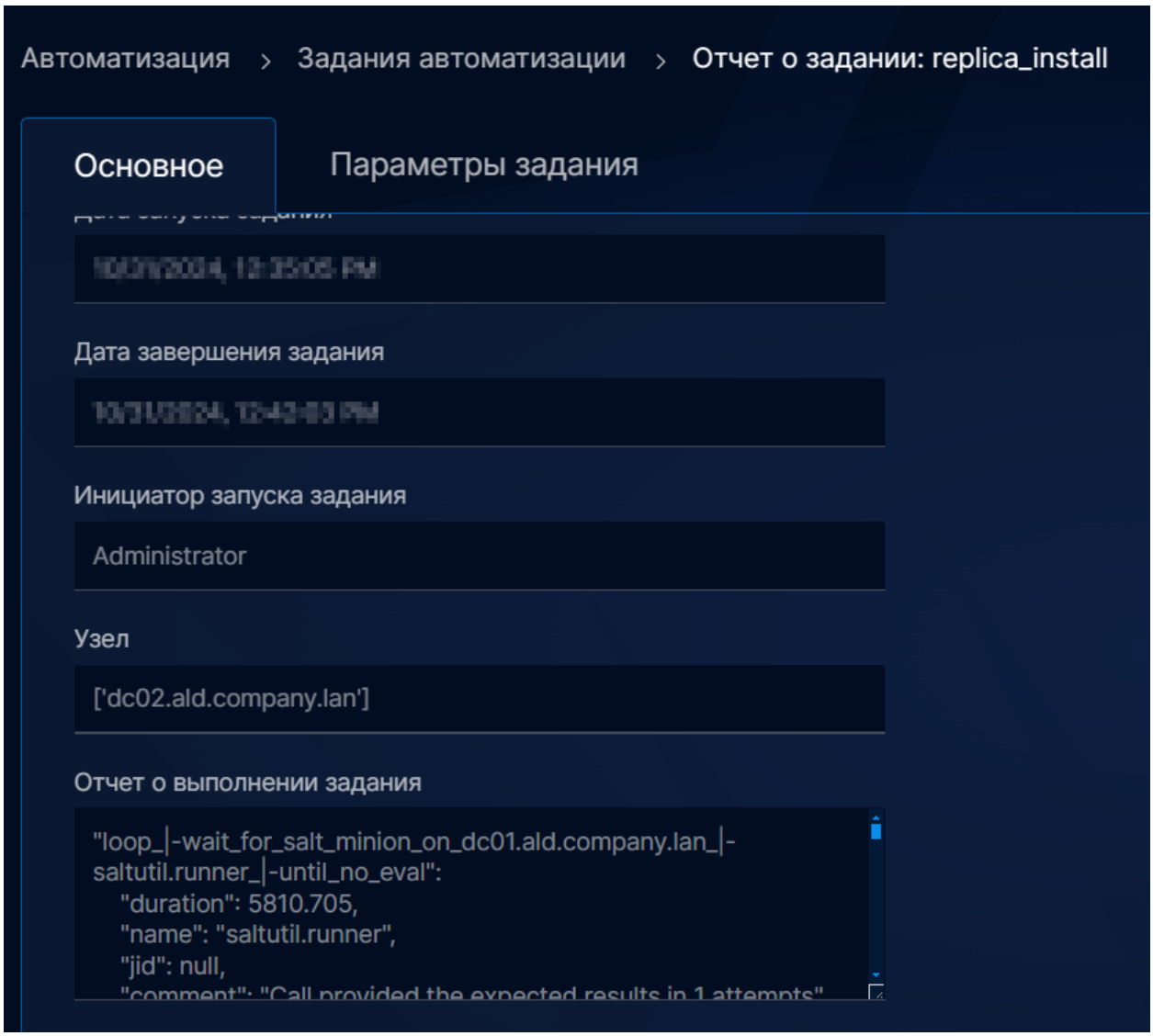
5.13. Reboot the system.

5.14. Installation Verification.

Open the management portal on the primary domain controller and go to "Задания автоматизации" page. The replica_install task should have the status "Успешно" (Successful).



A more detailed execution report of the automation task can be found inside the task entry:


Автоматизация › Задания автоматизации › Отчет о задании: replica_install
Основное
Параметры задания
Дата завершения задания
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,