Интеграция Foreman со службой каталога ALD Pro

06/04/2025

Содержание

Foreman - это открытый инструмент для взаимодействия с Puppet (или Chef), позволяющий автоматизировать выполнение задач и развёртывание приложений.

Инструкция предназначена для интеграции сервера Foreman со службой каталога ALD Pro. Интеграция обеспечит возможность сопоставления доменных учетных записей с пользователями Foreman для аутентификации по протоколам LDAP и Kerberos V5 при авторизации в веб-интерфейсе.

1 Описание стенда

В инструкции будут представлены этапы настройки для Foreman 2.14, работающем на Astra Linux 1.7.4. На момент написания инструкции Foreman 2.14 – это самая последняя версия ПО, доступная для установки из репозиториев AstraLinux.

В Foreman можно настроить внешние источники аутентификации такие как LDAP или Kerberos, но официальная документация нас предупреждает, что можно выбрать только один внешний источник.

2 Настройка LDAP

Для настойки LDAP рекомендуется создать отдельную учетную запись, у которой должны быть права на поиск и чтение в каталоге, по умолчанию при создании учетной записи в веб-интерфейсе ALD Pro такие права будут присутствовать.

Далее нужно зайти в веб-интерфейс Foreman и создать источник LDAP-аутентификации в меню Администратор > Authentication sources (рис. 1).

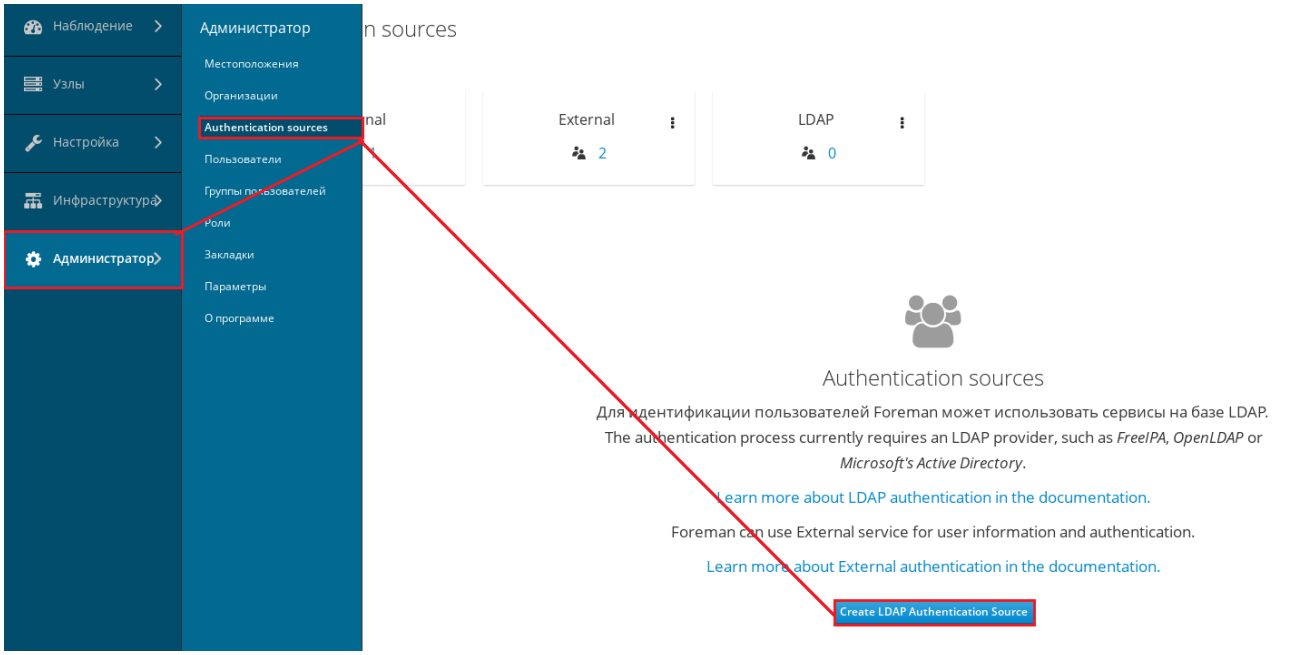

Рисунок 1 - Создание источника LDAP-аутентификации

Далее требуется заполнить данные сервера LDAP и учетных данных (Таблица 1, рис. 2).

ОБЯЗАТЕЛЬНО активируйте чекбокс LDAPS, иначе будет использоваться незашифрованное соединение, и будет возможность перехватить учетные данные и читать LDAP-запросы.

Таблица 1 – Данные для подключения к LDAP-серверу

Параметр	Значение
Имя	Указывается любое имя, влияет только на отображение в интерфейсе.
Узел	FQDN контроллера домена
Порт	636

Тип Сервера	FreeIPA

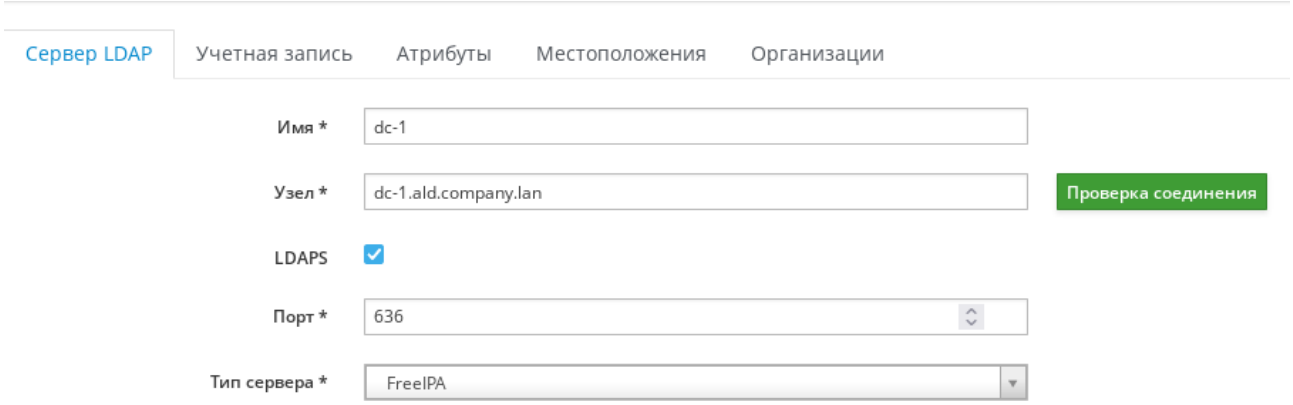

Рисунок 2 - Данные для подключения к LDAP-серверу

Во вкладке Account указываем данные учетной записи и активируем чекбоксы Automatically Create Accounts In Foreman и Usergroup Sync (Таблица 2, рис.3).

Таблица 2 – Данные учетной записи для подключения к LDAP-серверу

Параметр	Значение
Account Username	uid=username,cn=users,cn=accounts,dc=domain,dc=lan
Account Password	Указывается пароль от учетной записи
Base DN	cn=users,cn=accounts,dc=ald,dc=company,dc=lan
Groups base DN	cn=groups,cn=accounts,dc=ald,dc=company,dc=lan

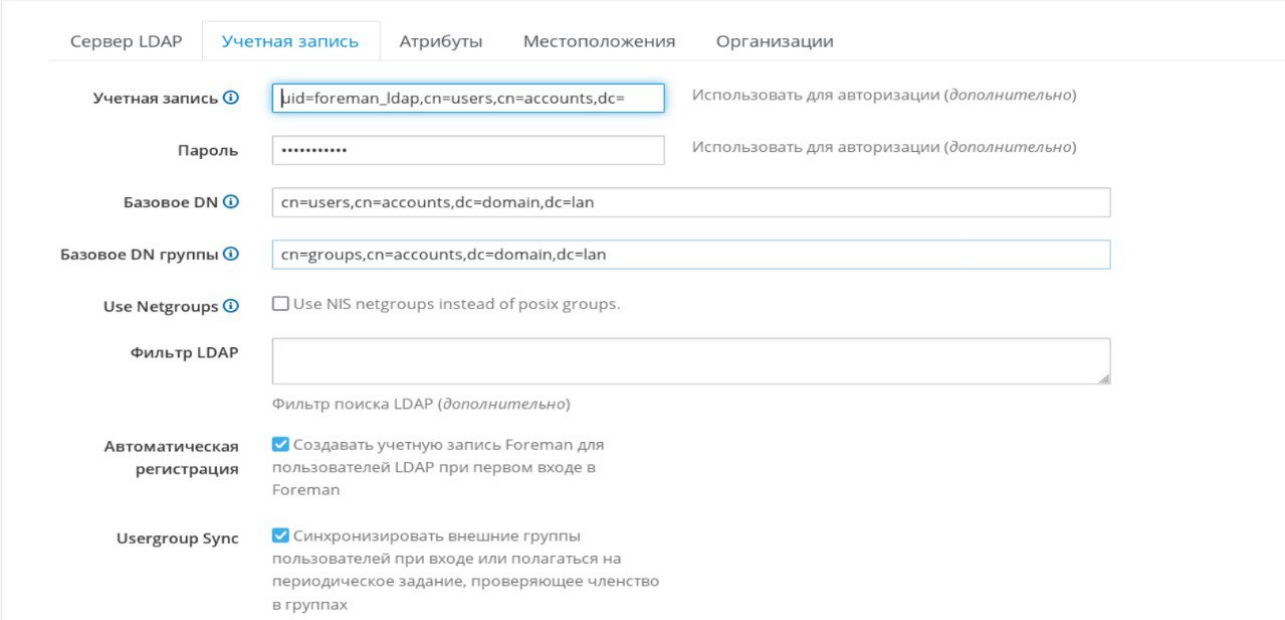

Рисунок 3 – Данные учетной записи для подключения к LDAP-серверу

Теперь для входа в веб-интерфейс Foreman можно использовать учетные данные из каталога LDAP. Также можно проводить синхронизацию групп LDAP с группами Foreman. Для этого в заранее созданной группе Foreman (auditors) нужно указать внешний источник синхронизации (LDAP-dc-1), при этом имя группы в Foreman может не совпадать с именем группы в LDAP (рис. 4).

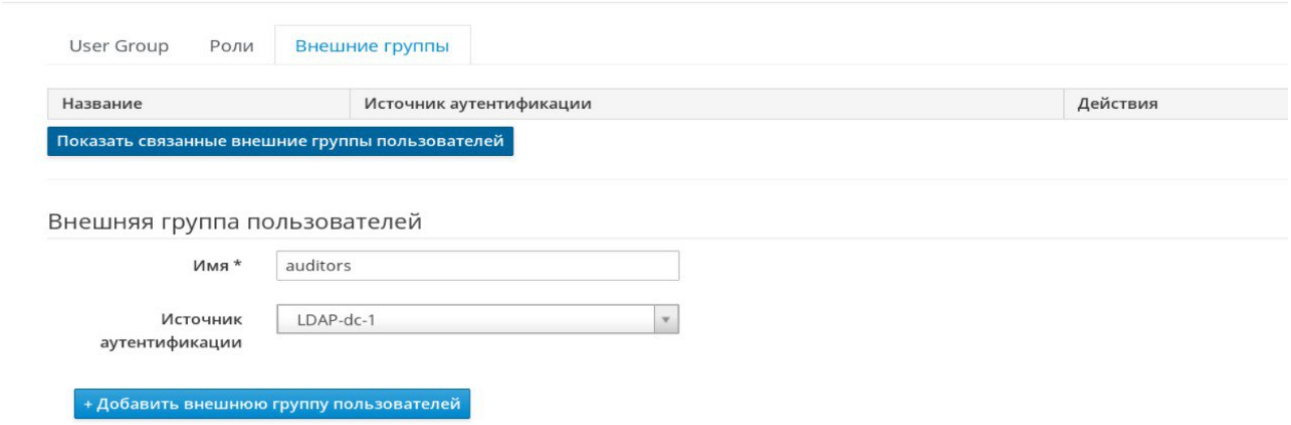

Рисунок 4 – Настройка внешней группы

3 Конфигурация домена

3.1 Добавление службы

Для работы протокола Kerberos необходимо зарегистрировать службу. Сделать это можно на контролере домена следующей командой:

```
ipa service-add HTTP/foreman.ald.company.lan@ALD.COMPANY.LAN
```

, где

- HTTP — класс службы,
- foreman.ald.company.lan — FQDN сервера,
- ALD.COMPANY.LAN — зона Kerberos.

3.2 Создание HBAC-правила

В веб-интерфейсе переходим к групповым политикам, в меню «Политики доступа к узлу» в разделе «Службы HBAC» создаем новую службу. Называем ее foreman-prod (рис. 5).

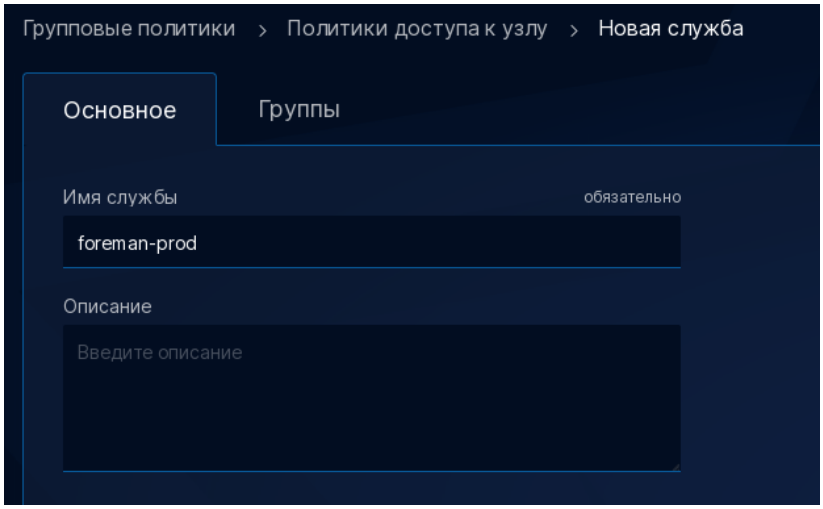

Рисунок 5 – Создание новой службы foreman-prod

После того как служба зарегистрирована переходим к созданию правила.

В соседнем разделе «Правила HBAC» нужно создать новое правило, например, allow_foreman_prod (рис. 6).

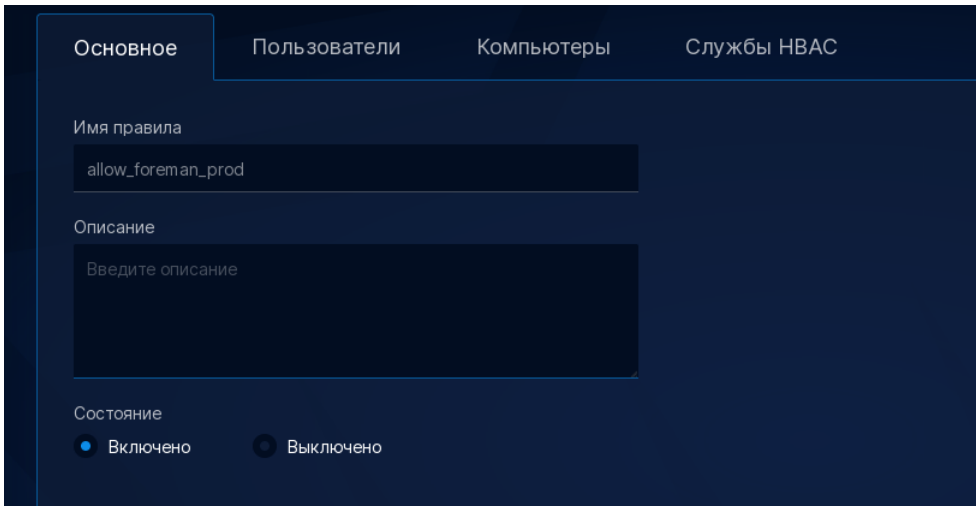

Рисунок 6 – Создание правила allow_foreman_prod

В разделах «Пользователи» и «Компьютеры» определяем сам сервер Foreman и пользователей, у которых должен быть к нему доступ. В разделе «Службы HBAC» добавляем foreman-prod (рис. 7).

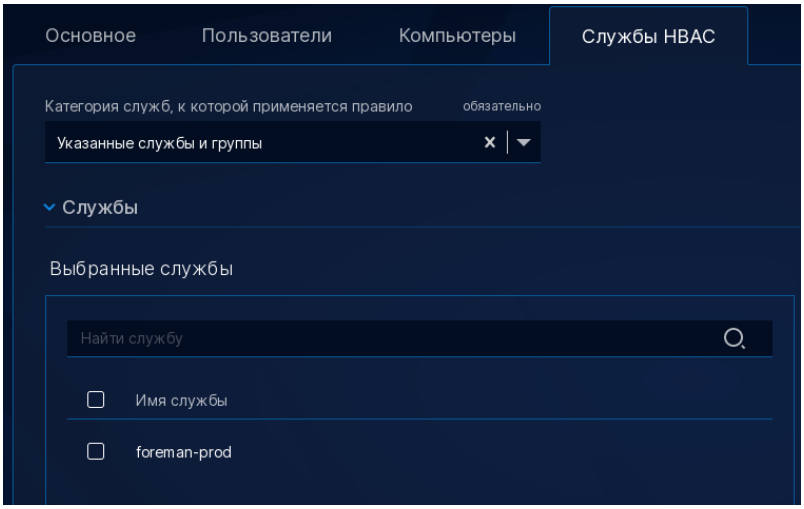

Рисунок 7 – Добавление foreman-prod в разделе «Службы HBAC»

Данные настройки можно выполнить из командной строки:

```
ipa hbacsvc-add foreman-prod
ipa hbacrule-add allow_foreman_prod
ipa hbacrule-add-service allow_foreman_prod --hbacsvcs=foreman-prod
ipa hbacrule-add-user allow_foreman_prod --user=<username>
ipa hbacrule-add-host allow_foreman_prod --hosts=<the-foreman-fqdn>
```

После можно проверить наличие правила и его работу:

```
ipa hbacrule-find foreman-prod
ipa hbactest --user=<username> --host=<the-foreman-fqdn> --service=foreman-prod
```

4 Конфигурация сервера Foreman

ВАЖНО!

Для настройки Kerberos аутентификации требуется, чтобы сервер, на котором установлен Foreman, был введен в домен, так как для создания пользователей в базе данных Foreman используются запросы к службе **SSSD.**

4.1 Загрузка keytab

В первую очередь выгружаем keytab для ранее созданной службы и определяем ему владельца и права, чтобы apache мог его использовать для расшифровки направляемых ему TGS.

```
ipa-getkeytab -p HTTP/foreman.ald.company.lan@ALD.COMPANY.LAN -k /etc/http.keytab
chown www-data:www-data /etc/http.keytab
chmod 600 /etc/http.keytab
```

4.2 Настройка PAM

После в файле **/etc/pam.d/foreman-prod** определяем модуль pam_sss.so для предоставления доступа. Для этого требуется добавить в него следующие строки:

```
auth    required   pam_sss.so
account required   pam_sss.so
```

4.3 Редактирование конфигурационного файла Foreman

На заметку

По умолчанию Foreman использует сервер приложений Puma, но в версии 2.14 интеграция Puma с FreeIPA и ALD Pro работает некорректно, поэтому перед редактированием конфигурационных файлов требуется активировать сервер приложений Passenger.

Для того, чтобы скрипт установщика отработал корректно, нужно создать папку foreman в каталоге /home:

```
mkdir -p /home/foreman
foreman-installer --foreman-passenger=true
```

В основном файле настроек **/etc/foreman/settings.yaml** требуется добавить следующую строку:

```
:authorize_login_delegation: true
```

Для проверки применения настроек нужно перезапустить службу и зайти в «Параметры» в раздел «Безопасность и проверка подлинности». Параметр «Делегирование авторизации» должен иметь значение «Да» (рис. 8):

```
systemctl restart foreman
```

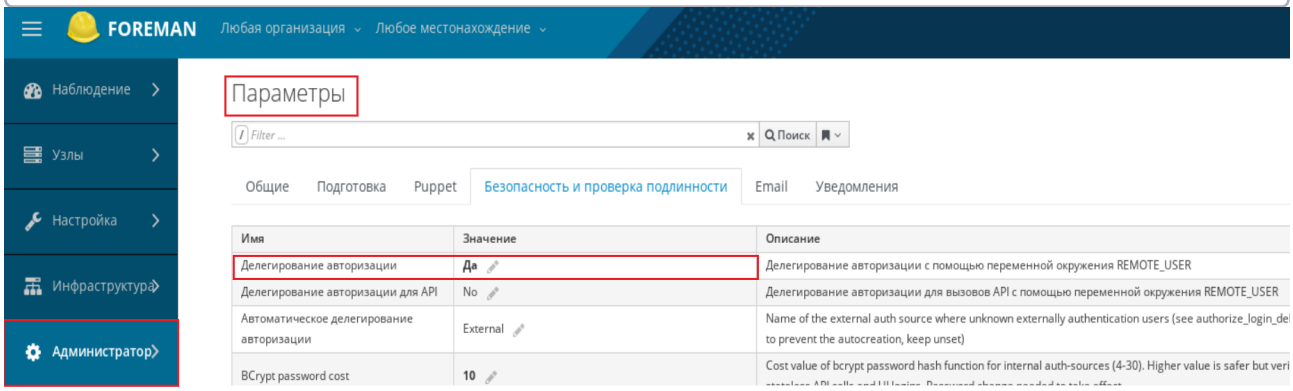

Рисунок 8 – Проверка значения параметра «Делегирование авторизации»

4.4 Настройка Apache

Последовательно создайте файлы конфигурации в директории **/etc/apache2/conf.d/05-foreman-ssl.d/**.

Для работы Kerberos требуется создать файл **/etc/apache2/conf.d/05-foreman-ssl.d/auth_kerb.conf** и добавить следующий текст конфигурации:

```
LoadModule auth_gssapi_module modules/mod_auth_gssapi.so
LoadModule authnz_pam_module modules/mod_authnz_pam.so
<Location /users/extlogin>
AuthType GSSAPI
  AuthName "GSSAPI Single Sign On Login"
  GssapiCredStore keytab:/etc/http.keytab
  GssapiSSLonly On
  GssapiLocalName On
  require pam-account foreman-prod
  ErrorDocument 401 '<html><meta http-equiv="refresh" content="0; URL=/users/
login"><body>Kerberos authentication did not pass.</body></html>'
  ErrorDocument 500 '<html><meta http-equiv="refresh" content="0; URL=/users/
login"><body>Kerberos authentication did not pass.</body></html>'
</Location>
```

Для того, чтобы пользователи могли создаваться «на лету», создадим файл **/etc/apache2/conf.d/05-foreman-ssl.d/lookup_identity.conf** со следующим текстом:

```
LoadModule lookup_identity_module modules/mod_lookup_identity.so
<LocationMatch ^/users/(ext)?login$>
  LookupUserAttr email REMOTE_USER_EMAIL " "
  LookupUserAttr firstname REMOTE_USER_FIRSTNAME
  LookupUserAttr lastname REMOTE_USER_LASTNAME
  LookupUserGroupsIter REMOTE_USER_GROUP
</LocationMatch>
```

Назначьте созданным конфигурационным файлам владельца и группу root, а права доступа 644:

```
chown root:root  lookup_identity.conf   auth_kerb.conf
chmod 644 lookup_identity.conf   auth_kerb.conf
```

Теперь можно установить используемые модули Apache и инструмент sssd-dbus:

```
sudo apt update
sudo apt install libapache2-mod-authnz-pam libapache2-mod-auth-gssapi libapache2-mod-
lookup-identity sssd-dbus
```

4.5 Конфигурация службы SSSD

Для создания пользователей и получения их атрибутов, таких как email, имя и фамилия, Foreman обращается к SSSD по D-Bus, и чтобы этот функционал мог работать, вносятся правки в конфигурационный файл **/etc/sssd/sssd.conf**:

```
ldap_user_extra_attrs = email:mail, firstname:givenname, lastname:sn
services = nss, pam, ssh, ifp
[ifp]
allowed_uids = apache, www-data, root
user_attributes = +email, +firstname, +lastname
```

Все настройки проведены и нужно перезапустить службы:

```
systemctl restart apache2.service
systemctl restart sssd
```

Теперь, переходя по URL https://FQDN:/login/extusers при наличии TGT билета и прав доступа HBAC, можно проходить аутентификацию Kerberos и при положительном результате получить доступ в веб-интерфейс. Если пользователя нет в локальной базе, сервер обратится к SSSD, получит необходимые атрибуты и создаст нового пользователя.