

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

Московский институт электроники и математики им. А.Н.Тихонова

Развертывание и настройка FreeIPA

Лабораторная работа № 14
по направлению 10.03.01 Информационная безопасность курса
«Администрирование систем и сетей»
студента образовательной программы бакалавриата
«Информационная безопасность»

Проверил:

преп. Якименко С. И.

Подпись _____

Выполнил:

Казанов А.М. БИБ242

Подпись _____

Оглавление

Тема и цель работы.....	3
Оборудование, ПО	4
Выполнение.....	5
Вывод.....	14
Контрольные вопросы.....	15

Тема и цель работы

Тема лабораторной работы: «Развертывание и настройка FreeIPA».

Цель работы: научиться устанавливать и настраивать FreeIPA на примере Astra Linux SE в виртуальной среде Oracle VirtualBox.

Оборудование, ПО

Устройство	Операционная система	IP адрес/Маска	Шлюз	DNS
CLI_A1	Astra Linux SE 1.8.x	10.0.0.2/24	-	10.0.0.2
CLI_A2	Astra Linux SE 1.8.x	10.0.0.3/24	-	10.0.0.2

Выполнение

1. Ставим на обеих машинах вторым адаптером NAT:

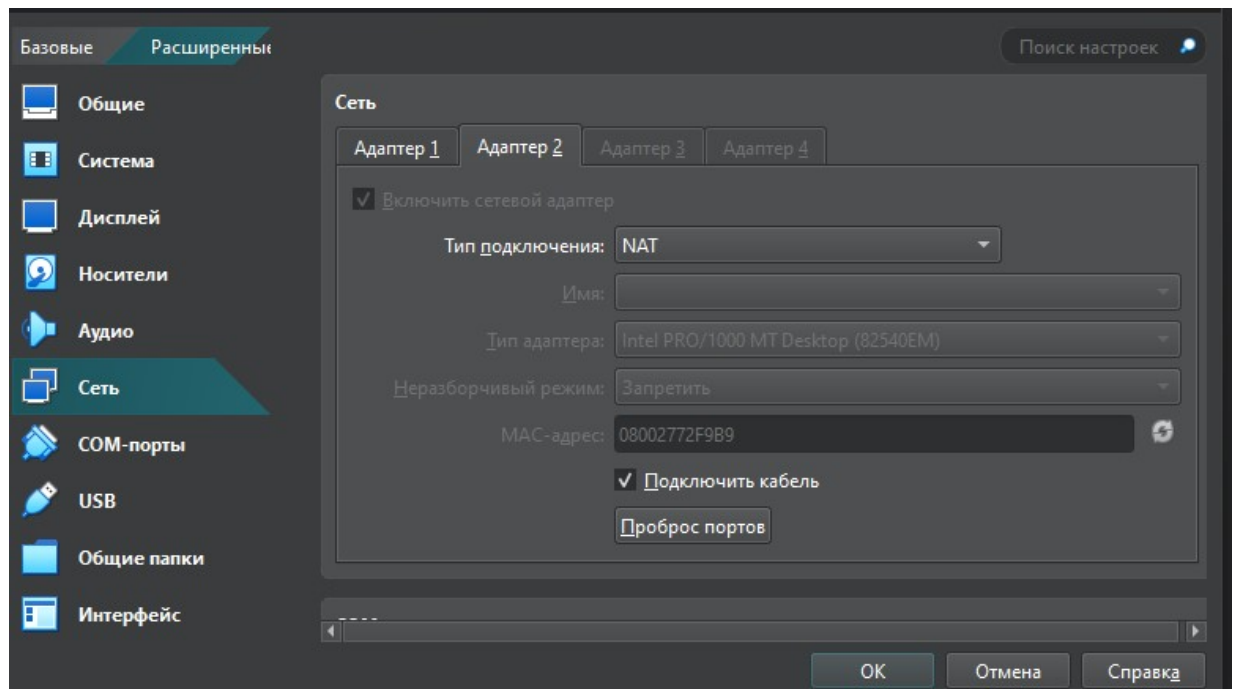


Рисунок 1 – Настройка машин

2. Заходим на первой машине в nmtui и настраиваем сеть:

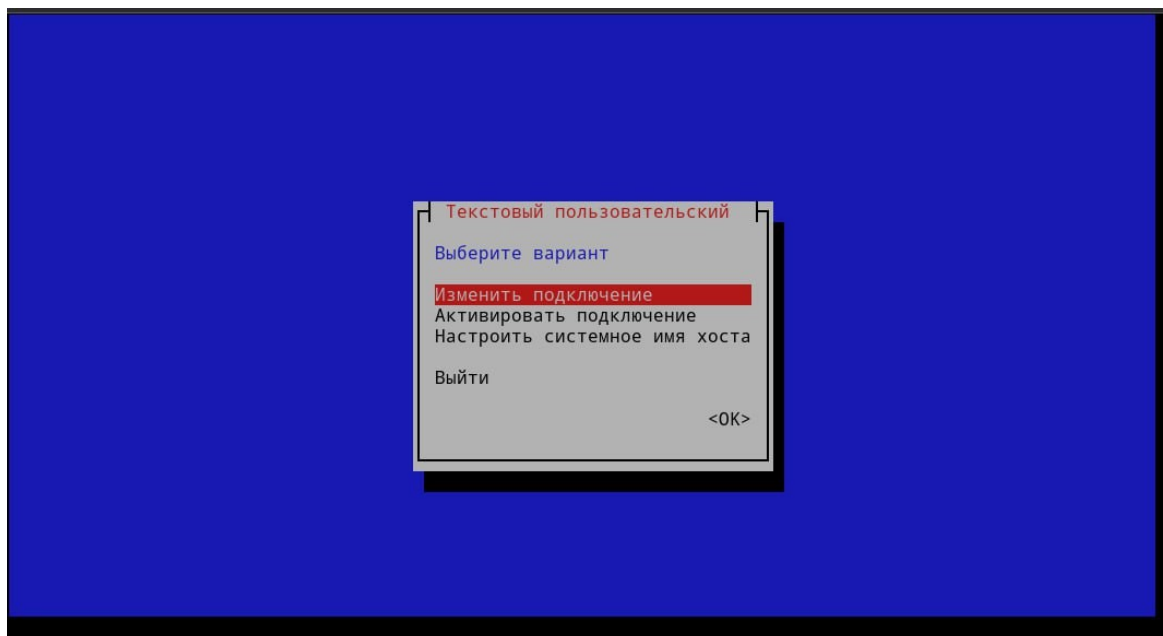


Рисунок 2 – Настройка сети

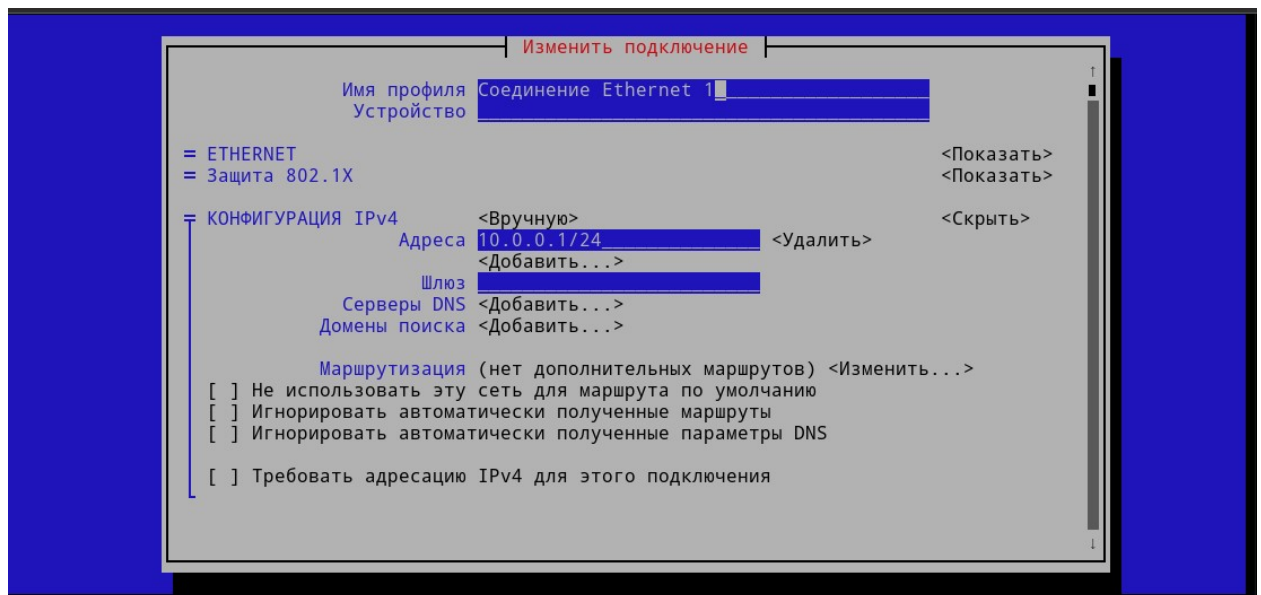


Рисунок 3 – Настройка сети

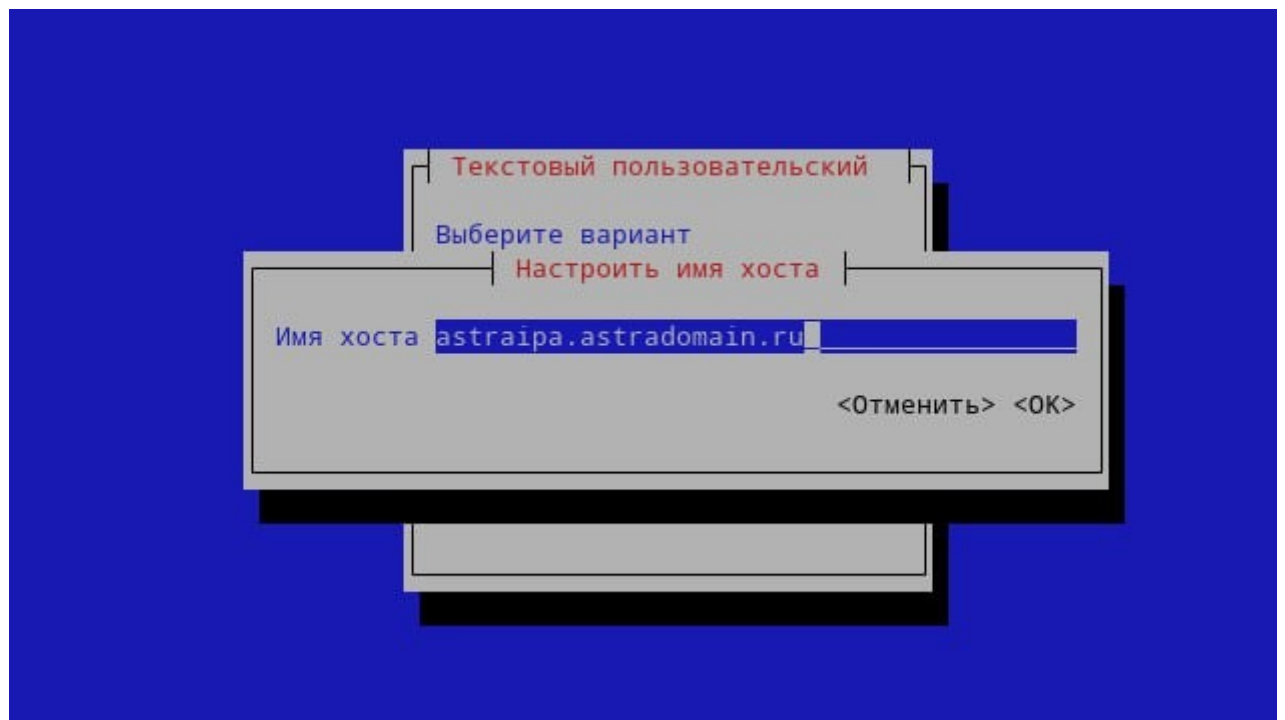


Рисунок 4 – Ручная настройка имени сервера

3. Устанавливаем комплект пакетов FreeIPA с помощью команды `apt install astra-freeipaserver`:

```

root@astra:/media/cdrom# apt install astra-freeipa-server
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
389-ds-base 389-ds-base-libs ant ant-optional astra-domain-data astra-freeipa-data augeas-lenses bind9
bind9-dnsutils bind9-dyndb-ldap bind9-host bind9-libs bind9-utils blt ca-certificates-java certmonger
checkpolicy chrony cpp-12 custodia default-jre-headless dirmngr dnsutils dogtag-pki-server-theme
fonts-font-awesome fonts-lyx fonts-open-sans freeipa-client freeipa-common freeipa-server
freeipa-server-dns freeipa-server-trust-ad g++ g++-12 gcc gcc-12 gcc-12-base gdal-data gdal-plugins gnupg
gnupg-l10n gnupg-utils gnupg2 gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv gssproxy
isymPy-common isymPy3 java-common junit4 keyutils krb5-admin-server krb5-config krb5-kdc krb5-kdc-ldap
krb5-otp krb5-pkinit krb5-user ldap-utils libactivation-java libaopalliance-java libapache-pom-java
libapache2-mod-auth-gssapi libapache2-mod-lookup-identity libapache2-mod-wsgi-py3 libargs4j-java libasan8
libatinject-jsr330-api-java libatomic1 libaugeas0 libbasicobjects0 libboost-dev libboost-filesystem1.74.0
libboost-iostreams1.74.0 libboost-locale1.74.0 libboost-thread1.74.0 libboost1.74-dev libbrotli1 libc-bin
libc-dev-bin libc-devtools libc-l10n libc6 libc6-dev libcc1-0 libcdi-api-java libcephfs2 libcodemodel-java
libcollection4 libcommons-cli-java libcommons-codec-java libcommons-compress-java libcommons-dbcp-java
libcommons-io-java libcommons-lang3-java libcommons-logging-java libcommons-net-java
libcommons-parent-java libcommons-pool-java libcrypt-dev libdbd-sqlite3-perl libdbi-perl libdhash1
libdom4j-java libdtd-parser-java libeclipse-jdt-core-java liberror-prone-java libexpat1 libexpat1-dev
libfastinfoset-java libgcc-12-dev libgcc-s1 libgdal32 libgeronimo-annotation-1.3-spec-java
libgeronimo-interceptor-3.0-spec-java libgfortran5 libgomp1 libgssapi-krb5-2 libgssrpc4 libguava-java
libguice-java libhamcrest-java libhsm-bin libhttpclient-java libhttpcore-java libini-config5 libipa-hbac0
libisorelax-java libistack-commons-java libitm1 libjackson-json-java libjackson2-annotations-java

```

Рисунок 5 – Установка пакета

4. Теперь нам необходимо отключить режим AstraMode web-сервера Apache2. Для этого меняем значение на AstraMode off в файле /etc/apache2/apache2.conf:

```

GNU nano 7.2 /etc/apache2/apache2.conf *
#Mutex file:${APACHE_LOCK_DIR} default
#
# The directory where shm and other runtime files will be stored.
#
DefaultRuntimeDir ${APACHE_RUN_DIR}
# Astra security mode.
#
AstraMode off
#
# Including realm to user name for astra mode.
#
# IncludeRealm off
#
# Controls which parsec capabilities are allowed for child processes
#
# ChildCapabilitiesParsec none
#

```

Рисунок 6 – Настройка файла

5. Теперь выключаем сетевой интерфейс и перезагружаем виртуальную машину:

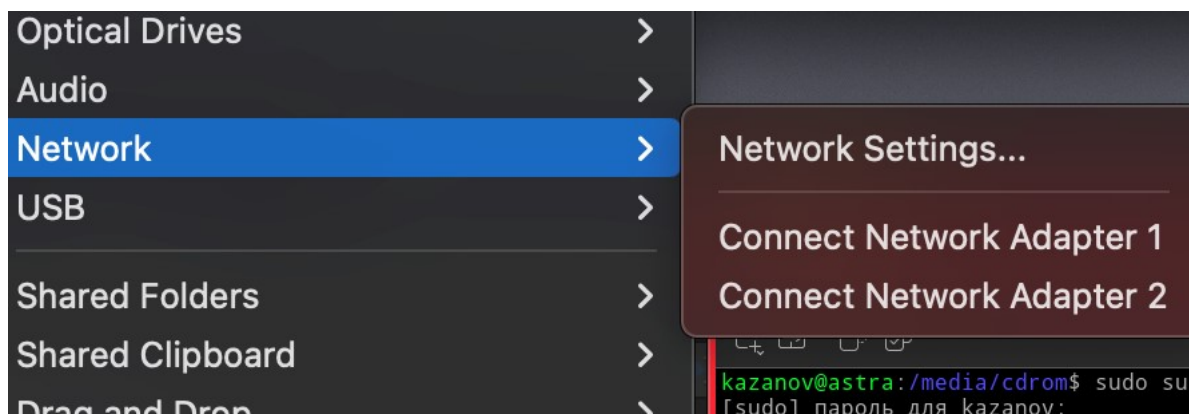


Рисунок 7 – Выключение сетевого интерфейса

6. Инициализируем сервера FreeIPA с помощью командной строки `astra-freeipa-server -o n astraipa -d astradomain.ru`:

```
root@astra:/media/cdrom# astra-freeipa-server -o -n astraipa -d astradomain.ru
compname= astraipa
domain= astradomain.ru
Сертификаты будут сгенерированы с помощью OpenSSL
get_ip: Обнаружено несколько сетевых интерфейсов:
      # NIC      IP      Type
      1 enp0s3 10.0.2.15 динамический
      2 enp0s8 10.0.0.1 статический
get_ip: Выберите номер сетевого интерфейса: 2
get_ip: Будет использован сетевой интерфейс "enp0s8", имеющий статический IP-адрес 10.0.0.1.
продолжать ? (y\n)
y
введите пароль администратора домена (login: admin):
```

Рисунок 8 – Инициализация сервера

После ввода пароля автоматически будет выполнен процесс инициализации входящих в FreeIPA подсистем. Ход выполнения будет отображаться на экране. В завершение будут выданы сообщения о перезапуске различных служб. Эти сообщения говорят об успешном завершении процесса:


```
* 389, 636: LDAP/LDAPS
* 88, 464: kerberos
* 53: bind
UDP Ports:
* 88, 464: kerberos
* 53: bind
* 123: ntp

2. You can now obtain a kerberos ticket using the command: 'kinit admin'
This ticket will allow you to use the IPA tools (e.g., ipa user-add)
and the web user interface.

The ipa-server-install command was successful
Restarting Directory Service
Restarting krb5kdc Service
Restarting kadmind Service
Restarting named Service
Restarting httpd Service
Restarting ipa-custodia Service
Restarting ipa-otpd Service
Restarting ipa-dnskeysyncd Service
ipa: INFO: The ipactl command was successful
Завершено.
Для продолжения работы, необходимо перезагрузить компьютер!
Обнаружен настроенный домен astradomain.ru
WEB: https://astraipa.astradomain.ru
```

Рисунок 9 – Инициализация сервера

7. Проверяем состояние запущенных служб FreeIPA с помощью инструмента командной строки `ipactl status`.
8. После завершения процедур запуска для входа в web-интерфейс можно просто перейти по ссылке, предоставленной использованным инструментом:

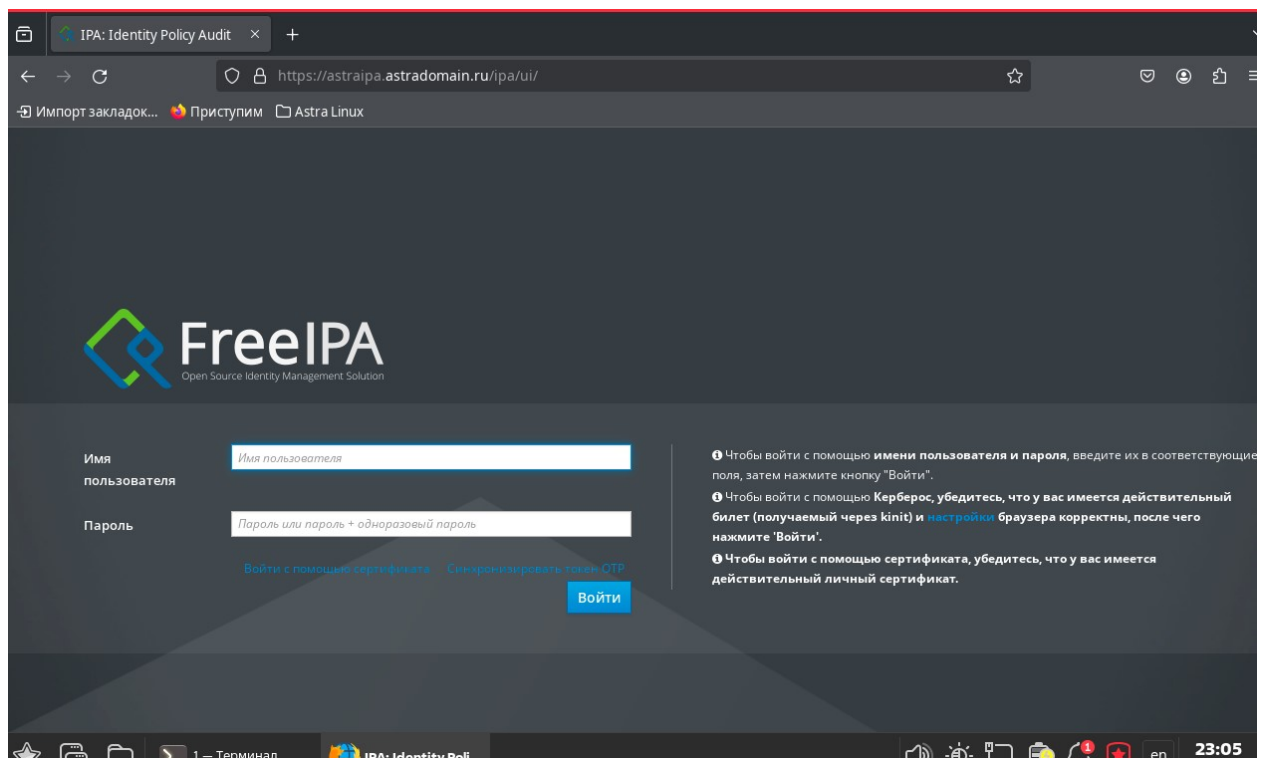


Рисунок 10 – Вход в web-интерфейс

Для проверки ролей сервера можно использовать web-интерфейс FreeIPA, например:

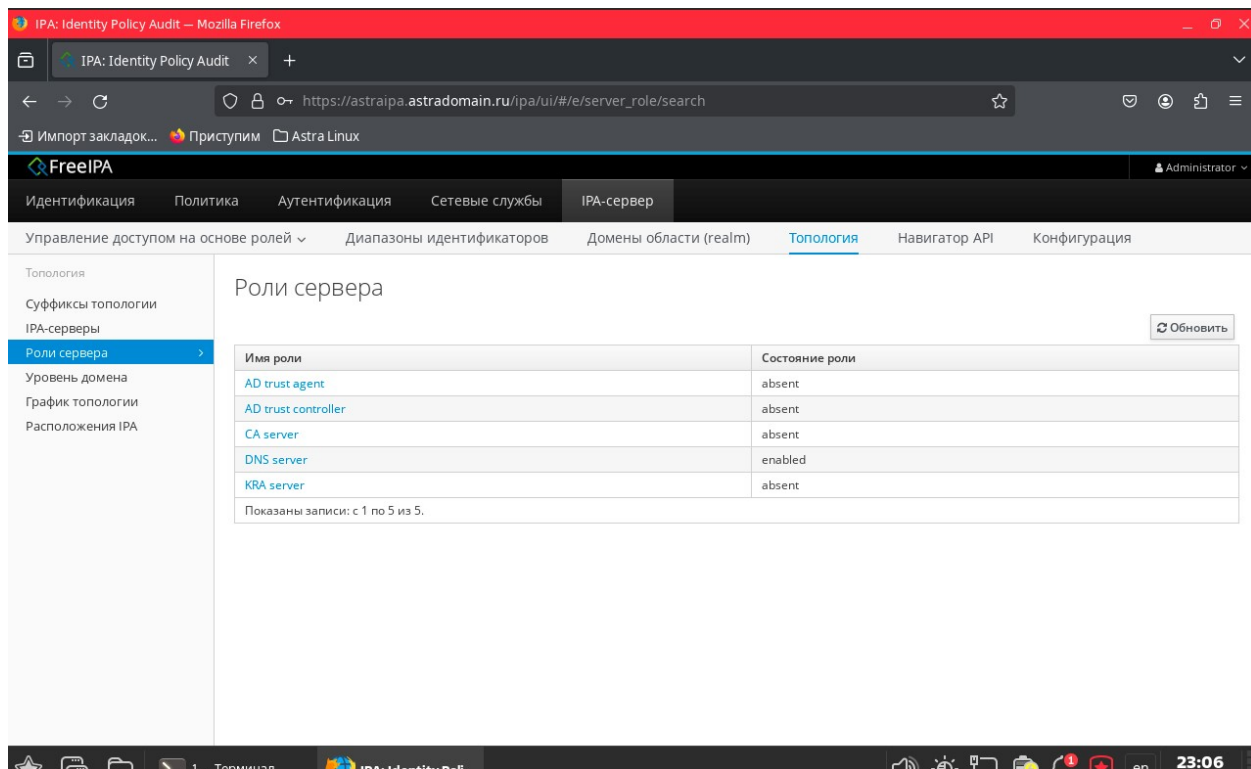


Рисунок 11 – Проверка ролей

- Запустим вторую машину. Для ввода компьютер в домен FreeIPA должны быть выполнены следующие условия, клиент и контроллер домена FreeIPA должны находиться в одной широковещательной сети и иметь доступ друг к другу. Для проверки доступности можно использовать команду на клиенте и на КД:

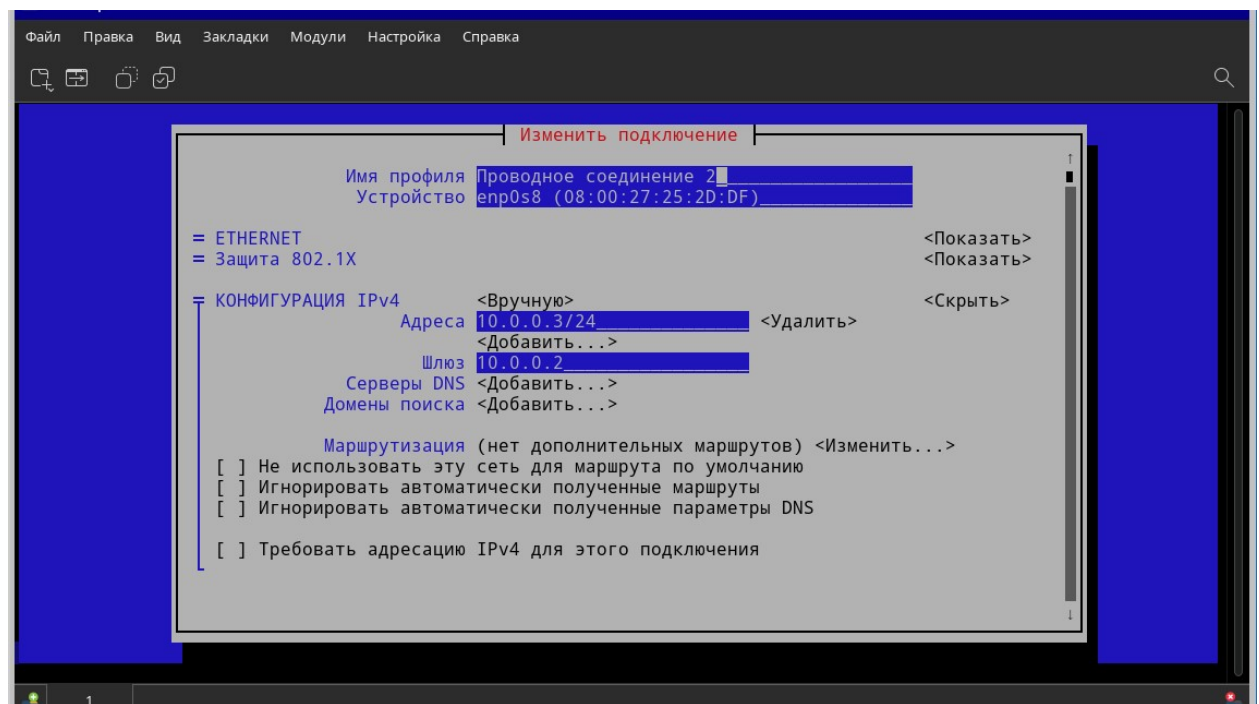


Рисунок 12 – Настройка сети

10. Проверим связь с первой машиной:

```
root@astra:/home/kazanov# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data:
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=2.15 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=1.04 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=1.14 ms
```

Рисунок 13 – Проверка соединения

11. Для установки инструмента командной строки используем команду `apt install astra-freeipa-client`:

```
Чтение списков пакетов... Готово
root@astra:/home/kazanov# apt install astra-freeipa-client
Чтение списков пакетов... Готово
Построение дерева зависимостей... Готово
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
 astra-domain-data astra-freeipa-data augeas-lenses bind9-dnsutils bind9-host bind9-libs bind9-utils
 bind9utils certmonger chrony dirmngr dnsutils freeipa-client freeipa-common gnupg gnupg-l10n gnupg-utils
 gnupg2 gpg gpg-agent gpg-wks-client gpg-wks-server gpgconf gpgsm gpgv haveged ieee-data keyutils
 krb5-config krb5-user ldap-utils libaugeas0 libbasicobjects0 libc-ares2 libcollection4 libdhash1
 libgssapi-krb5-2 libgssrpc4 libhavege2 libini-config5 libipa-hbac0 libk5crypto3 libkadm5clnt-mit12
 libkadm5srv-mit12 libkdb5-10 libkrb5-3 libkrb5support0 libldap-common libldb2 libnfsidmap1 libnss-sss
 libnss-sudo libnss3-tools libpam-sss libparsec-aud-db-sssd3 libparsec-aud3 libparsec-base3
```

Рисунок 14 – Установка пакетов

12. Проверим, что все названия машин указаны в файле `/etc/hosts` на обеих машинах:

```
GNU nano 7.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 astra2.astradomain.ru
10.0.0.3 astra2.astradomain.ru
10.0.0.2 astraipa.astradomain.ru

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Рисунок 15– Проверка названий машин

```
GNU nano 7.2 /etc/hosts
#astra-freeipa-server
127.0.0.1 localhost localhost.localdomain
10.0.0.2 astraipa.astradomain.ru astraipa
127.0.1.1 astraipa.astradomain.ru
10.0.0.3 astra2.astradomain.ru

::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Рисунок 16 – Проверка названий машин

13. Введем компьютер в домен FreeIPA командой `astra-freeipa-client -d astradomain.ru`:
14. Попробуем войти в домен:

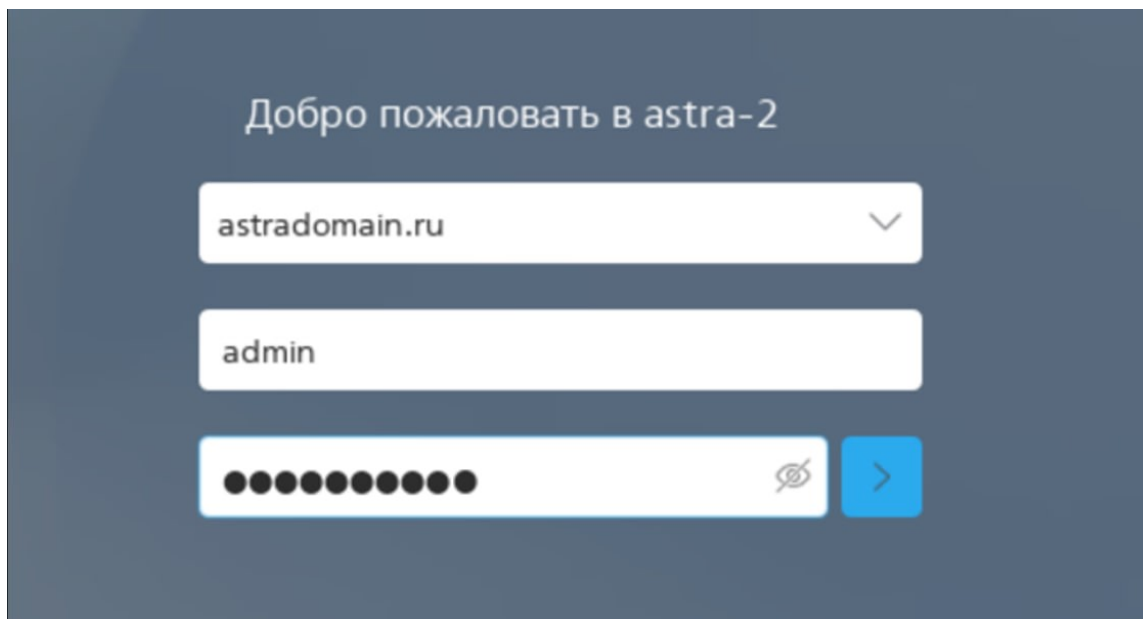


Рисунок 17 – Вход в домен

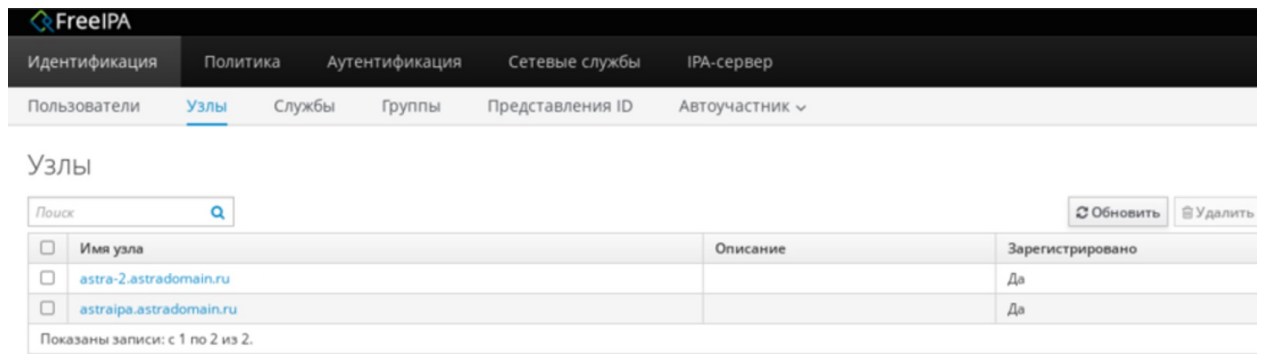


Рисунок 18 – Проверка домена на стороне сервера

Вывод

Мы научились устанавливать и настраивать FreeIPA на примере Astra Linux SE в виртуальной среде Oracle VirtualBox.

Контрольные вопросы

1. Что такое FreeIPA?

FreeIPA — это система управления удостоверениями и доступом (IAM), предоставляющая централизованное управление пользователями, группами, компьютерами и политиками безопасности..

2. Для чего используется FreeIPA и каковы минимальные требования для ее служб?

Используется для централизованного управления идентификацией и доступом в сети. Минимальные требования зависят от масштаба развертывания, но обычно включают сервер с достаточной мощностью, сеть и необходимые пакеты программного обеспечения.

3. Каких правил следует придерживаться для запуска FreeIPA?

Следует придерживаться рекомендованных практик безопасности, использовать сильные пароли, регулярно обновлять систему и следовать официальной документации FreeIPA.