

FreeIPA

- Подготовка к установке сервера
 - Доменное имя
 - Сервер
 - Установка пакетов
 - Описание тестового примера
 - Быстрая настройка и запуск сервера
 - Быстрый запуск сервиса FreeIPA с помощью графического инструмента fly-admin-freeipa-server
 - Установка с использованием центра сертификации DogTag (только для ОС ОН Орёл)
 - Быстрый запуск сервиса FreeIPA с помощью инструмента командной строки astra-freeipa-server
 - Установка с использованием центра сертификации DogTag (только для ОС ОН Орёл)
 - Первый вход в WEB-интерфейс инструмента FreeIPA
 - Проверка запущенных служб и ролей FreeIPA
-
- Ввод клиентского компьютера в домен FreeIPA
 - Динамическое обновление DNS FreeIPA
 - Настройка доверительных отношений FreeIPA -- Active Directory
 - FreeIPA: настройка репликации
 - Подключение центра сертификации DogTag.
 - Создание сертификатов для FreeIPA с помощью XCA
 - FreeIPA: настройка стенда с генерацией сертификатов
 - Samba + FreeIPA аутентификация пользователей Samba в Kerberos



Данная статья применима к:

- ОС ОН Орёл 2.12
- ОС СН Смоленск 1.6 (кроме работы с DogTag)
- ОС СН Ленинград 8.1 (кроме работы с DogTag)

Подготовка к установке сервера



ВАЖНО!

Сервис FreeIPA крайне чувствителен к правильным настройкам параметров операционной системы. Даже при запуске сервиса в тестовом режиме следует придерживаться приведённых ниже правил.

Работа FreeIPA в ОС СН (Astra Linux SE) осуществляется только при отключенном режиме AstraMode web-сервера Apache2.

Доменное имя

- Доменное имя не должно быть именем первого уровня. Это значит, что нежелательно использовать имена доменов, состоящие из одного слова, например domain, testdomain, mydomian. Следует использовать имена уровней два и более, то есть имена вида:



domain.net
testdomain.test.lan
mycompany.ru
и т. д.

- В случаях, если при запуске службы FreeIPA используется имя домена, не имеющее IP-адреса (например, при запуске в тестовых целях), запуск службы следует производить в режиме «для изолированной сети» (опция -o инструмента astra-freeipa-server или пункт «Изолированная сеть (без шлюза/DNS)» в меню «Расширенные опции» графического инструмента fly-admin-freeipa-server). Далее в примерах подразумевается запуск именно сервиса в режиме «для изолированной сети». Проверить, имеет ли выбранный домен IP-адрес, можно из терминала командой nslookup или dig, например:

```
nslookup mydomain.net
```

или

```
dig mydomain.net
```

- В имени домена нельзя использовать кириллицу;

- Выбранное доменное имя не должно обслуживаться другим контроллером домена. Это значит, что при первичной настройке службы FreeIPA будет проверено, существует ли уже в домене любой иной контроллер домена, и, если он будет обнаружен, настройка не будет выполнена.
- Пароль администратора домена должен состоять не менее, чем из восьми символов.

Сервер

Для нормальной работы сервиса FreeIPA следует:

- Выделить для использования в качестве сервера FreeIPA отдельный (возможно, виртуальный) компьютер;
- **При использовании виртуального компьютера выделить этому компьютеру не менее 2ГБ ОЗУ и 3-х процессоров;**
- Назначить этому компьютеру фиксированный IP-адрес, который, впоследствии, не должен изменяться.



В /etc/hostname должно содержаться FQDN (astraipa.astradomain.ad).

Файл /etc/hosts не должен использоваться в качестве базы данных доменных имен других хостов. Так как запрос к этому файлу имеет приоритет перед обращением к DNS.

Чтобы не было путаницы, в нем рекомендуется только запись "самого себя", <ip адрес> + имя в формате FQDN + короткое имя. Данная запись добавляется автоматически во время установки FreeIPA сервера.

Для добавления имени хоста можно выполнить команду:

```
hostnamectl set-hostname astraipa.astradomain.ad
```



Разрешить загрузку модулей протокола IPv6, при необходимости запретив их работу (см. [IPv6: включение и выключение, выключение с сохранением стека IPv6](#))

- Остальные настройки для быстрого запуска, инструменты Astra Linux выполняют самостоятельно.

Установка пакетов

Комплекты пакетов FreeIPA для сервера и клиентов входят в стандартный репозиторий ОС ОН Орёл.

Установить необходимые для установки сервера пакеты можно из [графического менеджера пакетов](#), или из командной строки:

- Графический инструмент

```
apt install fly-admin-freeipa-server
```

- или инструмент командной строки

```
astra-freeipa-server
```

В ходе установки будет выдано несколько предупреждений, просто нажать "ОК".

После установки графический инструмент fly-admin-freeipa-server будет доступен через меню:



"Пуск" - "Панель управления" - "Сеть" - "Настройка FreeIPA server fly"

Установить необходимые для установки клиента пакеты можно с помощью [графического менеджера пакетов](#) или из командной строки. Команды для установки из командной строки:

- графический инструмент

```
apt install fly-admin-freeipa-client
```

- или инструмент командной строки

```
apt install astra-freeipa-client
```

На предупреждения, возникающие при установке, также нажать "ОК"

После установки графический инструмент fly-admin-freeipa-client будет доступен через меню:



"Пуск" - "Панель управления" - "Сеть" - "Настройка FreeIPA clientfly"

Описание тестового примера

Для дальнейшего описания настройки сервиса FreeIPA примем следующие допущения:

- мы хотим создать собственный домен второго уровня с названием: `astradomain.ad`;
- имя будущего контроллера сервера:
 - имя в краткой форме: `astraipa`
 - имя в полной форме (FQDN): `astraipa.astradomain.ad`

При этом, в тестовом примере будет использован несуществующий домен `astradomain.ad`

Быстрая настройка и запуск сервера

Быстрый запуск сервиса FreeIPA с помощью графического инструмента fly-admin-freeipa-server

Графический инструмент fly-admin-freeipa-server запускается из командной строки командой:

```
fly-admin-freeipa-server
```

После запуска на экране появляется форма для ввода данных, в которой нужно указать:

- «Домен» - имя домена, в используемом примере это будет `astradomain.ad`
- «Имя компьютера» - имя компьютера определяется автоматически, в используемом примере заменим его на `astraipa`
- «Пароль» - пароль для администратора домена. Введённый пароль понадобится в дальнейшем для входа в WEB-интерфейс FreeIPA, и для работы с инструментами командной строки FreeIPA.

После ввода данных запуск сервиса осуществляется нажатием кнопки «»

В процессе запуска в соответствующем окне отображаются выполняющиеся операции.

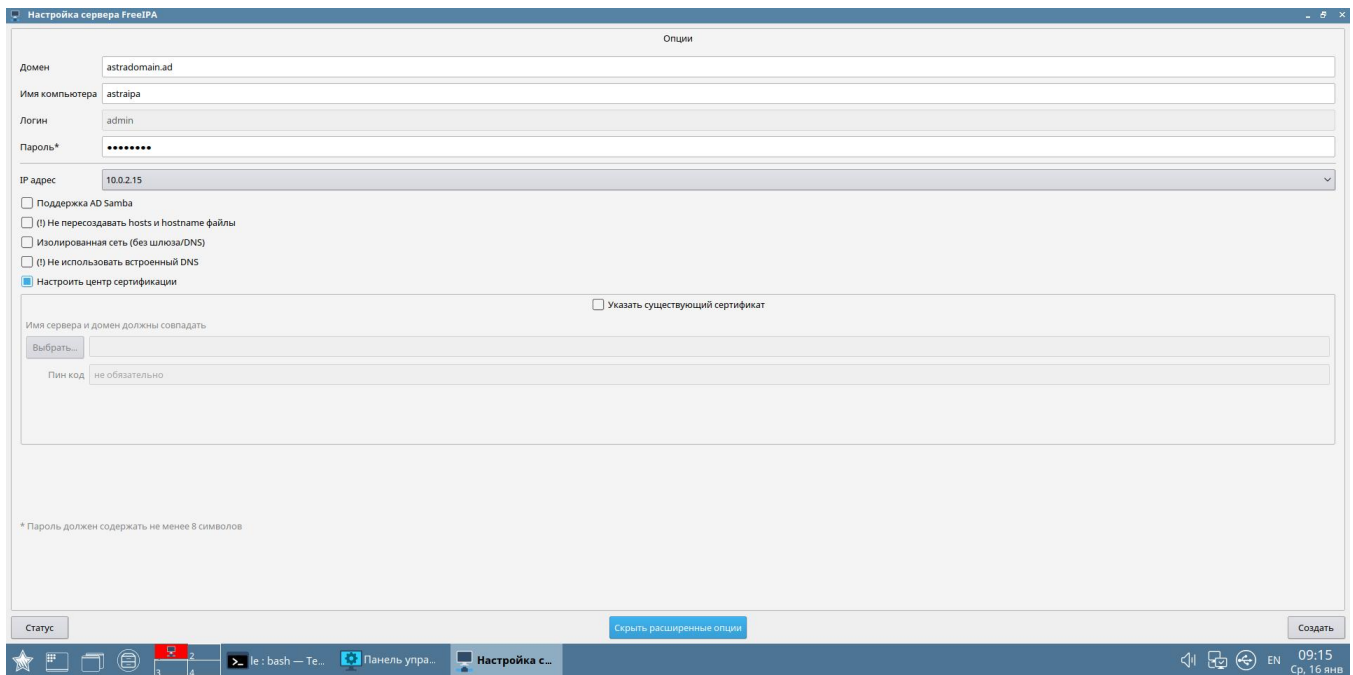
После успешного выполнения запуск на нижней рамке окна инструмента появится WEB-ссылка для перехода в WEB-интерфейс FreeIPA.

Теперь можно войти в WEB-интерфейс FreeIPA по указанному в последней строчке адресу, и продолжить настройку через него.

Первый вход в WEB-интерфейс и процедуры работы с ним описаны ниже.

Установка с использованием центра сертификации DogTag (только для ОС ОН Орёл)

Для автоматической установки FreeIPA с одновременной установкой сервиса центра сертификации DogTag в интерфейсе графического инструмента fly-admin-freeipa-server нажмите кнопку "Показать расширенные опции" и отметьте пункт "Настроить центр сертификации":



Быстрый запуск сервиса FreeIPA с помощью инструмента командной строки astra-freeipa-server

При правильно выполненных предварительных настройках запуск сервиса FreeIPA с помощью инструмента командной строки astra-freeipa-server может быть осуществлён простой командой:

```
astra-freeipa-server
```

При этом инструмент должен сам определить все необходимые параметры.

При запуске инструмента также можно указать имя домена, имя компьютера и прочие параметры (подробнее см. подсказку astra-freeipa-server --help), например:

```
astra-freeipa-server -d astradomain.ad -n astraipa -o
```

После ввода команды инструмент определит адрес компьютера, выведет на экран все исходные данные, и запросит подтверждение дальнейших действий:

```
❗ compname= astraipa
  domain= astradomain.ad
  будет использован ip address = 192.168.32.97 или укажите ip адрес ключем -ip
  продолжить ? (y\n)
```

Для подтверждения введите «у» и нажмите Enter.

После подтверждения инструмент попросит ввести и подтвердить пароль для администратора домена.

Введённый пароль понадобится в дальнейшем для входа в WEB-интерфейс FreeIPA, и для работы с инструментами командной строки FreeIPA.

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 системных служб:

```
i Restarting Directory Service
Restarting krb5kdc Service
Restarting kadmin Service
Restarting named Service
Restarting ipa_memcached Service
Restarting httpd Service
Restarting ipa-custodia Service
Restarting ipa-otpd Service
Restarting ipa-dnskeysyncd Service
Starting ntpd Service
ipa: INFO: The ipactl command was successful
Существует настроенный домен
host = astraipa.astradomain.ad
basedn = dc=astradomain,dc=ad
domain = astradomain.ad
xmlrpc_uri = https://astraipa.astradomain.ad/ipa/xml
WEB: https://astraipa.astradomain.ad
```

Эти сообщения говорят об успешном завершении процесса.

Теперь можно войти в WEB-интерфейс FreeIPA по указанному в последней строчке адресу, и продолжить настройку через него. Первый вход в WEB-интерфейс и процедуры работы с ним описаны ниже.

Установка с использованием центра сертификации DogTag (только для ОС ОН Орёл)

Для автоматической установки FreeIPA с одновременной автоматической установкой сервиса центра сертификации DogTag используйте опцию `--dogtag`, например:

```
astra-freeipa-server -d astradomain.ad -n astraipa -o --dogtag
```

Первый вход в WEB-интерфейс инструмента FreeIPA

После завершения процедур запуска для входа в WEB-интерфейс можно просто перейти по ссылке, предоставленной использованным инструментом.

В примерах, приведенных в настоящем документе, для обеспечения защиты подключения используются сертификаты автоматически создаваемого удостоверяющего центра, неизвестного системе безопасности WEB-сервера.

Поэтому, при первой попытке подключения на экране браузера, появится сообщение о том, что соединение не защищено. В такой ситуации следует:

- нажать кнопку «Дополнительно»
- в открывшемся окне нажать кнопку «Добавить исключение»
- в открывшейся экранной форме нажать кнопку «Подтвердить исключение безопасности»

и на экране браузера откроется WEB-интерфейс FreeIPA.

Для входа в WEB-интерфейс используйте имя `admin`, и пароль, ранее введённый при запуске системы. Также, теперь с помощью программы `astra-freeipa-client`, к созданному сервису можно подключать другие машины.

В случае, если при входе в WEB-интерфейс открывается пустая страница — внимательно проверьте, что для подключения к WEB-интерфейсу используются:

- протокол HTTPS (адресная строка в браузере должна начинаться с тега `<https://>`, например, правильно: <https://astraipa.astradomain.ad>);
- полное доменное имя сервера FreeIPA (например, неправильно: <https://localhost> или <https://127.0.0.1>)

Проверка запущенных служб и ролей FreeIPA

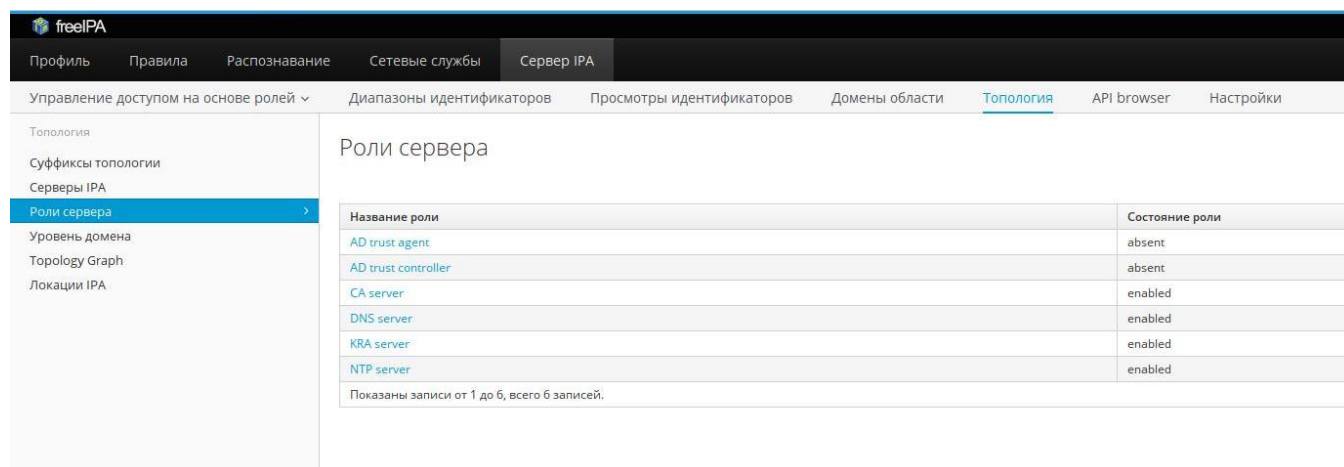
Для проверки состояния запущенных служб FreeIPA можно использовать инструмент командной строки `ipactl`:

```
ipactl status
```

Примерный вывод команды:

```
$ sudo ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmind Service: RUNNING
named Service: RUNNING
ipa_memcached Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
ntpd Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

Для проверки ролей сервера можно использовать WEB-интерфейс FreeIPA (путь Закладка "FreeIPA" => Пункт "Топология" => Пункт "Роли сервера"), например:



The screenshot shows the FreeIPA web interface. The top navigation bar includes 'Профиль', 'Правила', 'Распознавание', 'Сетевые службы', and 'Сервер IPA'. The 'Топология' (Topology) tab is selected. The left sidebar shows a tree view with 'Роли сервера' (Roles of the server) highlighted. The main content area displays a table of server roles.

Название роли	Состояние роли
AD trust agent	absent
AD trust controller	absent
CA server	enabled
DNS server	enabled
KRA server	enabled
NTP server	enabled

Показаны записи от 1 до 6, всего 6 записей.