ДОКУМЕНТАЦИЯ ALT LINUX TEAM

Доменная инфраструктура на базе FreeIPA

Руководство пользователя

Редакция октябрь, 2025

Аннотация

FreeIPA — это комплексное решение по управлению безопасностью Linux-систем, 389 Directory Server, MIT Kerberos, NTP, DNS, Dogtag. Оно состоит из веб-интерфейса и интерфейса командной строки. FreeIPA является интегрированной системой проверки подлинности и авторизации в сетевой среде Linux, FreeIPA сервер обеспечивает централизованную проверку подлинности, авторизацию и контроль за аккаунтами пользователей сохраняя сведения о пользователе, группах, узлах и других объектах необходимых для обеспечения сетевой безопасности.

Данное руководство соответствует текущему состоянию сведений, но какие-либо окончательные правки могли не попасть в него. В случае обнаружения ошибок и неточностей в руководство вносятся изменения.

Часть I. Разворачивание FreeIPA

В этой части приводится общая информация по разворачиванию FreeIPA.

Содержание

Глава 1. Подготовка системы к установке сервера FreeIPA

В этом разделе перечислены требования для установки сервера FreeIPA. Перед установкой необходимо убедиться, что система соответствует этим требованиям.

Примечание

Для установки сервера FreeIPA нужны привилегии суперпользователя.

1.1. Системные требования к серверу FreeIPA

Сервер FreeIPA следует устанавливать на чистую систему, в которой отсутствуют какие-либо пользовательские настройки служб: DNS, Kerberos, Apache и Directory Server.

FreeIPA при настройке домена перезаписывает системные файлы. Резервные копии исходных файлов сохраняются в каталоге **`/var/lib/ipa/sysrestore/`**. При удалении сервера FreeIPA эти файлы автоматически восстанавливаются.

1.1.1. Оперативная память (RAM)

Для установки с встроенным центром сертификации (CA) требуется минимум 1,2 ГБ RAM. Для демонстрационной или тестовой системы рекомендуется не менее 2 ГБ.

Типичные требования к оперативной памяти:

- для 10 000 пользователей и 100 групп: не менее 4 ГБ RAM и 4 ГБ Swap;
- для 100 000 пользователей и 50 000 групп: не менее 16 ГБ RAM и 4 ГБ Swap.

1.1.2. DNS

Корректная работа Kerberos и SSL невозможна без правильно настроенной DNS-инфраструктуры.

Важно

Домен DNS нельзя изменить после установки FreeIPA.

Установщик FreeIPA довольно требователен к настройке DNS. Установщик выполняет следующие проверки:

- имя узла не должно быть localhost или localhost6;
- имя узла должно быть полным (FQDN), например: ipa.example.test;
- имя узла должно разрешаться в IP-адрес (прямая запись);
- обратная DNS-запись (PTR) должна совпадать с FQDN.

Не следует использовать существующий публичный домен, если вы не являетесь его владельцем. Для тестовых установок рекомендуется использовать домены из резервированных зон, указанных в RFC2606 (**`https://tools.ietf.org/html/rfc2606`**), например: ipa.test, example.net.

1.1.3. IPv6

В ядре системы должен быть включен протокол IPv6. Если IPv6 отключен, подключаемый модуль CLDAP, используемый службами FreeIPA, не инициализируется.

Примечание

Фактическое использование IPv6 в сети не обязательно — достаточно, чтобы протокол был включён на уровне ядра.

1.2. Поддержка типов шифрования в FreeIPA

FreeIPA по умолчанию использует современные типы шифрования Kerberos, такие как aes256-cts-hmac-sha1-96 и aes128-cts-hmac-sha1-96. Устаревшие типы (des-cbc-crc, des-cbc-md5) отключены по соображениям безопасности.

Важно

Все клиенты и серверы должны поддерживать одинаковые типы шифрования, иначе аутентификация Kerberos работать не будет.

1.3. Синхронизация времени

FreeIPA требует точной синхронизации времени между всеми узлами домена. Максимально допустимое расхождение — 5 минут (ограничение Kerberos).

Рекомендуется использовать NTP-сервер, например chrony или ntpd.

Если сервер FreeIPA будет выступать в роли основного NTP-источника, это следует настроить отдельно.

1.4. Требования к портам

Таблица 1.1. Порты FreeIPA

Служба	Порт(ы)	Протокол
HTTP/HTTPS	80, 443	TCP
LDAP/LDAPS	389, 636	TCP
Kerberos	88, 464	TCP и UDP
DNS	53	TCP и UDP (опционально, если используется встроенный DNS)
NTP (опционально)	123	UDP

Примечание

Все перечисленные порты должны быть открыты в межсетевом экране и не заняты другими службами.

Следующие порты используются внутренними компонентами FreeIPA и не требуют открытия во внешнем интерфейсе:

- 8080/TCP, 8443/TCP — используются службой pki-tomcat для внутреннего взаимодействия с подсистемой сертификатов (Dogtag PKI);
- 749/TCP и UDP — используется для удалённого администрирования Kerberos (kadmin). Этот порт нужно открывать только при необходимости удалённого управления учётными записями Kerberos.

1.5. Подготовка сервера

Для корректной работы сервера необходимо задать ему полное доменное имя (FQDN). Имя серверу можно назначить командой:

```
# hostnamectl set-hostname ipa.example.test
```

Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

Примечание

IP-адрес сервера не должен изменяться после установки FreeIPA.

Чтобы избежать конфликтов с портами, используемыми FreeIPA нужно отключить ahttpd, работающий на порту 8080, и отключить HTTPS в Apache2:

```
# systemctl stop ahttpd
# a2dissite 000-default_https
# a2disport https
# systemctl condreload httpd2
```

Для ускорения генерации криптографических ключей (особенно на виртуальных машинах) рекомендуется установить демон энтропии *haveged*:

```
# apt-get install haveged
# systemctl enable --now haveged
```

1.6. Установка пакетов

В зависимости от того, какие функции будет выполнять сервер FreeIPA, необходимо установить один из следующих пакетов:

- без встроенного DNS-сервера:

```
# apt-get install freeipa-server
```

- с встроенным DNS-сервером:

```
# apt-get install freeipa-server-dns
```

- с поддержкой доверительных отношений с Active Directory:

```
# apt-get install freeipa-server-trust-ad
```

1.7. Параметры команд установки FreeIPA

Команды **ipa-server-install**, **ipa-replica-install**, **ipa-dns-install** и **ipa-ca-install** имеют множество опций, которые можно использовать для предоставления дополнительной информации при интерактивной установке сервера. Их также можно использовать в скриптах.

Ниже описаны некоторые самые распространённые опции. Для получения более подробной информации следует обратиться к man страницам **ipa-server-install(1)**, **ipa-replica-install(1)**, **ipa-dns-install(1)** и **ipa-ca-install(1)**.

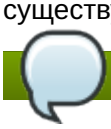
Таблица 1.2. Основные опции для ipa-server-install и ipa-replica-install

Опция	Описание
-d, **--debug**	Включает режим отладки.
-U, **--unattended**	Запускает автоматическую (пакетную) установку без запроса данных у пользователя.
--hostname=<*HOSTNAME*>	Полное доменное имя (FQDN) сервера FreeIPA (например, server.ipa.example.test). Должно содержать только строчные буквы, цифры, дефисы и точки.
--ip-address=<*IP_ADDRESS*>	Указывает IP-адрес сервера. IP-адрес должен быть назначен одному из локальных сетевых интерфейсов. Опцию можно использовать несколько раз.
--dirsrv-config-file=<*LDIF_file_name*>	Путь к файлу в формате LDIF, содержащему настройки для экземпляра Directory Server.
-n <*DOMAIN_NAME*>, **--domain=<*DOMAIN_NAME*>**	Имя LDAP-домена, используемого в качестве домена FreeIPA.
-p <*directory_manager_password*>, **--ds-password=<*directory_manager_password*>**	Пароль учётной записи ***cn=Directory Manager*** службы каталогов
-a <*ipa_admin_password*>, **--admin-password=<*ipa_admin_password*>**	Пароль учётной записи администратора FreeIPA (***admin***). Для **ipa-replica-install** вместо этой опции используется **-w**.
-r <*KERBEROS_REALM_NAME*>, **--realm=<*KERBEROS_REALM_NAME*>**	Имя области Kerberos, создаваемой для домена FreeIPA (в верхнем регистре, например, EXAMPLE.TEST). Для **ipa-replica-install** указывает имя Kerberos-области существующего развёртывания FreeIPA.
--setup-dns	Настраивает встроенную службу DNS в домене FreeIPA.
--setup-ca	Устанавливает и настраивает локальный центр сертификации (CA). Если CA не установлен, операции с сертификатами перенаправляются на другую реплику с установленным CA. Для **ipa-server-install** CA устанавливается по умолчанию, поэтому указывать эту опцию не требуется.

Таблица 1.3. Опции CA для ipa-ca-install и ipa-server-install

Опция	Описание
--ca-subject=***<SUBJECT>***	Задаёт различающееся имя (DN) субъекта сертификата CA (по умолчанию: ***CN=Certificate Authority,O=<REALM_NAME>***). Относительные различающиеся имена (RDN) указываются в порядке LDAP, начиная с наиболее конкретного RDN.
--subject-base=***<SUBJECT>***	Указывает базу субъекта для сертификатов, выдаваемых FreeIPA (по умолчанию: ***O=<REALM_NAME>***). Относительные различающиеся имена (RDN) указываются в порядке LDAP, начиная с наиболее конкретного RDN.
--external-ca	Генерирует запрос на подпись сертификата (CSR), который должен быть подписан внешним центром сертификации.
--external-ca-type={generic,ms-cs}	Тип внешнего центра сертификации (CA). По умолчанию: ***generic***.
--ca-signing-algorithm={SHA1withRSA,SHA256withRSA,SHA384withRSA,SHA512withRSA}	Алгоритм подписи сертификата CA. По умолчанию: ***SHA256withRSA***. Эту опцию следует использовать совместно с **--external-ca**, если внешний CA не поддерживает алгоритм подписи по умолчанию.

Таблица 1.4. Опции DNS (доступны для ipa-dns-install, ipa-server-install и ipa-replica-install если используется опция --setup-dns)

Опция	Описание
--allow-zone-overlap	Разрешает создание DNS-зоны, даже если зона с таким именем уже существует.
--forwarder=***<FORWARDERS>***	Указывает DNS-сервер пересылки. Параметр можно использовать несколько раз для задания нескольких серверов.
--no-forwarders	Использовать корневые DNS-серверы вместо серверов пересылки.
--auto-forwarders	Автоматически использовать серверы пересылки из файла **/etc/resolv.conf**.
--forward-policy={only,first}	Политика пересылки DNS-запросов для глобальных серверов пересылки.
--reverse-zone=***<REVERSE_ZONE>***	Указывает обратную DNS-зону. Параметр можно использовать несколько раз.
--no-reverse	Отключает автоматическое создание обратных зон DNS. Если обратная зона уже существует, она не изменяется.  **Примечание**

Опция	Описание
	Если параметр не указан, установщик автоматически создаёт необходимые обратные зоны DNS.
--auto-reverse	Автоматически создаёт необходимые обратные зоны на основе указанных IP-адресов.
--no-dnssec-validation	Отключает проверку DNSSEC.

Таблица 1.5. Опции конфигурации NTP для ipa-server-install, ipa-replica-install и ipa-client-install

Опция	Описание
--ntp-server	Указывает NTP-сервер. Можно использовать несколько раз, чтобы указать несколько серверов.
--ntp-pool	Указывает пул NTP-серверов (DNS-имя, разрешающееся в несколько адресов).
-N, **--no-ntp**	Не настраивать и не запускать службу синхронизации времени.

Примечание

Все пароли должны соответствовать политике сложности FreeIPA.

Примечание

При автоматической установке (**--unattended**) необходимо указать все обязательные параметры, иначе команда завершится ошибкой.

Глава 2. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA

Преимущества установки сервера FreeIPA со встроенным DNS:

- можно автоматизировать большую часть обслуживания и управления записями DNS, используя инструменты FreeIPA. Например, SRV-записи создаются во время установки, а затем автоматически обновляются;

- можно обеспечить стабильное подключение к глобальному Интернету, настроив глобальные DNS-серверы пересылки во время установки. Это особенно полезно при настройке доверительных отношений с Active Directory;
- можно настроить обратные DNS-зоны, чтобы письма отправляемые из домена FreeIPA, не помечались как спам внешними почтовыми серверами.

Ограничения установки сервера FreeIPA со встроенным DNS:

- FreeIPA DNS не предназначен для использования в качестве общедоступного DNS-сервера. Некоторые расширенные функции DNS не поддерживаются.

Примечание

Если при запуске **ipa-server-install** не указаны параметры, связанные с центром сертификации (например, **--external-ca** или **--ca-less**), сервер FreeIPA устанавливается с встроенным центром сертификации (CA).

2.1. Интерактивная установка

Для запуска интерактивной установки необходимо выполнить команду:

```
# ipa-server-install

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will set up the IPA Server.
Version 4.12.4

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the NTP client (CHRONY)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure SID generation
  * Configure the KDC to enable PKINIT

To accept the default shown in brackets, press the Enter key.
```

На вопрос о настройке встроенного DNS-сервера следует ответить утвердительно:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **Enter**.

Далее нужно указать имя узла, на котором будет установлен сервер FreeIPA, доменное имя и Kerberos-область:

```
Server host name [ipa.example.test]:
Please confirm the domain name [example.test]:
Please provide a realm name [EXAMPLE.TEST]:
```

Важно

Эти значения нельзя изменить после завершения установки.

Задать пароль для Directory Manager (***cn=Directory Manager***):

```
Directory Manager password:
Password (confirm):
```

Задать пароль для администратора FreeIPA (будет создана учетная запись ***admin*** с правами администратора):

```
IPA admin password:
Password (confirm):
```

Предупреждение

Пароли должны быть не менее 8 символов.

Для настройки DNS-пересылки на первый запрос, нужно ли настроить перенаправления, следует ответить утвердительно:

```
Do you want to configure DNS forwarders? [yes]: yes
```

Система предложит использовать DNS-серверы из настроек сети (если они прописаны) — если это устроит, можно оставить значение по умолчанию:

```
Following DNS servers are configured in /etc/resolv.conf: 192.168.0.1
Do you want to configure these servers as DNS forwarders? [yes]:
```

При необходимости можно добавить дополнительные серверы:

```
All detected DNS servers were added. You can enter additional addresses now:
Enter an IP address for a DNS forwarder, or press Enter to skip: 8.8.8.8
DNS forwarder 8.8.8.8 added. You may add another.
Enter an IP address for a DNS forwarder, or press Enter to skip:
DNS forwarders: 192.168.0.1, 8.8.8.8
Checking DNS forwarders, please wait ...
```

Примечание

Этот шаг необходим в том случае, если предполагается использовать внешние DNS-серверы для разрешения имён за пределами домена FreeIPA.

Для попыток найти обратные зоны можно оставить значения по умолчанию:

```
Do you want to search for missing reverse zones? [yes]:
Checking DNS domain 0.168.192.in-addr.arpa., please wait ...
Do you want to create reverse zone for IP 192.168.0.113 [yes]:
Please specify the reverse zone name [0.168.192.in-addr.arpa.]:
Checking DNS domain 0.168.192.in-addr.arpa., please wait ...
Using reverse zone(s) 0.168.192.in-addr.arpa.
```

Примечание

Управление обратными зонами через FreeIPA не обязательно — их можно настроить на внешнем DNS-сервере.

Далее можно указать имя NetBIOS:

```
NetBIOS domain name [EXAMPLE]:
```

Указать, если это необходимо, NTP-сервер или пул серверов:

```
Do you want to configure CHRONY with NTP server or pool address? [no]:
```

Перед завершением установщик выведет информацию о конфигурации и попросит ее подтвердить:

```
The IPA Master Server will be configured with:
Hostname:       ipa.example.test
IP address(es): 192.168.0.113
Domain name:    example.test
Realm name:     EXAMPLE.TEST

The CA will be configured with:
Subject DN:   CN=Certificate Authority,O=EXAMPLE.TEST
Subject base: O=EXAMPLE.TEST
Chaining:     self-signed

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       192.168.0.1, 8.8.8.8
Forward policy:   only
Reverse zone(s):  0.168.192.in-addr.arpa.

Continue to configure the system with these values? [no]: yes
```

После успешной установки отобразится сообщение:

```
==============================================================================
Setup complete

Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 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.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
The ipa-server-install command was successful
```

2.2. Установка в пакетном (неинтерактивном) режиме

Примечание

Скрипт установки **ipa-server-install** создает файл журнала **/var/log/ipaserver-install.log**. Он поможет диагностировать ошибки, если установка завершится неудачно.

Пример команды установки сервера FreeIPA в пакетном режиме:

```
# ipa-server-install -U \
  --hostname=$(hostname) \
  -r EXAMPLE.TEST \
  -n example.test \
  -p 12345678 \
  -a 12345678 \
  --setup-dns \
  --no-forwarders \
  --no-reverse
```

Обязательные параметры для пакетного режима:

- **-r REALM_NAME**, **--realm=REALM_NAME** — имя Kerberos-области для сервера FreeIPA;
- **-n DOMAIN_NAME**, **--domain=DOMAIN_NAME** — DNS-домен;
- **-p DM_PASSWORD**, **--ds-password=DM_PASSWORD** — пароль учётной записи ***cn=Directory Manager***;
- **-a ADMIN_PASSWORD**, **--admin-password=ADMIN_PASSWORD** — пароль администратора FreeIPA (***admin***);
- **-U**, **--unattended** — позволить процессу установки выбрать параметры по умолчанию, не запрашивая у пользователя информацию;
- **--hostname=HOST_NAME** — полное доменное имя (FQDN) сервера.

Предупреждение

Пароли должны содержать не менее 8 символов. Если пароль содержит специальные символы, следует заключить его в одинарные кавычки: 'P@ssw0rd!'.

Дополнительные параметры для DNS:

- **`--setup-dns`** — включить встроенный DNS-сервер;
- **`--forwarder`** или **`--no-forwarders`** — настроить или отключить DNS-пересылку;
- **`--auto-reverse`** или **`--no-reverse`** — включить или отключить автоматическое создание обратных зон;
- **`--allow-zone-overlap`** — разрешить создание зоны, даже если она уже существует. Если имя домена уже где-то используется, установка сервера FreeIPA может завершиться с ошибкой, этот параметр позволяет игнорировать эту ошибку;
- **`--no-dnssec-validation`** — отключить проверку DNSSEC.

Примечание

Отключение DNSSEC может потребоваться при интеграции с Active Directory, если внешние DNS-серверы не поддерживают DNSSEC.

Примечание

Полный список параметров, используемых для настройки сервера, см. в справочной странице **`man ipa-server-install`**.

Глава 3. Установка сервера FreeIPA в режиме CA-less

В этом разделе описывается установка сервера FreeIPA без встроенного центра сертификации (CA-less).

Конфигурация без CA требуется в тех случаях, когда по какой-либо причине нет возможности развернуть на FreeIPA встроенный PKI-сервис Dogtag.

Для установки в режиме CA-less необходимо предоставить следующие сертификаты:

- сертификат и приватный ключ сервера Directory Server:
  - **`--dirsrv-cert-file`** — путь к одному или нескольким файлам, содержащим:
    - сертификат сервера Directory Server;

- опционально — часть или полную цепочку сертификатов CA;
- приватный ключ (если используется формат PKCS#12 или PKCS#8);

- **`--dirsrv-pin`** — пароль для доступа к приватному ключу (требуется только для PKCS#12);

- сертификат и приватный ключ веб-сервера Apache:
  - **`--http-cert-file`** —путь к одному или нескольким файлам, содержащим:
    - сертификат сервера Apache;
    - опционально — часть или полную цепочку сертификатов CA;
    - приватный ключ (если используется формат PKCS#12 или PKCS#8);
  - **`--http-pin`** — пароль для доступа к приватному ключу (требуется только для PKCS#12);
- Сертификат центра сертификации (CA):
  - **`--ca-cert-file`** — путь к одному или нескольким файлам в формате PEM, содержащим сертификат(ы) CA, выдавшего сертификаты для:
    - сервера Directory Server;
    - веб-сервера Apache;
    - (опционально) Kerberos KDC (если используется PKINIT).

Примечание

Этот параметр необязателен, если полная цепочка CA уже включена в файлы, указанные через **`--dirsrv-cert-file`** и **`--http-cert-file`**.

Однако в большинстве случаев корневой сертификат CA не входит в PKCS#12-архив серверного сертификата, поэтому его необходимо передать отдельно через **`--ca-cert-file`**.

- сертификат и приватный ключ для PKINIT (опционально):
  - **`--pkinit-cert-file`** — путь к файлу сертификата;
  - **`--pkinit-pin`** — пароль для доступа к приватному ключу;;
  - **`--no-pkinit`** — отключает настройку PKINIT. Если сертификат PKINIT не предоставлен, FreeIPA настроит KDC без поддержки PKINIT.

Параметры **`--dirsrv-cert-file`** и **`--http-cert-file`** можно указывать несколько раз, чтобы передать отдельные файлы (например, сертификат, ключ и промежуточный CA).

Комбинация файлов, переданных через **`--dirsrv-cert-file`**, **`--http-cert-file`** и **`--ca-cert-file`**, должна содержать полную цепочку сертификатов от серверного сертификата до корневого CA, включительно. Без этого установка завершится ошибкой.

3.1. Подготовка сертификатов для сервера FreeIPA

Предупреждение

Перед генерацией сертификатов необходимо убедиться, что следующая команда возвращает полное доменное имя (FQDN) сервера FreeIPA:

```
# echo $HOSTNAME
ipa.example.test
```

Создать каталог для сертификатов:

```
# mkdir ~/test_ca
```

Создать файл **password.txt** с паролем к закрытому ключу (длина пароля должна быть не меньше 8 символов):

```
# echo "SECret.123" > ~/test_ca/password.txt
```

Инициализировать базу данных NSS:

```
# certutil -d ~/test_ca -N -f ~/test_ca/password.txt
```

Создать файл с энтропией:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

Выполнить экспорт переменной CERT_SERIAL:

```
# export CERT_SERIAL=1
```

Создать корневой сертификат CA:

```
# SKID="0x`openssl rand -hex 20`"
# echo $SKID
0xfa012b30b9407b0750b786ff5ed9f49ce3998622
# certutil -d ~/test_ca -S -n "CA" -s "CN=Certificate Authority" -x -t CT,,C -1
-2 -5 -m $CERT_SERIAL -v 120 -z ~/test_ca/noise.txt -f ~/test_ca/password.txt --
extSKID
```

В ответ на запросы команды дать следующие ответы (на запрос «Enter value for the key identifier fields», следует ввести вывод команды **echo $SKID**):

```
  0 - Digital Signature
  1 - Non-repudiation
  5 - Cert signing key
  9 - done
  Is this a critical extension [y/N]? y
  Is this a CA certificate [y/N]?  y
  Enter the path length constraint, enter to skip [<0 for unlimited path] 0
  Is this a critical extension [y/N]? y
  Enter value for the key identifier fields,enter to omit:
```

```
0xfa012b30b9407b0750b786ff5ed9f49ce3998622
  Is this a critical extension [y/N]? n
  5 - SSL CA
  6 - S/MIME CA
  7 - Object Signing CA
  9 - done
  Is this a critical extension [y/N]? n
```

Создать noise файл, заполненный случайными числами:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

Создать запрос на сертификат (на запрос «Enter value for the key identifier fields», следует ввести вывод команды **`echo $SKID`**):

```
# SKID="0x`openssl rand -hex 20`"
# echo $SKID
0xb17caf72b46288bcc9c887c89894dc917e06f724
#
certutil -d ~/test_ca -R -s CN=$HOSTNAME,O=IPA -o /tmp/servercert.req -k rsa -g
2048 -z ~/test_ca/noise.txt -f ~/test_ca/password.txt -a --extSKID --extSAN
dns:ipa.example.test
Generating key.  This may take a few moments...

Adding Subject Key ID extension.
Enter value for the key identifier fields,enter to omit:
0xb17caf72b46288bcc9c887c89894dc917e06f724
Is this a critical extension [y/N]?
n
```

Подписать запрос на сертификат:

```
# export CERT_SERIAL=$(($CERT_SERIAL + 1))
# certutil -d ~/test_ca -C -c "CA" -i /tmp/servercert.req -o /tmp/servercert.pem
-m $CERT_SERIAL -v 120 -f ~/test_ca/password.txt -1 -5 -8 ipa.example.test -a
```

Примечание

Опция **`-8`** указывает **`certutil`** добавить расширение ***`Subject Alternative Name (SAN)`*** в сертификат.

Это расширение должно содержать полное доменное имя (FQDN) сервера FreeIPA (например, ipa.example.test), так как современные службы (включая Apache и Directory Server) требуют, чтобы имя хоста присутствовало в SAN, а не только в поле Subject DN.

Если расширение SAN отсутствует, команда **`ipa-server-install`** завершится ошибкой:

```
The server certificate in /root/test_ca/servercert.p12 is not valid:
invalid for server ipa.example.test
```

поскольку сертификат будет считаться недействительным для указанного имени хоста.

В ответ на запросы команды дать следующие ответы:

```
  0 - Digital Signature
  2 - Key encipherment
  9 - done
  Is this a critical extension [y/N]? n
  1 - SSL Server
  9 - done
  Is this a critical extension [y/N]? n
```

Примечание

Для эксплуатации в рабочей среде рекомендуется использовать отдельные сертификаты для Directory Server и Apache.

3.2. Экспорт сертификатов в правильные форматы

Импортировать сертификат в базу NSS (на запрос команды, следует ввести пароль к закрытому ключу, указанный в файле **password.txt**):

```
# certutil -d ~/test_ca -A -i /tmp/servercert.pem -n Server-Cert -a -t ,,
Enter Password or Pin for "NSS Certificate DB":
```

Экспортировать сертификат в PKCS#12:

```
# pk12util -o ~/test_ca/servercert.p12 -n Server-Cert -d ~/test_ca -k ~/test_ca/
password.txt -w ~/test_ca/password.txt
pk12util: PKCS12 EXPORT SUCCESSFUL
```

Экспортировать сертификат CA в PEM:

```
# certutil -d ~/test_ca -L -n "CA" -a > ~/test_ca/cacert.pem
```

3.3. Установка FreeIPA в режиме CA-less

Установить пароль к закрытому ключу в значение переменной PSWD:

```
# export PSWD=$(cat ~/test_ca/password.txt)
```

Запустить установку:

```
# ipa-server-install \
    --http-cert-file ~/test_ca/servercert.p12 \
    --http-pin $PSWD \
    --dirsrv-cert-file ~/test_ca/servercert.p12 \
    --dirsrv-pin $PSWD \
    --ca-cert-file ~/test_ca/cacert.pem \
    --no-pkinit

The log file for this installation can be found in /var/log/ipaserver-install.log
==============================================================================
This program will set up the IPA Server.
Version 4.12.4
```

```
This includes:
  * Configure the NTP client (CHRONY)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure SID generation

To accept the default shown in brackets, press the Enter key.
```

На вопрос о настройке встроенного DNS-сервера следует ответить утвердительно:

```
Do you want to configure integrated DNS (BIND)? [no]: yes
```

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **Enter**.

Далее нужно указать имя узла, на котором будет установлен сервер FreeIPA, доменное имя и Kerberos-область:

```
Server host name [ipa.example.test]:
Please confirm the domain name [example.test]:
Please provide a realm name [EXAMPLE.TEST]:
```

Важно

Эти значения нельзя изменить после завершения установки.

Задать пароль для Directory Manager (***cn=Directory Manager***):

```
Directory Manager password:
Password (confirm):
```

Задать пароль для администратора FreeIPA (будет создана учетная запись ***admin*** с правами администратора):

```
IPA admin password:
Password (confirm):
```

Предупреждение

Пароли должны содержать не менее 8 символов.

Для настройки DNS-пересылки на первый запрос, нужно ли настроить перенаправления, следует ответить утвердительно:

```
Do you want to configure DNS forwarders? [yes]:
```

Система предложит использовать DNS-серверы из настроек сети (если они прописаны) — если это устроит, можно оставить значение по умолчанию:

```
Do you want to configure these servers as DNS forwarders? [yes]:
```

При необходимости можно добавить дополнительные серверы:

```
All detected DNS servers were added. You can enter additional addresses now:
Enter an IP address for a DNS forwarder, or press Enter to skip: 8.8.8.8
DNS forwarder 8.8.8.8 added. You may add another.
Enter an IP address for a DNS forwarder, or press Enter to skip:
DNS forwarders: 192.168.0.1, 8.8.8.8
Checking DNS forwarders, please wait ...
```

Примечание

Этот шаг необходим в том случае, если предполагается использовать внешние DNS-серверы для разрешения имён за пределами домена FreeIPA.

Для попыток найти обратные зоны можно оставить значения по умолчанию:

```
Do you want to search for missing reverse zones? [yes]:
Checking DNS domain 0.168.192.in-addr.arpa., please wait ...
Do you want to create reverse zone for IP 192.168.0.113 [yes]:
Please specify the reverse zone name [0.168.192.in-addr.arpa.]:
Checking DNS domain 0.168.192.in-addr.arpa., please wait ...
Using reverse zone(s) 0.168.192.in-addr.arpa.
```

Примечание

Управление обратными зонами через FreeIPA не обязательно — их можно настроить на внешнем DNS-сервере.

Далее можно указать имя NetBIOS:

```
NetBIOS domain name [EXAMPLE]:
```

Указать, если это необходимо, NTP-сервер или пул серверов:

```
Do you want to configure CHRONY with NTP server or pool address? [no]:
```

Перед завершением установщик выведет информацию о конфигурации и попросит ее подтвердить:

```
The IPA Master Server will be configured with:
Hostname:       ipa.example.test
IP address(es): 192.168.0.141
Domain name:    example.test
Realm name:     EXAMPLE.TEST

BIND DNS server will be configured to serve IPA domain with:
```

```
Forwarders:       192.168.0.1, 8.8.8.8
Forward policy:   only
Reverse zone(s):  0.168.192.in-addr.arpa.

Continue to configure the system with these values? [no]: yes
```

После успешной установки отобразится сообщение:

```
==============================================================================
Setup complete

Next steps:
        1. You must make sure these network ports are open:
                TCP Ports:
                  * 80, 443: HTTP/HTTPS
                  * 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
```

Глава 4. Завершение установки

После завершения сценария установки следует обновить записи DNS следующим образом:

- получить Kerberos-билет администратора FreeIPA:

```
# kinit admin
```

- настроить делегирование DNS из родительского домена в домен DNS FreeIPA. Например, если DNS-домен FreeIPA — ipa.example.test, добавить запись NS (Name Server) для этой зоны в родительскую зону example.test;

- добавить SRV-запись для NTP (это обеспечит автоматическую настройку времени для будущих реплик и клиентов):

```
# ipa dnsrecord-add example.test _ntp._udp \
  --srv-priority=0 \
  --srv-weight=100 \
  --srv-port=123 \
  --srv-target=ipa.example.test
```

  проверить работу NTP-сервера можно командой:

```
# ntpdate -q localhost
server 127.0.0.1, stratum 4, offset -0.000460, delay 0.02570
14 Oct 15:34:01 ntpdate[2971]: adjust time server 127.0.0.1 offset -0.000460
sec
```

Убедиться, что сервер FreeIPA работает:

```
$ kinit admin
Password for admin@EXAMPLE.TEST:
$ klist
Ticket cache: KEYRING:persistent:1000:1000
Default principal: admin@EXAMPLE.TEST

Valid starting       Expires              Service principal
11.09.2025 14:35:36  12.09.2025 13:45:01  krbtgt/EXAMPLE.TEST@EXAMPLE.TEST
```

Проверить статус подсистем:

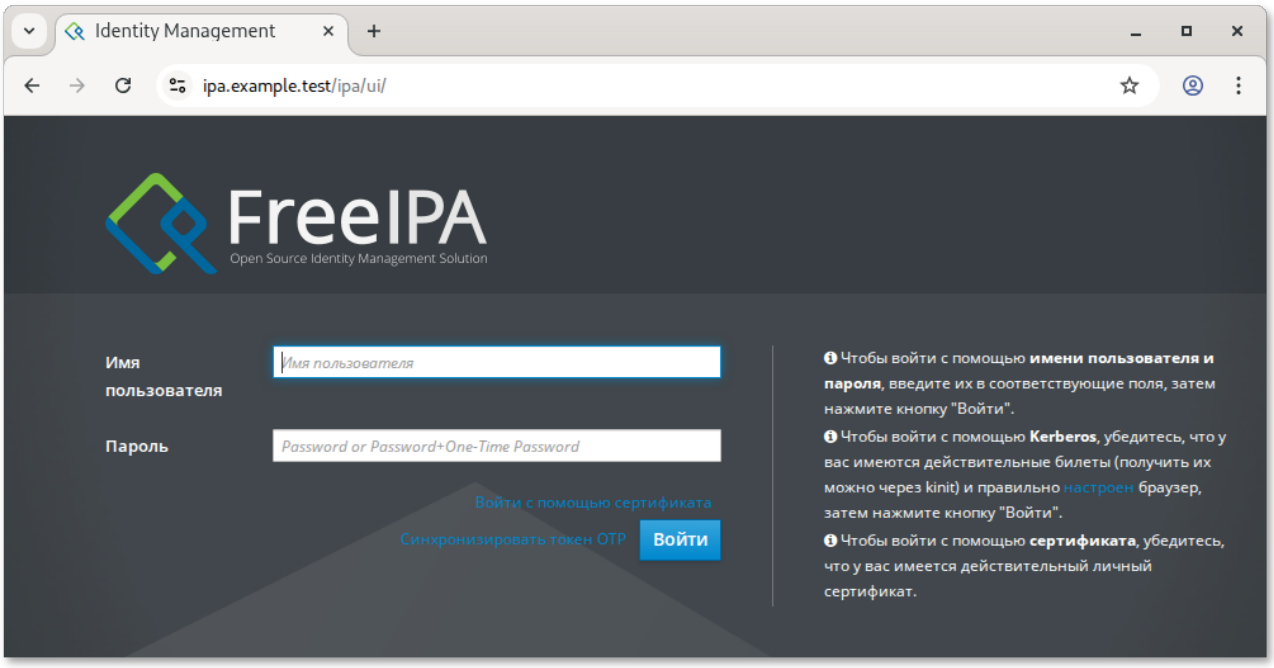
```
# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmin Service: RUNNING
named Service: RUNNING
httpd Service: RUNNING
ipa-custodia Service: RUNNING
pki-tomcatd Service: RUNNING
ipa-otpd Service: RUNNING
ipa-dnskeysyncd Service: RUNNING
ipa: INFO: The ipactl command was successful
```

Проверить наличие прямой и обратной зон можно, выполнив команды:

```
# ipa dnszone-show example.test
  Имя зоны: example.test.
  Активная зона: True
  Полномочный сервер имён: ipa.example.test.
…

# ipa dnszone-show 0.168.192.in-addr.arpa.
  Имя зоны: 0.168.192.in-addr.arpa.
  Активная зона: True
  Полномочный сервер имён: ipa.example.test.
…
```

Веб-интерфейс FreeIPA доступен по адресу https://<FQDN>/ipa/ui/, например, **https://ipa.example.test/ipa/ui/**:



Глава 5. Отладочная информация

При установке сервера FreeIPA отладочная информация записывается в следующие файлы журнала:

- **`/var/log/ipaserver-install.log`**
- **`/var/log/httpd2/error_log`**
- **`/var/log/dirsrv/slapd-INSTANCE-NAME/access`**
- **`/var/log/dirsrv/slapd-INSTANCE-NAME/errors`**

Если устанавливался центр сертификации (CA), также можно проверить:

- **`/var/log/pki/pki-ca-spawn.$TIME_OF_INSTALLATION.log`** — лог установки pkispawn;
- вывод команды **`journalctl -u pki-tomcatd@pki-tomcat`** — ошибки службы pki-tomcatd@pki-tomcat
- **`/var/log/pki/pki-tomcat/ca/debug.$DATE.log`**
- **`/var/log/pki/pki-tomcat/ca/signedAudit/ca_audit`**
- **`/var/log/pki/pki-tomcat/ca/system`**, **`/var/log/pki/pki-tomcat/ca/transactions`**,**`/var/log/`**

5.1. Удаление неудачной установки сервера FreeIPA

Если установка завершилась ошибкой, часть компонентов может быть уже настроена. Повторная попытка установки завершится с сообщением:

```
IPA server is already configured on this system.
```

Чтобы решить эту проблему следует удалить частичную конфигурацию сервера FreeIPA и повторить процесс установки.

Команда удаления конфигурации сервера FreeIPA:

```
# ipa-server-install --uninstall
```

Примечание

В большинстве случаев повторная установка возможна без переустановки ОС. Одним из требований для установки сервера FreeIPA является чистая система без каких-либо настроек.

Глава 6. Удаление сервера FreeIPA

Примечание

Перед удалением FreeIPA-сервера необходимо убедиться, что он не выполняет критических ролей в топологии.

Процедура удаления сервера FreeIPA ipabackup.example.test:

1. Если в среде FreeIPA используется встроенный DNS, следует убедиться, что ipabackup.example.test не является единственным DNS-сервером в состоянии enabled:

   ```
   # ipa server-role-find --role 'DNS server'
   ----------------------------------------
   установлено соответствие 2 ролей сервера
   ----------------------------------------
     Имя сервера: ipa.example.test
     Имя роли: DNS server
     Состояние роли: enabled

     Имя сервера: ipabackup.example.test
     Имя роли: DNS server
     Состояние роли: enabled
   --------------------------------
   Количество возвращённых записей 2
   --------------------------------
   ```

   Если ipabackup.example.test — единственный DNS-сервер в топологии, следует сначала добавить роль DNS-сервера на другой сервер FreeIPA (см. man **ipa-dns-install(1)**).

2. Если в среде используется встроенный CA:

   убедиться, что ipabackup.example.test — не единственный CA в состоянии enabled:

   ```
   # ipa server-role-find --role 'CA server'
   ----------------------------------------
   установлено соответствие 2 ролей сервера
   ----------------------------------------
     Имя сервера: ipa.example.test
   ```

```
  Имя роли: CA server
  Состояние роли: enabled

  Имя сервера: ipabackup.example.test
  Имя роли: CA server
  Состояние роли: enabled
------------------------------
Количество возвращённых записей 2
------------------------------
```

Если ipabackup.example.test — единственный CA в топологии, следует сначала добавить роль CA-сервера на другой сервер FreeIPA (см. man **ipa-ca-install(1)**).

- если в среде используются хранилища (enabled vaults), убедиться что ipabackup.example.test не является единственным включённым сервером Key Recovery Authority (KRA):

```
# ipa server-role-find --role 'KRA server'
----------------------------------------
установлено соответствие 2 ролей сервера
----------------------------------------
  Имя сервера: ipa.example.test
  Имя роли: KRA server
  Состояние роли: absent

  Имя сервера: ipabackup.example.test
  Имя роли: KRA server
  Состояние роли: absent
------------------------------
Количество возвращённых записей 2
------------------------------
```

Если ipabackup.example.test — единственный сервер KRA в топологии, следует сначала установите KRA на другой сервер FreeIPA (см. man **ipa-kra-install(1)**).

- убедиться, что ipabackup.example.test не отвечает за обновление сертификатов CA:

```
# ipa config-show | grep 'CA renewal'
```

Если вывод содержит ipabackup.example.test, необходимо переместить роль обновления на другой сервер.

- убедиться, что ipabackup.example.test не генерирует список отзыва сертификатов (CRL):

```
# ipa-crlgen-manage status
```

Если вывод команды показывает, что генерация CRL включена, следует отключить её и настроить CRL на другом сервере.

3. Подключиться к другому серверу FreeIPA в топологии:

```
$ ssh ipa_user@another_server
```

4. Авторизоваться:

```
$ kinit admin
```

5. Удалить сервер ipabackup.example.test из топологии:

```
$ ipa server-del ipabackup.example.test
```

6. Вернуться на ipabackup.example.test и выполнить локальное удаление:

```
# ipa-server-install --uninstall
This is a NON REVERSIBLE operation and will delete all data and
configuration!
It is highly recommended to take a backup of existing data and configuration
using ipa-backup utility before proceeding.

Are you sure you want to continue with the uninstall procedure? [no]: yes
Updating DNS system records
Принудительное удаление ipabackup.example.test
----------------------------------
Удалён IPA-сервер "ipabackup.example.test"
----------------------------------
Shutting down all IPA services
Unconfiguring named
Unconfiguring ipa-dnskeysyncd
Unconfiguring web server
Unconfiguring krb5kdc
Unconfiguring kadmin
Unconfiguring directory server
selinux is disabled, will not relabel ports or files.
Unconfiguring ipa-custodia
Unconfiguring ipa-otpd
Removing IPA client configuration
Removing Kerberos service principals from /etc/krb5.keytab
Disabling client Kerberos and LDAP configurations
Restoring client configuration files
Restoring (none) as NIS domain.
nscd daemon is not installed, skip configuration
nslcd daemon is not installed, skip configuration
Systemwide CA database updated.
Client uninstall complete.
The ipa-client-install command was successful
The ipa-server-install command was successful
```

7. Далее необходимо убедиться, что все NS-записи, A/AAAA-записи и SRV-записи, ссылающиеся на ipabackup.example.test, удалены из зон DNS.

Часть II. Доступ к службам FreeIPA

Содержание

Глава 7. Интерфейс командной строки FreeIPA

Администрировать FreeIPA можно в командной строке.

Примечание

Перед началом работы необходимо получить Kerberos-билет администратора:

```
$ kinit admin
```

Большинство административных задач выполняются с помощью команды **ipa**. Список доступных команд можно получить, выполнив команду:

```
$ ipa help commands
automember-add                  Добавить правило автоучастия.
automember-add-condition        Добавить условия в правило автоучастия.
automember-default-group-remove Удалить группу по умолчанию (резервную) для всех
несоответствующих записей.
automember-default-group-set    Установить группу по умолчанию (резервную) для
всех несоответствующих записей.
automember-default-group-show   Показать сведения о группах автоучастия по
умолчанию (резервных).
automember-del                  Удалить правило автоучастия.
…
vaultcontainer-show             Показать сведения о контейнере хранилищ.
```

Команды сгруппированы по типу объекта. Список всех групп (тем) можно получить командой:

```
$ ipa help topics
automember         Правило автоучастия.
automount          Автомонтирование
ca                 Управление службами сертификации
caacl              Управление правилами CA ACL.
cert               Операции с сертификатами IPA
…
vault              Хранилища
```

Для получения справки по конкретной теме используется команда:

```
$ ipa help <тема>
```

Например, справка по управлению центром сертификации:

```
$ ipa help ca
```

Справку по конкретной команде можно получить двумя способами:

```
$ ipa <команда> --help
```

или

```
$ ipa help <команда>
```

Например:

```
$ ipa user-add --help
```

Для поиска определённых типов записей в FreeIPA можно использовать команды вида **`ipa *-find`**. Список всех таких команд:

```
$ ipa help commands | grep find
```

Примеры использования:

- вывести всех пользователей:

  ```
  $ ipa user-find
  ```

- вывести все группы, в имени или описании которых содержится слово admin:

  ```
  $ ipa group-find admin
  ```

- вывести все группы, в которые входит пользователь ivanov:

  ```
  $ ipa group-find --user=ivanov
  ```

- вывести все группы, в которые не входит пользователь ivanov:

  ```
  $ ipa group-find --no-user=ivanov
  ```

Подробную информацию о конкретной записи можно получить с помощью команд вида **`ipa *-show`**. Например, сведения об узле comp01.example.test:

```
$ ipa host-show comp01.example.test
```

Глава 8. Администрирование через веб-интерфейс

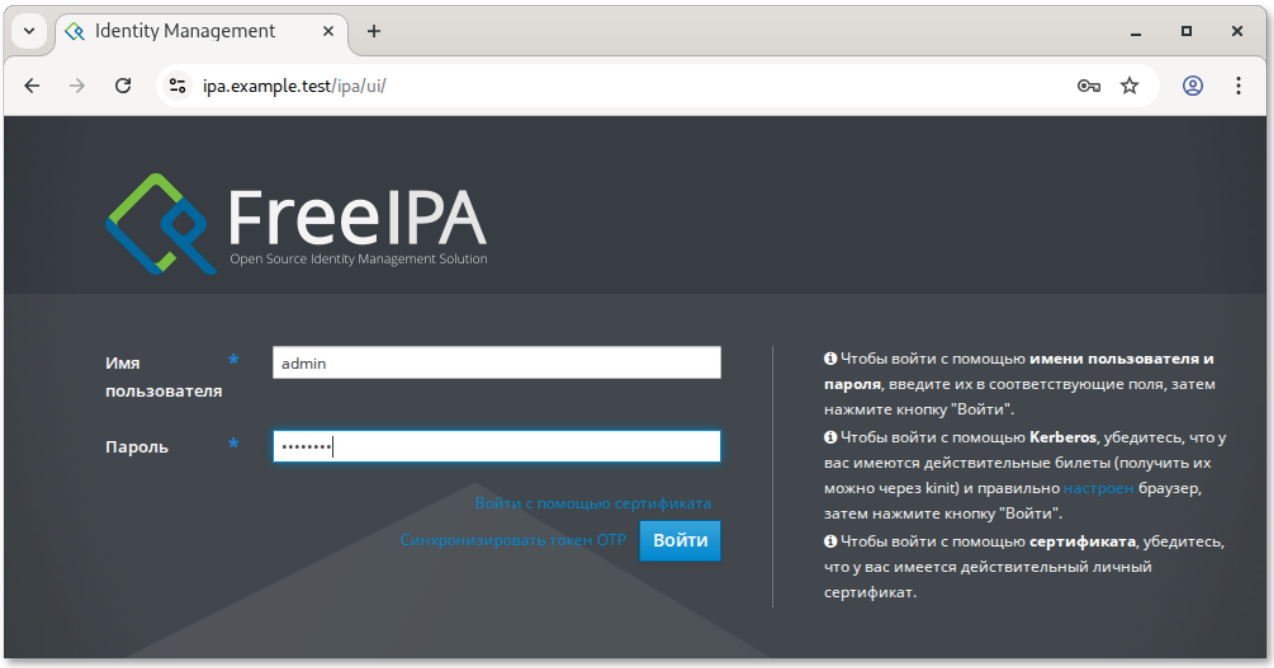
Администрировать FreeIPA можно через веб-интерфейс.

В веб-интерфейсе FreeIPA:

- администраторы имеют полный доступ ко всем настройкам сервера FreeIPA и учётных записей пользователей;
- обычные пользователи могут выполнять ограниченный набор операций в зависимости от назначенных прав. По умолчанию активные пользователи могут изменять только свою собственную учётную запись.

8.1. Доступ к веб-интерфейсу

Веб-интерфейс FreeIPA доступен по адресу https://<FQDN>/ipa/ui/, например, **`https://ipa.example.test/ipa/ui/`**:

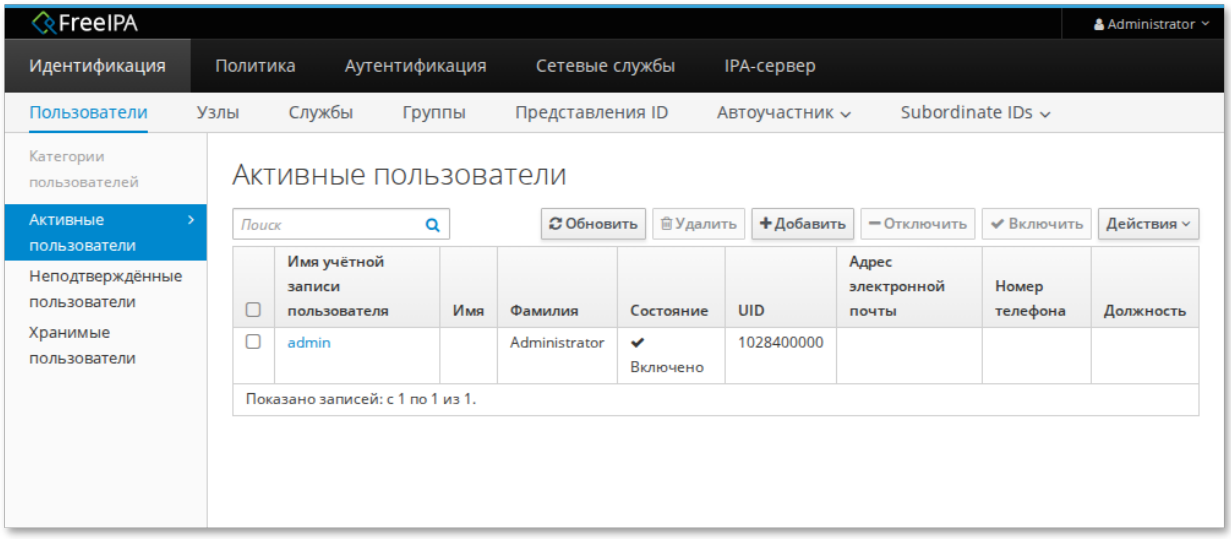


На сервере FreeIPA можно настроить следующие типы аутентификации:

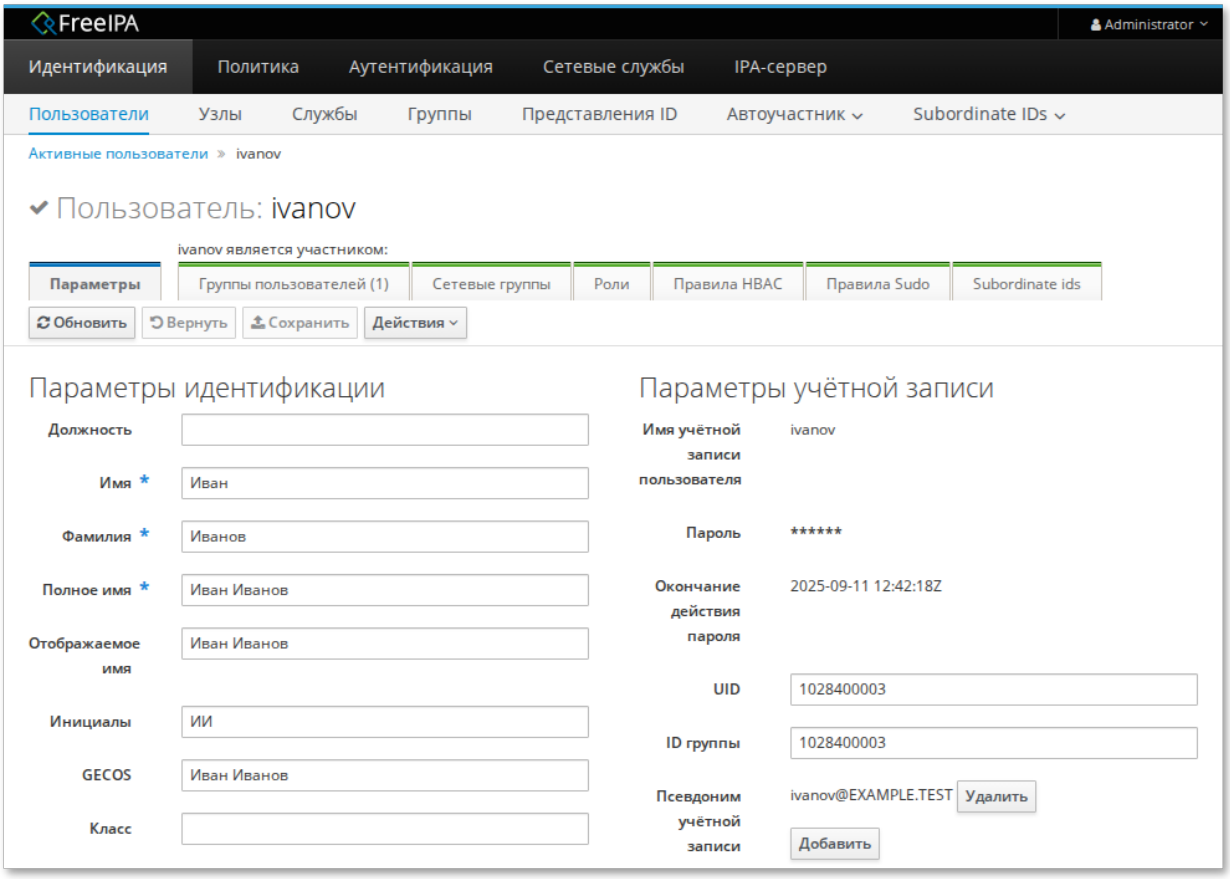
- пароль (данный тип аутентификации настроен по умолчанию);
- билет Kerberos (см. раздел Использование билета Kerberos);
- смарт-карта;
- одноразовый пароль (OTP) (см. раздел Использование одноразового пароля (OTP)). OTP можно комбинировать с паролем и аутентификацией Kerberos.

После входа:

- Администратор получает полный доступ к настройке сервера:



- Обычный пользователь может редактировать только свою учётную запись:

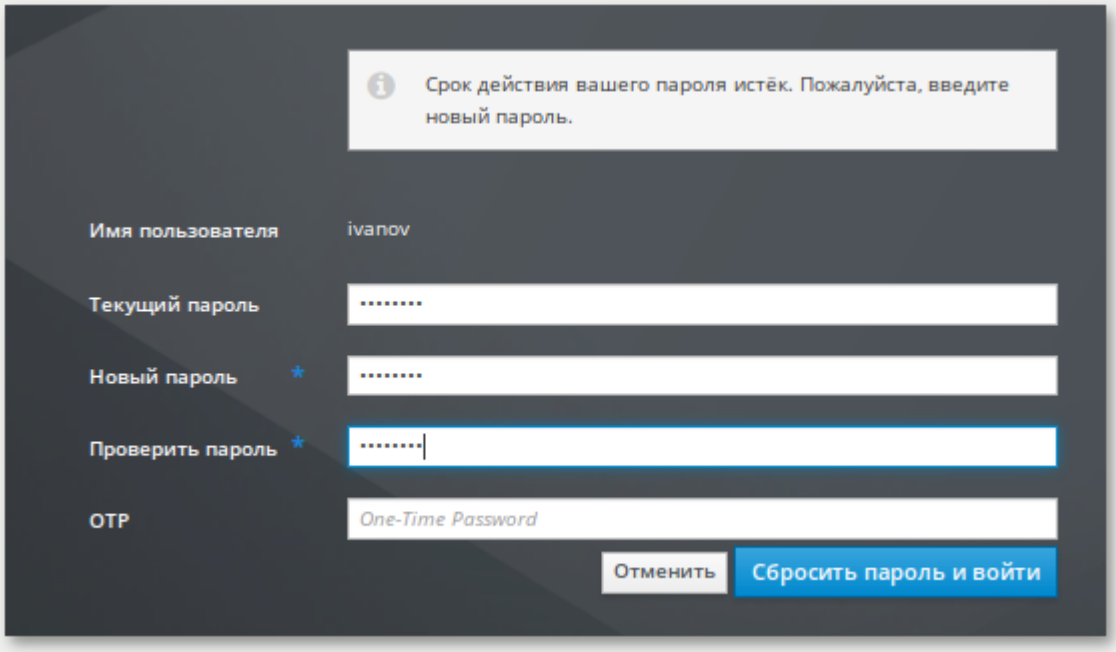


Примечание

Администратор может потребовать от пользователя сменить пароль при следующем входе в систему.

Если при входе в систему появляется диалоговое окно с сообщением **`Срок действия вашего пароля истёк. Пожалуйста, введите новый пароль`**, необходимо:

- ввести старый пароль;
- дважды указать новый пароль;
- при необходимости — ввести одноразовый пароль;
- нажать кнопку **`Сбросить пароль и войти`**:



Если для пользователя не включена аутентификация OTP, поле **OTP** следует оставить пустым.

8.2. Использование билета Kerberos

FreeIPA использует протокол Kerberos для поддержки единого входа (Single Sign-On). Это позволяет указать имя пользователя и пароль только один раз, после чего можно получить доступ ко всем интегрированным службам без повторного ввода учётных данных.

Важно

Получать билет Kerberos вручную (**kinit**) нужно только в том случае, если текущий билет отсутствует, уничтожен или истёк.

Если пользователь вошёл в систему как доменный пользователь (например, через SSSD), он автоматически получает Kerberos-билет и может использовать FreeIPA без вызова **kinit**.

По умолчанию срок действия билета Kerberos составляет 24 часа:

```
$ ipa krbtpolicy-show
  Максимальный срок жизни: 86400
  Максимальный срок для обновления: 604800
```

Изменить это значение можно как в веб-интерфейсе, так и в командной строке, например:

```
$ ipa krbtpolicy-mod --maxlife=43200 --maxrenew=86400
  Максимальный срок жизни: 43200
  Максимальный срок для обновления: 86400
```

Получение билета вручную:

- чтобы получить Kerberos-билет для текущего пользователя, следует использовать **`kinit`** без указания имени пользователя:

```
[ivanov@comp01 ~]$ kinit
Password for ivanov@EXAMPLE.TEST:
```

- чтобы получить Kerberos-билет для другого пользователя (например, администратора), следует передать имя пользователя утилите **`kinit`**:

```
[ivanov@comp01 ~]$ kinit admin
Password for admin@EXAMPLE.TEST:
```

- проверка билета:

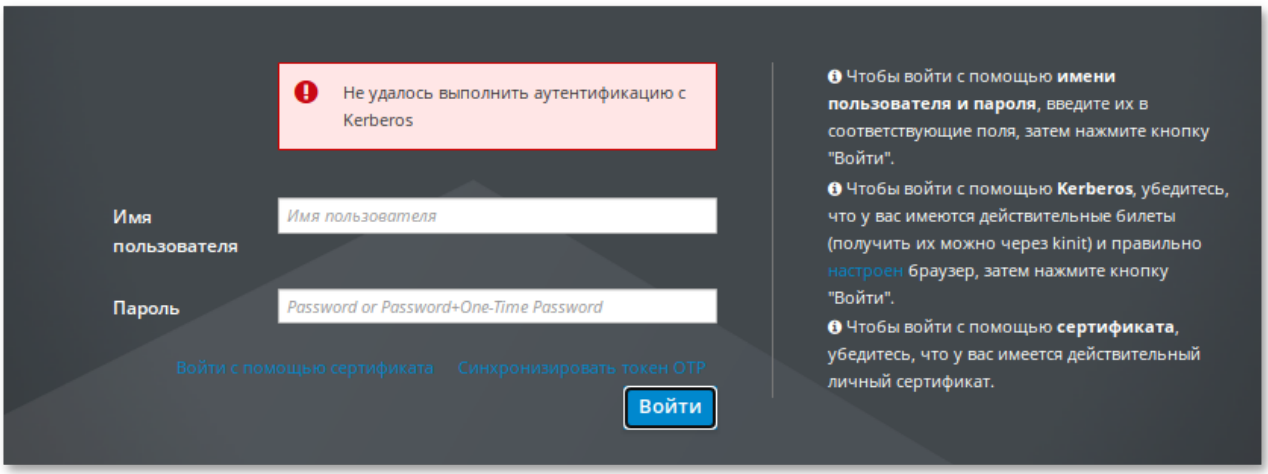
```
[ivanov@comp01 ~]$ klist
Ticket cache: KEYRING:persistent:1028400003:1028400003
Default principal: ivanov@EXAMPLE.TEST

Valid starting       Expires              Service principal
11.09.2025 19:06:30  12.09.2025 19:06:18  krbtgt/EXAMPLE.TEST@EXAMPLE.TEST
```

Если у пользователя есть действительный билет Kerberos и браузер настроен правильно, при открытии **`https://ipa.example.test`** произойдёт автоматическая аутентификация без диалогового окна и пользователь получит доступ к веб-интерфейсу.

Если билет истёк, потребуется ввести учётные данные вручную. После успешного входа последующие сеансы (в течение срока действия нового билета) будут автоматическими.

Если у пользователя есть действительный билет Kerberos, но автоматической проверки подлинности не происходит, а при нажатии кнопки **`Войти`** появляется ошибка **`Не удалось выполнить аутентификацию с Kerberos`**, необходимо убедиться, что браузер настроен для аутентификации Kerberos (см. раздел Настройка браузера для аутентификации Kerberos).



8.2.1. Настройка браузера для аутентификации Kerberos

Перед настройкой необходимо убедиться, что:

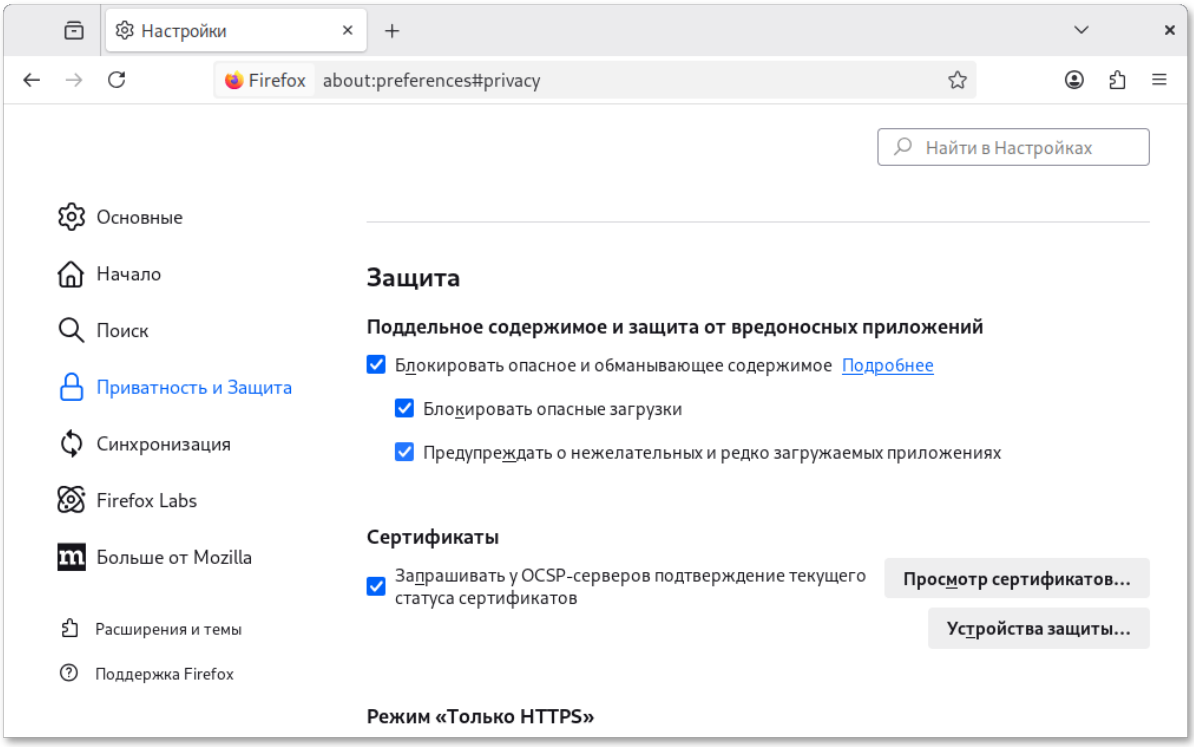
- компьютер присоединён к домену FreeIPA (см. Разворачивание клиента FreeIPA);

- доменный пользователь получает Kerberos-билет (**`kinit`** работает).

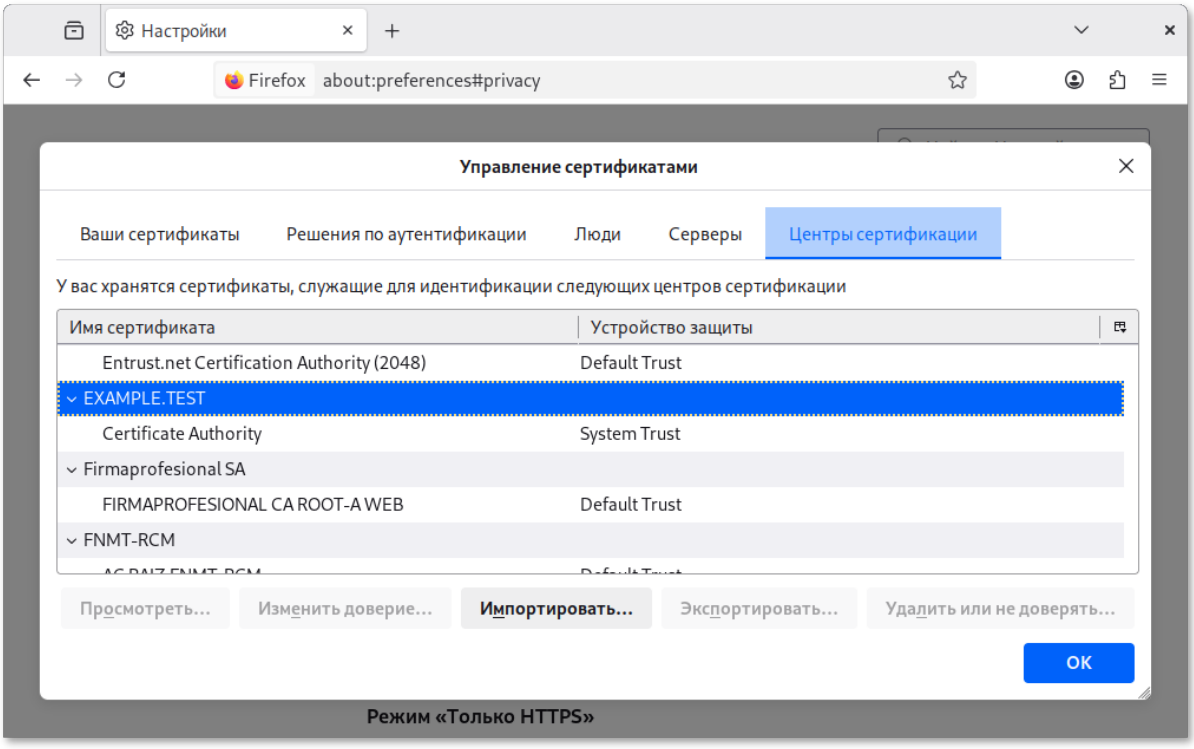
8.2.1.1. Mozilla Firefox

Порядок действий:

1. В настройках браузера на странице **Приватность и защита** (**about:preferences#privacy**) нажать кнопку **`Просмотр сертификатов…`**:



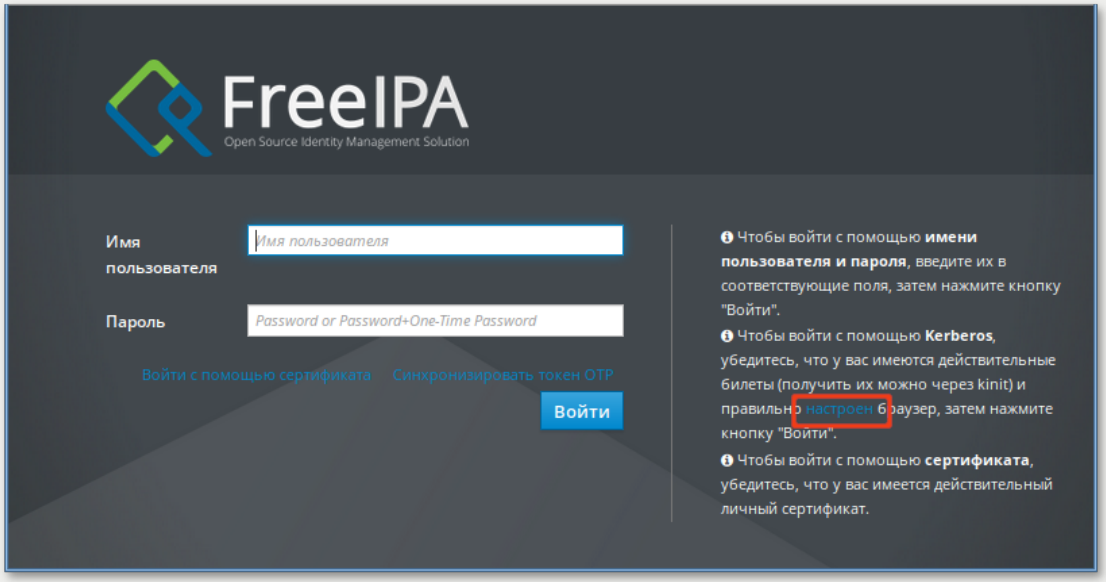
2. В открывшемся окне на вкладке **Центры сертификации** убедиться в наличии сертификата для example.test:



3. Если сертификат отсутствует, загрузить его по ссылке **`https://ipa.example.test/ipa/config/ca.crt`** и импортировать полученный сертификат, нажав кнопку **`Импортировать…`**.

Примечание

Для загрузки сертификата также можно щёлкнуть ссылку для настройки браузера на экране входа в веб-интерфейс:



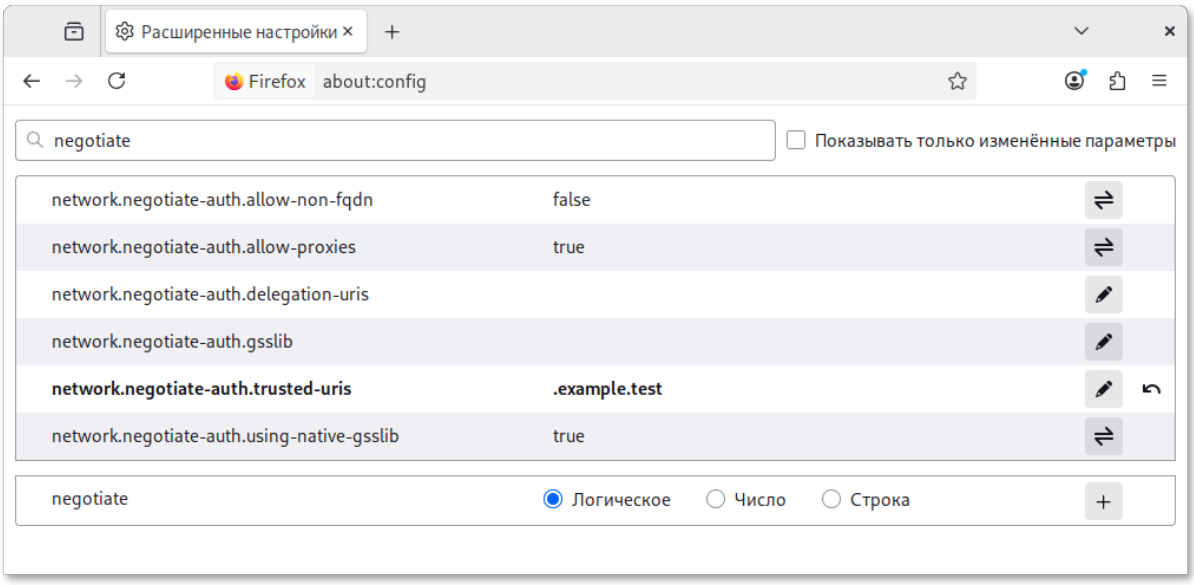
И на открывшейся странице нажать кнопку **`Import Certificate Authority certificate`**.

4. В адресной строке ввести **about:config**, чтобы отобразить список текущих параметров конфигурации (необходимо будет нажать кнопку **`Принять риск и продолжить`**).

5. В поле **`Фильтр`** ввести **negotiate**, чтобы ограничить список параметров.

6. Найти параметр ***`network.negotiate-auth.trusted-uris`***.

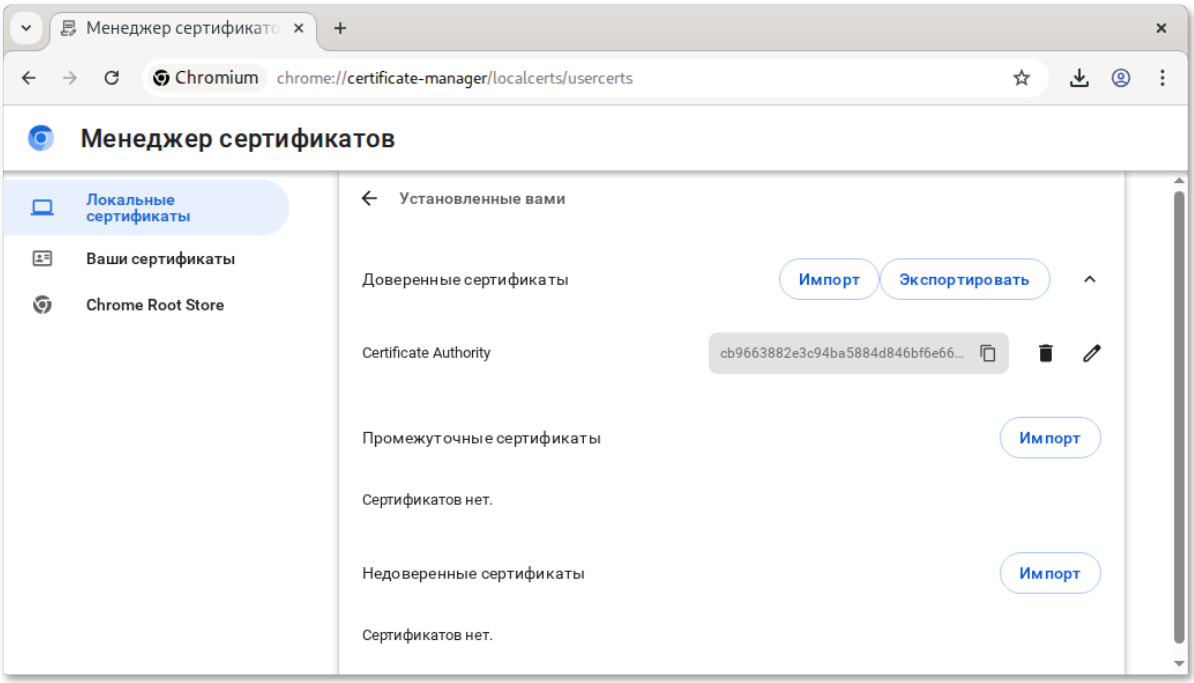
7. Указать в этом параметре имя kerberos области (realm), включая предшествующую точку (.). Если нужно добавить несколько доменов, их необходимо указать через запятую.



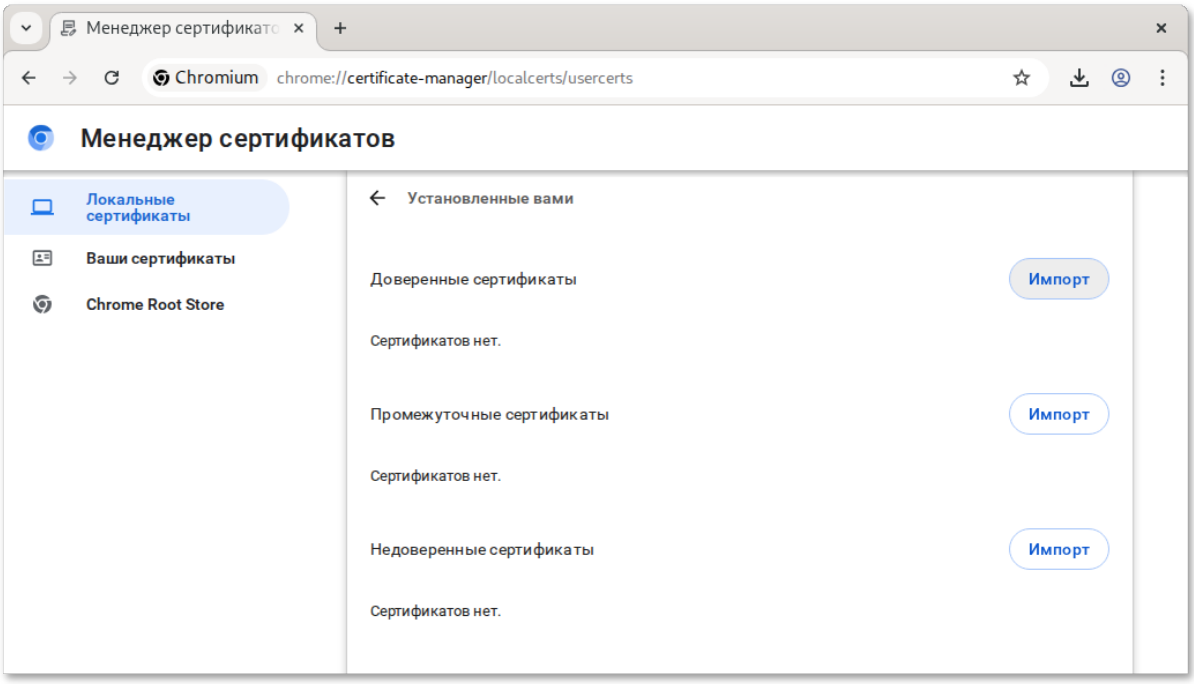
8.2.1.2. Chromium

Порядок действий:

1. В настройках браузера на странице **Конфиденциальность и безопасность** в разделе **Безопасность** открыть вкладку **Настроить сертификаты** (**chrome://certificate-manager/localcerts/usercerts**) и убедиться в наличии сертификата:

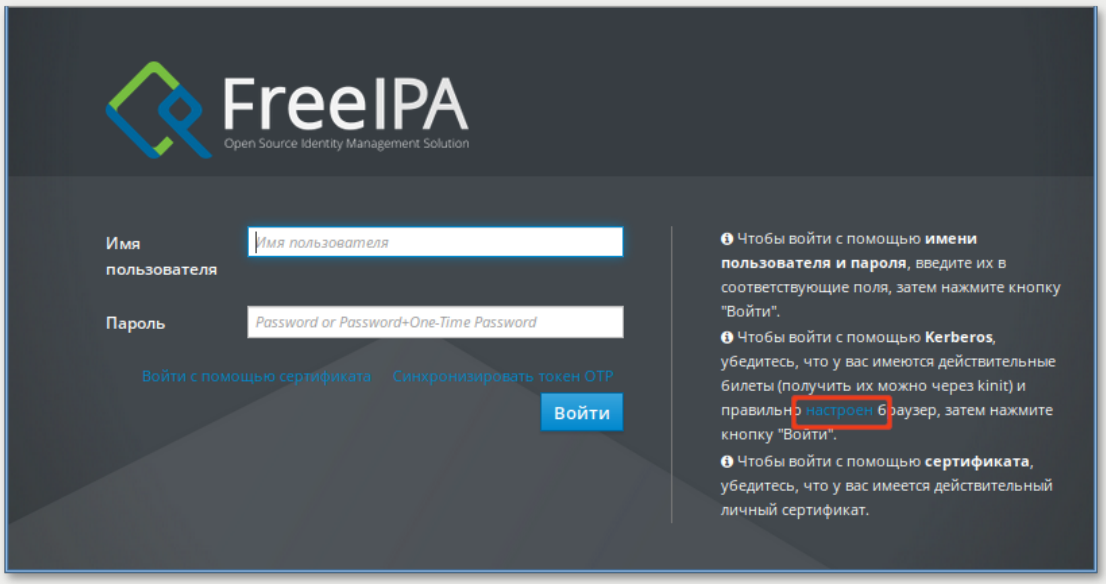


2. Если сертификат отсутствует, загрузить его по ссылке **`https://ipa.example.test/ipa/config/ca.crt`** и импортировать полученный сертификат в раздел **Доверенные сертификаты**, нажав кнопку **Импорт**:



Примечание

Для загрузки сертификата также можно щёлкнуть ссылку для настройки браузера на экране входа в веб-интерфейс:



И на открывшейся странице нажать кнопку **`Import Certificate Authority certificate`**.

3. Создать или отредактировать файл политики **`/etc/chromium/policies/managed/policies.json`**, добавив строку:

```
{
    "AuthServerAllowlist": "*.example.test"
}
```

где .example.test — имя Kerberos-области (realm).

4. Перезапустить браузер.

5. Проверить применение политик, указав в адресной строке URL: **chrome://policy**.

Примечание

Для проверки работы аутентификации без изменения настроек браузера можно запустить браузер из командной строки, выполнив команду:

```
$ chromium-browser --auth-server-allowlist="*.example.test"
```

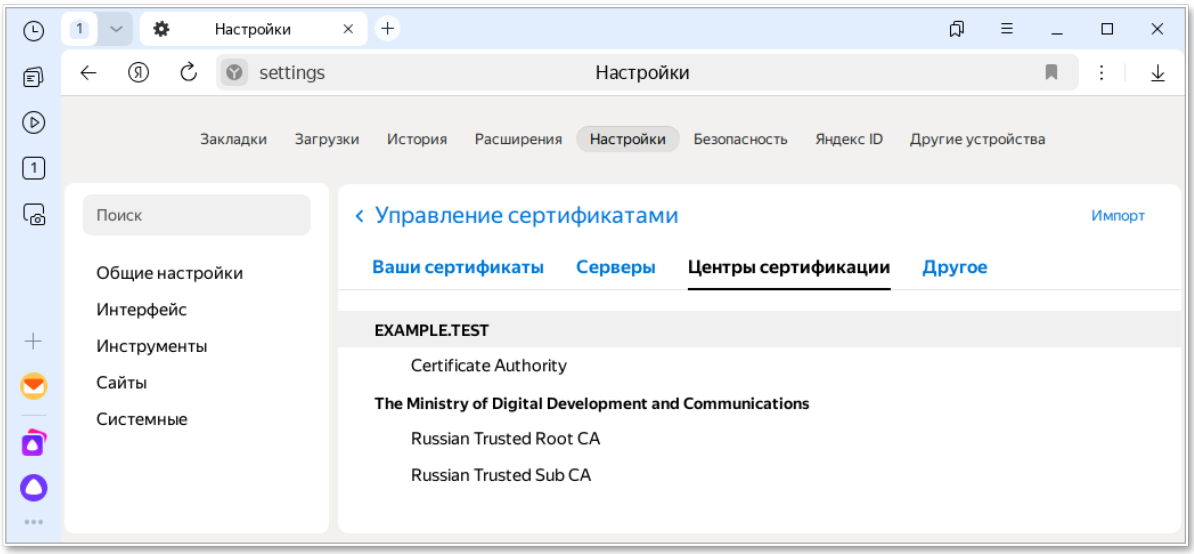
или

```
$ chromium --auth-server-allowlist="*.example.test"
```

8.2.1.3. Яндекс.Браузер

Порядок действий:

1. В настройках браузера на странице **Конфиденциальность и безопасность** (**browser://settings/certificates**) на вкладке **Центры сертификации** убедиться в наличии сертификата:



2. Если сертификат отсутствует, загрузить его по ссылке **https://ipa.example.test/ipa/config/ca.crt** и импортировать полученный сертификат, нажав кнопку **Импорт**.

3. Создать или отредактировать файл **/etc/opt/yandex/browser/policies/managed/policies.json** добавить строку:

```
{
    "AuthServerAllowlist": "*.example.test"
}
```

где .example.test — имя kerberos области (realm).

Примечание

Если каталоги **/etc/opt/yandex/browser/policies/managed/** отсутствуют, их необходимо создать заранее:

```
# mkdir -p /etc/opt/yandex/browser/policies/managed/
```

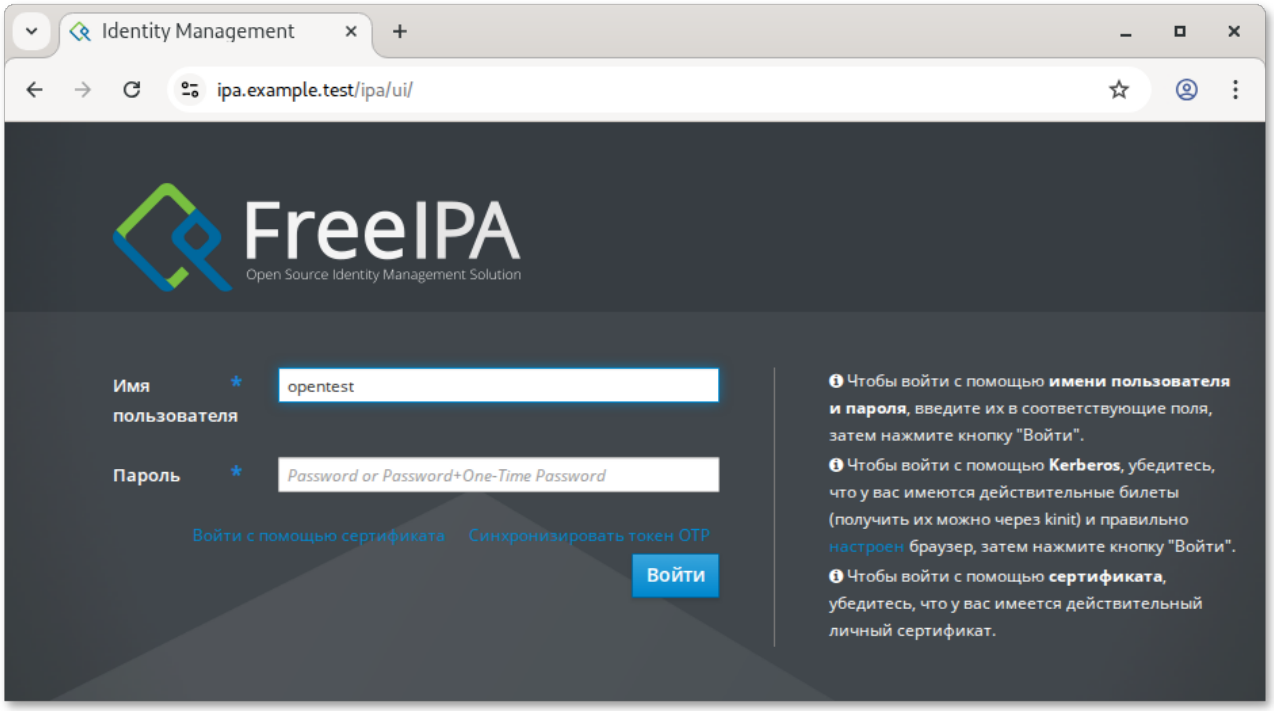
4. Перезапустить браузер.

5. Проверить применение политик, указав в адресной строке URL: **browser://policy**.

8.3. Использование одноразового пароля (OTP)

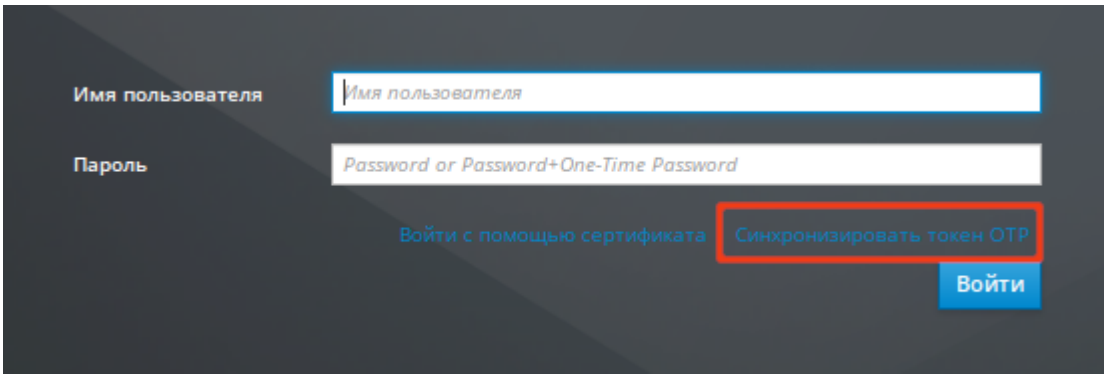
Настройка двухфакторной аутентификации описана в главе Двухфакторная аутентификация.

Если используется двухфакторная аутентификация, при аутентификации в веб-интерфейсе FreeIPA в поле **Пароль** необходимо ввести пароль и код токена (в форме <пароль><код токена> — без пробела и разделителей):

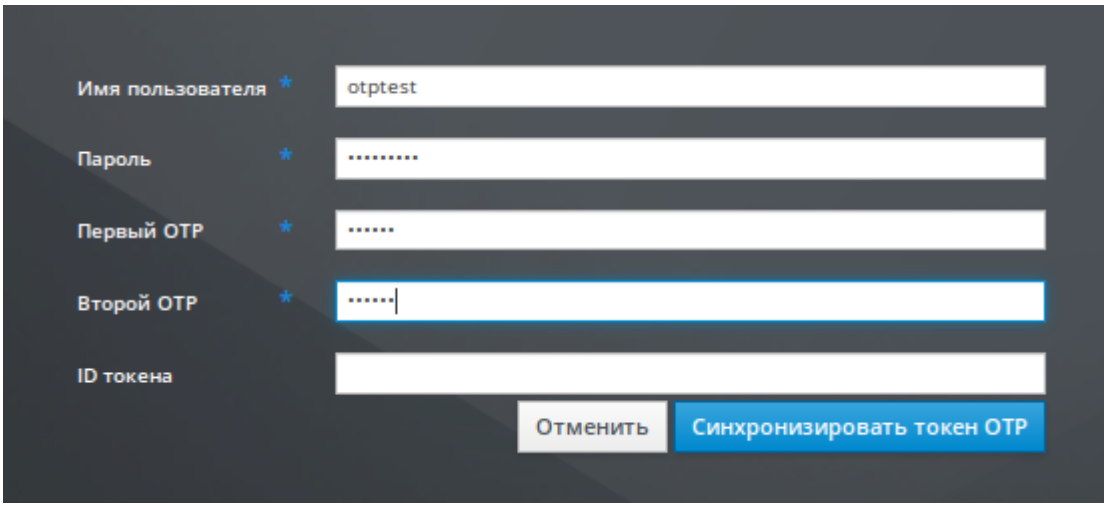


Если аутентификация не удалась, нужно синхронизировать токены OTP:

1. На экране входа нажать кнопку **Синхронизировать токен OTP**:



2. Ввести имя пользователя и его пароль.
3. Сгенерировать два последовательных OTP-кода и ввести их в поля **`Первый OTP`** и **`Второй OTP`**.
4. При необходимости указать идентификатор токена.
5. Нажать кнопку **`Синхронизировать токен OTP`**:



Глава 9. Журналирование FreeIPA

9.1. Файлы журналов сервера и клиента FreeIPA

В следующей таблице перечислены каталоги и файлы, используемые сервером и клиентом FreeIPA для ведения журналов.

Таблица 9.1. Файлы журналов сервера и клиента FreeIPA

Файл/каталог	Описание
/var/log/ipaserver-install.log	Журнал установки сервера FreeIPA
/var/log/ipareplica-install.log	Журнал установки реплики FreeIPA
/var/log/ipaclient-install.log	Журнал установки клиента FreeIPA
/var/log/sssd/	Журналы службы SSSD. Подробное логирование можно включить в файле **/etc/sssd/sssd.conf** или командой **sssctl**
/etc/logrotate.d/	Политики ротации журналов для служб DNS, SSSD, Apache, Tomcat и Kerberos
/etc/pki/pki-tomcat/logging.properties	Ссылка на конфигурацию ведения журнала центра сертификации (по умолчанию указывает на **/usr/share/pki/server/conf/logging.properties**)

9.2. Файлы журналов сервера каталогов (Directory Service)

В следующей таблице перечислены журналы, создаваемые экземпляром сервера каталогов (Directory Server) FreeIPA.

Таблица 9.2. Файлы журналов сервера каталогов (Directory Service)

Файл/каталог	Описание
/var/log/dirsrv/slapd-<REALM_NAME>	Каталог журналов экземпляра Directory Server. Основная часть записей относится к взаимодействию между серверами и репликами
/var/log/dirsrv/slapd-<REALM_NAME>/audit	Журнал аудита всех операций Directory Server (если аудит включён в конфигурации)
/var/log/dirsrv/slapd-<REALM_NAME>/access	Журнал попыток доступа к экземпляру Directory Server
/var/log/dirsrv/slapd-<REALM_NAME>/errors	Журнал ошибок при выполнении операций Directory Server

9.3. Файлы журналов веб-сервера Apache

В следующей таблице перечислены журналы, создаваемые веб-сервером Apache в составе FreeIPA.

Таблица 9.3. Файлы журналов веб-сервера Apache

Файл/каталог	Описание
/var/log/httpd2/	Каталог журналов веб-сервера Apache
/var/log/httpd2/access_log	

Файл/каталог	Описание
	Стандартный журнал доступа. Содержит записи о запросах к веб-интерфейсу и API FreeIPA. Обычно фиксируются принципал пользователя и URI (часто — RPC-эндпоинт)
/var/log/httpd2/error_log	Журнал ошибок Apache, включая ошибки компонентов FreeIPA

9.4. Файлы журналов системы сертификатов FreeIPA

В следующей таблице перечислены журналы, создаваемые подсистемой сертификатов (PKI) FreeIPA.

Таблица 9.4. Файлы журналов системы сертификатов FreeIPA

Файл/каталог	Описание
/var/log/pki/pki-ca-spawn.<time_of_installation>.log	Журнал установки центра сертификации (CA)
/var/log/pki/pki-kra-spawn.<time_of_installation>.log	Журнал установки центра восстановления ключей (KRA)
/var/log/pki/pki-tomcat/	Корневой каталог журналов PKI-сервисов
/var/log/pki/pki-tomcat/ca/	Журналы операций с сертификатами (для служб, хостов и других объектов)
/var/log/pki/pki-tomcat/kra/	Журналы, связанные с работой KRA

Сообщения об ошибках, связанные с сертификатами, также добавляются в системный журнал.

9.5. Файлы журналов Kerberos

В следующей таблице перечислены журналы, создаваемые службами Kerberos.

Таблица 9.5. Файлы журналов Kerberos

Файл/каталог	Описание
/var/log/krb5kdc.log	Журнал сервера Kerberos KDC
/var/log/kadmind.log	Журнал сервера администрирования Kerberos (kadmin)

Расположение этих файлов настраивается в конфигурационном файле **/etc/krb5.conf**.

9.6. Файлы журналов DNS

Ошибки и события, связанные с работой DNS-сервера BIND в составе FreeIPA, записываются в системный журнал.

Часть III. Разворачивание клиента FreeIPA

В этой части приводится общая информация по разворачиванию клиента FreeIPA.

Содержание

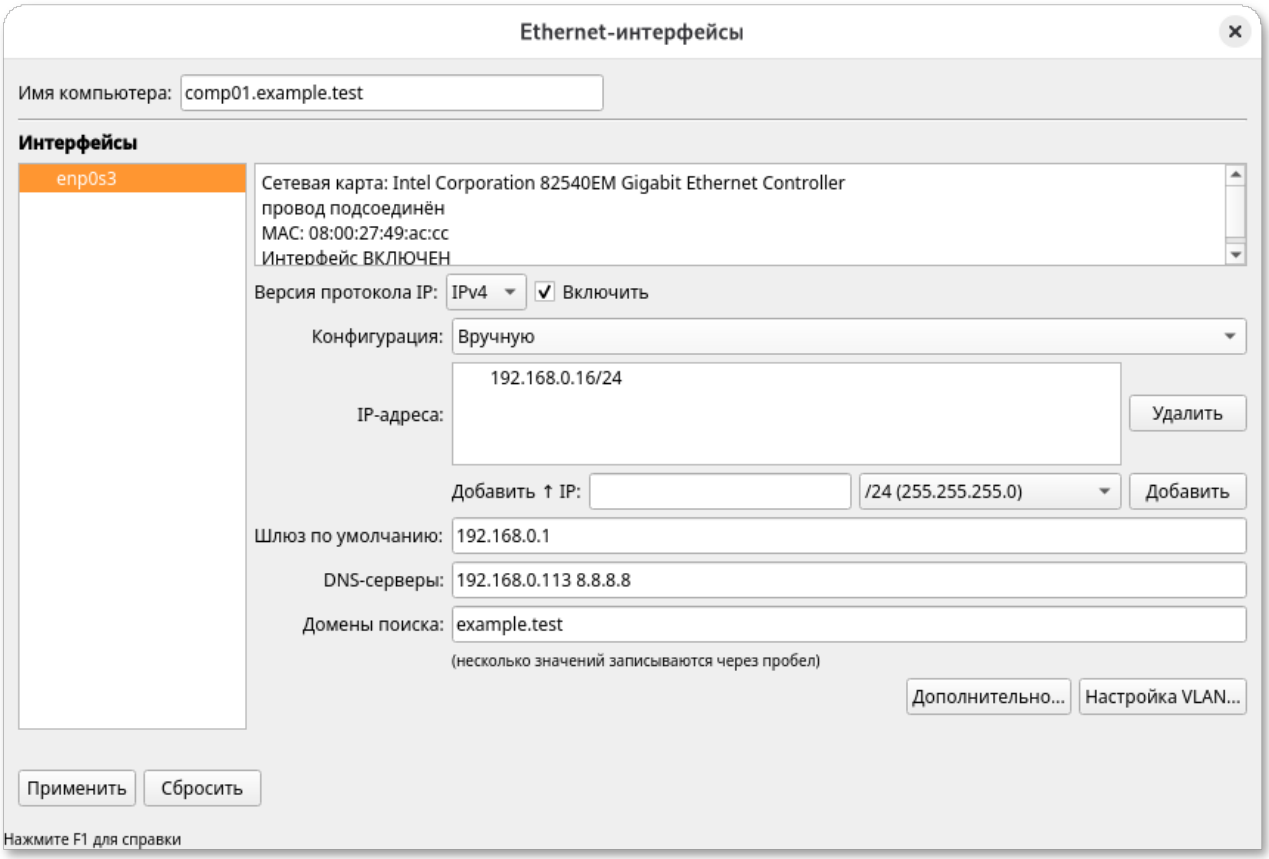
Глава 10. Подготовка системы к установке клиента FreeIPA

В этом разделе перечислены требования к клиентской системе. Перед установкой необходимо убедиться, что система соответствует этим требованиям.

10.1. Требования к DNS для клиентов FreeIPA

Клиент должен использовать DNS-сервер, настроенный на основном сервере FreeIPA. В сетевых настройках необходимо указать IP-адрес сервера FreeIPA как DNS-сервер и задать домен поиска. Эти настройки можно выполнить как в графическом интерфейсе, так и в консоли.

В Центре управления системой в разделе **Сеть** → **Ethernet интерфейсы** задать имя компьютера, указать в поле **DNS-серверы** IP-адрес сервера FreeIPA и в поле **Домены поиска** — домен для поиска:



Примечание

После изменения имени компьютера могут перестать запускаться приложения. Для решения этой проблемы необходимо перезагрузить систему.

В консоли:

- задать имя компьютера:

```
# hostnamectl set-hostname comp01.example.test
```

- указать DNS-сервер, для этого создать файл **/etc/net/ifaces/eth0/resolv.conf** со следующим содержимым:

```
# nameserver 192.168.0.113
```

где 192.168.0.113 — IP-адрес сервера FreeIPA;

- обновить конфигурацию DNS:

```
# resolvconf -u
```

В результате выполненных действий файл **/etc/resolv.conf** должен содержать строки:

```
search example.test
nameserver 192.168.0.113
```

Предупреждение

В строке *search* не должно быть домена localdomain.

Примечание

Если в результате выполненных действий IP-адрес DNS-сервера не появился в файле **/etc/resolv.conf**, необходимо перезагрузить систему.

10.2. Требования к сетевым портам

Клиенты FreeIPA взаимодействуют с серверами через ряд сетевых портов. На клиентской машине должны быть открыты исходящие соединения к этим портам.

Дополнительную информацию см. в разделе Требования к портам

10.3. Требования к IPv6

FreeIPA не требует, чтобы протокол IPv6 был включён в ядре клиентской системы.

Если в сети используется только IPv4, можно настроить SSSD на использование исключительно IPv4. Для этого нужно добавить следующую строку в секцию ***[domain/ИМЯ_ДОМЕНА]*** файла **/etc/sssd/sssd.conf**:

```
lookup_family_order = ipv4_only
```

и перезапустить службу SSSD:

```
# systemctl restart sssd
```

Глава 11. Установка пакетов

Установить пакеты:

```
# apt-get install freeipa-client zip
```

Установка пакета *freeipa-client* автоматически устанавливает все необходимые зависимости.

Примечание

Пакет *zip* требуется для корректной работы некоторых вспомогательных утилит FreeIPA.

Глава 12. Подключение к серверу

При настройке клиент регистрируется в домене FreeIPA и получает доступ к его службам.

Для установки клиента FreeIPA необходимо предоставить учётные данные, которые можно использовать для регистрации клиента. Доступны следующие методы аутентификации:

- учётные данные привилегированного пользователя (по умолчанию);
- одноразовый пароль (OTP);
- таблица ключей (keytab) из предыдущей регистрации.

12.1. Интерактивная установка

Запуск установки в интерактивном режиме:

```
# ipa-client-install --mkhomedir
```

Параметр **`--mkhomedir`** настраивает PAM на автоматическое создание домашнего каталога пользователя при первом входе, если он отсутствует.

Чтобы разрешить автоматическое обновление DNS-записей, можно добавить параметр **`--enable-dns-updates`**. Это особенно важно, если клиент использует динамический IP-адрес.

Важно

Автоматическое обновление DNS-записей возможно только если выполняется одно из следующих условий:

- сервер FreeIPA использует встроенный DNS-сервер;
- внешний DNS-сервер поддерживает обновления по GSS-TSIG.

Скрипт установки автоматически обнаружит необходимые параметры на сервере FreeIPA. Для подтверждения необходимо ввести ***`yes`***:

```
This program will set up IPA client.
Version 4.12.4

Discovery was successful!
Do you want to configure CHRONY with NTP server or pool address? [no]:
Client hostname: comp08.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
```

```
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test

Continue to configure the system with these values? [no]: yes
```

Примечание

Для установки системы с другими значениями, следует отказаться от автоматической конфигурации (ввести ***no***), а затем запустить команду **ipa-client-install** с нужными параметрами:

- **--hostname** — полное доменное имя клиента;
- **--realm** — имя Kerberos-области;
- **--domain** — DNS-домен FreeIPA;
- **--server** — FQDN сервера FreeIPA.

Далее будет запрошен пользователь с правами на регистрацию машин (например, admin):

```
User authorized to enroll computers: admin
Password for admin@EXAMPLE.TEST:
```

При успешной установке будет выведена информация:

```
Client configuration complete.
The ipa-client-install command was successful
```

12.1.1. Установка с одноразовым паролем

На сервере FreeIPA добавить будущую клиентскую систему с генерацией пароля:

```
# ipa host-add comp03.example.test --random --ip-address=192.168.0.104
----------------------------------
Добавлен узел "comp03.example.test"
----------------------------------
  Имя узла: comp03.example.test
  Случайный пароль: 3SeOaJ5GyOxbPcLmF5wpFQH
  Пароль: True
  Таблица ключей: False
  Managed by: comp03.example.test
```

Примечание

Если имя клиента разрешается через DNS, параметр **--ip-address** можно не указывать.

Примечание

Одноразовый пароль автоматически удаляется после успешной регистрации и заменяется таблицей ключей.

На клиенте запустить установку, указав сгенерированный пароль в параметре **--password**:

```
# ipa-client-install --password='3SeOaJ5GyOxbPcLmF5wpFQH' \
  --mkhomedir
```

Примечание

Так как пароль часто содержит специальные символы, следует заключить его в одинарные кавычки.

Чтобы разрешить автоматическое обновление DNS-записей, можно добавить параметр **--enable-dns-updates**:

```
# ipa-client-install --password='3SeOaJ5GyOxbPcLmF5wpFQH' \
  --mkhomedir \
  --enable-dns-updates
```

12.2. Установка в пакетном режиме

Для установки в пакетном режиме нужно указать все параметры:

1. Аутентификация:
   - **-p**, **--principal** и **-w**, **--password** — учётные данные пользователя, уполномоченного регистрировать клиентов;
   - **--random** — одноразовый пароль;
   - **-k KEYTAB**, **--keytab=KEYTAB** — таблица ключей из предыдущей регистрации.
2. Режим:
   - **--unattended**, **-U** — без интерактивных запросов.

Если SRV-записи установлены правильно в зоне DNS FreeIPA, сценарий автоматически обнаруживает все остальные требуемые значения. Если обнаружение параметров не работает, можно указать их вручную:

- **--hostname** — полное доменное имя (FQDN) для клиентского компьютера;
- **--realm** — имя Kerberos-области для сервера FreeIPA;
- **--domain** — доменное имя;
- **--server** — FQDN сервера FreeIPA.

Пример настройки клиента в пакетном режиме:

```
# ipa-client-install -U -p admin -w 12345678
```

Пример настройки клиента в пакетном режиме с дополнительными параметрами:

```
# ipa-client-install -U  \
  --password='3SeOaJ5GyOxbPcLmF5wpFQH' \
  --domain example.test \
  --server ipa.example.test \
  --realm EXAMPLE.TEST \
  --mkhomedir
```

Примечание

Полный список параметров, используемых для настройки клиента, см. в справочной странице **man ipa-client-install**.

12.3. Настройка через Центр управления системой

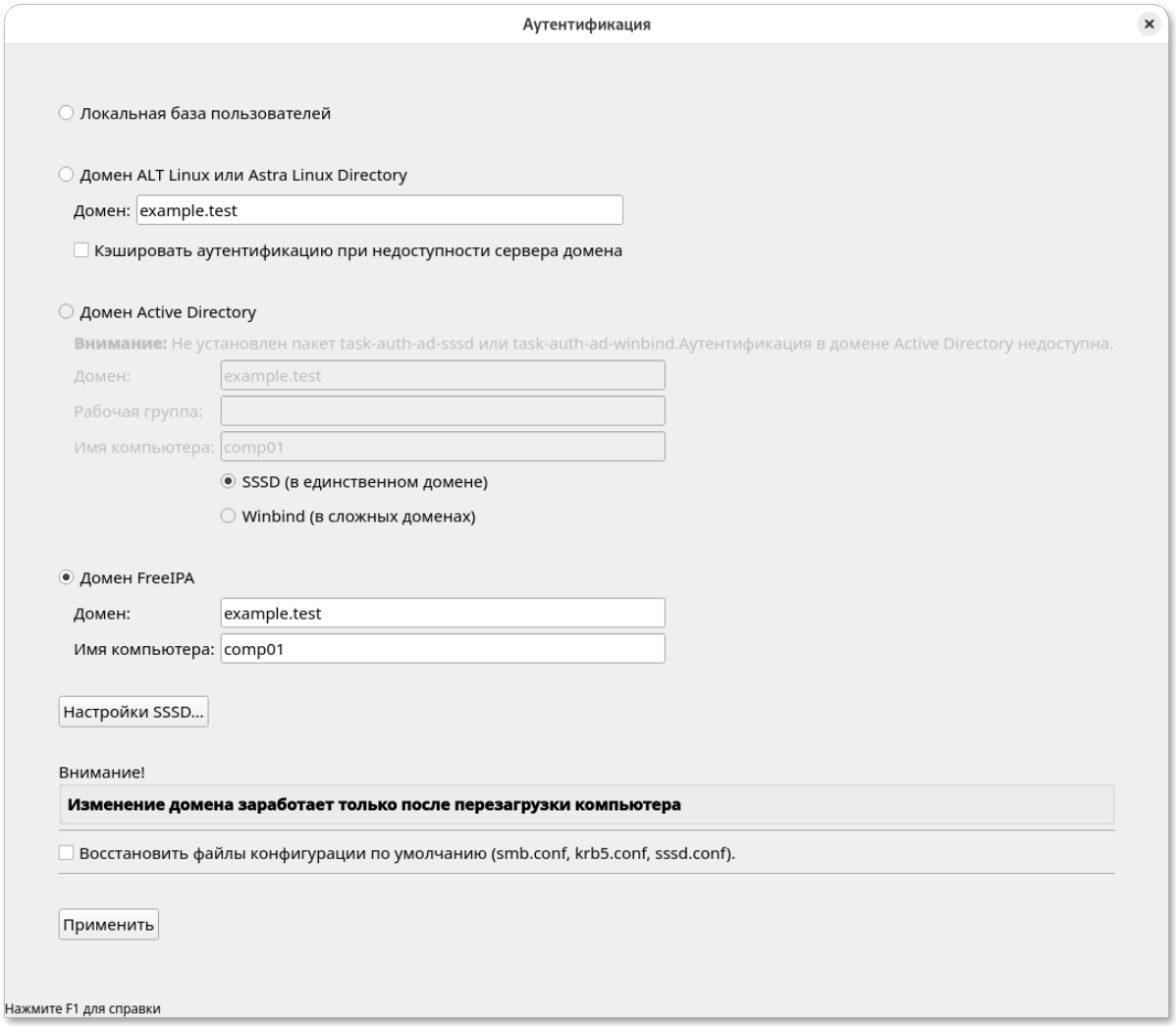
Примечание

Для возможности ввода в домен в Центр управления системой должен быть установлен пакет *task-auth-freeipa*:

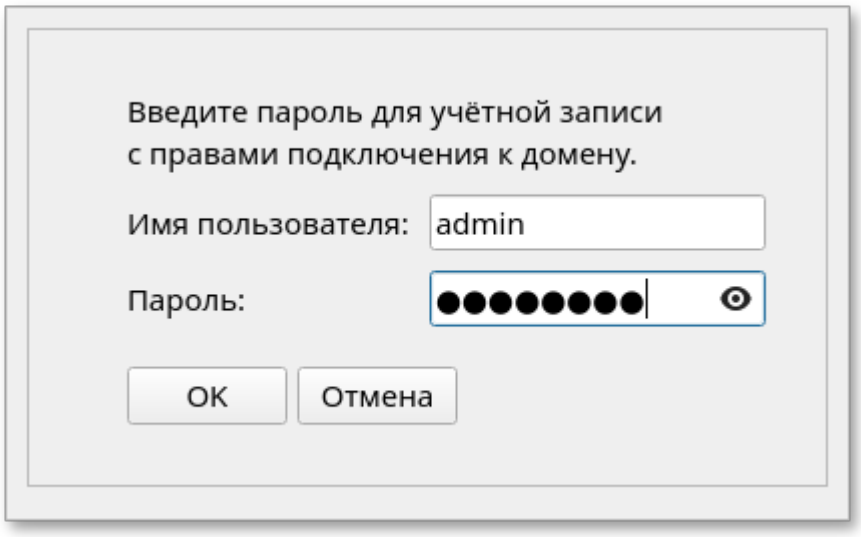
```
# apt-get install task-auth-freeipa
```

Ввод рабочей станции в домен FreeIPA в Центр управления системой:

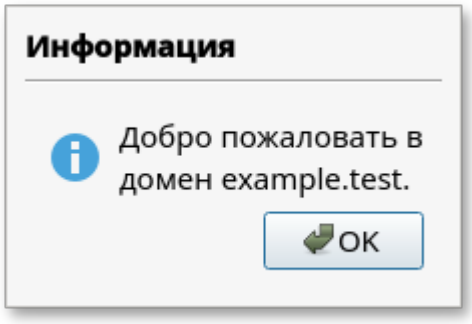
1. Перейти в раздел **Пользователи** → **Аутентификация**.
2. В окне модуля **Аутентификация** выбрать пункт **Домен FreeIPA**.
3. Заполнить поля **Домен** и **Имя компьютера**.
4. Нажать кнопку **Применить**:



5. В открывшемся окне ввести учётные данные пользователя, с правами на регистрацию машин, и нажать кнопку **OK**:



6. При успешном подключении к домену отобразится соответствующая информация:



7. Перезагрузить рабочую станцию.

Глава 13. Проверка клиента FreeIPA

Убедиться, что клиент может получать информацию о пользователях FreeIPA:

```
# id admin
uid=821600000(admin) gid=821600000(admins) группы=821600000(admins)
```

Глава 14. Отладочная информация

При установке клиента FreeIPA отладочная информация добавляется в файл **/var/log/ipaclient-install.log**.

В случае сбоя установки клиента установщик регистрирует ошибку в журнале и откатывает изменения. Причина сбоя установки может быть указана не в конце файла журнала, так как после ошибки записывается лог отката. Для устранения неполадок при неудачной установке клиента FreeIPA следует просмотреть строки с пометкой ScriptError.

Глава 15. Повторная регистрация клиента FreeIPA

В этом разделе описана процедура повторной регистрации клиента в домене FreeIPA с тем же именем хоста. Повторная регистрация может потребоваться, если клиент был утерян (например, из-за аппаратного сбоя) и утратил связь с серверами FreeIPA.

При повторной регистрации:

- создаются новые ключи SSH и новая таблица ключей (keytab);
- идентификатор узла в LDAP остаётся прежним;
- объект узла в каталоге обновляется новыми ключами, но сохраняет то же FQDN.

Примечание

Повторная регистрация возможна только если запись узла в домене активна. Если клиент был удалён (**`ipa-client-install --uninstall`**) или отключён (**`ipa host-disable`**) повторная регистрация невозможна.

Также нельзя переименовать клиент — единственный способ сменить имя: удалить узел из FreeIPA, изменить FQDN и зарегистрировать как новый клиент.

Важно

При повторной регистрации FreeIPA обновляет keytab и SSH-ключи. Если клиент использует сертификаты (например, в CA-режиме), старый сертификат отзывается, и выдаётся новый.

15.1. В интерактивном режиме

Процедура повторной регистрации клиента FreeIPA в интерактивном режиме:

1. Восстановить клиентскую систему с тем же FQDN (comp01.example.test).
2. Выполнить команду на клиентской машине:

```
# ipa-client-install --force-join
```

3. Указать учётные данные пользователя с правами на регистрацию машин (например, admin):

```
User authorized to enroll computers: admin
Password for admin@EXAMPLE.TEST:
```

Примечание

Параметр **`--force-join`** позволяет повторно зарегистрировать узел с тем же именем.

15.2. В пакетном режиме с использованием keytab

Примечание

Keytab, указанный в параметре **`--keytab`**, используется только для аутентификации при запуске регистрации. После успешной регистрации FreeIPA создаёт новый keytab для клиента.

Повторная регистрация клиента FreeIPA в пакетном режиме:

1. Создать резервную копию старого keytab (если доступен).
2. Восстановить клиентскую систему с тем же FQDN (comp01.example.test).

3. Запустить установку, с указанием местоположения файла keytab:

```
# ipa-client-install --keytab /tmp/krb5.keytab -U
This program will set up IPA client.
Version 4.12.4

Discovery was successful!
Client hostname: comp01.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test

Attempting to sync time with CHRONY
It may take a few seconds
Time successfully synchronized with IPA server
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=EXAMPLE.TEST
    Issuer:      CN=Certificate Authority,O=EXAMPLE.TEST
    Valid From:  2025-09-15 18:53:49+00:00
    Valid Until: 2045-09-15 18:53:49+00:00

Enrolled in IPA realm EXAMPLE.TEST
Created /etc/ipa/default.conf
Configured /etc/sssd/sssd.conf
Systemwide CA database updated.
Adding SSH public key from /etc/openssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/openssh/ssh_host_ed25519_key.pub
Adding SSH public key from /etc/openssh/ssh_host_rsa_key.pub
Configured passwd in /etc/nsswitch.conf
Configured group in /etc/nsswitch.conf
Configured netgroup in /etc/nsswitch.conf
Configured automount in /etc/nsswitch.conf
Configured services in /etc/nsswitch.conf
Configured sudoers in /etc/nsswitch.conf
SSSD enabled
Configured /etc/openldap/ldap.conf
Principal is not set when enrolling with OTP or PKINIT; using principal
'admin@example.test' for 'getent passwd'.
Configured /etc/openssh/ssh_config
Configured /etc/openssh/sshd_config
Configuring example.test as NIS domain.
Configured /etc/krb5.conf for IPA realm EXAMPLE.TEST
Client configuration complete.
The ipa-client-install command was successful
```

Глава 16. Удаление клиента FreeIPA

Удаление клиента включает:

- отключение от домена;
- восстановление исходной конфигурации системных служб (SSSD, NSS, Kerberos и др.);
- (опционально) удаление записей с сервера FreeIPA.

Процедура удаления клиента FreeIPA:

1. На клиенте выполнить команду:

```
# ipa-client-install --uninstall
…
Client uninstall complete.
The original nsswitch.conf configuration has been restored.
You may need to restart services or reboot the machine.
Do you want to reboot the machine? [no]: yes
The ipa-client-install command was successful
```

Примечание

Команда автоматически очищает **/etc/krb5.keytab** и откатывает конфигурацию.

2. На сервере FreeIPA удалить DNS-записи клиента:

```
# ipa dnsrecord-del example.test comp04
```

или в интерактивном режиме:

```
# ipa dnsrecord-del
Имя записи: comp04
Имя зоны: example.test
Возможность удаления определённой записи не предусмотрена.
Удалить все? Yes/No (default No): yes
-----------------------
Удалена запись "comp04"
-----------------------
```

3. На сервере FreeIPA удалить объект узла из LDAP:

```
# ipa host-del comp04.example.test
--------------------------------
Удалён узел "comp04.example.test"
--------------------------------
```

Эта операция удаляет все связанные службы и отзывает все сертификаты, выданные для этого узла (если использовался CA).

Примечание

Удаление записи узла обязательно, если в будущем планируется зарегистрировать клиент с тем же именем, но другим IP-адресом или ключами.

Часть IV. Настройка репликации

В этой части приводятся общие сведения о настройке репликации FreeIPA.

Содержание

Глава 17. Системные требования

Требования к установке реплики такие же, как и для установки сервера FreeIPA (см. раздел Системные требования к серверу FreeIPA).

Для установки реплики должны быть установлены те же пакеты, что и для сервера (см. Установка сервера FreeIPA):

```
# apt-get install freeipa-server freeipa-server-dns
```

На реплике должна быть установлена та же или более новая версия FreeIPA, что и на сервере, с которого выполняется репликация. Это обеспечивает совместимость схемы каталога, конфигурационных файлов и протоколов репликации.

Примечание

Версию FreeIPA, установленную на сервере, можно узнать с помощью одной из следующих команд:

```
$ ipa --version
VERSION: 4.12.4, API_VERSION: 2.25
```

или:

```
$ rpm -q freeipa-server
freeipa-server-4.12.4-alt1.x86_64
```

Версию FreeIPA также можно посмотреть в веб-интерфейсе, выбрав пункт **О программе** в меню пользователя (меню пользователя расположено в правом верхнем углу).

Глава 18. Способы установки реплики

Для установки реплики используется утилита **`ipa-replica-install`**. Реплики необходимо устанавливать по одной. Установка нескольких реплик одновременно не поддерживается.

Новую реплику можно развернуть двумя способами:

- на существующем клиенте FreeIPA (путём преобразования клиента в реплику);
- на машине, не зарегистрированной в домене FreeIPA.

В обоих случаях установка выполняется с помощью команды **ipa-replica-install** с соответствующими параметрами.

18.1. Авторизация при установке реплики на существующем клиенте FreeIPA

При установке реплики на существующем клиенте FreeIPA можно использовать один из двух способов авторизации.

Способ 1. Использовать учётные данные привилегированного пользователя:

- пароль администратора FreeIPA будет запрошен в интерактивном режиме после запуска утилиты **ipa-replica-install** (поведение по умолчанию);
- получить Kerberos-билет администратора FreeIPA (по умолчанию пользователь admin) непосредственно перед запуском утилиты **ipa-replica-install**:

```
$ kinit admin
```

- указать учётные данные при запуске утилиты **ipa-replica-install**:

```
# ipa-replica-install --principal admin --admin-password password
```

Способ 2. Добавить узел в группу ***ipaservers***. Если хост входит в группу узлов ***ipaservers***, он получает право на самостоятельную регистрацию в качестве реплики. В этом случае не требуется указывать учётные данные администратора при запуске **ipa-replica-install**.

Примечание

Добавление в группу узлов выполняется командой:

```
$ ipa hostgroup-add-member ipaservers --hosts replica.example.test
```

18.2. Авторизация при установке реплики на машине, не зарегистрированной в домене FreeIPA

Примечание

Перед установкой убедитесь, что система использует DNS-сервер, настроенный на основном сервере FreeIPA (см. Подготовка системы к установке клиента FreeIPA).

В сценарии установки реплики на машине, которая еще не зарегистрирована в домене FreeIPA, утилита **ipa-replica-install** сначала регистрирует машину как клиента, а затем устанавливает компоненты реплики.

Для этого сценария также можно выбрать один из двух способов авторизации.

Способ 1. Использовать учётные данные администратора, указав их непосредственно во время установки реплики:

```
# ipa-replica-install --principal admin --admin-password password
```

Способ 2. Использовать одноразовый пароль репликации. Пароль генерируется на основном сервере командой:

```
$ ipa host-add replica.example.test --random
```

Примечание

Одноразовый пароль становится недействительным сразу после успешной регистрации узла в домене.

Глава 19. Параметры утилиты ipa-replica-install

По умолчанию реплика синхронизируется с первым доступным сервером FreeIPA, обнаруженным клиентом. Чтобы указать конкретный сервер, используются параметры:

- **--server** — полное доменное имя (FQDN) сервера-источника;
- **--domain** — DNS-домен FreeIPA.

При запуске команды **ipa-replica-install** без параметров устанавливаются только основные службы. Для включения дополнительных компонентов используются параметры:

- **--setup-dns** и **--forwarder** — для установки реплики с DNS;
- **--setup-ca** — для установки локального центра сертификации (CA);
- **--dirsrv-cert-file**, **--dirsrv-pin**, **--http-cert-file** и **--http-pin** — для установки в режиме CA-less (без встроенного CA).

Полный список параметров, используемых для настройки реплики, см. в справочной странице **man ipa-replica-install**.

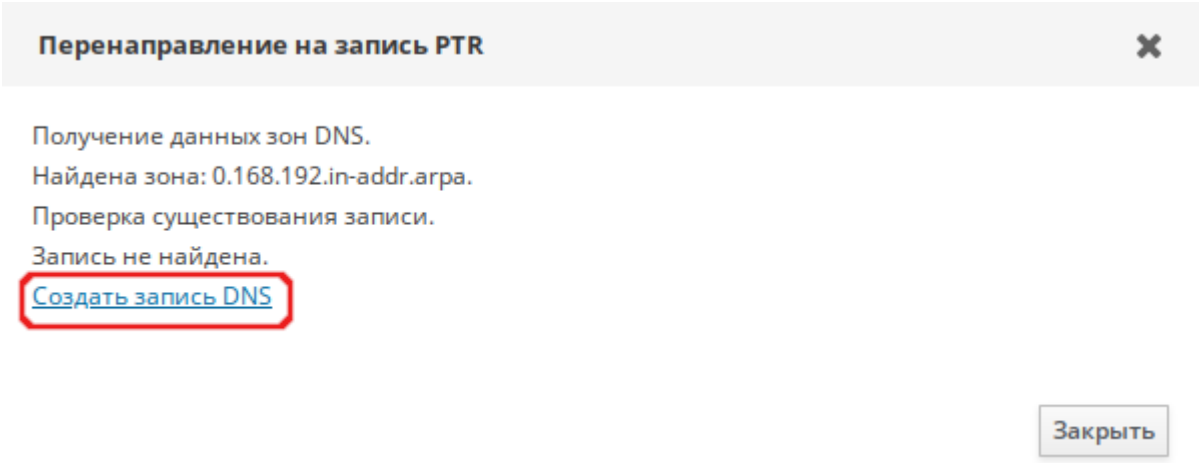
Глава 20. Установка реплики

20.1. Установка реплики на существующем клиенте FreeIPA с использованием Host Keytab

В данной процедуре клиент FreeIPA повышается до реплики с использованием собственной таблицы ключей хоста (host keytab). Этот метод не требует указания учётных данных администратора или Directory Manager, что повышает безопасность (пароли не передаются в аргументах команды).

До запуска процедуры установки реплики, необходимо создать обратный адрес для реплики на DNS-сервере основного сервера:

1. В веб-интерфейсе FreeIPA перейти в **Сетевые службы** → **DNS** → **Зоны DNS**.
2. Выбрать в таблице зону домена (например, example.test.).
3. Найти запись реплики (например, ipabackup), нажать на IP-адрес в поле A-записи, затем на ссылку **`Создать запись DNS`**:



Примечание

Обратная запись (PTR) необходима для корректной работы репликации.

Установка реплики:

1. На любом узле FreeIPA получить Kerberos-билет администратора:

```
$ kinit admin
```

2. Добавить клиентскую машину в группу узлов ***`ipaservers`***:

```
$ ipa hostgroup-add-member ipaservers --hosts ipabackup.example.test
  Группа узлов: ipaservers
  Описание: IPA server hosts
  Узлы-участники: ipa.example.test, ipabackup.example.test
-------------------------------------
Количество добавленных участников 1
-------------------------------------
```

3. На клиенте запустить установку реплики:

```
# ipa-replica-install
```

Примечание

В редких случаях служба D-Bus может мешать проверке соединений при установке реплики. При возникновении ошибок может помочь перезапуск сервиса:

```
# systemctl reload dbus
```

20.2. Установка реплики с использованием одноразового пароля

Этот метод применяется для установки реплики на машине, не зарегистрированной в домене FreeIPA. Авторизация выполняется с помощью одноразового пароля, сгенерированного на основном сервере. Пароль действителен только для одной регистрации и не требует передачи учётных данных администратора.

Установка реплики:

1. На любом узле FreeIPA получить билет Kerberos:

```
$ kinit admin
```

2. Добавить новый узел с генерацией случайного пароля (сгенерированный случайный пароль будет использоваться для последующей установки реплики):

```
$ ipa host-add hostb.example.test --random --ip-address=192.168.0.145
--------------------------------
Добавлен узел "hostb.example.test"
--------------------------------
  Имя узла: hostb.example.test
  Случайный пароль: 2AaT0Ix8itDsYugdDGoRtBt
  Пароль: True
  Таблица ключей: False
  Managed by: hostb.example.test
```

3. Добавить узел в группу ***ipaservers***:

```
$ ipa hostgroup-add-member ipaservers --hosts hostb.example.test
  Группа узлов: ipaservers
  Описание: IPA server hosts
  Узлы-участники: ipa.example.test, ipabackup.example.test,
hostb.example.test
-------------------------------------
Количество добавленных участников 1
-------------------------------------
```

4. На целевой машине запустить установку, указав сгенерированный пароль в параметре **--password**:

```
# ipa-replica-install --password '2AaT0Ix8itDsYugdDGoRtBt'
```

Примечание

Так как пароль часто содержит специальные символы, следует заключить его в одинарные кавычки.

Пример команды установки реплики с DNS и CA:

```
# ipa-replica-install  \
  --password '2AaT0Ix8itDsYugdDGoRtBt' \
  --setup-ca \
  --setup-dns \
  --forwarder 192.168.0.151 \
  --forwarder 8.8.8.8
```

Примечание

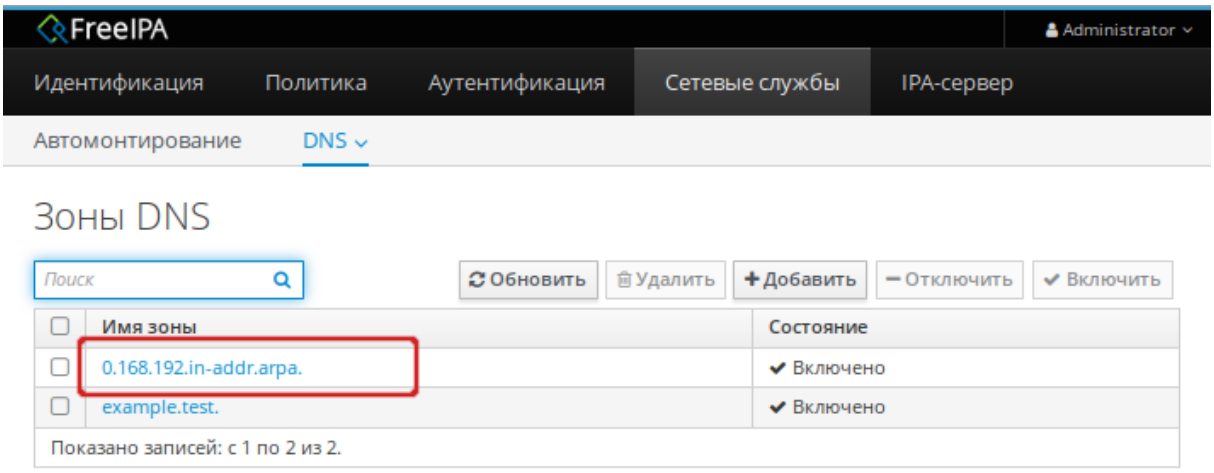
Одноразовый пароль автоматически удаляется после успешной регистрации.

20.3. Установка реплики с использованием учётных данных администратора

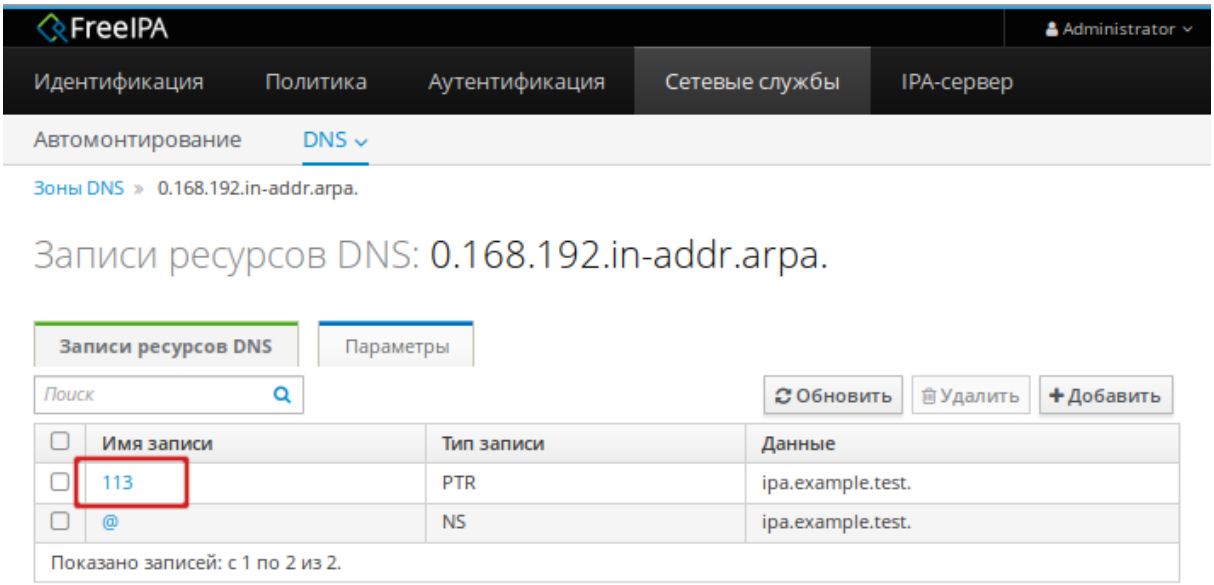
Этот метод применяется для установки реплики на машине, не зарегистрированной в домене FreeIPA. Для авторизации регистрации используются учётные данные привилегированного пользователя FreeIPA.

Подготовка DNS:

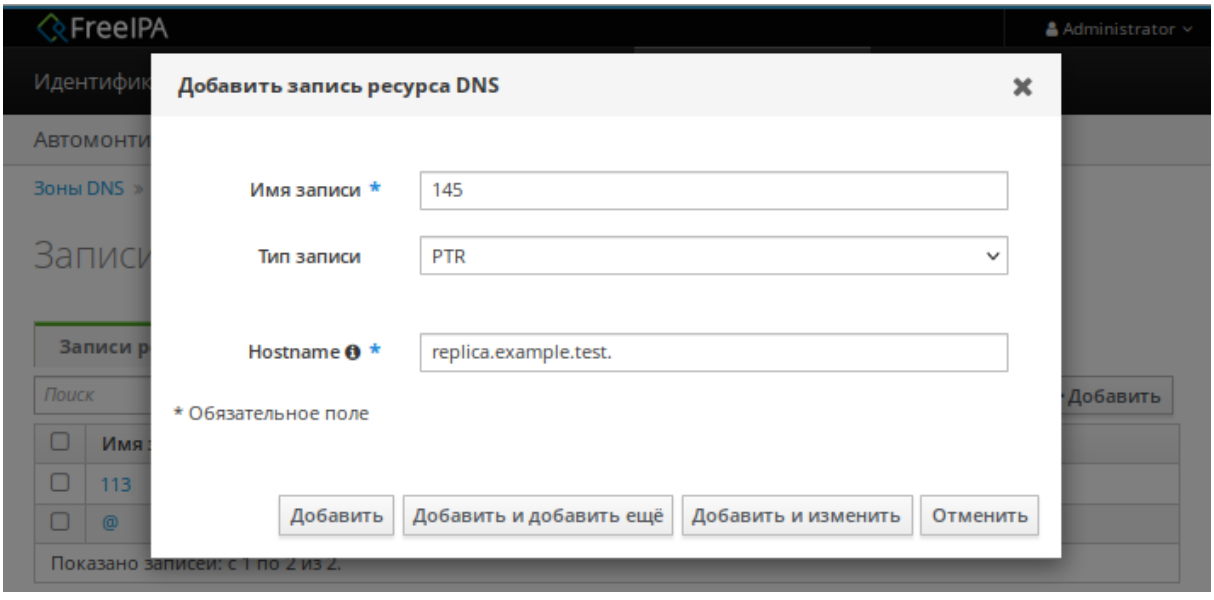
1. Необходимо убедиться, что при настройке DNS в процессе инициализации FreeIPA, была создана обратная зона DNS (**Сетевые службы** → **DNS** → **Зоны DNS**):



И в обратной зоне (0.168.192.in-addr.arpa) существует PTR-запись для основного сервера 192.168.0.113:



2. В реверсивной зоне создать PTR-запись для IP-адреса реплики (кнопка **Добавить**):



Реверсивную запись можно также создать, выполнив команду:

```
$ ipa dnsrecord-add 0.168.192.in-addr.arpa 145 --ptr-rec
'replica.example.test.'
```

Установка реплики:

```
# ipa-replica-install --principal admin --admin-password 12345678
```

Примечание

Пример запуска утилиты **ipa-replica-install** с указанием дополнительных параметров:

```
# ipa-replica-install \
  --principal admin \
  --admin-password 12345678 \
  --setup-ca \
  --setup-dns \
  --forwarder 192.168.0.151 \
  --forwarder 8.8.8.8
```

20.4. Установка реплики в режиме CA-less (без встроенного CA)

Здесь предполагается, что основной сервер был установлен в режиме CA-less (см. Установка сервера FreeIPA в режиме CA-less). В этом случае для реплики нужно предоставить сертификаты вручную.

20.4.1. Генерация сертификата для реплики

На сервере, где создавались сертификаты для сервера:

1. Создать файл энтропии:

```
# head -c20 /dev/random > ~/test_ca/noise.txt
```

2. Создать запрос на сертификат (в CN необходимо указать имя хоста будущей реплики, на запрос «Enter value for the key identifier fields», следует ввести вывод команды **echo $SKID**):

```
# SKID="0x`openssl rand -hex 20`"
# echo $SKID
0xa30f48abf89afae77e481c712d234ff0e312d44e
# certutil -d ~/test_ca -R  \
  -s CN=replica.example.test,O=IPA \
  -o /tmp/replicacert.req \
  -k rsa -g 2048 \
  -z ~/test_ca/noise.txt \
  -f ~/test_ca/password.txt \
  -a --extSKID -extSAN dns:replica.example.test
```

```
Generating key.  This may take a few moments...

Adding Subject Key ID extension.
Enter value for the key identifier fields,enter to omit:
0xa30f48abf89afae77e481c712d234ff0e312d44e
Is this a critical extension [y/N]?
n
```

3. Подписать запрос на сертификат:

```
# export CERT_SERIAL=$(($(date +%s) % 100000))
# certutil -d ~/test_ca -C -c "CA"  \
  -i /tmp/replicacert.req \
  -o /tmp/replicacert.pem \
  -m $CERT_SERIAL -v 120 \
  -f ~/test_ca/password.txt -1 -5 -8 replica.example.test -a
```

В ответ на запросы команды дать следующие ответы:

```
  0 - Digital Signature
  2 - Key encipherment
  9 - done
  Is this a critical extension [y/N]? n
  1 - SSL Server
  9 - done
  Is this a critical extension [y/N]? n
```

4. Импортировать сертификат (на запрос команды, следует ввести пароль к закрытому ключу):

```
# certutil -d ~/test_ca -A -i /tmp/replicacert.pem -n Replica-Cert -a -t ,,
Enter Password or Pin for "NSS Certificate DB":
```

5. Экспортировать сертификат в PKCS#12:

```
# pk12util -o ~/test_ca/replicacert.p12 -n Replica-Cert \
  -d ~/test_ca -k ~/test_ca/password.txt -w ~/test_ca/password.txt

pk12util: PKCS12 EXPORT SUCCESSFUL
```

6. Скопировать сертификат в формате PKCS#12 (**`replicacert.p12`**) на целевую машину (replica.example.test) в каталог **`/root/test_ca`**.

20.4.2. Установка реплики

Установка реплики:

```
# ipa-replica-install \
  --dirsrv-cert-file ~/test_ca/replicacert.p12 \
  --dirsrv-pin SECret.123 \
  --http-cert-file ~/test_ca/replicacert.p12 \
  --http-pin SECret.123 \
```

```
  --no-pkinit

…
The ipa-replica-install command was successful
```

20.5. Установка реплики с DNS и CA на машине, не зарегистрированной в домене FreeIPA

Пример установки с одноразовым паролем:

```
# ipa-replica-install --password='2AaT0Ix8itDsYugdDGoRtBt'
Configuring client side components
This program will set up IPA client.
Version 4.12.4

Discovery was successful!
Client hostname: hostb.example.test
Realm: EXAMPLE.TEST
DNS Domain: example.test
IPA Server: ipa.example.test
BaseDN: dc=example,dc=test

The ipa-client-install command was successful

The ipa-replica-install command was successful
```

Примечание

Сначала выполняется установка клиента, затем — компонентов реплики.

20.6. Проверка репликации

После создания реплики можно проверить, реплицирует ли реплика данные должным образом:

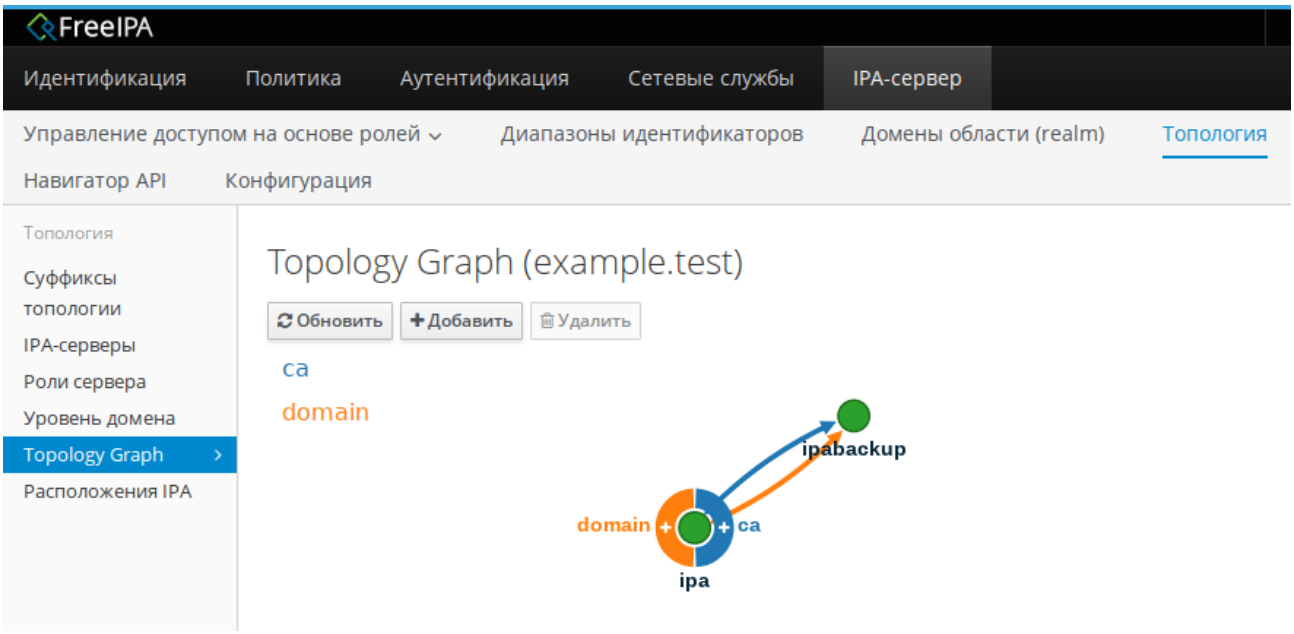
1. Создать пользователя на новой реплике:

```
$ ipa user-add test_user
```

2. Убедиться, что он отображается на других серверах:

```
$ ipa user-show test_user
```

Визуализировать топологию можно в веб-интерфейсе: **IPA-сервер** → **Топология** → **Topology Graph**.



Глава 21. Отладочная информация

При установке реплики FreeIPA отладочная информация добавляется в следующие журналы на реплике:

- **/var/log/ipareplica-install.log**
- **/var/log/ipareplica-conncheck.log**
- **/var/log/ipaclient-install.log**
- **/var/log/httpd2/error_log**
- **/var/log/dirsrv/slapd-<INSTANCE-NAME>/access**
- **/var/log/dirsrv/slapd-<INSTANCE-NAME>/errors**

При установке реплики FreeIPA отладочная информация также добавляется в журналы на основном сервере:

- **/var/log/httpd2/error_log**
- **/var/log/dirsrv/slapd-<INSTANCE-NAME>/access**
- **/var/log/dirsrv/slapd-<INSTANCE-NAME>/errors**

Глава 22. Удаление реплики

Администратор FreeIPA может удалить реплику FreeIPA из топологии.

Удаление реплики выполняется в два этапа:

1. Удаление из топологии на другом сервере:

```
$ ipa server-del replica.example.test
```

2. Локальное удаление на самой реплике:

```
# ipa-server-install --uninstall
```

Дополнительные сведения см. Удаление сервера FreeIPA

Часть V. Миграция сервера FreeIPA

В этой части приводится инструкция по миграции сервера FreeIPA.

Содержание

Глава 23. Миграция по сети

Для миграции необходимо подготовить новый сервер с теми же DNS-доменом и Kerberos-областью, что и у исходного (см. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA).

Доступны два режима миграции:

- Режим production (***prod mode***) — для переноса с действующего сервера, сохраняет существующие диапазоны UID/GID и SID;
- Режим staging (***stage mode***) — для тестовых сред; генерирует новые диапазоны UID/GID и SID.

Процедура миграции:

1. Подключиться к новому (локальному) серверу.
2. Выполнить команду:

   ```
   # ipa-migrate prod-mode ipa.example.test
   ```

   где ***ipa.example.test*** — FQDN сервера, с которого будет производиться миграция (удалённый сервер).
3. Ввести пароль Directory Manager:

   ```
   Enter the password for cn=directory manager:
   ```
4. Подтвердить необратимость операции (для продолжения необходимо ввести **yes**):

   ```
   Warning - the migration process is irreversible!  Make sure you have a
   backup of the local IPA server before doing the migration
   To proceed type "yes": yes
   ```
5. Дождаться завершения миграции:

```
Initializing ...
Connecting to local server ...
IPA to IPA migration starting ...
Migrating schema ...
Migrating configuration ...
Migrating database ... (this make take a while)
Processed 554 entries.
Running ipa-server-upgrade ... (this make take a while)
Running SIDGEN task ...
Migration complete!
…
```

6. После завершения отобразятся рекомендации:

```
Action Items (4 items)
----------------------
 - You will have to manually migrate IDM related configuration files.  Here
are some, but not all, of the configuration files to look into:
    - /etc/ipa/*
    - /etc/sssd/sssd.conf
    - /etc/named.conf
    - /etc/named/*
    - ...
 - SSSD should be restarted after a successful migration
 - The local server is in migration mode. Once all migration tasks are done
you will have to take the server out of migration mode.
 - The admin password is not migrated from the remote server. Reset it
manually if needed.
==============================================================================
===
```

Завершение миграции:

1. Сравнить файлы на локальном и удалённом сервере и, при необходимости, обновить конфигурационные файлы на новом сервере:
   - **/etc/ipa/*** — основные файлы FreeIPA;
   - **/etc/sssd/sssd.conf** — конфигурация SSSD;
   - **/etc/named.conf** — конфигурация BIND;
   - **/etc/named/*** — зоны и ключи DNS.
2. Перезапустить SSSD:

```
# systemctl restart sssd
```

3. Сбросить пароль администратора (пароль не переносится автоматически):

```
$ kinit admin
$ ipa passwd admin
```

4. Обновить сервер:

```
# ipa-server-upgrade
```

Примечание

Записи узлов сохраняются в каталоге, но клиенты могут потребовать обновления keytab или сертификатов (необходима перерегистрация командой **ipa-client-install**). Сертификаты, выданные старым CA, недействительны — их необходимо перевыпустить. Keytab, созданные вручную, следует воссоздать с помощью команды **ipa-getkeytab**

Глава 24. Офлайн-миграция

Офлайн-миграция выполняется без прямого подключения к исходному серверу — данные переносятся через файлы.

Для миграции необходимо подготовить новый сервер с теми же DNS-доменом и Kerberos-областью, что и у исходного (см. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA).

Режимы миграции — те же, что и при онлайн-миграции.

24.1. Подготовка файлов на исходном сервере

На исходном (удалённом) сервере необходимо подготовить файлы для переноса на новый сервер:

1. Создать каталог **/tmp/migration/schema**:

```
# mkdir -p /tmp/migration/schema
```

2. Скопировать основную схему:

```
# cp /etc/dirsrv/schema/*.ldif /tmp/migration/schema/
```

3. Скопировать пользовательскую схему:

```
# cp /etc/dirsrv/slapd-EXAMPLE-TEST/schema/*.ldif /tmp/migration/schema/
```

Примечание

При копировании файлов схем необходимо разрешить перезапись, если потребуется.

4. Скопировать конфигурацию:

```
# cp /etc/dirsrv/slapd-EXAMPLE-TEST/dse.ldif /tmp/migration/
```

5. Экспортировать базу данных:

```
# ldapsearch -x -H ldap://localhost -D "cn=directory manager" -W \
  -b "dc=example,dc=test" > /tmp/migration/EXAMPLE-TEST-userRoot.ldif
```

24.2. Перенос файлов на новый сервер

Примечание

Перед переносом необходимо убедиться, что файлы имеют корректные права.

Скопировать подготовленные файлы с исходного сервера, например:

```
$ scp -r user@192.168.0.59:/tmp/migration/ /tmp/
```

где 192.168.0.59 — IP-адрес исходного сервера.

24.3. Выполнение миграции

Процедура миграции:

1. Создать объединённый файл схем:

```
# cd /tmp/migration
# cat schema/*.ldif > schema.ldif
```

2. Запустить миграцию:

```
# ipa-migrate prod-mode ipa.example.test  \
  --db-ldif=/tmp/migration/EXAMPLE-TEST-userRoot.ldif \
  --schema-ldif=/tmp/migration/schema.ldif \
  --config-ldif=/tmp/migration/dse.ldif \
  -w 12345678
```

где:

- **-f**, **--db-ldif** — LDIF-файл с данными каталога. Если этот параметр не указан, будет запрошен удалённый сервер;
- **-m**, **--schema-ldif** — LDIF-файл, содержащий схему. Если этот параметр не указан, будет запрошен удалённый сервер;
- **-g**, **--config-ldif** — LDIF-файл с конфигурацией Directory Server. Если этот параметр не указан, будет запрошен удалённый сервер;
- **-w**, **--bind-pw** — пароль Directory Manager. Если пароль не указан, он будет запрошен.

3. Подтвердить необратимость операции (для продолжения необходимо ввести **yes**):

```
Warning - the migration process is irreversible!  Make sure you have a
backup of the local IPA server before doing the migration
To proceed type "yes": yes
```

4. Дождаться завершения миграции:

```
Initializing ...
Connecting to local server ...
IPA to IPA migration starting ...
Migrating schema ...
Migrating configuration ...
Migrating database ... (this make take a while)
Processed 554 entries.
Running ipa-server-upgrade ... (this make take a while)
Running SIDGEN task ...
Migration complete!
…
```

5. После завершения отобразятся рекомендации:

```
Action Items (4 items)
----------------------
 - You will have to manually migrate IDM related configuration files.  Here
are some, but not all, of the configuration files to look into:
    - /etc/ipa/*
    - /etc/sssd/sssd.conf
    - /etc/named.conf
    - /etc/named/*
    - ...
 - SSSD should be restarted after a successful migration
 - The local server is in migration mode. Once all migration tasks are done
you will have to take the server out of migration mode.
 - The admin password is not migrated from the remote server. Reset it
manually if needed.
============================================================================
===
```

Завершение миграции:

1. Сравнить файлы на локальном и удалённом сервере и, при необходимости, обновить конфигурационные файлы на новом сервере:
   - **`/etc/ipa/*`** — основные файлы FreeIPA;
   - **`/etc/sssd/sssd.conf`** — конфигурация SSSD;
   - **`/etc/named.conf`** — конфигурация BIND;
   - **`/etc/named/*`** — зоны и ключи DNS.
2. Перезапустить SSSD:

```
# systemctl restart sssd
```

3. Сбросить пароль администратора (пароль не переносится автоматически):

```
$ kinit admin
$ ipa passwd admin
```

4. Обновить сервер:

```
# ipa-server-upgrade
```

Часть VI. Интеграция с Active Directory

FreeIPA использует Samba для интеграции в с Active Directory (AD).

Примечание

Для работы Samba IPv6 должен быть включён на уровне ядра, даже если он не используется в сети.

В примере для создания доверительных отношений будут использоваться следующие данные:

- Домен FreeIPA — example.test;
- Сервер FreeIPA — ipa.example.test (192.168.0.113);
- NetBIOS-имя домена FreeIPA — EXAMPLE;
- Домен AD — test.alt;
- Контроллер домена AD — dc1.test.alt (192.168.0.132);
- NetBIOS имя домена AD — TEST.

Содержание

Глава 25. Настройка DNS

Перед настройкой доверия необходимо убедиться, что серверы FreeIPA и AD корректно разрешают доменные имена друг друга.

В этом сценарии описывается настройка DNS для разрешения доменных имен между:

- основной сервер FreeIPA, использующий встроенный сервер DNS и CA;
- контроллер домена AD.

Для настройки DNS необходимо:

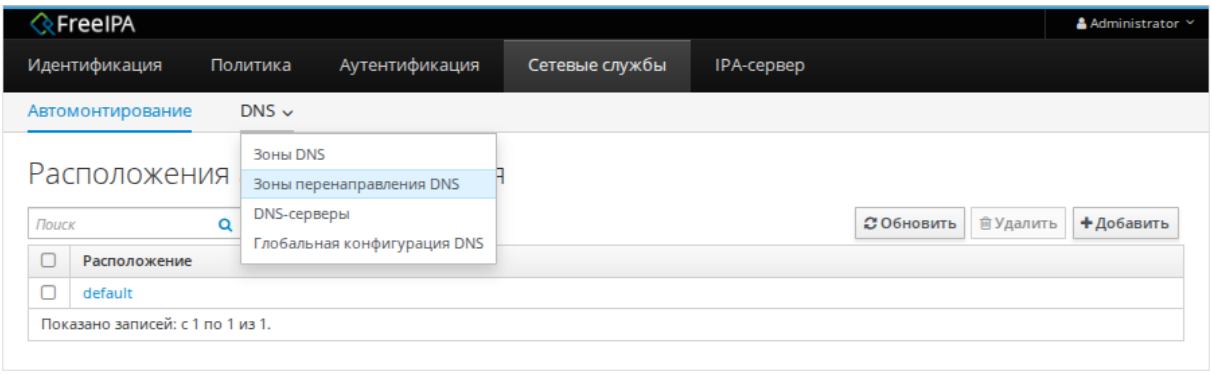
- настроить зону пересылки на сервере FreeIPA для домена AD;
- настроить условную пересылку на стороне AD для домена FreeIPA;
- проверить корректность DNS-записей.

25.1. Настройка зоны пересылки на сервере FreeIPA

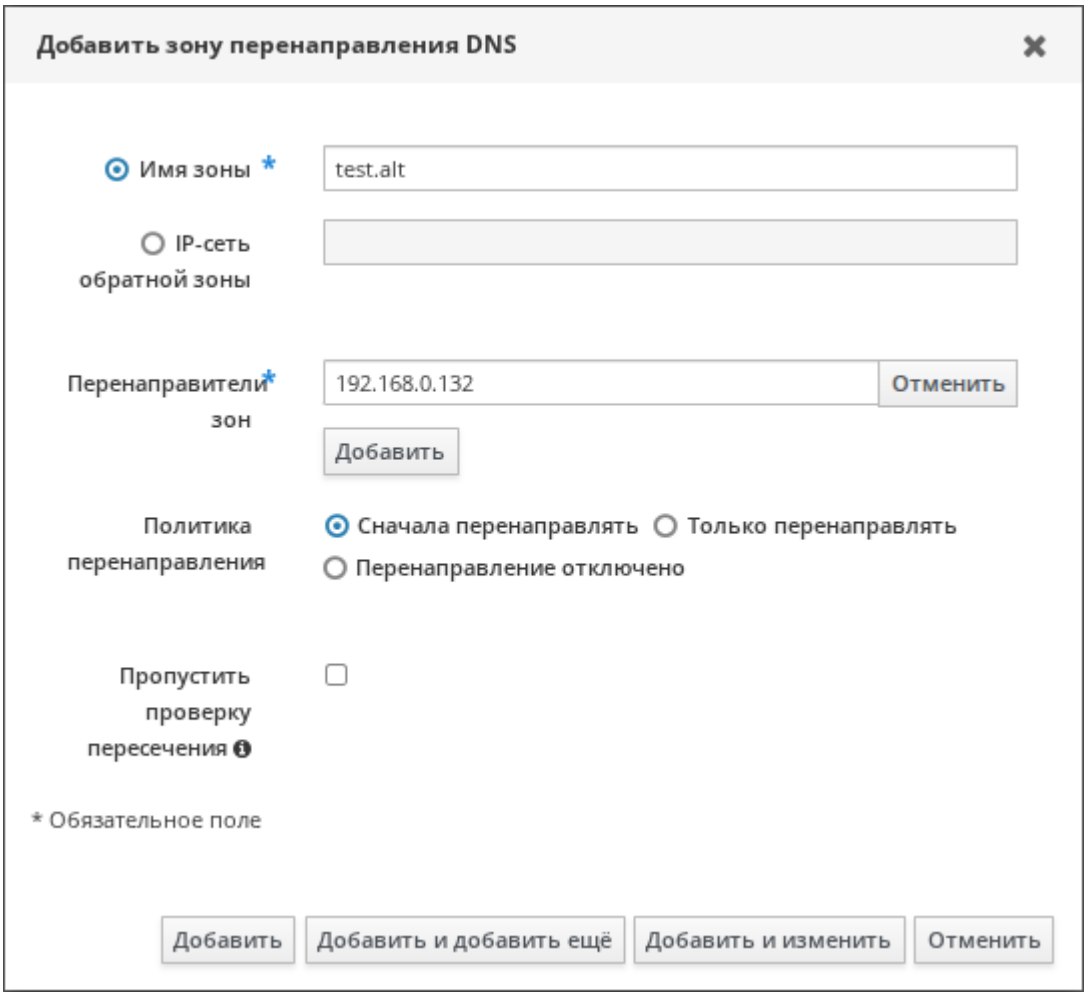
Зона пересылки позволяет направлять DNS-запросы для домена test.alt на DNS-сервер AD (192.168.0.132).

Настройка зоны пересылки в веб-интерфейсе FreeIPA:

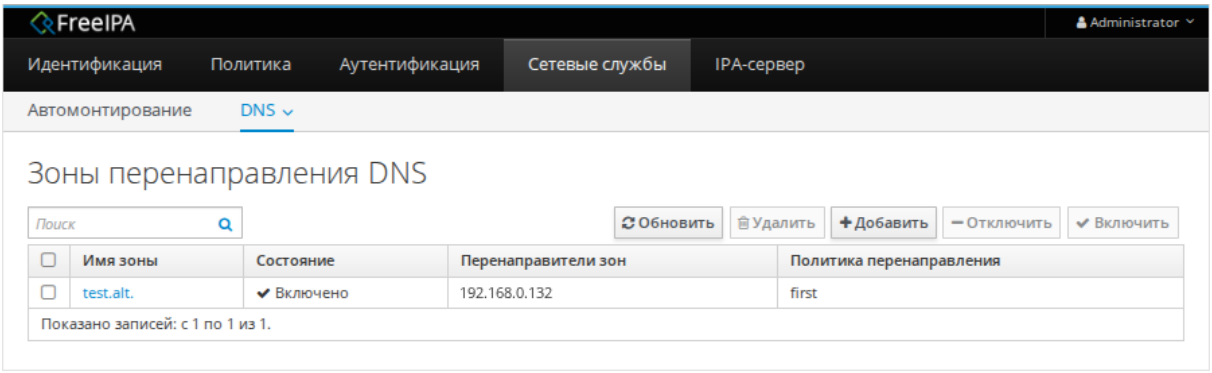
1. Перейти на вкладку **Сетевые службы**.
2. В выпадающем меню выбрать **DNS** → **Зоны перенаправления DNS**:



3. Нажать кнопку **Добавить**.
4. В диалоговом окне **Добавить зону перенаправления DNS** добавить имя зоны (test.alt).
5. В строке **Перенаправители зон** нажать кнопку **Добавить**.
6. В поле **Перенаправители зон** добавить IP-адрес сервера, для которого создается зона пересылки (192.168.0.132):



7. Нажать кнопку **Добавить**. Зона перенаправления DNS будет пересылки:



Настройка зоны пересылки в командной строке (указать IP-адрес удалённого DNS-сервера в параметре **`--forwarder`**):

```
$ kinit admin
$ ipa dnsforwardzone-add test.alt --forwarder=192.168.0.132 --forward-
policy=first
Сервер проверит DNS-перенаправитель (перенаправители).
Это может занять некоторое время; пожалуйста, подождите...
Имя зоны: test.alt.
Активная зона: TRUE
Перенаправители зон: 192.168.0.132
Политика перенаправления: first
```

Примечание

Если при добавлении зоны перенаправления появляется предупреждение об ошибке проверки DNSSEC, это означает, что удалённый DNS-сервер не поддерживает DNSSEC. Рекомендуется включить DNSSEC на удалённом DNS-сервере.

Если включить DNSSEC на стороне AD невозможно, можно отключить его на сервере FreeIPA. Для этого в файле **`/etc/bind/ipa-options-ext.conf`** следует привести параметр **`dnssec-validation`** к виду:

```
dnssec-validation no;
```

И перезапустить службу DNS:

```
# systemctl restart bind.service
```

Проверка настройки:

```
$ dig dc1.test.alt +noall +answer
dc1.test.alt.       709 IN  A   192.168.0.132
```

25.2. Настройка условной пересылки в AD

25.2.1. Samba в роли контроллера домена (BIND9_DLZ)

Если используется dns_backend BIND9_DLZ, добавить в файл **`/etc/bind/options.conf`** строки:

```
zone "example.test" {
    type forward;
    forwarders { 192.168.0.113; };
};
```

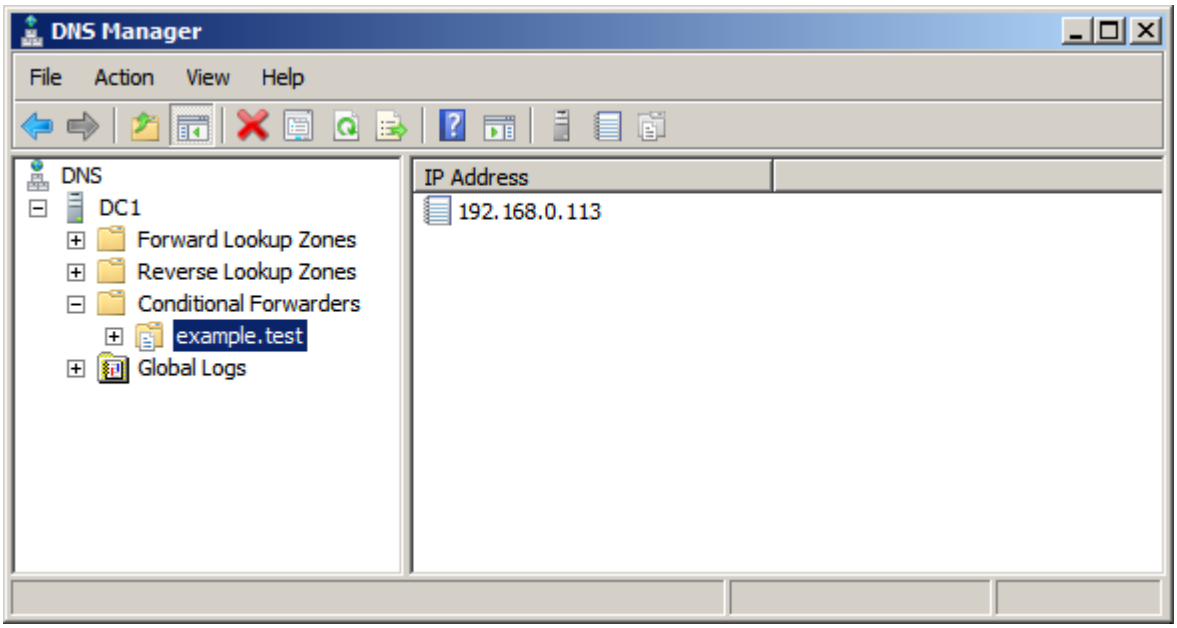
Перезапустить службу DNS:

```
# systemctl restart bind.service
```

25.2.2. Windows Server с AD

В графическом интерфейсе:

1. Открыть **`Диспетчер DNS`** (**`DNS Manager`**).
2. В разделе **`Серверы условной пересылки`** (**`Conditional Forwarders`**) добавить зону example.test с IP-адресом 192.168.0.113:



3. Сохранить настройки.

В командной строке:

```
C:\> dnscmd 127.0.0.1 /ZoneAdd example.test /Forwarder 192.168.0.113
DNS Server 127.0.0.1 created zone example.test:

Command completed successfully
```

25.3. Проверка конфигурации DNS

25.3.1. На сервере FreeIPA

Проверка SRV-записей FreeIPA:

- запись отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
$ dig +short -t SRV _kerberos._udp.example.test
0 100 88 ipa.example.test.
$ dig +short -t SRV _ldap._tcp.example.test
0 100 389 ipa.example.test.
```

В выводе команд должен быть отображен список всех серверов FreeIPA.

- запись отвечающая за имя Kerberos realm FreeIPA:

```
$ dig +short -t TXT _kerberos.example.test
"EXAMPLE.TEST"
```

- наличие записей для работы сервисов AD на DNS-сервере FreeIPA:

```
$ dig +short -t SRV _kerberos._tcp.dc._msdcs.test.alt
0 100 88 dc1.test.alt.
$ dig +short -t SRV _ldap._tcp.dc._msdcs.test.alt
0 100 389 dc1.test.alt.
```

Примечание

Если два первых шага не вернули все ожидаемые записи, следует обновить конфигурацию DNS, добавив недостающие записи:

- при использовании встроенного DNS:

```
$ ipa dns-update-system-records
```

- при внешнем DNS:

```
# ipa dns-update-system-records --dry-run --out dns_records.nsupdate
```

Затем отправить запрос на обновление DNS на DNS-сервер с помощью утилиты **nsupdate** и файла **dns_records.nsupdate**.

25.3.2. На сервере AD

Проверьте разрешение записей FreeIPA:

1. Запустить утилиту nslookup.exe для поиска служебных записей:

```
C:\> nslookup.exe
> set type=SRV
```

Ввести доменное имя для служебных записей Kerberos через UDP и LDAP через TCP:

```
> _kerberos._udp.example.test
_kerberos._udp.example.test       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 88
    svr hostname            = ipa.example.test
ipa.example.test internet address = 192.168.0.113
> _ldap._tcp.example.test
_ldap._tcp.example.test       SRV service location:
    priority                = 0
    weight                  = 100
    port                    = 389
    svr hostname            = ipa.example.test
ipa.example.test internet address = 192.168.0.113
```

2. Запись, отвечающая за имя Kerberos realm FreeIPA:

```
C:\> nslookup.exe
> set type=TXT
> _kerberos.example.test
_kerberos.example.test        text =

    "EXAMPLE.TEST"
```

Глава 26. Подготовка сервера FreeIPA к доверию

Установить пакет:

```
# apt-get install freeipa-server-trust-ad
```

Прежде чем устанавливать доверительные отношения с AD, следует подготовить домен FreeIPA с помощью утилиты **ipa-adtrust-install**. Сконфигурировать сервер FreeIPA для доверительных отношений с AD:

```
# ipa-adtrust-install
The log file for this installation can be found in /var/log/ipaserver-adtrust-
install.log
==============================================================================
This program will setup components needed to establish trust to AD domains for
the IPA Server.

This includes:
  * Configure Samba
  * Add trust related objects to IPA LDAP server

To accept the default shown in brackets, press the Enter key.

Configuring cross-realm trusts for IPA server requires password for user 'admin'.
This user is a regular system account used for IPA server administration.
```

Примечание

Записи DNS создаются автоматически, если FreeIPA был установлен с встроенным DNS-сервером. Если FreeIPA установлен без встроенного DNS-сервера, **ipa-adtrust-install** выведет список служебных записей, которые нужно вручную добавить в DNS.

Скрипт запросит пароль администратора:

```
admin password:
```

Далее скрипт сообщит, что файл **/etc/samba/smb.conf** уже существует и будет переписан:

```
WARNING: The smb.conf already exists. Running ipa-adtrust-install will break your
existing samba configuration.
Do you wish to continue? [no]: yes
```

При необходимости можно включить поддержку старых клиентов (SSSD < 1.9):

```
Do you want to enable support for trusted domains in Schema Compatibility plugin?
This will allow clients older than SSSD 1.9 and non-Linux clients to work with
trusted users.

Enable trusted domains support in slapi-nis? [no]: yes
```

Результат:

```
Done configuring CIFS.
==============================================================================
Setup complete

You must make sure these network ports are open:
    TCP Ports:
      * 135: epmap
      * 138: netbios-dgm
      * 139: netbios-ssn
      * 445: microsoft-ds
      * 1024..1300: epmap listener range
      * 3268: msft-gc
    UDP Ports:
      * 138: netbios-dgm
      * 139: netbios-ssn
      * 389: (C)LDAP
      * 445: microsoft-ds

See the ipa-adtrust-install(1) man page for more details
```

После завершения необходимо перезапустить службы:

```
# ipactl restart
Restarting Directory Service
Restarting krb5kdc Service
Restarting kadmin Service
Restarting named Service
Restarting httpd Service
Restarting ipa-custodia Service
Restarting pki-tomcatd Service
Restarting smb Service
Restarting winbind Service
Restarting ipa-otpd Service
Restarting ipa-dnskeysyncd Service
ipa: INFO: The ipactl command was successful
```

Можно воспользоваться утилитой **`smbclient`**, чтобы убедиться, что Samba отвечает на аутентификацию Kerberos со стороны FreeIPA:

```
# smbclient -L ipa.example.test --use-kerberos=yes
lpcfg_do_global_parameter: WARNING: The "domain logons" option is deprecated

    Sharename       Type      Comment
    ---------       ----      -------
    IPC$            IPC       IPC Service (Samba 4.21.7-alt4)
SMB1 disabled -- no workgroup available
```

Глава 27. Настройка доверия

Сервер FreeIPA поддерживает внешние доверительные отношения с доменами Active Directory.

Доступны следующие типы доверия:

- Одностороннее доверие (по умолчанию) — пользователи и группы из AD могут получать доступ к ресурсам FreeIPA, но не наоборот. FreeIPA доверяет AD, но AD не доверяет FreeIPA.
- Двустороннее доверие (**`--two-way=true`**) — AD также доверяет FreeIPA. Однако пользователи FreeIPA не могут входить в системы Windows, и функционально это не расширяет возможности по сравнению с односторонним доверием из-за включённой по умолчанию фильтрации SID.
- Внешнее доверие (**`--external=true`**) — используется для установления доверия с доменом внутри леса AD, если невозможно настроить доверие с корневым доменом. Рекомендуется только при административных ограничениях.

27.1. В командной строке

Добавление двустороннего внешнего доверия:

```
$ kinit admin
$ ipa trust-add --type=ad test.alt --admin Administrator --password --two-
way=true
Пароль администратора домена Active Directory:
----------------------------------------------------------
Повторно установлено отношение доверия с доменом "test.alt"
----------------------------------------------------------
  Имя области (realm): test.alt
  Имя домена NetBIOS: TEST
  Идентификатор безопасности домена: S-1-5-21-350745825-2392200591-20856689
  Направление отношения доверия: Двустороннее отношение доверия
  Тип отношения доверия: Домен Active Directory
  Состояние отношения доверия: Установлено и проверено
```

При появлении запроса следует ввести пароль администратора домена AD.

Важно

Учётная запись, указанная через **`--admin`**, должна быть членом группы Domain Admins и иметь имя на латинице.

Примечание

Чтобы принять значение по умолчанию, необходимо нажать **`Enter`**.

После создания доверия следует обновить список доменов леса:

```
$ ipa trust-fetch-domains test.alt
-----------------------------------------------------------------------------
----------------------
Список надёжных доменов успешно обновлён. Используйте команду trustdomain-find
для вывода этого списка.
-----------------------------------------------------------------------------
----------------------
---------------------------------
Количество возвращённых записей 0
---------------------------------
```

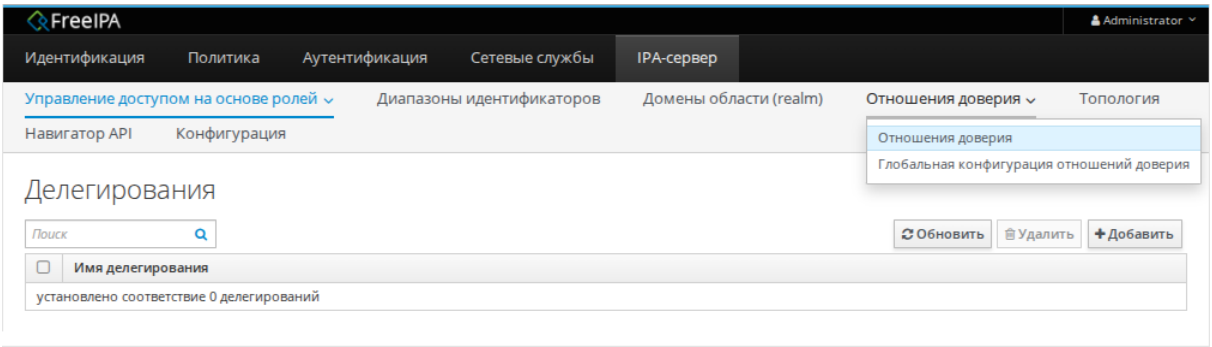
Просмотр доверенных доменов:

```
$ ipa trustdomain-find test.alt
  Имя домена: test.alt
  Имя домена NetBIOS: TEST
  Идентификатор безопасности домена: S-1-5-21-350745825-2392200591-20856689
  Домен включён: True
---------------------------------
Количество возвращённых записей 1
---------------------------------
```

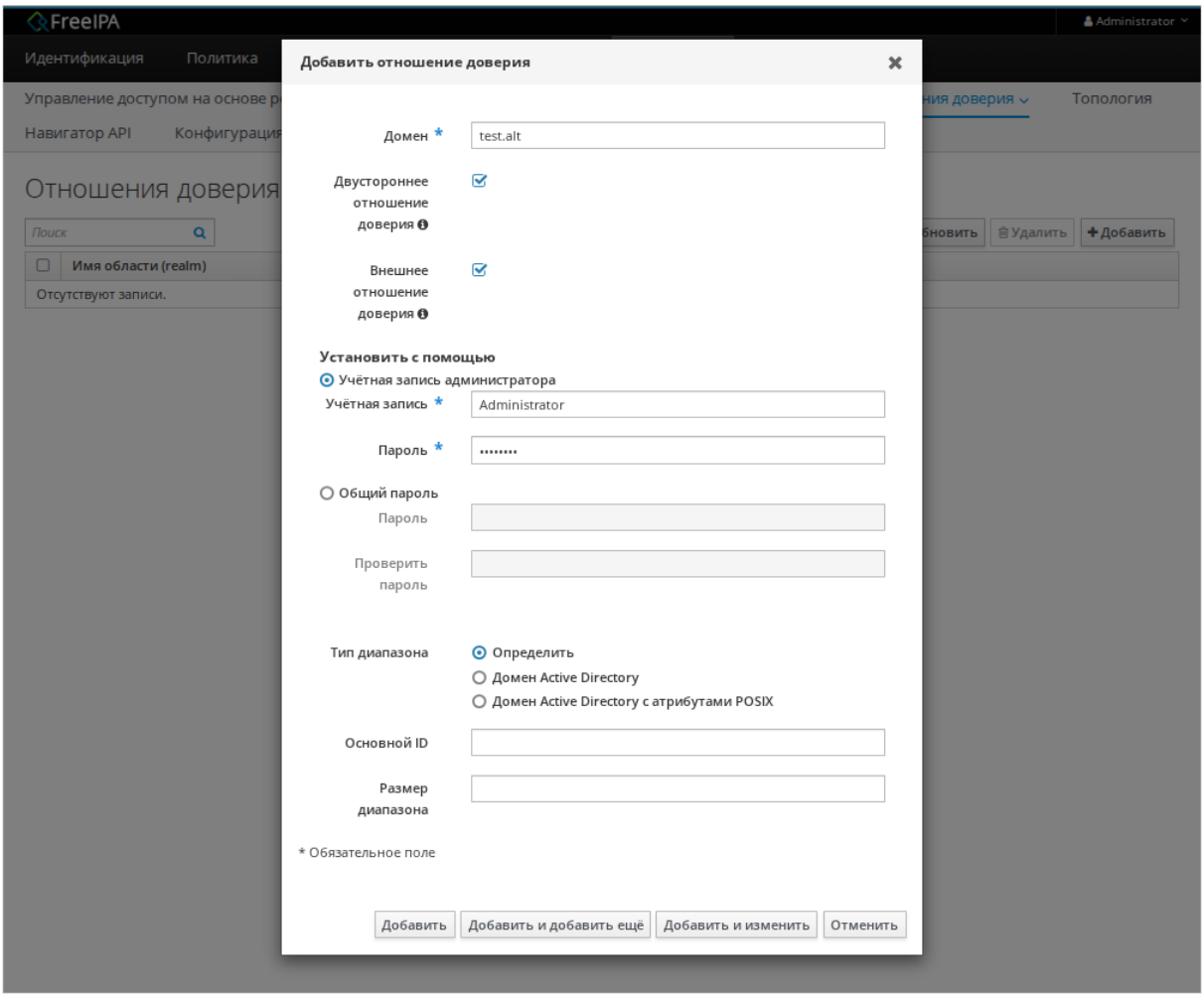
27.2. В веб-интерфейсе

Настройка доверительных отношений:

1. Перейти на вкладку **IPA-сервер**.
2. Выбрать пункт меню **Отношения доверия** → **Отношения доверия**:



3. Нажать кнопку **Добавить**.
4. В диалоговом окне **Добавить отношение доверия** ввести имя домена AD (test.alt). В полях **Учетная запись** и **Пароль** указать учётные данные администратора AD:



5. (Опционально) Отметить пункт **Двустороннее отношение доверия**, если требуется, чтобы AD доверял FreeIPA.

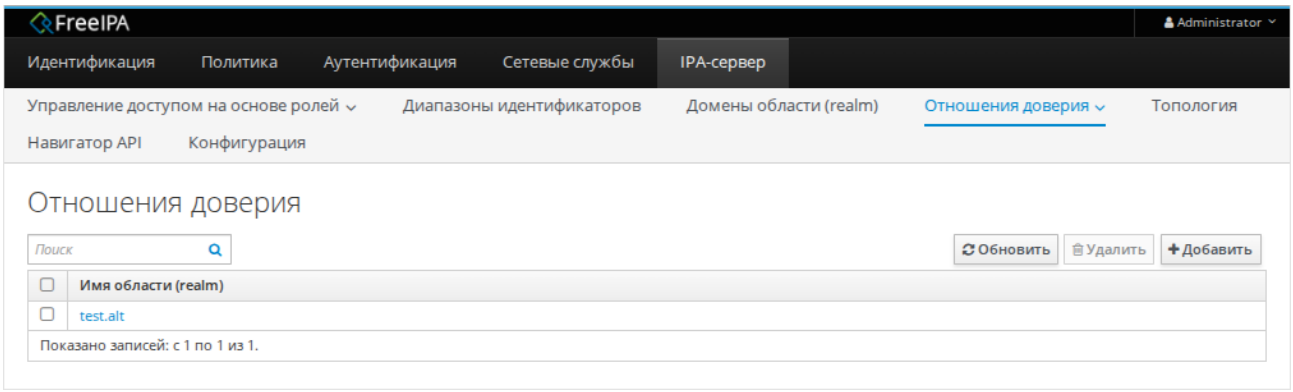
6. (Опционально) Отметить пункт **Внешнее отношение доверия**, если доверие устанавливается не с корневым доменом леса.

7. Нажать кнопку **Добавить**.

Примечание

Оба типа доверия (одностороннее и двустороннее) считаются одинаково безопасными благодаря фильтрации SID.

Если доверие было успешно добавлено, сообщение об этом появится во всплывающем окне.



27.3. Проверка конфигурации Kerberos

Для проверки конфигурации Kerberos, следует проверить, возможно ли получить билет для пользователя AD и может ли пользователь AD запрашивать служебные билеты.

Получить билет пользователя AD:

```
$ kinit ivanov@test.alt
Password for ivanov@test.alt:
```

Запросить service-билеты:

```
$ kvno -S host $(hostname)    # для FreeIPA
host/ipa.example.test@EXAMPLE.TEST: kvno = 2

$ kvno -S cifs dc1.test.alt   # для AD
cifs/dc1.test.alt@TEST.ALT: kvno = 1
```

Проверить наличие межобластного TGT:

```
$ klist
Ticket cache: KEYRING:persistent:0:krb_ccache_ls3PXsa
Default principal: ivanov@TEST.ALT

Valid starting       Expires              Service principal
17.09.2025 19:00:55  18.09.2025 05:00:30  cifs/dc1.test.alt@
        renew until 18.09.2025 19:00:24
        Ticket server: cifs/dc1.test.alt@TEST.ALT
17.09.2025 19:00:45  18.09.2025 05:00:30  host/ipa.example.test@EXAMPLE.TEST
        renew until 18.09.2025 19:00:24
17.09.2025 19:00:45  18.09.2025 05:00:30  krbtgt/EXAMPLE.TEST@TEST.ALT
        renew until 18.09.2025 19:00:24
17.09.2025 19:00:30  18.09.2025 05:00:30  krbtgt/TEST.ALT@TEST.ALT
        renew until 18.09.2025 19:00:24
```

В выводе должен присутствовать билет:

```
krbtgt/EXAMPLE.TEST@TEST.ALT
```

27.4. Проверка DNS-записей на стороне FreeIPA

Проверка наличия записей на сервере FreeIPA:

1. Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
$ dig +short -t SRV _kerberos._udp.dc._msdcs.example.test
0 100 88 ipa.example.test.
$ dig +short -t SRV _ldap._tcp.dc._msdcs.example.test
0 100 389 ipa.example.test.
```

   В выводе этих команд должны быть перечислены все серверы FreeIPA, на которых была выполнена команда **ipa-adtrust-install**.

2. Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP (проверка того, что FreeIPA может разрешать записи служб для AD):

```
$ dig +short -t SRV _kerberos._udp.dc._msdcs.test.alt
0 100 88 dc1.test.alt.
$ dig +short -t SRV _ldap._tcp.dc._msdcs.test.alt
0 100 389 dc1.test.alt.
```

Важно

Если запись ***_kerberos._udp.dc._msdcs.test.alt*** не доступна, следует проверить ***_kerberos._tcp.dc._msdcs.test.alt***.

27.5. Проверка DNS-записей на стороне AD

Примечание

Необходимо войти в систему с правами администратора.

Проверка конфигурации доверия в AD:

1. После выполнения команды **ipa-adtrust-install** должны появится записи отвечающие за работу сервисов MS DC Kerberos через UDP и LDAP через TCP:

```
C:\> nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.example.test.
_kerberos._udp.dc._msdcs.example.test        SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = ipa.example.test
> _ldap._tcp.dc._msdcs.example.test.
_ldap._tcp.dc._msdcs.example.test        SRV service location:
    priority = 0
```

```
    weight = 100
    port = 389
    svr hostname = ipa.example.test
ipa.example.test internet address = 192.168.0.113
```

2. Проверить наличие записей для работы сервисов AD на DNS-сервере AD. Запись, отвечающая за работу сервисов Kerberos через UDP и LDAP через TCP:

```
C:\> nslookup.exe
> set type=SRV
> _kerberos._udp.dc._msdcs.test.alt.
_kerberos._udp.dc._msdcs.test.alt.    SRV service location:
    priority = 0
    weight = 100
    port = 88
    svr hostname = dc1.test.alt.
dc1.test.alt internet address = 192.168.0.132
> _ldap._tcp.dc._msdcs.test.alt.
_ldap._tcp.dc._msdcs.example.test        SRV service location:
_ldap._tcp.dc._msdcs.test.alt.    SRV service location:
    priority = 0
    weight = 100
    port = 389
    svr hostname = dc1.dtest.alt.
dc1.test.alt internet address = 192.168.0.132
```

27.6. Проверка пользователей доверенного домена

Необходимо проверить имеют ли рабочие станции FreeIPA доступ к пользователям из доверенного домена.

На клиенте FreeIPA:

```
$ getent passwd ivanov@test.alt
ivanov@test.alt:*:348001105:348001105:Иван Иванов:/home/test.alt/ivanov:
```

где ivanov — это пользователь из домена AD.

Назначить оболочку входа для пользователей из доверенного домена можно, добавив на сервере FreeIPA в файл **/etc/sssd/sssd.conf** строку:

```
[domain/example.test]
...
default_shell = /bin/bash
...
```

Перезапустить SSSD:

```
# systemctl restart sssd
```

Теперь вывод будет включать оболочку:

```
$ getent passwd ivanov@test.alt
ivanov@test.alt:*:348001105:348001105:Иван Иванов:/home/test.alt/ivanov:/bin/bash
```

Пользователи AD могут входить на клиенты FreeIPA, указывая имя в формате <ИМЯ_ДОМЕНА>\<идентификатор_пользователя_AD> или <идентификатор_пользователя_AD>@<имя_домена> (например, TEST\ivanov, TEST.ALT\ivanov, ivanov@test, ivanov@test.alt).

Глава 28. Удаление доверия

В этом разделе описывается процедура удаления доверительных отношений между FreeIPA и Active Directory на стороне FreeIPA.

Важно

Удаление доверия в FreeIPA не удаляет соответствующий объект доверия в Active Directory. Это действие необходимо выполнить вручную на контроллере домена AD.

28.1. В командной строке

Удаление доверия из FreeIPA:

1. Удалить конфигурацию доверия:

```
$ kinit admin
$ ipa trust-del test.alt
```

2. Удалить объект доверия в Active Directory (вручную, через **`Active Directory Domains and Trusts`** или PowerShell).

3. Проверить, что доверие удалено:

```
$ ipa trust-show test.alt
ipa: ERROR: test.alt: отношение доверия не найден
```

Примечание

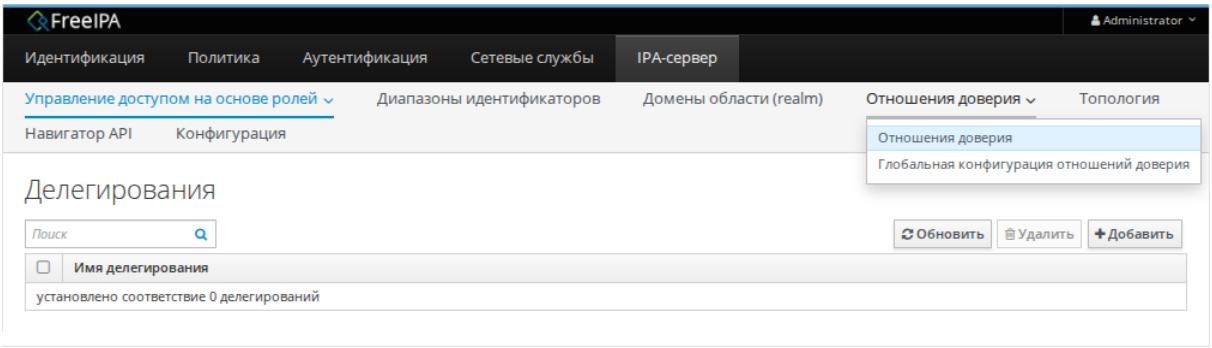
Удаление доверия не удаляет автоматически диапазон идентификаторов (ID range), созданный для пользователей AD. Если в будущем доверие будет восстановлено, FreeIPA повторно использует существующий диапазон, что может привести к неожиданному поведению.

Рекомендуется вручную удалить диапазон идентификаторов (см. Удаление диапазона идентификаторов после удаления доверия).

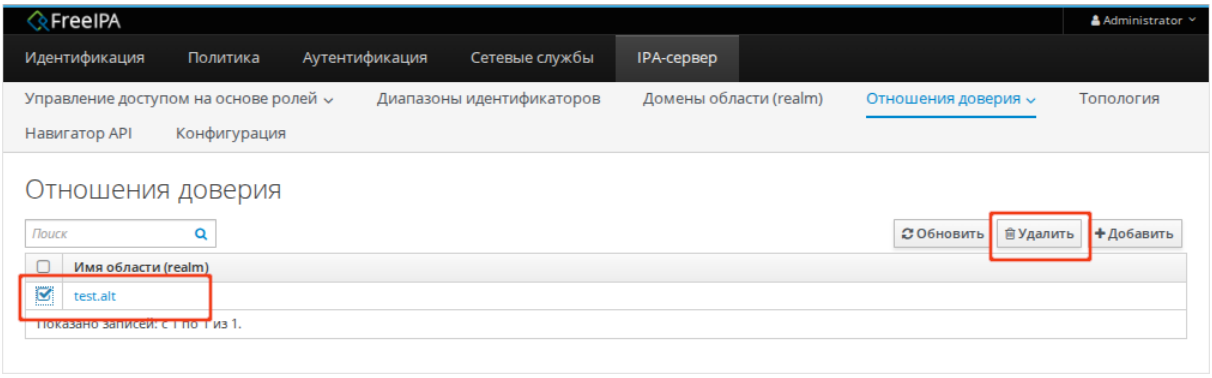
28.2. В веб-интерфейсе

Удаление доверия:

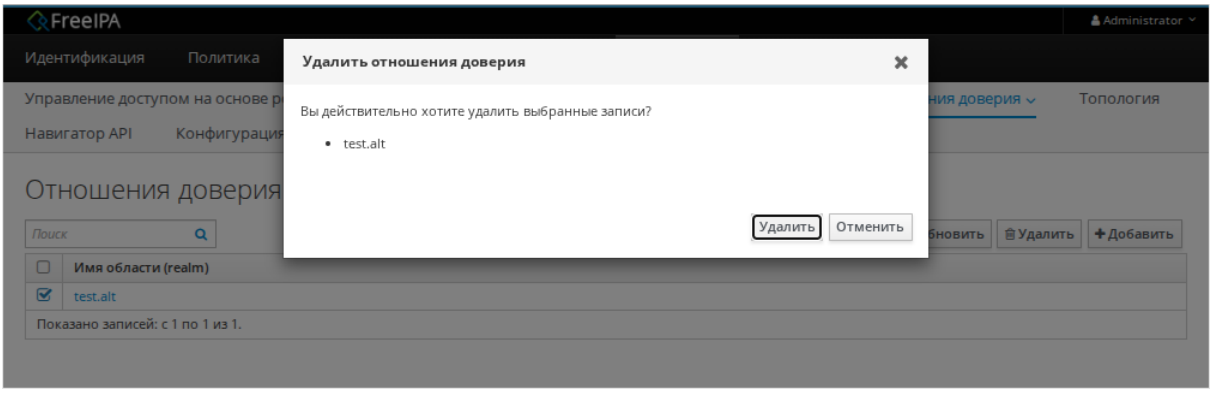
1. Перейти на вкладку **IPA-сервер**.
2. Выбрать пункт меню **Отношения доверия** → **Отношения доверия**:



3. Выбрать объект доверия.
4. Нажать кнопку **`Удалить`**:



5. Подтвердить удаление во всплывающем окне:



6. Удалить объект доверия в Active Directory (вручную, через **`Active Directory Domains and Trusts`** или PowerShell).

Если доверие было успешно удалено, сообщение об этом появится во всплывающем окне.

Примечание

Удаление доверия не удаляет автоматически диапазон идентификаторов (ID range), созданный для пользователей AD. Если в будущем доверие будет восстановлено, FreeIPA повторно использует существующий диапазон, что может привести к неожиданному поведению.

Рекомендуется вручную удалить диапазон идентификаторов (см. Удаление диапазона идентификаторов после удаления доверия).

28.3. Удаление диапазона идентификаторов после удаления доверия

Чтобы полностью очистить следы доверия, следует удалить диапазон идентификаторов пользователей AD.

Процедура удаления диапазона идентификаторов пользователей AD:

1. Вывести все диапазоны идентификаторов:

```
$ ipa idrange-find
----------------------------------
установлено соответствие 2 диапазонов
----------------------------------
Имя диапазона: EXAMPLE.TEST_id_range
Первый идентификатор POSIX диапазона: 1034400000
Количество идентификаторов в диапазоне: 200000
Первый RID соответствующего диапазона RID: 1000
Первый RID вторичного диапазона RID: 100000000
Тип диапазона: local domain range

Имя диапазона: TEST.ALT_id_range
Первый идентификатор POSIX диапазона: 1939200000
Количество идентификаторов в диапазоне: 200000
Первый RID соответствующего диапазона RID: 0
SID доверенного домена: S-1-5-21-578923263-1107570656-1287136478
Тип диапазона: Active Directory domain range
Auto private groups: hybrid
---------------------------------
Количество возвращённых записей 2
---------------------------------
```

2. Удалить диапазон, связанный с удалённым доверием:

```
$ ipa idrange-del TEST.ALT_id_range
```

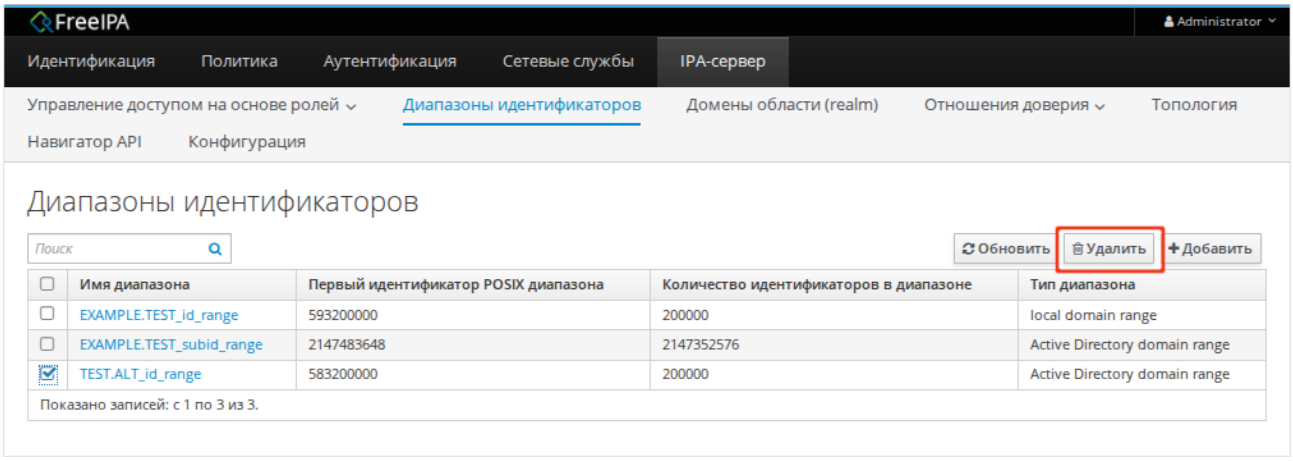
Примечание

Первая часть имени диапазона идентификаторов — это имя доверия, например, TEST.ALT_id_range.

3. Перезапустить SSSD, чтобы применить изменения:

```
# systemctl restart sssd
```

Удалить диапазон идентификаторов пользователей AD можно в веб-интерфейсе на вкладке **Диапазоны идентификаторов**:



Часть VII. Конфигурирование FreeIPA

Содержание

Глава 29. Управление пользователями

FreeIPA поддерживает три состояния учётной записи пользователя:

- Неподтверждённые пользователи (Stage Users) — учётные записи в стадии подготовки. Аутентификация запрещена, невозможно назначить членство в группах. Используются для предварительного создания записей с последующей активацией.
- Активные пользователи — полноценные учётные записи, которым разрешена аутентификация. Все атрибуты (группы, пароли, ключи) должны быть настроены.
- Сохранённые пользователи (Preserved Users) — бывшие активные пользователи, переведённые в неактивное состояние. Аутентификация запрещена, членство в группах удалено, но основные атрибуты сохраняются для возможного восстановления.

Имя учётной записи (логин) должно соответствовать следующему регулярному выражению:

```
[a-zA-Z0-9_.][a-zA-Z0-9_.-]{0,252}[a-zA-Z0-9_.$-]?
```

Примечание

FreeIPA не позволяет создавать пользователей с именами, отличающимися только регистром (например, user и User).

При аутентификации имена обрабатываются без учёта регистра.

Максимальная длина имени учётной записи по умолчанию составляет 32 символа. Для изменения длины используется команда **`ipa config-mod --maxusername`**. Пример увеличения максимальной длины логина до 64 символов:

```
$ ipa config-mod --maxusername=64
  Максимальная длина имени пользователя: 64
  Максимальная длина имени узла: 64
  Основа домашних каталогов: /home
  Оболочка по умолчанию: /bin/bash
  Группа пользователей по умолчанию: ipausers
  Почтовый домен по умолчанию: example.test
  …
```

Важно

Удалённые учётные записи не подлежат восстановлению, если не были сохранены с помощью флага **`--preserve`**. Вся связанная информация (пароли, ключи, членство в группах) безвозвратно удаляется.

Важно

Не следует удалять пользователя admin. Если требуется использовать другого администратора, необходимо сначала назначить права администратора другому пользователю, затем отключить учётную запись admin: **`ipa user-disable admin`**.

29.1. Управление пользователями в командной строке

Для работы с пользователями требуются:

- права администратора или роль ***`User Administrator`***;
- действительный Kerberos-билет.

Примечание

FreeIPA автоматически назначает UID. Ручное указание возможно, но не проверяется на уникальность.

Основные команды:

- Добавление активного пользователя:

```
$ ipa user-add kim --first=Эдуард --last=Ким --email=kim@example.test
---------------------------
Добавлен пользователь "kim"
---------------------------
  Имя учётной записи пользователя: kim
  Имя: Эдуард
  Фамилия: Ким
  Полное имя: Эдуард Ким
  Отображаемое имя: Эдуард Ким
  Инициалы: ЭК
  Домашний каталог: /home/kim
  GECOS: Эдуард Ким
  Оболочка входа: /bin/bash
  Имя учётной записи: kim@EXAMPLE.TEST
  Псевдоним учётной записи: kim@EXAMPLE.TEST
  Адрес электронной почты: kim@example.test
  UID: 593200005
  ID группы: 593200005
  Пароль: False
  Участник групп: ipausers
  Доступные ключи Kerberos: False
```

Примечание

Просмотр всех параметров команды **ipa user-add**:

```
$ ipa help user-add
```

- Добавление неподтверждённого пользователя:

```
$ ipa stageuser-add markov --first=Илья --last=Марков --
email=markov@example.test
-----------------------------------------------
Добавлен неподтверждённый пользователь "markov"
-----------------------------------------------
  Имя учётной записи пользователя: markov
  Имя: Илья
  Фамилия: Марков
  Полное имя: Илья Марков
  Отображаемое имя: Илья Марков
  Инициалы: ИМ
  Домашний каталог: /home/markov
  GECOS: Илья Марков
  Оболочка входа: /bin/bash
  Имя учётной записи: markov@EXAMPLE.TEST
  Псевдоним учётной записи: markov@EXAMPLE.TEST
  Адрес электронной почты: markov@example.test
```

```
  UID: -1
  ID группы: -1
  Пароль: False
  Доступные ключи Kerberos: False
```

Активация неподтверждённого пользователя:

```
$ ipa stageuser-activate markov
---------------------------
Stage user markov activated
---------------------------
  Имя учётной записи пользователя: markov
  Имя: Илья
  Фамилия: Марков
  Домашний каталог: /home/markov
  Оболочка входа: /bin/bash
  Имя учётной записи: markov@EXAMPLE.TEST
  Псевдоним учётной записи: markov@EXAMPLE.TEST
  Адрес электронной почты: markov@example.test
  UID: 948000005
  ID группы: 948000005
  Пароль: False
  Участник групп: ipausers
  Доступные ключи Kerberos: False
```

Просмотр списка всех пользователей с подробной информацией:

```
$ ipa user-find
```

Сохранение учётной записи:

```
$ ipa user-del --preserve markov
-----------------------
Preserved user "markov"
-----------------------
```

Удаление учётной записи (без сохранения):

```
$ ipa user-del markov      # удаление активного или хранимого пользователя
----------------------------
Удален пользователь "markov"
----------------------------
$ ipa stageuser-del ivanov # удаление неподтверждённого пользователя
```

Массовое удаление пользователей:

```
$ ipa user-del --continue user1 user2 user3
-----------------------
Удален пользователь "user1,user2,user3"
-----------------------
```

Восстановление сохранённого пользователя:

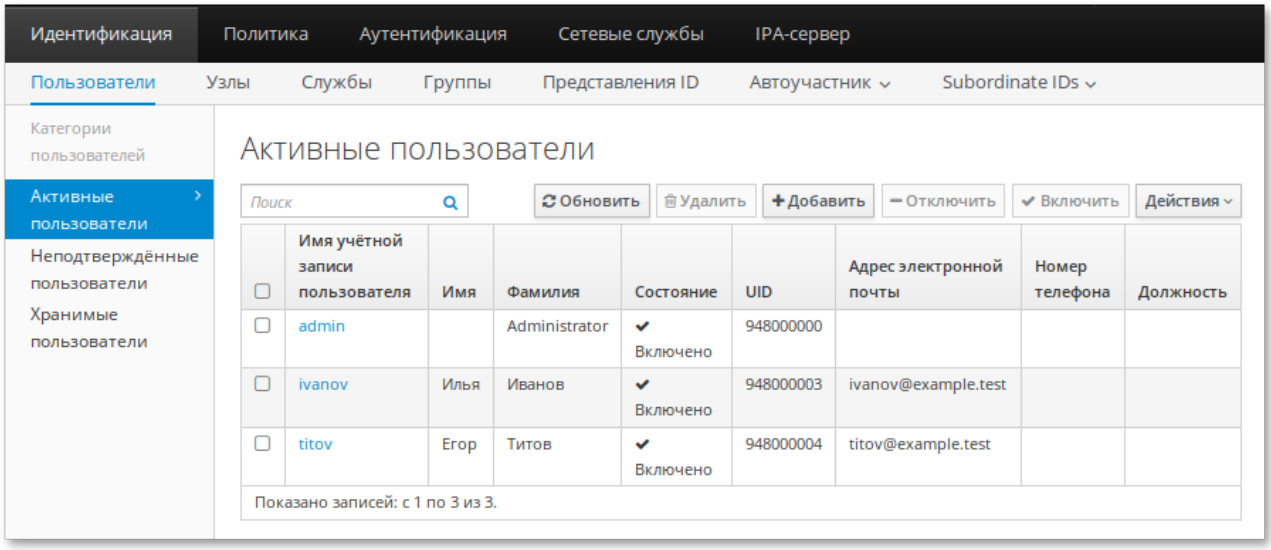
```
$ ipa user-undel markov
-----------------------------------------------------------
Учётная запись пользователя "markov" возвращена после удаления
-----------------------------------------------------------
```

Примечание

Пароль не восстанавливается — его нужно задать заново.

29.2. Управление пользователями в веб-интерфейсе

Управление пользователями осуществляется на странице **Идентификация** → **Пользователи**:



Для управления пользователями требуются права администратора или роль ***User Administrator***.

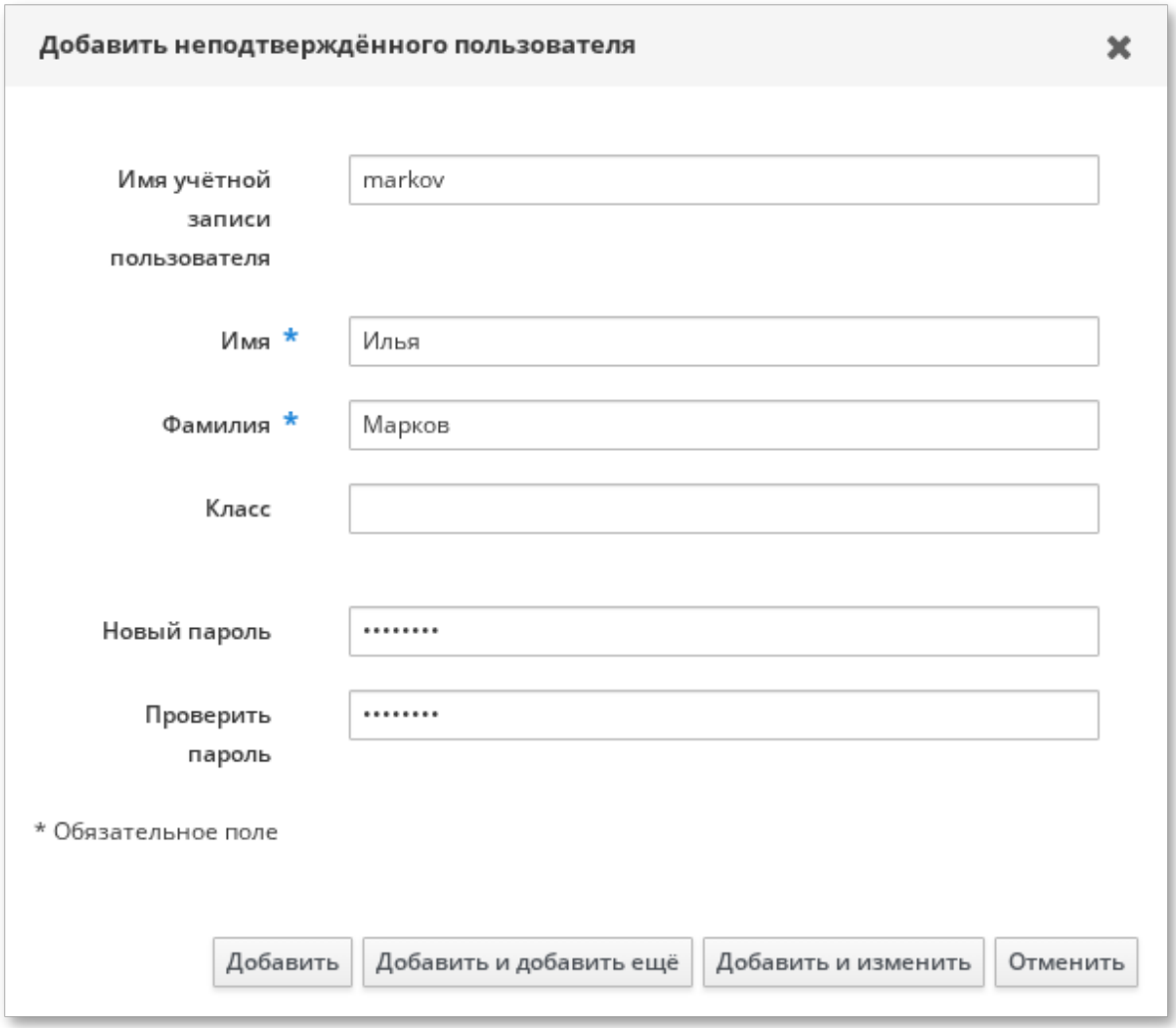
29.2.1. Добавление нового пользователя

Для создания неподтверждённой учётной записи пользователя необходимо добавлять на вкладке **Неподтверждённые пользователи**. Такую учётную запись позже нужно будет активировать.

Чтобы создать активную учётную запись, пользователя нужно добавлять на вкладке **Активные пользователи**.

Процедура добавления пользователя:

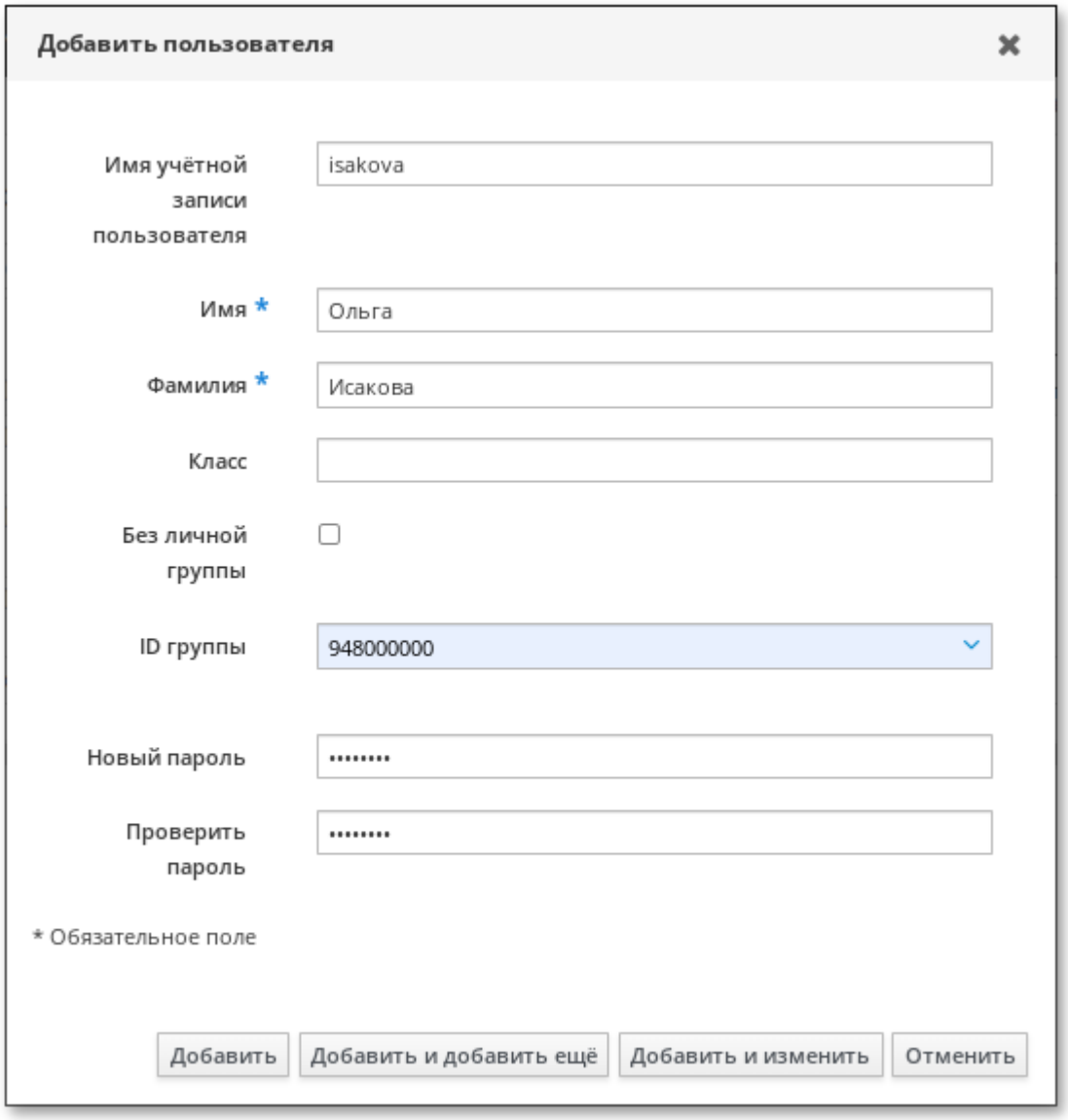
1. Перейти на вкладку **Пользователи** → **Неподтверждённые пользователи** (или на вкладку **Пользователи** → **Активные пользователи**);
2. Нажать кнопку **Добавить**.
3. Для создания пользователя достаточно заполнить поля **Имя учётной записи пользователя**, **Имя** и **Фамилия**.



Примечание

Если оставить поле **Имя учётной записи пользователя** пустым, FreeIPA сгенерирует логин таким образом: <первая буква имени><фамилия>. Автоматическая генерация логина возможна только в том случае, если поля **Имя** и **Фамилия** записываются на латинице.

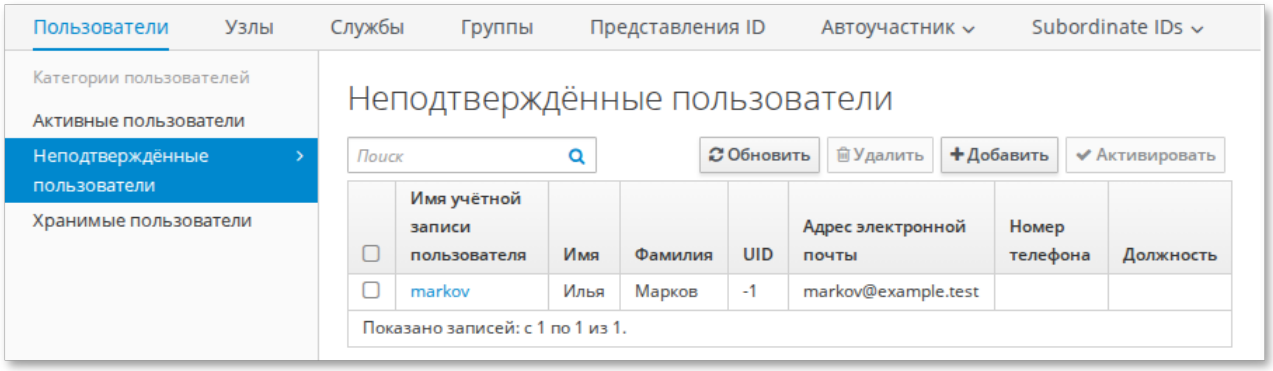
При создании активного пользователя в раскрывающемся списке заполнить **ID группы** можно выбрать группу, в которую будет включён пользователь:



В поля **Новый пароль** и **Повторите пароль** можно ввести пароль пользователя.

4. Нажать кнопку **Добавить**.

Созданную учётную запись можно увидеть на соответствующей вкладке (**Неподтверждённые пользователи** или **Активные пользователи**):



Примечание

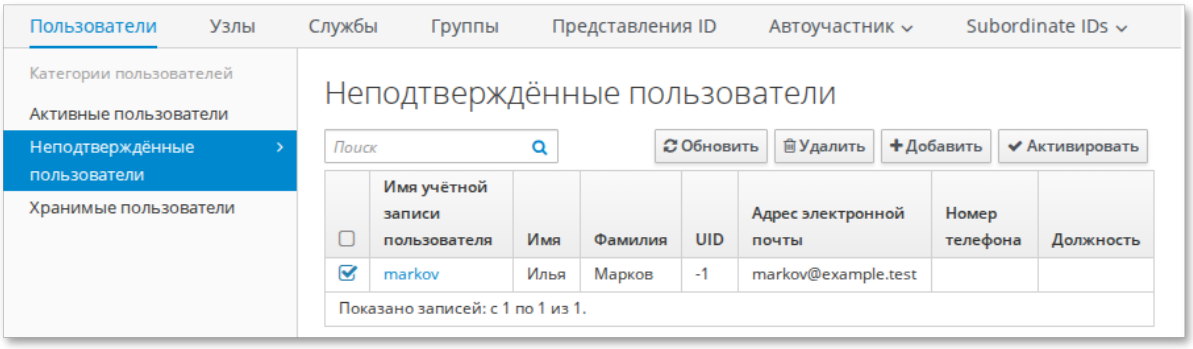
Если щёлкнуть мышью по имени пользователя, откроется окно, где можно отредактировать дополнительные параметры, такие как номер телефона, адрес, должность и т.д.

29.2.2. Активация неподтверждённого пользователя

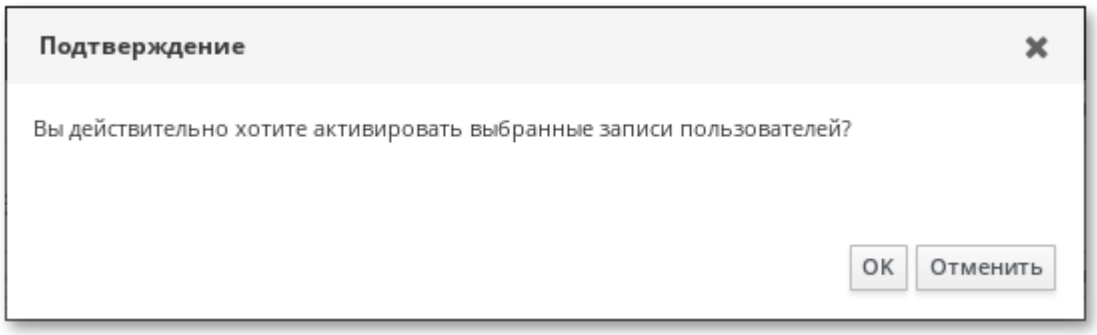
Неподтверждённая учётная запись должна быть активирована до того, как пользователь сможет войти во FreeIPA или до того, как пользователя можно будет добавить в группу FreeIPA.

Активация пользователя:

1. Перейти на вкладку **Пользователи** → **Неподтверждённые пользователи**;
2. Выбрать учётную запись, которую необходимо активировать:



3. Нажать кнопку **Активировать**.
4. В открывшемся диалоговом окне нажать кнопку **OK**:



Если активация прошла успешно, учётная запись будет перемещена в список активных пользователей.

29.2.3. Отключение/Включение учётной записи

Активную учётную запись можно отключить.

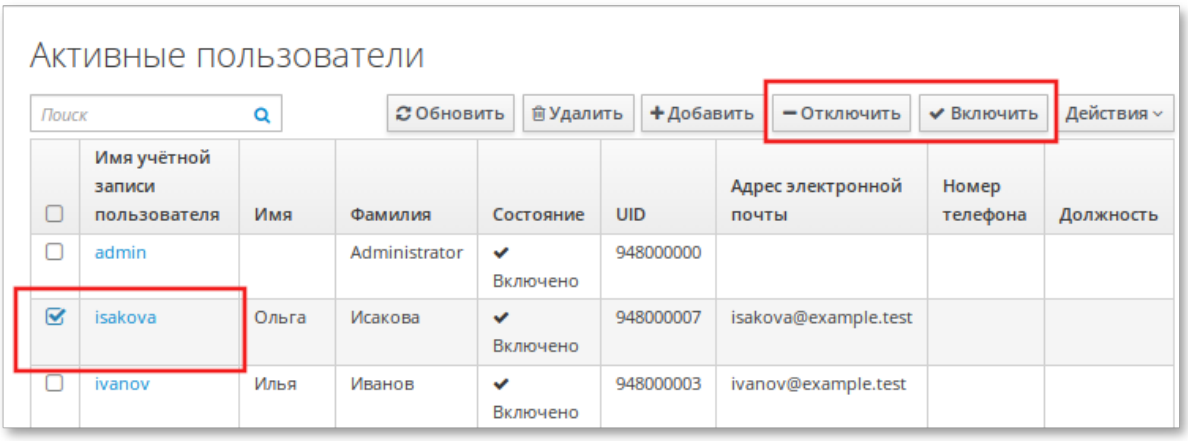
Отключённый пользователь не может аутентифицироваться, но остаётся в группах.

Примечание

После отключения учётной записи любые существующие подключения работают до истечения срока действия билета Kerberos. По истечении срока действия билета пользователь не сможет его обновить.

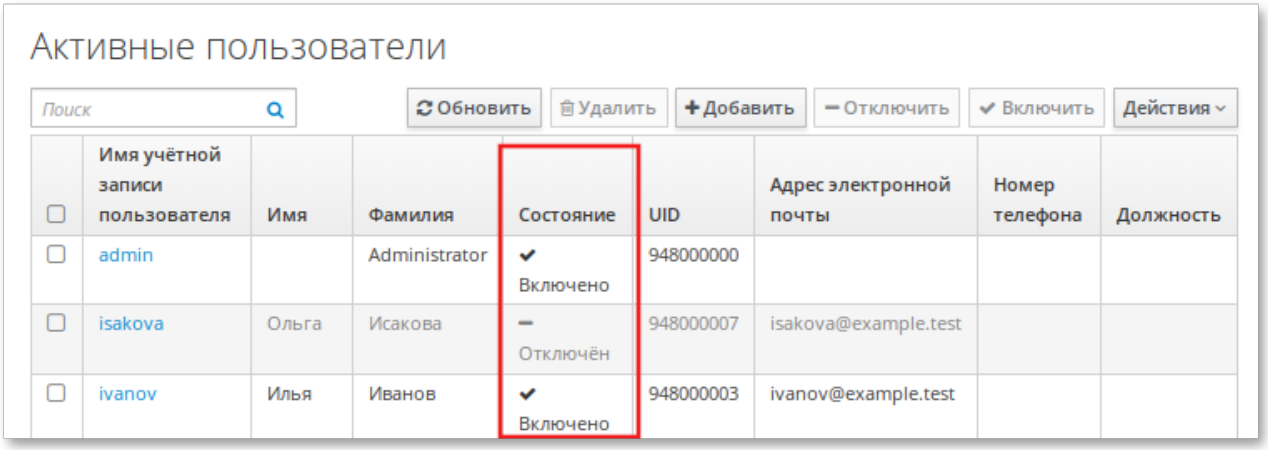
Для отключения/включения пользователя необходимо:

1. Перейти на вкладку **Пользователи** → **Активные пользователи**;
2. Выбрать учётные записи, которые необходимо отключить/включить.
3. Нажать кнопку **`Отключить`**/**`Включить`**:



4. В открывшемся диалоговом окне нажать кнопку **`OK`**.

Статус отображается учётной записи отображается в столбце **`Состояние`**:



29.2.4. Сохранение учётной записи

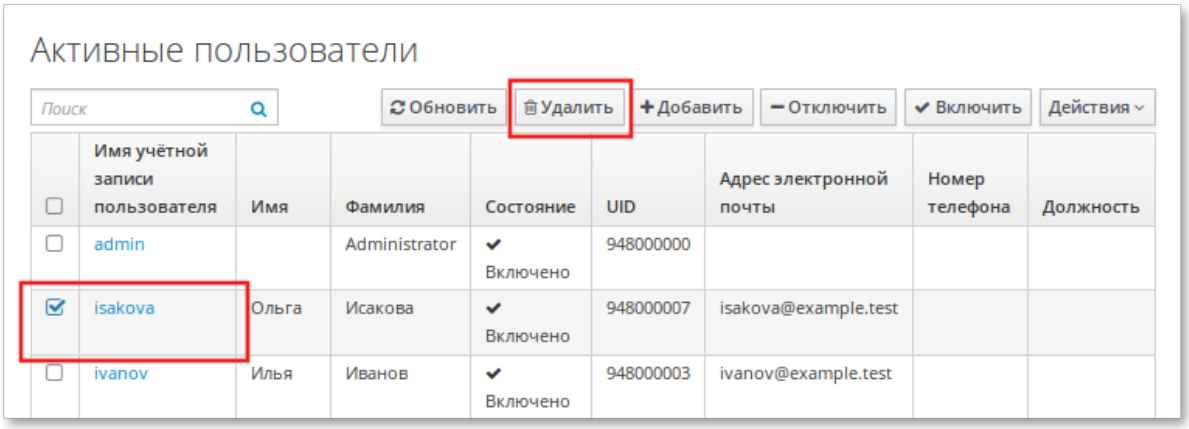
Сохранение учётной записи позволяет удалить пользователей с вкладки **Активные пользователи**, сохраняя его при этом в FreeIPA.

Примечание

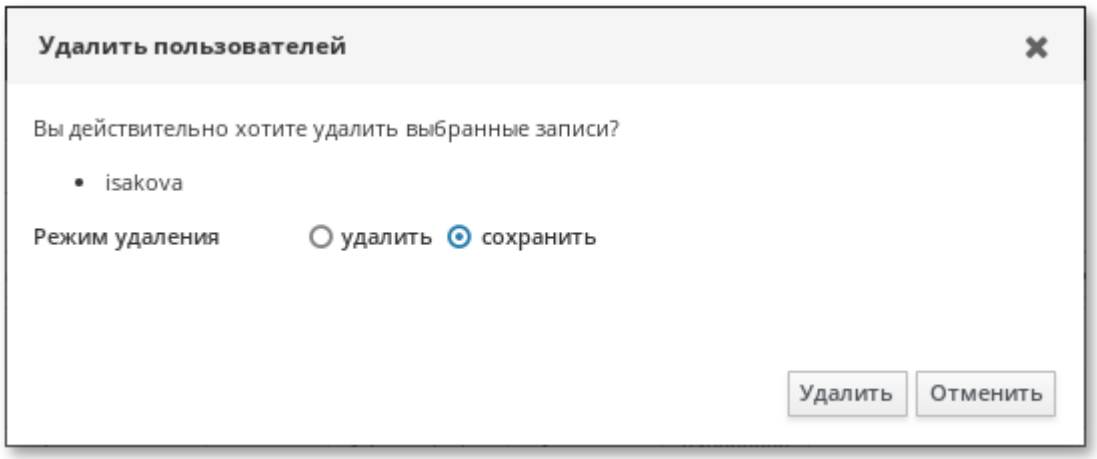
Список сохранённых пользователей может использоваться для аудита и восстановления.

Перевод учётной записи в статус хранимой:

1. Перейти на вкладку **Пользователи** → **Активные пользователи**;
2. Выбрать учётные записи, которые необходимо сохранить.
3. Нажать кнопку **Удалить**:



4. В открывшемся диалоговом окне в поле **Режим удаления** выбрать **сохранить** и нажать кнопку **Удалить**:



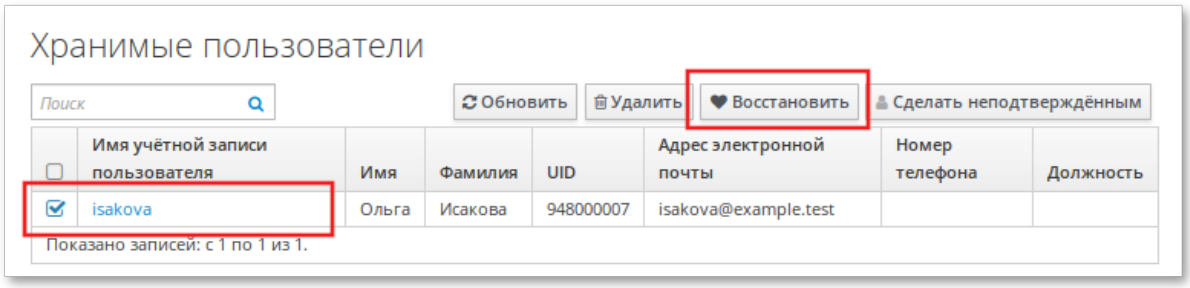
Учётная запись будет перемещена в список хранимых пользователей.

29.2.5. Восстановление учётной записи

Сохранённую учётную запись можно перевести в активное или неподтверждённое состояние.

Восстановления учётной записи:

1. Перейти на вкладку **Пользователи** → **Хранимые пользователи**;
2. Выбрать учётные записи, которые необходимо восстановить.
3. Нажать кнопку **Восстановить**:



4. В открывшемся диалоговом окне в поле и нажать кнопку **OK**.

Учётная запись будет перемещена в список активных пользователей.

29.2.6. Удаление учётной записи

Удаление пользователей является необратимой операцией.

Примечание

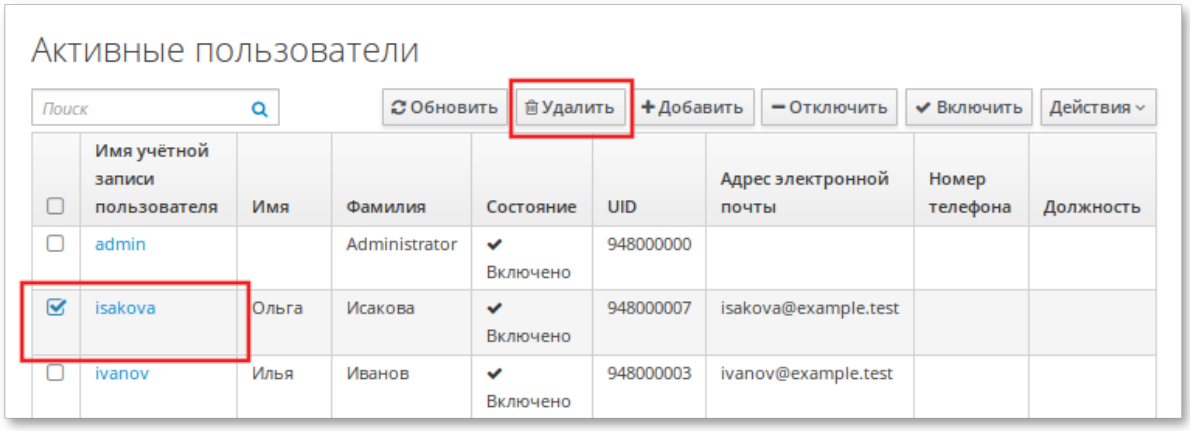
Учётная запись полностью удаляется из LDAP (включая членство в группах и пароли). Домашний каталог и системные данные не удаляются, но становятся недоступны через FreeIPA.

Безвозратное удаление учётной записи:

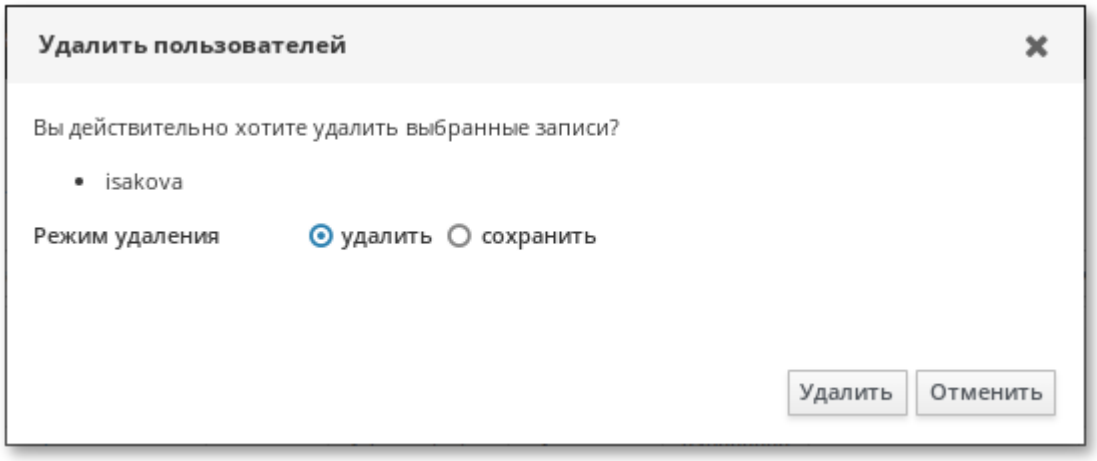
1. Перейти на вкладку **Пользователи** → **Активные пользователи** (или **Пользователи** → **Неподтверждённые пользователи**, **Пользователи** → **Хранимые пользователи**);

2. Выбрать учётные записи, которые необходимо удалить.

3. Нажать кнопку **Удалить**:



4. В открывшемся диалоговом окне в поле **Режим удаления** выбрать **удалить** и нажать кнопку **Удалить**:



Учётная запись будет удалена из FreeIPA.

Глава 30. Парольные политики

Парольная политика определяет требования, которым должны соответствовать пароли пользователей FreeIPA.

Таблица 30.1. Атрибуты политики паролей

Параметр	Описание	Пример
Максимальный срок действия (**--maxlife**)	Максимальный срок действия пароля в днях. Значение по умолчанию — 90 дней. Если задано значение 0, срок действия пароля не ограничен	***--maxlife=180***
Минимальный срок действия (**--minlife**)	Минимальный интервал между двумя операциями смены пароля (в часах)	***--minlife=1***
Размер журнала (**--history**)	Количество предыдущих паролей, которые нельзя повторно использовать. Если задано значение 0, пользователи могут повторно использовать любой из своих предыдущих паролей	***--history=0***
Классы символов (**--minclasses**)	Минимальное количество различных классов символов в пароле. Значение по умолчанию — 0. Классы символов: ▸Заглавные латинские буквы ▸Строчные латинские буквы	***--minclasses=0***

Параметр	Описание	Пример
	▸Цифры ▸Специальные символы, такие как запятая (,), точка (.), звездочка (*) ▸Другие символы UTF-8 Повтор одного символа три и более раз подряд уменьшает эффективное количество классов на 1. Пример: ▸***Pa55word*** — 3 класса символов (заглавные, строчные, цифры); ▸***Pa555word*** — 2 класса символов (3 − 1 за повторное использование цифры 5).	
Минимальная длина (**`--minlength`**)	Минимальная длина пароля. Если заданы другие параметры политики, минимальная длина автоматически устанавливается в 6 символов	***`--minlength=8`***
Максимальное количество ошибок (**`--maxfail`**)	Число неудачных попыток входа до блокировки учётной записи	***`--maxfail=6`*** (учётная запись будет заблокирована, если пользователь введёт неправильный пароль 7 раз подряд)
Интервал сброса ошибок (**`--failinterval`**)	Время (в секундах), после которого счётчик неудачных попыток сбрасывается	***`--failinterval=60`***
Длительность блокировки (**`--lockouttime`**)	Время (в секундах), на которое блокируется учётная запись после превышения лимита ошибок	***`--lockouttime=600`***

В FreeIPA существует глобальная политика (***`global_policy`***), которая применяется ко всем пользователям, не охваченным групповыми политиками. Можно также создать дополнительные групповые политики паролей. Для каждого пользователя действует только одна политика — либо групповая, либо глобальная.

Если пользователю назначено несколько политик паролей, приоритет будет иметь политика в соответствии со следующими правилами:

- Групповые политики имеют числовой приоритет (чем меньше значение, тем выше приоритет). Минимальное поддерживаемое значение — 0.
- Если пользователь входит в несколько групп с политиками, применяется политика с наименьшим значением приоритета. Все правила, определенные в других политиках, игнорируются.

- Глобальная политика не имеет приоритета и используется только как резервная.

Примечание

Если в групповой политике не задан какой-либо параметр (например, **--maxlife**), он не наследуется из глобальной политики — поведение по умолчанию определяется самой службой (обычно используется значение из глобальной политики, но это не гарантируется явно).

Примечание

Узнать, какая политика применяется к пользователю можно, выполнив команду:

```
$ ipa pwpolicy-show --user=kim
  Группа: global_policy
  Максимальный срок действия (в днях): 90
  Минимальный срок действия (в часах): 1
  Размер журнала : 0
  Классы символов: 0
  Минимальная длина: 8
  Максимальное количество ошибок: 6
  Интервал сброса ошибок: 60
  Длительность блокировки: 600
  Grace login limit: -1
```

30.1. Настройка парольных политик

30.1.1. Командная строка

Создать новую парольную политику для группы (потребуется указать группу пользователей и приоритет):

```
$ ipa pwpolicy-add
Группа: ipausers
Приоритет: 5
  Группа: ipausers
  Приоритет: 5
  Grace login limit: -1
```

Просмотреть парольные политики:

```
$ ipa pwpolicy-find
  Группа: ipausers
  Приоритет: 5
  Grace login limit: -1

  Группа: global_policy
  Максимальный срок действия (в днях): 90
  Минимальный срок действия (в часах): 1
  Размер журнала : 0
```

```
  Классы символов: 0
  Минимальная длина: 8
  Максимальное количество ошибок: 6
  Интервал сброса ошибок: 60
  Длительность блокировки: 600
  Grace login limit: -1
--------------------------------
Количество возвращённых записей 2
--------------------------------
```

Создать парольную политику для группы с указанием дополнительных параметров:

```
$ ipa pwpolicy-add --maxlife=30 --minlength=10 --maxfail=3 --priority=2 managers
  Группа: managers
  Максимальный срок действия (в днях): 30
  Минимальная длина: 10
  Приоритет: 2
  Максимальное количество ошибок: 3
  Grace login limit: -1
```

Изменить политику (например, установить минимальный срок в 24 часа для группы ipausers):

```
$ ipa pwpolicy-mod --minlife=24 ipausers
  Группа: ipausers
  Минимальный срок действия (в часах): 24
  Приоритет: 5
  Grace login limit: -1
```

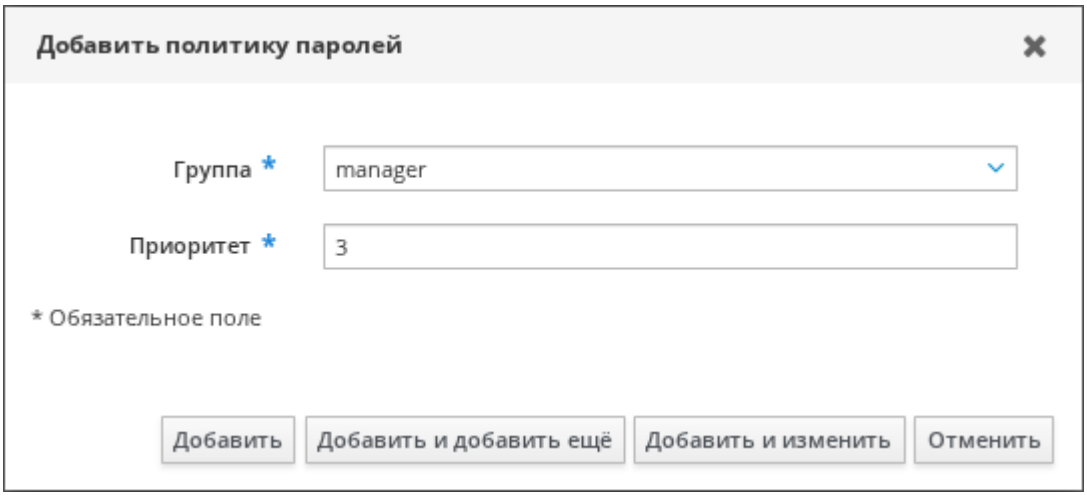
Примечание

Если не указать имя группы, команда изменит глобальную политику ***global_policy***.

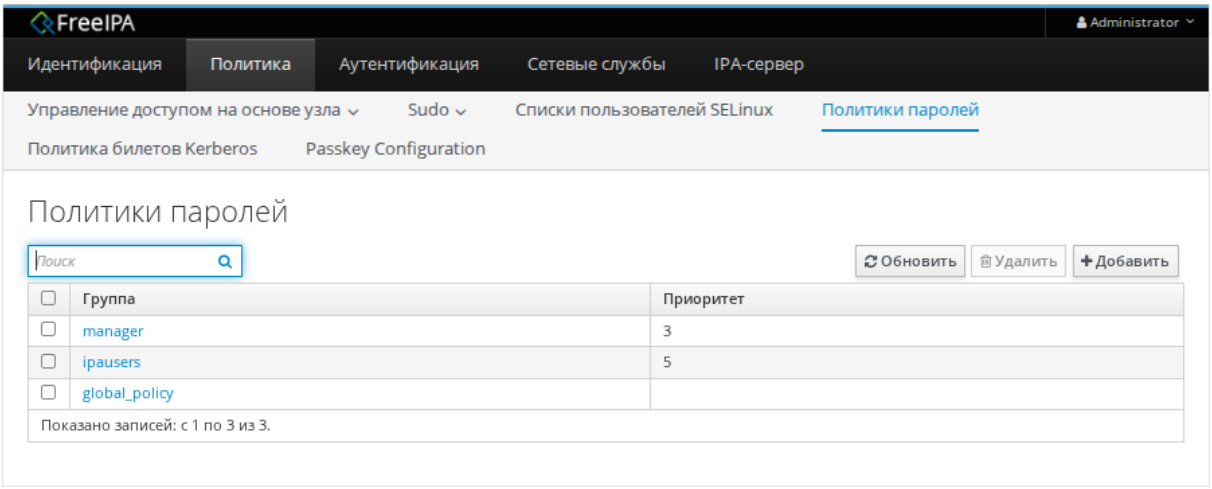
30.1.2. Веб-интерфейс

Добавление новой парольной политики:

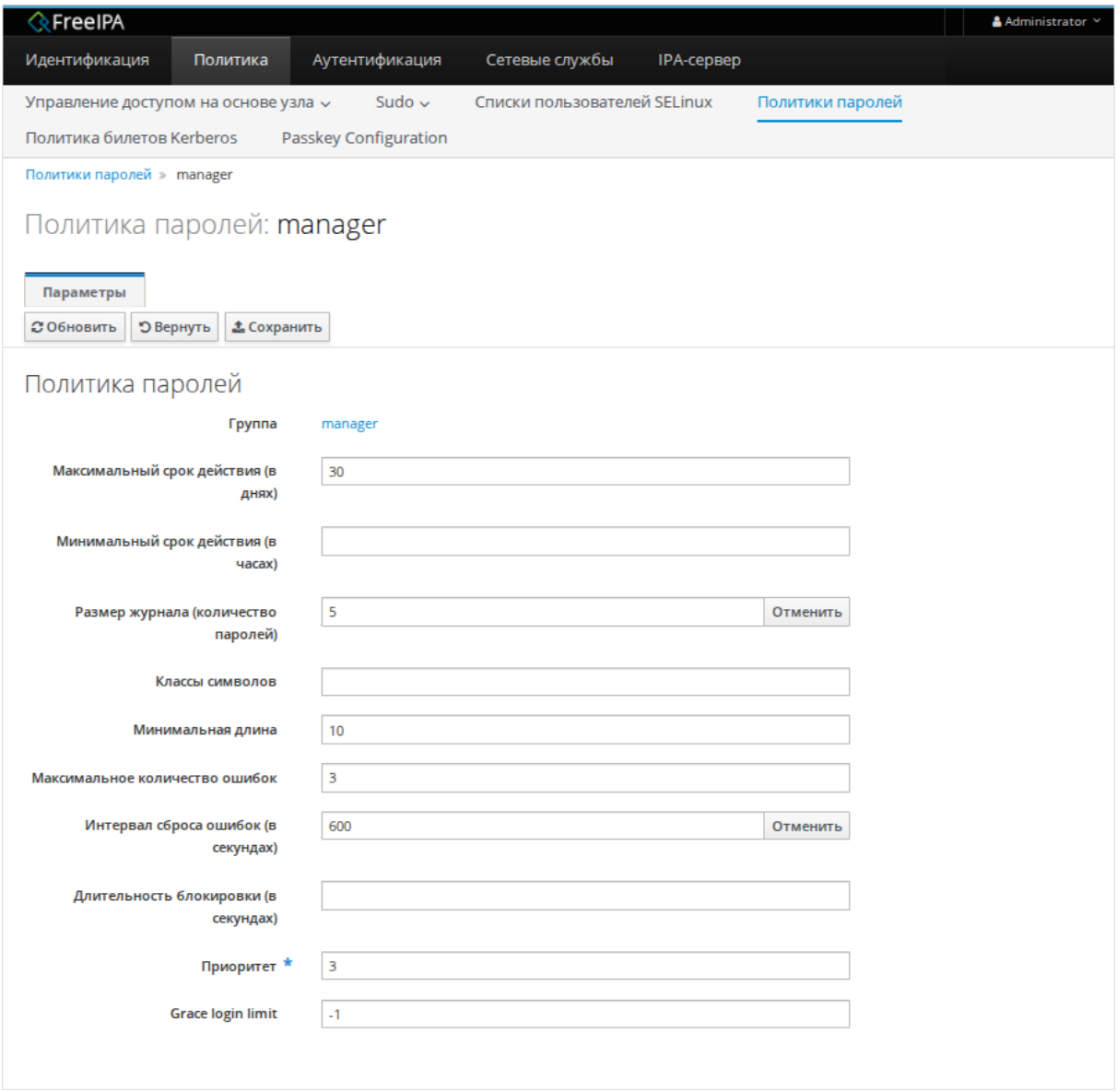
1. Открыть в веб-браузере адрес **https://ipa.example.test/ipa/ui/** и ввести данные администратора для входа в систему.
2. На вкладке **Политика** → **Политики паролей** нажать кнопку **Добавить**.
3. В открывшемся окне указать группу пользователей, приоритет и нажать кнопку **Добавить**:



4. Выбрать созданную парольную политику в списке



5. Настроить атрибуты политики и нажать кнопку **Сохранить**:



Глава 31. Двухфакторная аутентификация

Использование двухфакторной аутентификации (2FA) — это один из способов повысить безопасность аутентификации. Одним из распространённых методов 2FA является одноразовый пароль (OTP). Существуют открытые стандарты OTP:

- HOTP (на основе счётчика) — RFC 4226
- TOTP (на основе времени) — RFC 6238

31.1. Методы аутентификации

Во FreeIPA методы аутентификации можно задавать глобально или для отдельного пользователя. Если указано несколько методов, разрешается использовать любой из них (логическое ИЛИ).

Определены следующие методы аутентификации пользователей (но не все могут быть реализованы):

- Пароль
- RADIUS
- Двухфакторная аутентификация (пароль + OTP)
- PKINIT
- Пароль с усиленной защитой (SPAKE или FAST)
- External Identity Provider
- Passkey
- Отключить переопределение на уровне пользователя (только в глобальной конфигурации)

Если значение не задано, используется парольная аутентификация.

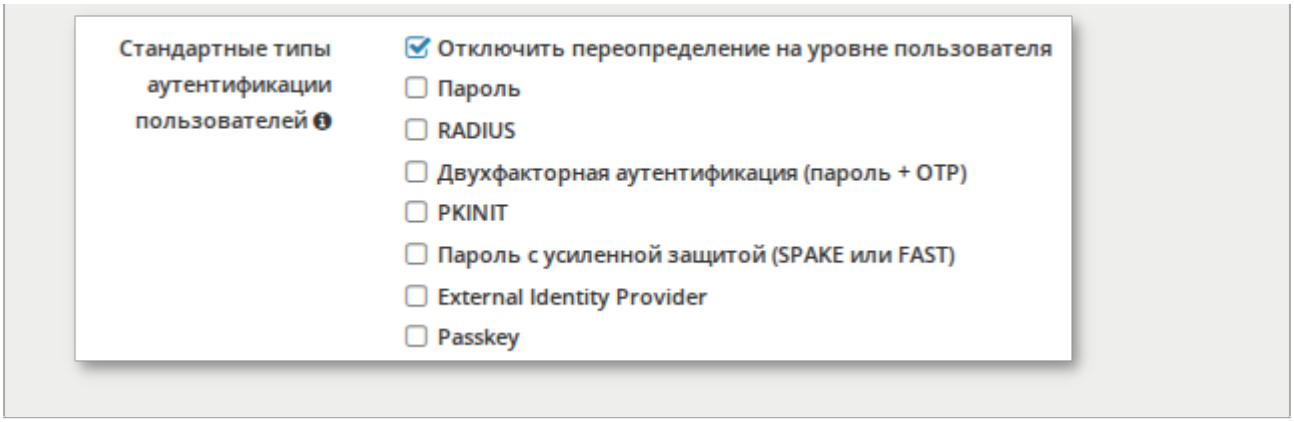
Примечание

Двухфакторная аутентификация означает «использовать пароль и значение OTP». Если для пользователя установлен метод ***двухфакторная аутентификация***, но у него нет токенов, разрешается вход только по паролю. Как только токен добавлен, требуется пароль + OTP.

По умолчанию пользовательские настройки аутентификации имеют приоритет над глобальными настройками. Если для пользователя не задан метод аутентификации, применяются глобально заданные методы.

Примечание

Опция **`Отключить переопределение на уровне пользователя`** (доступна только глобально) позволяет отключить пользовательские настройки аутентификации. Для всех пользователей будут применяться глобальные настройки.



Только администраторы могут изменять методы аутентификации (глобально или для каждого пользователя).

31.2. Разрешения (Permissions)

У токена может быть один владелец или ни одного (в этом случае токен считается неназначенным). У владельца токена есть следующие права:

- чтение (read)
- аутентификация (authenticate)
- синхронизация (synchronize)

У токенов может быть несколько менеджеров. У менеджера токена есть следующие права:

- чтение (read)
- изменение (write)
- удаление (delete)

Примечание

Нельзя удалить последний активный токен, если он принадлежит текущему пользователю.

Администраторы могут создавать токены для любых пользователей. Обычные пользователи могут создавать токены только для себя (становясь владельцем и менеджером).

31.3. Управление функциями

31.3.1. Веб-интерфейс

31.3.1.1. Методы аутентификации

Глобальные методы аутентификации доступны на вкладке настроек сервера (**IPA-сервер** → **Конфигурация** → **Стандартные типы аутентификации пользователей**).

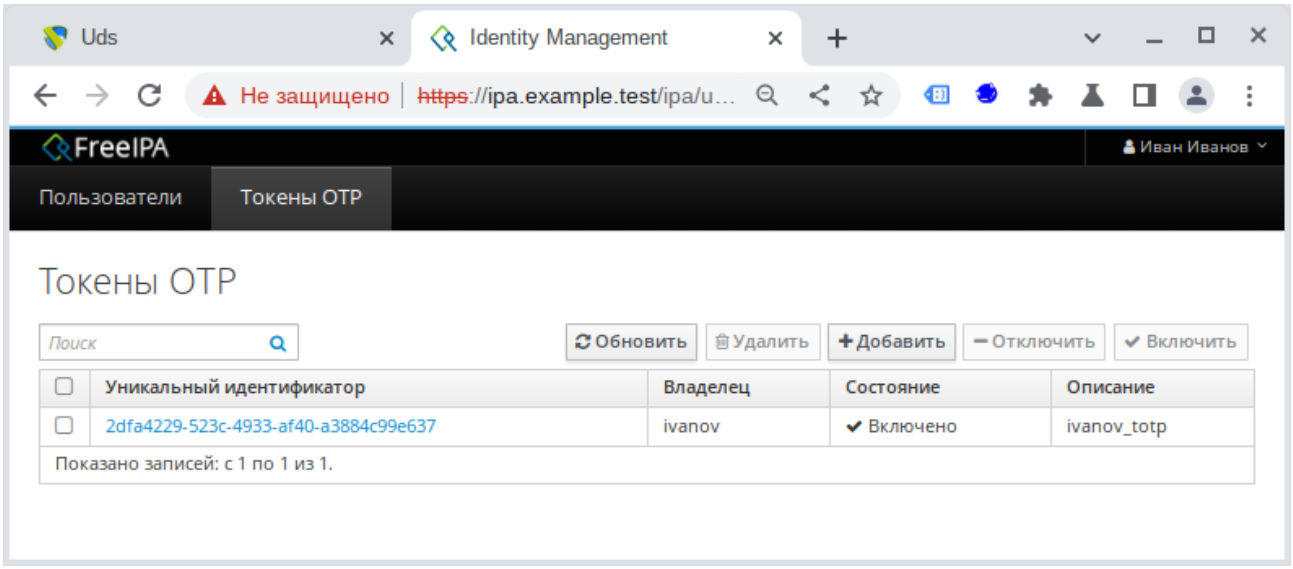
Методы аутентификации для отдельного пользователя доступны на странице пользователя (**Идентификация → Пользователи → Пользователь → Типы аутентификации пользователей**).

31.3.1.2. Конфигурация прокси-сервера RADIUS

Администраторам доступна вкладка **Аутентификация → Серверы RADIUS** для управления прокси-серверами RADIUS. Эти серверы могут быть назначены отдельным пользователям на странице конкретного пользователя.

31.3.1.3. OTP-токены

Пользователям доступна вкладка для управления токенами (**Токены OTP**), где можно добавлять, удалять и редактировать самоназначаемые/управляемые токены:



Администраторы на вкладке **Токены OTP** могут управлять токенами всех пользователей.

Ссылка на синхронизацию токена доступна на странице входа в систему FreeIPA.

31.3.2. Командная строка

31.3.2.1. Методы аутентификации

Таблица 31.1. Команды

Описание	Команда	Опции
Изменение глобальных методов аутентификации	**`config-mod`**	**`--user-auth-type=`*`password/otp/radius`***
Изменение метода аутентификации пользователя	**`user-mod`**	**`--user-auth-type=`*`password/otp/radius`* `--radius=`*`STR`*, `--radius-username=`*`STR`***

Примеры:

- глобально установить метод аутентификации **`Двухфакторная аутентификация (пароль + OTP)`**:

```
$ ipa config-mod --user-auth-type=otp
```

- установить для пользователя ivanov метод аутентификации **Двухфакторная аутентификация (пароль + OTP)**:

```
$ ipa user-mod ivanov --user-auth-type=otp
```

31.3.2.2. Конфигурация сервера RADIUS

Таблица 31.2. Команды

Описание	Команда	Опции
Добавить сервер RADIUS	**radiusproxy-add**	NAME --desc=STR --server=STR --secret --timeout=INT --retries=INT --userattr=STR
Найти сервер RADIUS	**radiusproxy-find**	--name=STR --desc=STR --server=STR --timeout=INT --retries=INT --userattr=STR
Изменить сервер RADIUS	**radiusproxy-mod**	--rename=STR --desc=STR --server=STR --secret --timeout=INT --retries=INT --userattr=STR
Удалить сервер RADIUS	**radiusproxy-del**	
Показать информацию о сервере RADIUS	**radiusproxy-show**	

Примеры:

- добавить сервер RADIUS:

```
$ ipa radiusproxy-add freeradius_test --server=192.168.0.101 --secret
Секрет:
Введите Секрет ещё раз для проверки:
-----------------------------------------------
Добавлен прокси-сервер RADIUS "freeradius_test"
-----------------------------------------------
  Имя прокси-сервера RADIUS: freeradius_test
  Сервер: 192.168.0.101
  Секрет: cGFzc3dvcmQ=
```

- показать информацию о сервере RADIUS:

```
$ ipa radiusproxy-show freeradius_test
  Имя прокси-сервера RADIUS: freeradius_test
  Сервер: 192.168.0.101
```

31.3.2.3. OTP-токены

Таблица 31.3. Команды

Описание	Команда	Опции
Добавить токен	**otptoken-add**	--type=STRENUM --desc=STR --owner=LOGIN --disabled=BOOL --not-before=STR --not-after=STR --vendor=STR --model=STR --serial=STR --key=STR --algo=STRENUM --digits=6/8 --offset=INT --interval=INT --no-qrcode
Добавить менеджера для токена	**otptoken-add-managedby**	--users=STR
Добавить токен yubikey	**otptoken-add-yubikey**	--desc=STR --owner=LOGIN --disabled=BOOL --notbefore=STR --not-after=STR --digits=6/8 --slot=1/2
Удалить токен	**otptoken-del**	
Найти токен	**otptoken-find**	--type=STRENUM --desc=STR --owner=LOGIN --disabled=BOOL --not-before=STR --not-after=STR --vendor=STR --model=STR --serial=STR --algo=STRENUM --digits=6/8 --offset=INT --interval=INT --id=STR
Изменить токен	**otptoken-mod**	--rename=STR --desc=STR --owner=LOGIN --disabled=BOOL --not-before=STR --not-after=STR --vendor=STR --model=STR --serial=STR
Удалить менеджера токена	**otptoken-remove-managedby**	--users=STR
Показать информацию о токене	**otptoken-show**	
Выполнить синхронизацию токена	**otptoken-sync**	--user=STR --password --first-code --second-code

Примеры:

- добавить токен для пользователя ivanov:

```
$ ipa otptoken-add ivanov_otp --type=TOTP --desc=ivanov_token --owner=ivanov
-----------------------------
Добавлен токен OTP "ivanov_otp"
-----------------------------
  Уникальный идентификатор: ivanov_otp
  Тип: TOTP
  Описание: ivanov_token
  Владелец: ivanov
  Ключ: mW+LBliuxKjy3PCb/JKOszbZGmTElSrhIg70E3QruXqu+W4=
  Алгоритм: sha1
```

```
  Цифры: 6
  Смещение времени: 0
  Временной интервал: 30
  Универсальный код ресурса (URI):
  otpauth://totp/ivanov@EXAMPLE.TEST:ivanov_otp?issuer=ivanov%40EXAMPLE.TEST

&secret=TFXYWBSYV3CKR4W46CN7ZEUOWM3NSGTEYSKSVYJCB32BG5BLXF5K56LO&digits=6&algo
rithm=SHA1&period=30
```

- назначить пользователя ivanov менеджером токена:

```
$ ipa otptoken-add-managedby ivanov_otp --users=ivanov
  Уникальный идентификатор: ivanov_otp
  Описание: ivanov_token
  Владелец: uid=ivanov,cn=users,cn=accounts,dc=example,dc=test
  Руководитель: ivanov
----------------------------------
Количество добавленных участников 1
----------------------------------
```

- удалить токен:

```
$ ipa otptoken-del
Уникальный идентификатор: ivanov_otp
-----------------------------
Удалён токен OTP "ivanov_otp"
-----------------------------
```

31.4. Пример настройки двухфакторной аутентификации

31.4.1. Командная строка

Создать нового пользователя:

```
$ kinit admin
Password for admin@EXAMPLE.TEST:

$ ipa user-add otptest
Имя: OTP
Фамилия: test
-------------------------------
Добавлен пользователь "otptest"
-------------------------------
  Имя учётной записи пользователя: otptest
  Имя: OTP
  Фамилия: test
  Полное имя: OTP test
  Отображаемое имя: OTP test
  Инициалы: Ot
  Домашний каталог: /home/otptest
  GECOS: OTP test
  Оболочка входа: /bin/bash
  Имя учётной записи: otptest@EXAMPLE.TEST
  Псевдоним учётной записи: otptest@EXAMPLE.TEST
  Адрес электронной почты: otptest@example.test
  UID: 587200007
```

```
  ID группы: 587200007
  Пароль: False
  Участник групп: ipausers
  Доступные ключи Kerberos: False

$ ipa passwd otptest
Новый пароль:
Введите Новый пароль ещё раз для проверки:
-----------------------------------
Изменён пароль "otptest@EXAMPLE.TEST"
-----------------------------------

$ kinit otptest
Password for otptest@EXAMPLE.TEST:
Password expired.  You must change it now.
Enter new password:
Enter it again:
```

Включить тип аутентификации **Двухфакторная аутентификация** для созданного пользователя:

```
$ kinit admin
Password for admin@EXAMPLE.TEST:

$ ipa user-mod otptest --user-auth-type=otp
-----------------------------
Изменён пользователь "otptest"
-----------------------------
  Имя учётной записи пользователя: otptest
  Имя: OTP
  Фамилия: test
  Домашний каталог: /home/otptest
  Оболочка входа: /bin/bash
  Имя учётной записи: otptest@EXAMPLE.TEST
  Псевдоним учётной записи: otptest@EXAMPLE.TEST
  Адрес электронной почты: otptest@example.test
  UID: 587200007
  ID группы: 587200007
  Типы аутентификации пользователей: otp
  Учётная запись отключена: False
  Пароль: True
  Участник групп: ipausers
  Доступные ключи Kerberos: True
```

Добавить токен:

```
$ ipa otptoken-add \
  --type=TOTP \
  --desc=otptest_token \
  --owner=otptest \
  --algo=sha1 \
  --digits=6 \
  --interval=30

Password for admin@EXAMPLE.TEST:

$ ipa user-mod otptest --user-auth-type=otp
---------------------
Добавлен токен OTP ""
```

```
--------------------
  Уникальный идентификатор: 33014fa0-0d7f-4775-a05c-05f09c6ff8e6
  Тип: TOTP
  Описание: otptest_token
  Владелец: otptest
  Ключ: hzNKJClpoG/nB0aer4/XQRfh7deLpTj0WKvaxNcZqAWX9SY=
  Алгоритм: sha1
  Цифры: 6
  Смещение времени: 0
  Временной интервал: 30
  Универсальный код ресурса (URI):
  otpauth://totp/otptest@EXAMPLE.TEST:33014fa0-0d7f-4775-a05c-05f09c6ff8e6?
issuer=otptest%40EXAMPLE.TEST

&secret=Q4ZUUJBJNGQG7ZYHI2PK7D6XIEL6D3OXROSTR5CYVPNMJVYZVACZP5JG&digits=6&algorit
hm=SHA1&period=30
```

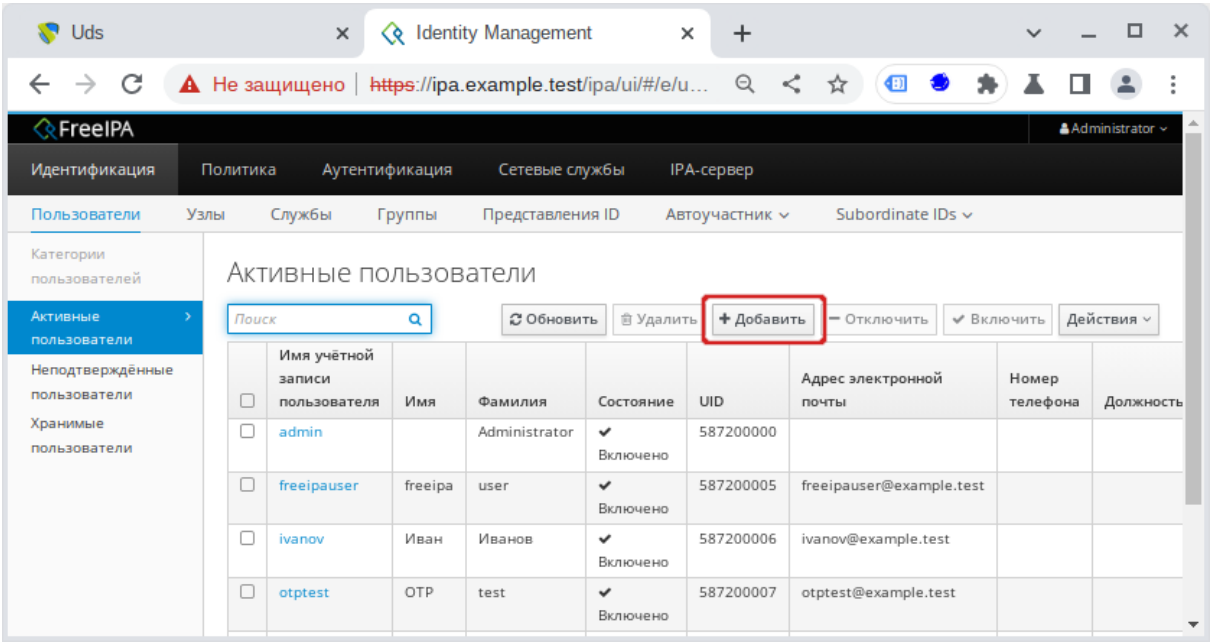
Отсканировать полученный QR-код с помощью FreeOTP или аналогичного приложени.

31.4.2. Веб-интерфейс

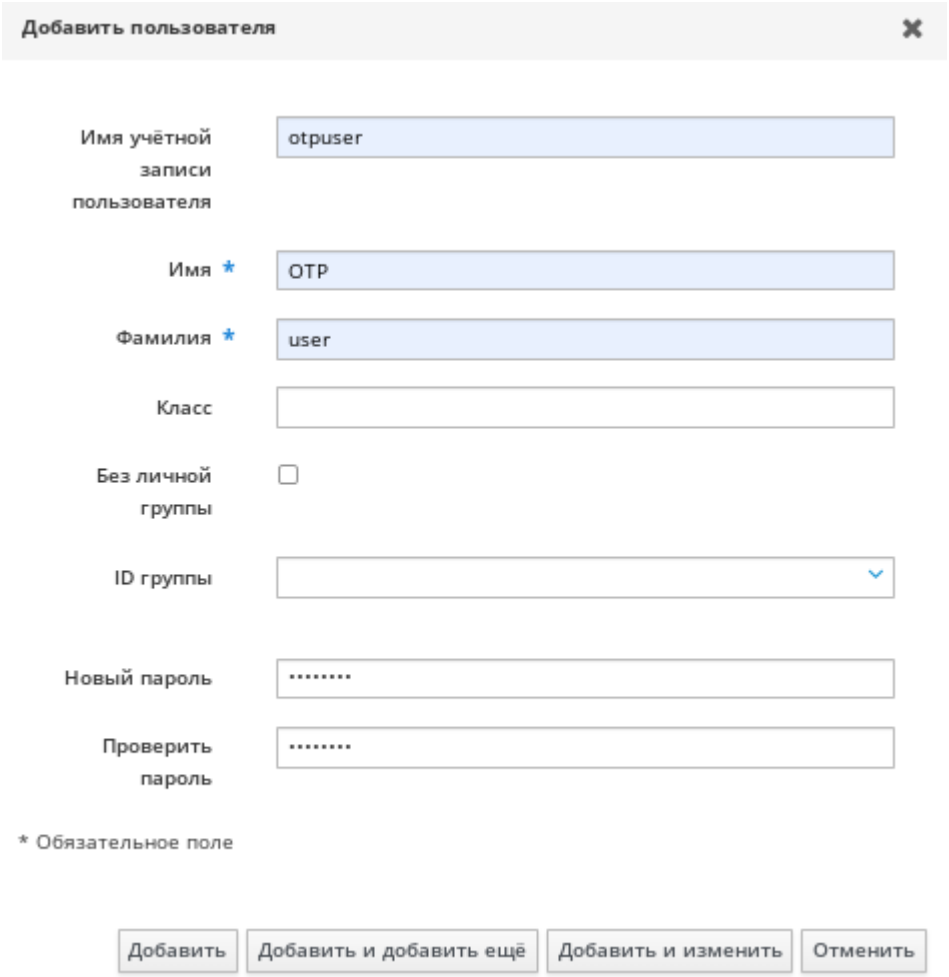
Для добавления новых пользователей можно воспользоваться веб-интерфейсом FreeIPA:

1. Открыть в веб-браузере адрес **`https://ipa.example.test/ipa/ui/`** и ввести данные администратора для входа в систему.

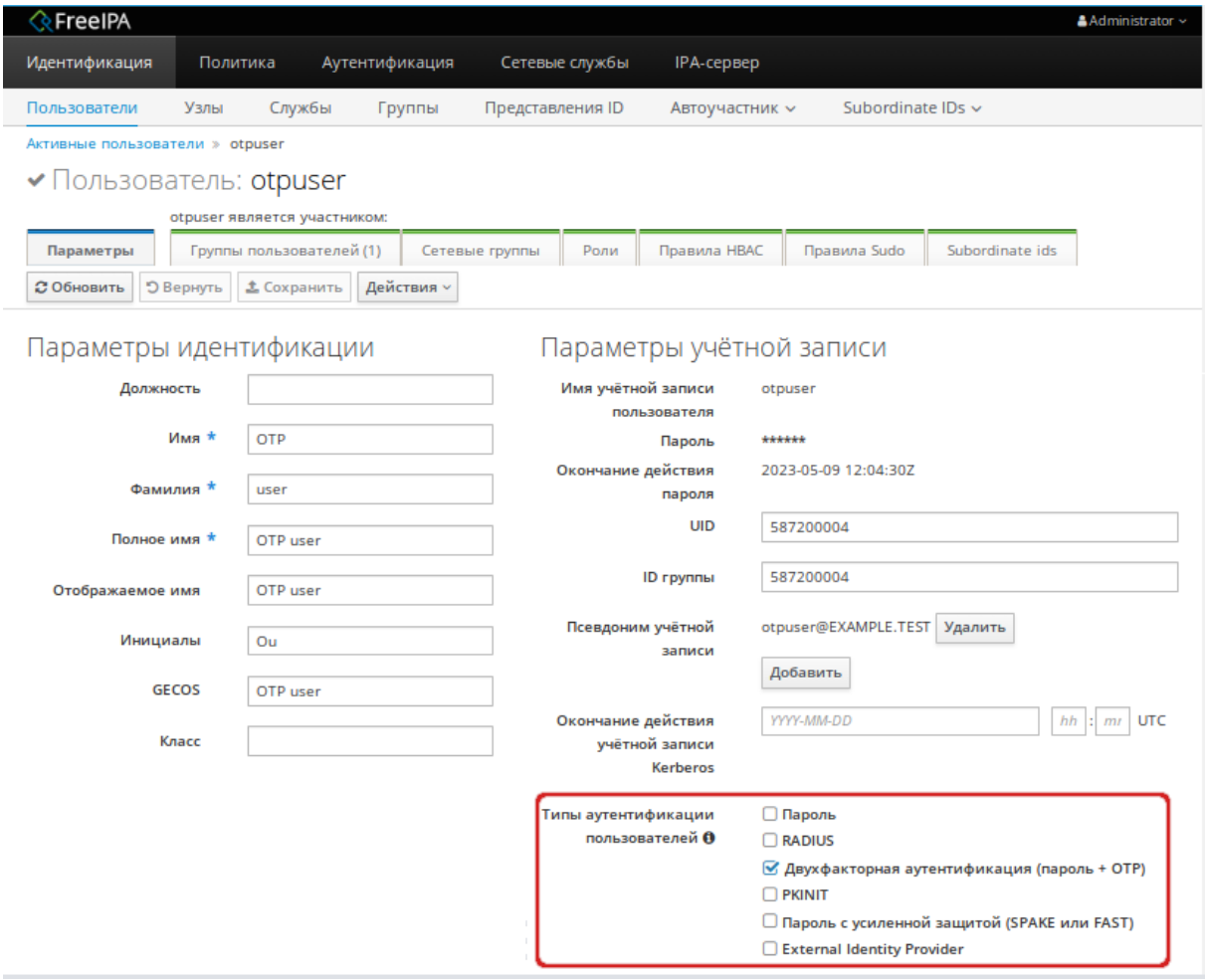
2. В окне **`Активные пользователи`** нажать кнопку **`Добавить`**:



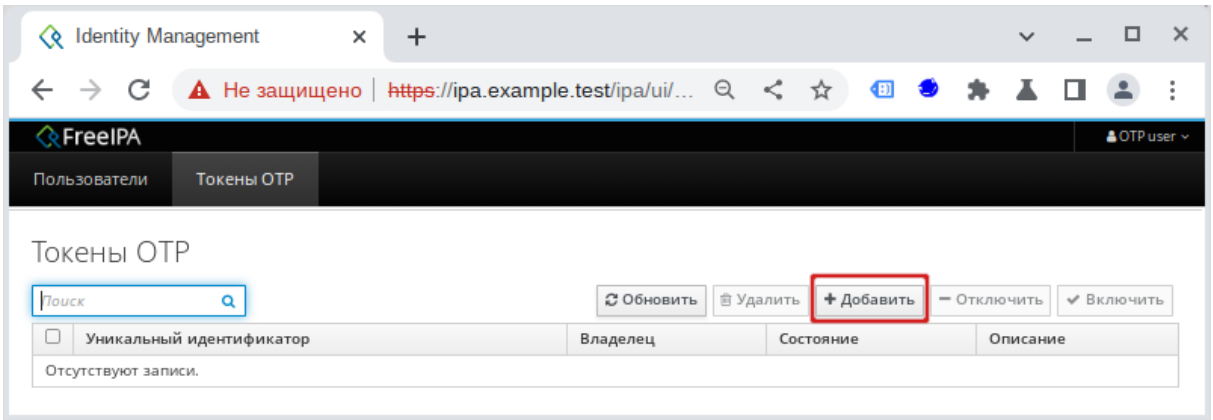
3. В открывшемся окне ввести данные пользователя и нажать кнопку **`Добавить`**:

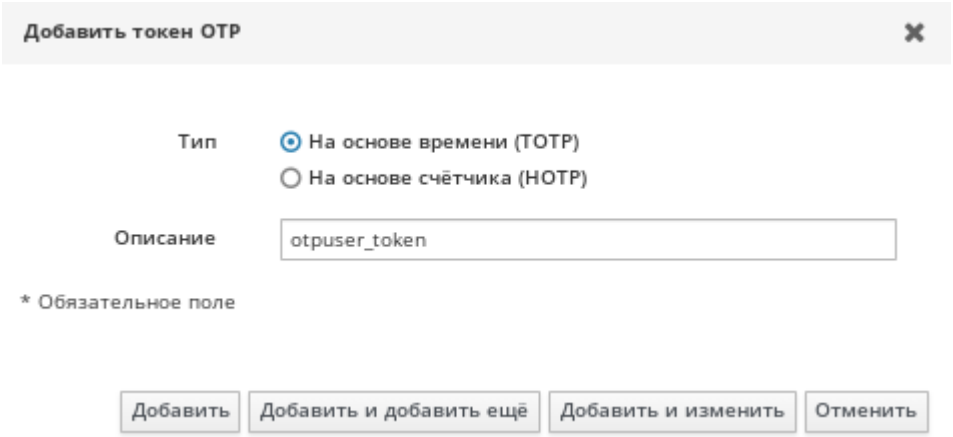


4. Выбрать созданного пользователя в списке пользователей и установить отметку в поле **`Двухфакторная аутентификация (пароль + OTP)`**:



5. Создать токен OTP. Это можно сделать, как под учётной записью администратора, так и авторизовавшись в веб-интерфейсе под учётной записью пользователя.

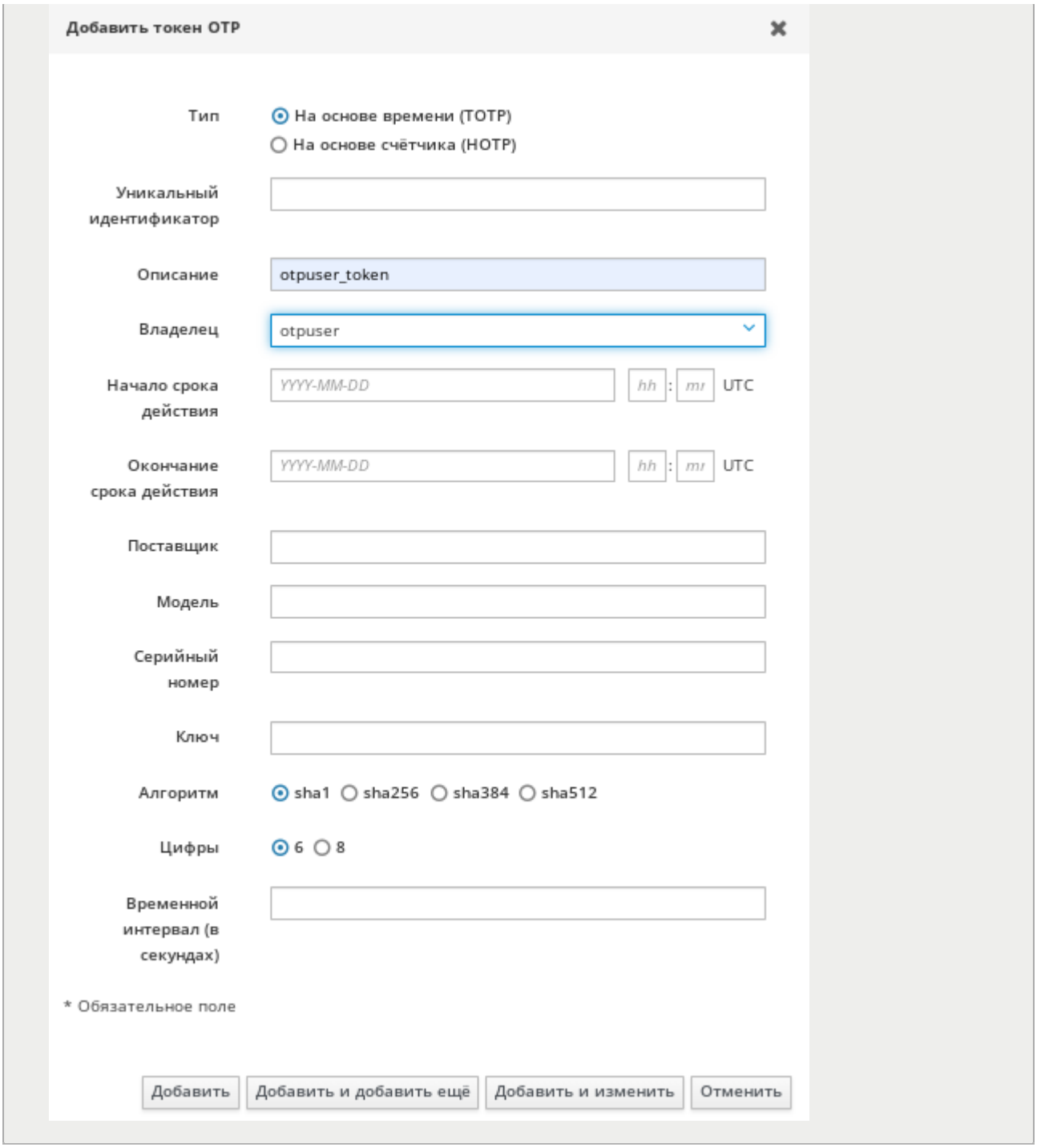




6. Отсканировать полученный QR-код с помощью FreeOTP или аналогичного приложени.

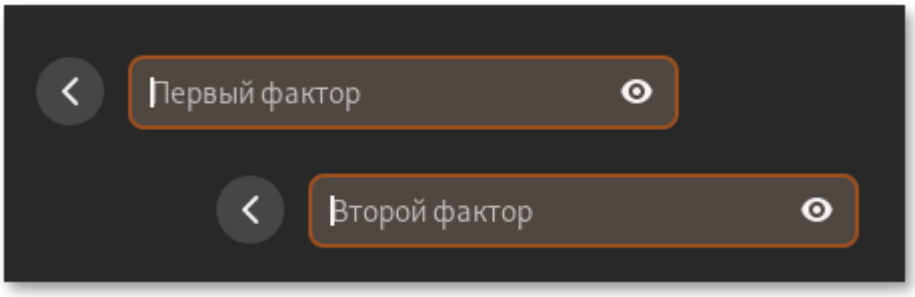
Примечание

Окно добавления токена под учётной записью администратора (**Аутентификация** → **Токены OTP** → **Добавить**):

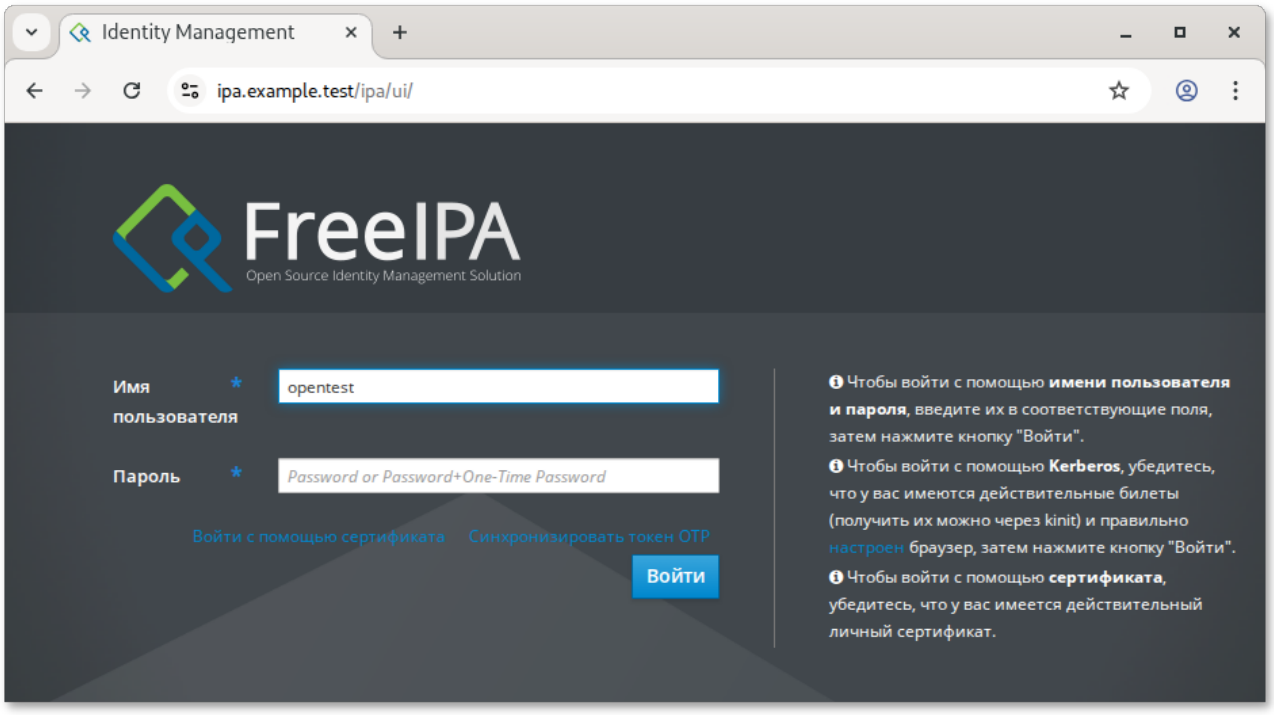


31.5. Аутентификация

При аутентификации на клиенте после ввода логина учётной записи FreeIPA необходимо последовательно ввести пароль (первый фактор) и код токена (второй фактор):



При аутентификации в веб-интерфейсе FreeIPA в поле **Пароль** необходимо ввести пароль и код токена слитно, без пробелов (в форме <пароль><код токена>):



Глава 32. Примечания

32.1. Настройка беспарольного доступа по SSH

Генерация SSH-ключа (на узле управления):

```
$ ssh-keygen -t ed25519
```

На запрос о файле для сохранения ключа можно нажать **Enter** (используется путь по умолчанию). На запрос о пароле для ключа можно также нажать **Enter** (без установки пароля).

Скопировать публичную часть SSH-ключа на управляемый узел для пользователя user:

```
$ ssh-copy-id -i ~/.ssh/id_ed25519.pub user@comp01.example.test
```

Скопировать публичную часть SSH-ключа на управляемый узел для администратора (root). Для этого подключиться к управляемому узлу от имени пользователя user, переключиться на пользователя root и скопировать публичную часть ключа:

```
$ ssh user@comp01.example.test
[user@comp01 ~]$ su -
Password:
[root@comp01 ~]# cat /home/user/.ssh/authorized_keys >>.ssh/authorized_keys
[root@comp01 ~]# exit
выход
[user@comp01 ~]$ exit
выход
Connection to comp01 closed.
```

Теперь можно подключаться удалённо выполнять команды на управляемом узле с привилегиями администратора (root) без ввода пароля.

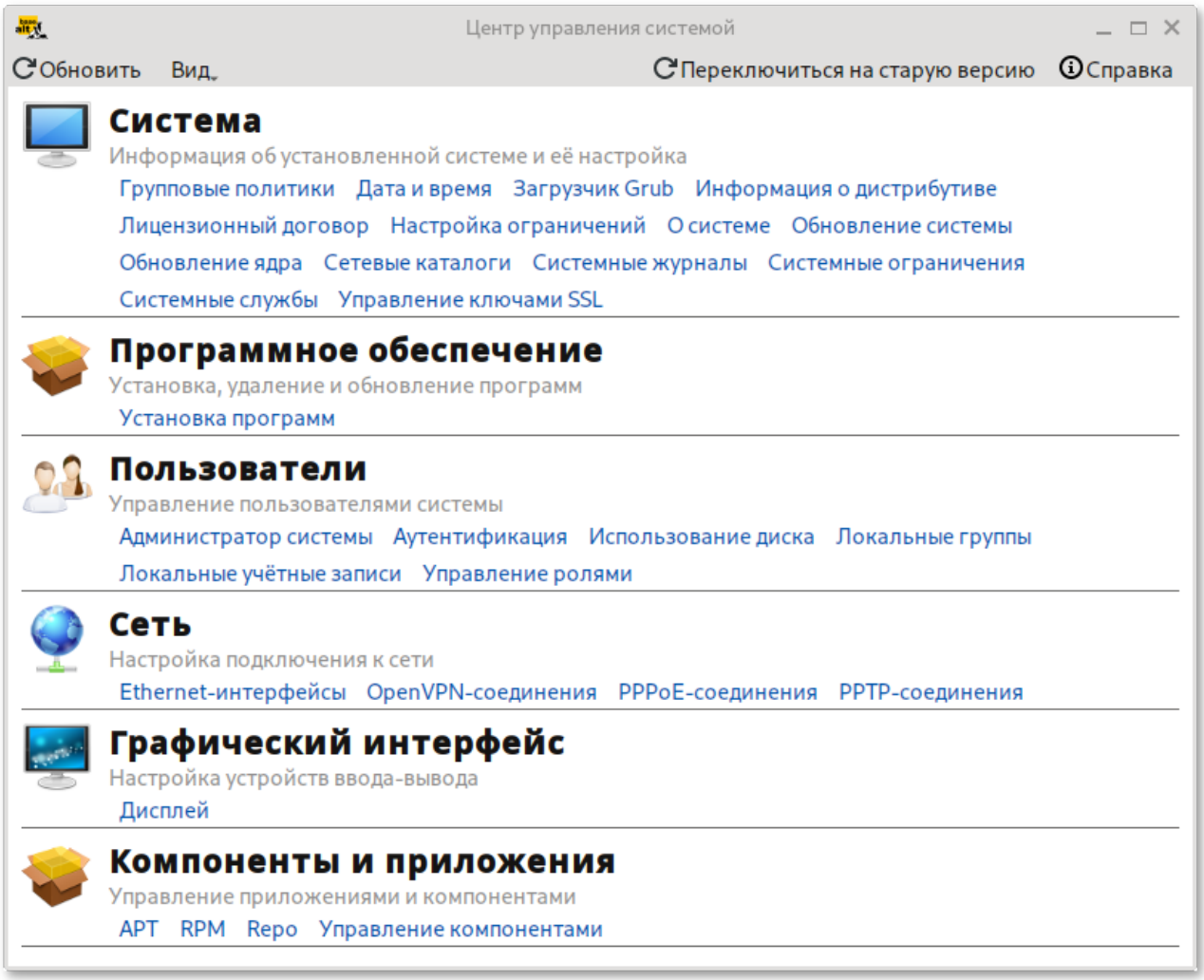
32.2. Центр управления системой

Центр управления системой (ЦУС, альтератор) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

ЦУС состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

Запустить ЦУС в графической среде можно следующими способами:

- в графической среде MATE: **Система** → **Администрирование** → **Центр управления системой**;
- в графической среде XFCE, KDE: **Меню запуска приложений** → **Настройки** → **Центр управления системой**;
- из командной строки: командой **`acc`**.



ЦУС имеет также веб-ориентированный интерфейс, позволяющий управлять сервером с любого компьютера сети.

Для запуска веб-ориентированного интерфейса, должен быть установлен пакет *alterator-fbi*:

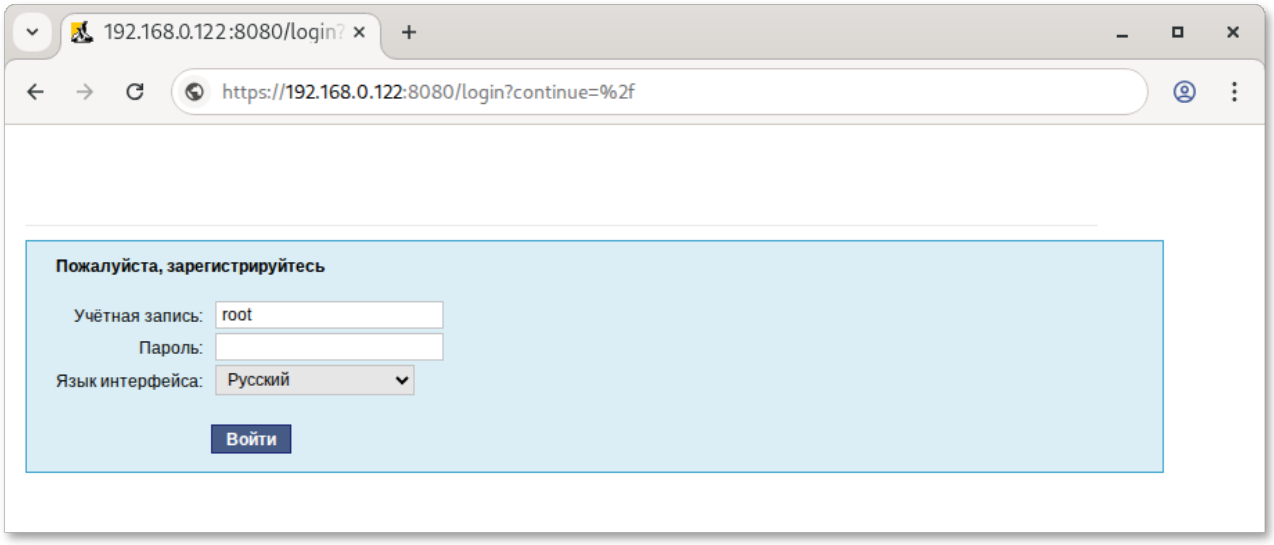
```
# apt-get install alterator-fbi
```

И запущены сервисы **ahttpd** и **alteratord**:

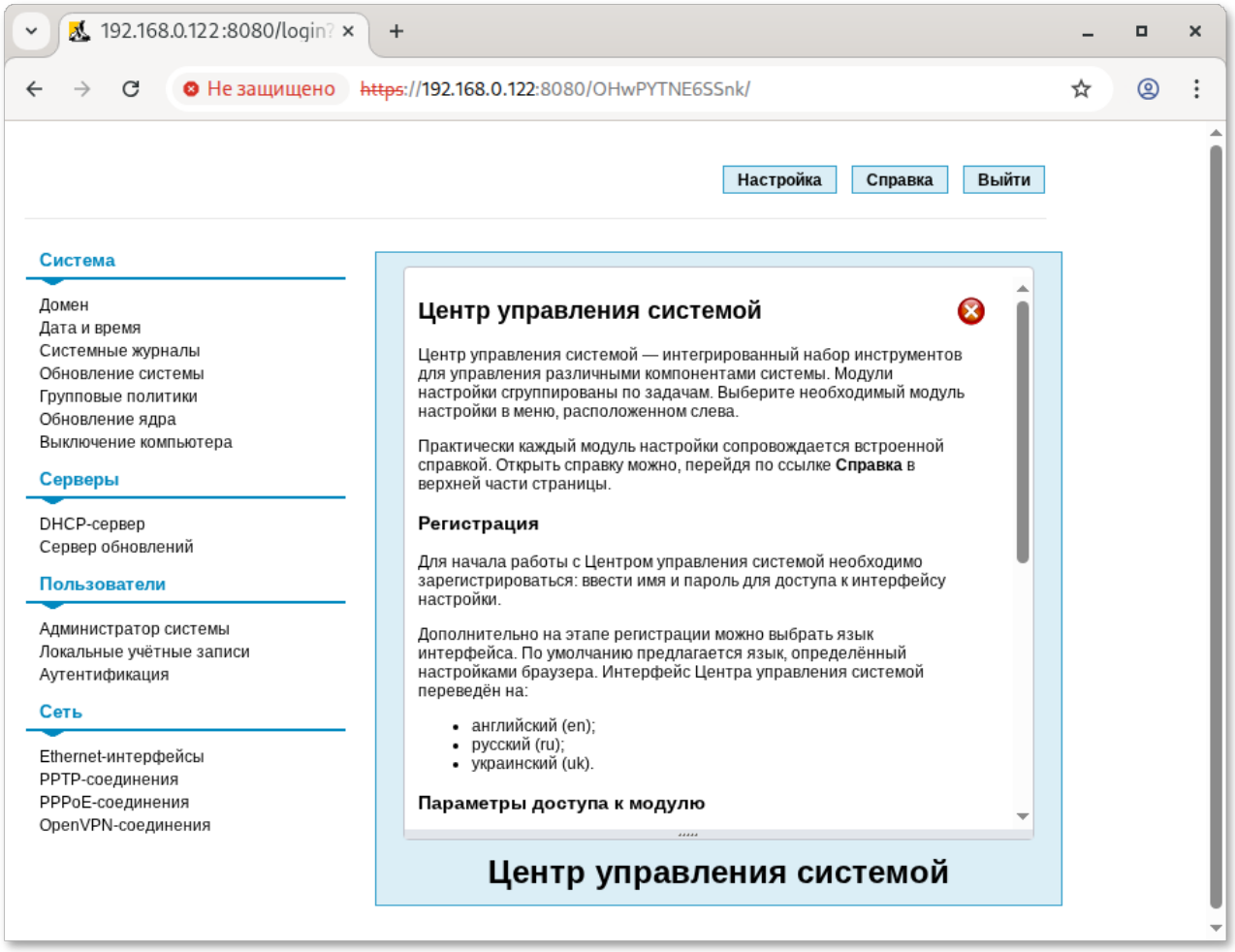
```
# systemctl enable --now ahttpd
# systemctl enable --now alteratord
```

Работа с ЦУС может происходить из любого веб-браузера. Для начала работы необходимо перейти по адресу **https://ip-адрес:8080/**.

При запуске центра управления системой необходимо ввести в соответствующие поля имя пользователя (**root**) и пароль пользователя:



После этого будут доступны все возможности ЦУС на той машине, к которой было произведено подключение через веб-интерфейс.



Установленные пакеты, которые относятся к ЦУС, можно посмотреть, выполнив команду:

```
rpm -qa | grep alterator*
```

Прочие пакеты для ЦУС можно найти, выполнив команду:

```
apt-cache search alterator*
```

Модули можно дополнительно загружать и удалять как обычные программы:

```
# apt-get install alterator-net-openvpn
# apt-get remove alterator-net-openvpn
```