



Доменная инфраструктура на базе FreeIPA

Руководство пользователя

Редакция сентябрь, 2023

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.

I. Разворачивание FreeIPA

1. Подготовка системы к установке сервера FreeIPA
2. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA
3. Установка сервера FreeIPA в режиме CA-less
4. Завершение установки
5. Отладочная информация
6. Удаление сервера FreeIPA

II. Доступ к службам FreeIPA

7. Интерфейс командной строки FreeIPA
8. Веб-интерфейс FreeIPA

9. Журналирование FreeIPA

III. Настройка репликации

- 10. Системные требования
- 11. Системные требования
- 12. Параметры утилиты ipa-replica-install
- 13. Установка реплики
- 14. Отладочная информация
- 15. Удаление реплики

IV. Разворачивание клиента FreeIPA

- 16. Подготовка системы к установке клиента FreeIPA
- 17. Установка пакетов
- 18. Подключение к серверу
- 19. Проверка клиента FreeIPA
- 20. Отладочная информация
- 21. Повторная регистрация клиента FreeIPA
- 22. Удаление клиента FreeIPA

V. Ansible

- 23. Предварительные настройки
- 24. Установка FreeIPA сервера с помощью Ansible
- 25. Установка FreeIPA клиентов с помощью Ansible

VI. Интеграция с AD

- 26. Настройка DNS
- 27. Подготовка сервера FreeIPA к доверию
- 28. Настройка доверия
- 29. Удаление доверия

VII. Конфигурирование FreeIPA

- 30. Управление пользователями
- 31. Двухфакторная аутентификация

32. Примечания

Часть I. Разворачивание FreeIPA

В этой части приводится общая информация по разворачиванию FreeIPA.

Содержание

1. Подготовка системы к установке сервера FreeIPA
2. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA
3. Установка сервера FreeIPA в режиме CA-less
4. Завершение установки
5. Отладочная информация
6. Удаление сервера FreeIPA

Глава 1. Подготовка системы к установке сервера FreeIPA

- 1.1. Системные требования к серверу FreeIPA
- 1.2. Поддержка типов шифрования в FreeIPA
- 1.3. Синхронизация времени
- 1.4. Имя узла и требования к DNS
- 1.5. Требования к портам
- 1.6. Подготовка сервера
- 1.7. Установка пакетов
- 1.8. Параметры команд установки 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 в чистой системе, в которой отсутствуют какие-либо пользовательские настройки служб: DNS, Kerberos, Apache и Directory Server.

FreeIPA при настройке домена перезаписывает системные файлы. FreeIPA создает резервные копии исходных системных файлов в **/var/lib/ipa/sysrestore/**. При удалении сервера FreeIPA, эти файлы восстанавливаются.

1.1.1. RAM

Для установки с СА требуется минимально 1,2 ГБ RAM. Для демонстрационной/тестовой системы рекомендуется 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

Без правильно настроенной конфигурации DNS не будут работать должным образом Kerberos и SSL.



Важно

Домен DNS не может быть изменен после установки.

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

- имя узла не может быть localhost или localhost6;
- имя узла должно быть полным (например, ipa.example.test);
- имя узла должно быть разрешимым;
- обратный адрес должен совпадать с именем хоста.

Не следует использовать существующий домен, если вы не являетесь владельцем домена. Рекомендуется использовать зарезервированный домен верхнего уровня RFC2606 (<https://tools.ietf.org/html/rfc2606>) для частных тестовых установок, например, ipa.test.

1.1.3. IPv6

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



Примечание

IPv6 не обязательно должен быть включен в сети.

1.2. Поддержка типов шифрования в FreeIPA

1.3. Синхронизация времени

1.4. Имя узла и требования к DNS

1.5. Требования к портам

Таблица 1.1. Порты FreeIPA

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

1.6. 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.

Отключить ahttpd, работающий на порту 8080, во избежание конфликтов с разворачиваемым tomcat и отключить HTTPS в Apache2:

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

Для ускорения установки можно установить демон энтропии haveged:

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

1.7. Установка пакетов

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

- для установки FreeIPA без интегрированного DNS-сервера:

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

- для установки FreeIPA с интегрированным DNS-сервером:

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

- для установки FreeIPA с отношениями доверия с Active Directory:

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

1.8. 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	Включить отладку
-U, --unattended	Включает сеанс автоматической (пакетной) установки, который не запрашивает ввод данных пользователем
--hostname=<HOSTNAME>	Полное доменное имя (FQDN) сервера FreeIPA (например, server.ipa.example.test). Допускаются только цифры, строчные буквы и дефисы (-).
--ip-address=<IP_ADDRESS>	Указывает IP-адрес сервера. Эта опция принимает только IP-адреса, связанные с локальным интерфейсом. Опцию можно использовать несколько раз.
--dirsrv-config-file=<LDIF_file_name>	Путь к файлу LDIF, используемому для изменения конфигурации экземпляра сервера каталогов.
-n <DOMAIN_NAME>, --domain=<DOMAIN_NAME>	Имя домена сервера LDAP для использования в качестве домена FreeIPA.
-p <directory_manager_password>, --ds-password=<directory_manager_password>	Пароль суперпользователя cn=Directory Manager для службы LDAP.

Опция	Описание
-a <ipa_admin_password>, --admin-password=<ipa_admin_password>	Пароль для учетной записи администратора FreeIPA (admin) для аутентификации в области Kerberos. Для ipa-replica-install вместо этой опции используется параметр -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 эта опция указывает имя области Kerberos существующего развертывания FreeIPA.
--setup-dns	Указывает сценарию установки настроить службу DNS в домене FreeIPA.
--setup-ca	Установить и настроить CA на этой реплике. Если CA не настроен, операции с сертификатами перенаправляются на другую реплику с установленным CA. Для ipa-server-install CA устанавливается по умолчанию, и эту опцию не нужно указывать.

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

Опция	Описание
--ca-subject=<SUBJECT>	Задаёт различающееся имя субъекта сертификата CA (по умолчанию: CN=Certificate Authority,O=<REALM_NAME>). Относительные отличительные имена (RDN) располагаются в порядке LDAP, начиная с наиболее конкретного RDN.
--subject-base=<SUBJECT>	Указывает базу субъекта для сертификатов, выданных FreeIPA (по умолчанию O=<REALM_NAME>). Относительные отличительные имена (RDN) располагаются в порядке LDAP, начиная с наиболее конкретного RDN.
--external-ca	Создаёт запрос на подпись сертификата, который должен быть подписан внешним центром сертификации.
--external-ca-type={generic,ms-cs}	Тип внешнего CA
--ca-signing-algorithm={SHA1withRSA,SHA256withRSA,SHA384withRSA,SHA512withRSA}	Определяет алгоритм подписи сертификата CA FreeIPA. Значение по умолчанию SHA256withRSA. Этот параметр следует использовать с параметром --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	Создать зону DNS, даже если она уже существует.
--forwarder=<FORWARDERS>	Указывает сервер пересылки DNS для использования со службой DNS. Чтобы указать более одного сервера пересылки, можно использовать этот параметр несколько раз.
--no-forwarders	Использует корневые серверы со службой DNS вместо серверов пересылки.
--auto-forwarders	Использовать серверы пересылки DNS, указанные в /etc/resolv.conf .
--forward-policy={only,first}	Политика пересылки DNS для глобальных серверов пересылки.
--reverse-zone=<REVERSE_ZONE>	Указывает обратную зону DNS. Этот параметр можно использовать несколько раз.
--no-reverse	<p>Не создает обратную зону DNS при настройке домена DNS. Если обратная зона DNS уже настроена, используется эта существующая обратная зона DNS.</p> <p>Если этот параметр не используется, значение по умолчанию равно true. Это указывает сценарию установки настроить обратный DNS.</p>
--auto-reverse	Создать необходимые обратные зоны.
--no-dnssec-validation	Отключить проверку DNSSEC.

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

Опция	Описание
--ntp-server	Позволяет указать один NTP-сервер. Можно использовать несколько раз, чтобы указать несколько серверов.
--ntp-pool	Позволяет указать пул из нескольких серверов NTP, разрешенных как одно имя хоста.
-N, --no-ntp	Не настраивать и не запускать chronyd.

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

2.1. Интерактивная установка

2.2. В пакетном режиме

Преимущества установки сервера FreeIPA со встроенным DNS:

- можно автоматизировать большую часть обслуживания и управления записями DNS, используя инструменты FreeIPA. Например, записи DNS SRV создаются во время установки, а затем автоматически обновляются;
- можно иметь стабильное соединение с остальной частью Интернета, настроив, во время установки сервера FreeIPA, глобальные серверы пересылки. Глобальные серверы пересылки также полезны для доверительных отношений с Active Directory;
- можно настроить обратную зону DNS, чтобы электронные письма из домена FreeIPA не считались спамом почтовыми серверами за пределами домена FreeIPA.

Ограничения установки сервера FreeIPA со встроенным DNS:

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



Примечание

Если в команде **ipa-server-install** в конфигурации по умолчанию, не указаны CA параметры, например, **--external-ca** или **--ca-less**, сервер FreeIPA устанавливается с интегрированным CA.

2.1. Интерактивная установка

Для запуска интерактивной установки необходимо выполнить команду:

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

На первый вопрос, нужно ли сконфигурировать DNS-сервер BIND 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 пространство Kerberos:

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



Важно

Эти имена нельзя изменить после завершения установки.

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

Directory Manager password:
Password (confirm):



Предупреждение

Пароли должны быть не менее 8 символов.

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

IPA admin password:
Password (confirm):

Для настройки DNS на первый запрос, нужно ли настроить перенаправления, ответить да:

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

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

Following DNS servers are configured in /etc/resolv.conf: 127.0.0.1
Do you want to configure these servers as DNS forwarders? [yes]:

Также 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: 127.0.0.1, 8.8.8.8
Checking DNS forwarders, please wait ...
```



Примечание

Этот шаг необходим в том случае, если предполагается использовать внешний сервер для обработки запросов службы имен DNS.

Оставить значение по умолчанию для попытки найти обратные зоны:

```
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 192.168.0.162 [yes]: 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

Использование FreeIPA для управления обратными зонами не является обязательным.
Для этой цели можно использовать внешнюю службу DNS.

Указать имя NetBIOS:

NetBIOS domain name [EXAMPLE]:

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

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

Далее система 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: 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

Начнется процесс конфигурации. После его завершения будет выведена подсказка со следующими шагами:

=====
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. В пакетном режиме



Примечание

Скрипт установки **ipa-server-install** создает файл журнала **/var/log/ipaserver-install.log**, который может помочь определить проблему если установка завершилась ошибкой.

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
```

Для пакетной установки необходимо указать следующие параметры:

- » **-r REALM_NAME, --realm=REALM_NAME** — имя области Kerberos для сервера FreeIPA;
- » **-n DOMAIN_NAME, --domain=DOMAIN_NAME** — доменное имя;
- » **-p DM_PASSWORD, --ds-password=DM_PASSWORD** — пароль, который будет использоваться сервером каталогов для пользователя Менеджера каталогов (DM);
- » **-a ADMIN_PASSWORD, --admin-password=ADMIN_PASSWORD** — пароль пользователя admin, администратора FreeIPA;
- » **-U, --unattended** — позволить процессу установки выбрать параметры по умолчанию, не запрашивая у пользователя информацию;
- » **--hostname=HOST_NAME** — полное DNS-имя этого сервера.



Предупреждение

Пароли должны быть не менее 8 символов. Если пароль содержит специальные символы, следует заключить его в одинарные кавычки.

Чтобы установить сервер со встроенным DNS, должны также быть добавлены следующие параметры:

- » **--setup-dns** — создать зону DNS, если она еще не существует, и настроить DNS-сервер;
- » **--forwarder** или **--no-forwarders** — в зависимости от того, нужно ли настроить серверы пересылки DNS или нет;
- » **--auto-reverse** или **--no-reverse** — в зависимости от того, нужно ли настроить автоматическое обнаружение обратных зон DNS, которые должны быть созданы в FreeIPA DNS, или отключить автоматическое определение обратных зон;

» **--allow-zone-overlap** — создать зону DNS, 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 DNSSEC. Если в дальнейшем планируется настраивать доверительные отношения с Active Directory и настраивать сервер пересылки DNS, то DNSSEC необходимо выключить. Иначе сервер DNS от FreeIPA будет ожидать защищенного ответа от DNS Active Directory.



Примечание

Полный список параметров можно увидеть, запустив команду:

```
# ipa-server-install --help
```

Глава 3. Установка сервера FreeIPA в режиме CA-less

3.1. Подготовка сертификатов для сервера FreeIPA

3.2. Экспорт сертификатов в правильные форматы

3.3. Установка CA-less IPA

В этом разделе описывается, как можно установить сервер FreeIPA без центра сертификации (CA).

CA-less конфигурация требуется в тех случаях, когда по какой-либо причине нет возможности развернуть на FreeIPA сервис PKI dogtag. Например, на данный момент это невозможно сделать в некоторых сертифицированных конфигурациях.

Сертификаты, необходимые для установки сервера FreeIPA без центра сертификации (CA):

» сертификат LDAP-сервера и закрытый ключ:

■ **--dirsrv-cert-file** для указания сертификата и файлов закрытого ключа сервера LDAP;

■ **--dirsrv-pin** для указания пароля доступа к закрытому ключу;

» сертификат веб-сервера Apache и закрытый ключ:

■ **--http-cert-file** для указания сертификата и файлов закрытого ключа сервера Apache;

■ **--http-pin** для указания пароля доступа к закрытому ключу;

» полная цепочка сертификатов CA, выдавших сертификаты серверов LDAP и Apache:

■ **--dirsrv-cert-file** и **--http-cert-file** для файлов сертификатов с полной цепочкой сертификатов ЦС или ее частью;

■ файлы сертификатов для полной цепочки сертификатов CA:

- **--ca-cert-file** для файла или файлов, содержащих сертификат центра сертификации, который выдал сертификаты LDAP, Apache Server и Kerberos KDC;

■ сертификат PKINIT центра распространения ключей Kerberos (KDC) и закрытый ключ (опционально):

- **--pkinit-cert-file** для SSL-сертификата Kerberos KDC и закрытого ключа;
- **--pkinit-pin** для пароля доступа к закрытому ключу Kerberos KDC;
- **--no-pkinit** — отключить шаги настройки pkinit. Если не предоставить сертификат PKINIT, **ipa-server-install** настроит сервер FreeIPA с локальным KDC с самоподписанным сертификатом.

Файлы, предоставленные с помощью **--dirsrv-cert-file** и **--http-cert-file**, в сочетании с файлом, предоставленным с помощью **--ca-cert-file** должны содержать полную цепочку сертификатов CA, выдавших сертификаты сервера LDAP и Apache.

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
```

Создать базу данных NSS:

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

Создать noise файл, заполненный случайными числами:

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

Выполнить экспорт переменной CERT_SERIAL:

```
# export CERT_SERIAL=1
```

Создать CA сертификат:

```
# 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,0=IPA -o /tmp/servercert.req -k rsa -g
2048 -z ~/test_ca/noise.txt -f ~/test_ca/password.txt -a --extSKID
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 -a
```

В ответ на запросы команды дать следующие ответы:

```
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

Можно также создать отдельные сертификаты для серверов HTTP и Directory.

3.2. Экспорт сертификатов в правильные форматы

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

```
# 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 формат PEM:

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

3.3. Установка CA-less IPA

Установить пароль к закрытому ключу в значение переменной PSWD:

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

Установить CA-less IPA:

```
# 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 4.9.11

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 первый вопрос, нужно ли сконфигурировать DNS-сервер BIND 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 пространство Kerberos:

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



Важно

Эти имена 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 на первый запрос, нужно ли настроить перенаправления, ответить да:

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

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

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

Также можно добавить дополнительные серверы:

Enter an IP address for a DNS forwarder, or press Enter to skip: 8.8.8.8



Примечание

Этот шаг необходим в том случае, если предполагается использовать внешний сервер для обработки запросов службы имен DNS.

Оставить значение по умолчанию для попытки найти обратные зоны:

```
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 192.168.0.162 [yes]: 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

Использование FreeIPA для управления обратными зонами не является обязательным. Для этой цели можно использовать внешнюю службу DNS.

Указать имя NetBIOS:

NetBIOS domain name [EXAMPLE]:

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

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

Далее система 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
```

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

```
Forwarders:      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

Начнется процесс конфигурации. После его завершения будет выведена подсказка со следующими шагами:

```
=====
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:

- добавить делегирование DNS из родительского домена в домен DNS FreeIPA. Например, если DNS-домен FreeIPA — ipa.example.test, добавить запись сервера имен (NS) в родительский домен example.test;
- добавить запись службы _ntp._udp (SRV) для сервера времени в DNS (наличие записи SRV для сервера времени только что установленного сервера FreeIPA в DNS гарантирует, что будущие установки реплик и клиентов будут автоматически настроены для синхронизации с сервером времени, используемым этим первичным сервером FreeIPA):

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

Убедиться, что сервер FreeIPA работает:

```
$ kinit admin
Password for admin@EXAMPLE.TEST:
$ klist
Ticket cache: KEYRING:persistent:0:0
Default principal: admin@EXAMPLE.TEST

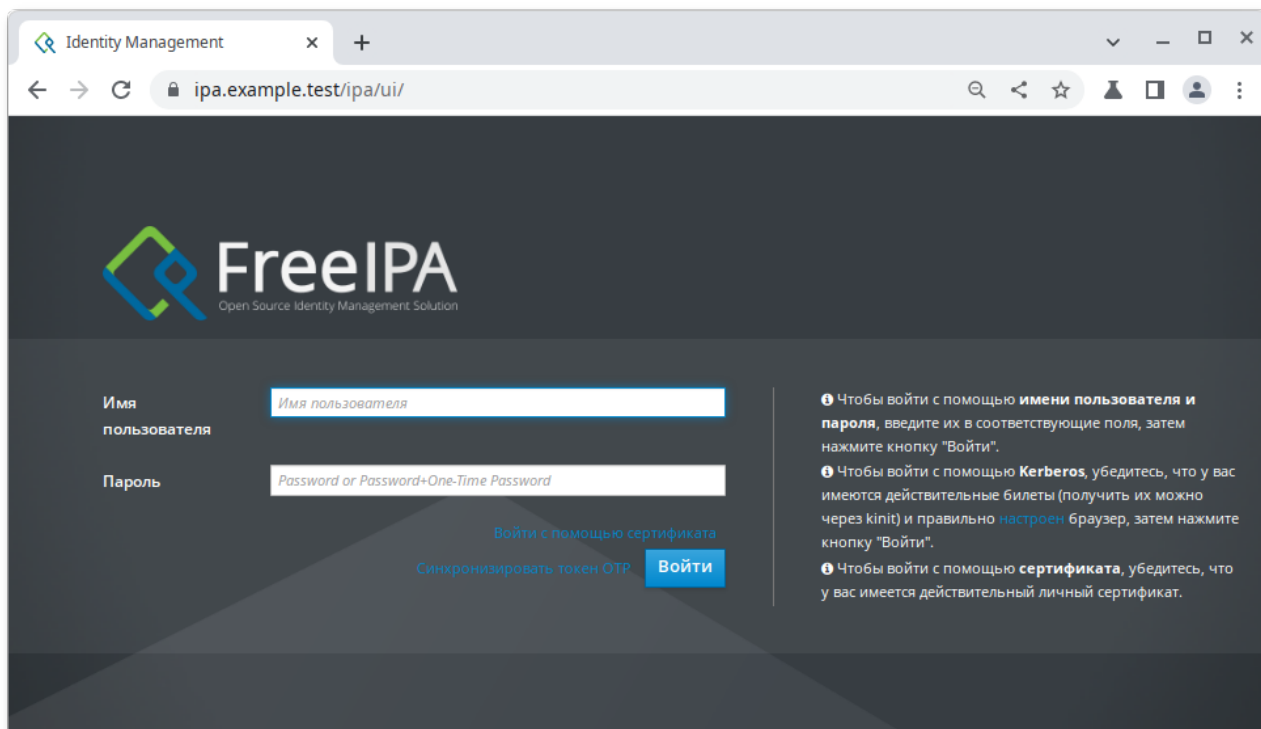
Valid starting          Expires                Service principal
29.08.2023 16:12:36    30.08.2023 15:51:19  krbtgt/EXAMPLE.TEST@EXAMPLE.TEST
```

Проверить статус подсистем FreeIPA:

```
# ipactl status
Directory Service: RUNNING
krb5kdc Service: RUNNING
kadmind 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
```

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



Глава 5. Отладочная информация

5.1. Удаление неудачной установки сервера FreeIPA

При установке сервера FreeIPA отладочная информация добавляется 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`

При установке CA отладочную информацию также можно просмотреть в:

- » `/var/log/pki/pki-ca-spawn.$TIME_OF_INSTALLATION.log` — общие вопросы, для процесса установки `pki-spawn`;
- » `journalctl -u pki-tomcatd@pki-tomcat`
- » `/var/log/pki/pki-tomcat/ca/debug.$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/pki/pki-tomcat/catalina.$DATE.log
```

5.1. Удаление неудачной установки сервера FreeIPA

В случае сбоя установки сервера FreeIPA некоторые файлы конфигурации могут быть уже сконфигурированы. В этом случае дополнительные попытки установить сервер FreeIPA завершатся неудачно, и сценарий установки сообщит, что FreeIPA уже настроен. Чтобы решить эту проблему следует удалить частичную конфигурацию сервера FreeIPA и повторить процесс установки.

Удалить частичную конфигурацию сервера FreeIPA:

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



Примечание

Если ошибки при установке сервера FreeIPA остаются, следует переустановить ОС. Одним из требований для установки сервера FreeIPA является чистая система без каких-либо настроек.

Глава 6. Удаление сервера FreeIPA

Процедура удаления сервера FreeIPA ipabackup.example.test:

1. Если в среде FreeIPA используется интегрированный DNS, необходимо 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 добавить роль DNS-сервера на другой сервер FreeIPA (см. **man ipa-dns-install(1)**).

2. Если в среде используется интегрированный CA:

- » убедиться, что ipabackup.example.test не является единственным 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 добавить роль CA-сервера на другой сервер FreeIPA (см. `man ipa-ca-install(1)`).

- если в среде были активированы 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 добавить роль сервера KRA на другой сервер FreeIPA (см. `man ipa-kra-install(1)`).

- убедиться, что `ipabackup.example.test` не является сервером обновления CA:

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

Если `ipabackup.example.test` является сервером обновления CA, необходимо переместить роль сервера обновления CA на другой сервер.

- убедиться, что `ipabackup.example.test` не является издателем текущего списка отзыва сертификатов (CRL):

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

Если вывод команды показывают, что генерация CRL включена на сервере `ipabackup.example.test`, следует переместить роль издателя CRL на другой сервер.

3. Подключиться к другому серверу в топологии:

```
$ ssh ipa_user@another_server
```

4. Получить учетные данные администратора FreeIPA:

```
$ kinit admin
```

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

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

6. Вернуться на ipabackup.example.test и удалить FreeIPA:

```
# 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 kadmind
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 записи DNS сервера имен (NS), указывающие на ipabackup.example.test, удалены из ваших зон DNS.

Часть II. Доступ к службам FreeIPA

Содержание

[7. Интерфейс командной строки FreeIPA](#)

[8. Веб-интерфейс FreeIPA](#)

Глава 7. Интерфейс командной строки FreeIPA

Администрировать FreeIPA можно в командной строке.



Примечание

Предварительно необходимо получить билет Kerberos для администратора FreeIPA:

```
$ kinit admin
```

Большинство административных действий FreeIPA можно выполнить с помощью команды **ipa**.
Список доступных команд:

```
$ 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.
...
```

Команды сгруппированы по типу объекта. Все объекты можно просмотреть, выполнив команду:
Список доступных команд:

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

Чтобы получить информацию по объекту (теме), используется команда:

```
$ ipa help <тема>
```

Например, вывести информацию об управлении службами сертификации:

```
$ ipa help ca
```

Чтобы получить справку по команде, используется команда:

```
$ ipa <команда> --help
```

или


```
$ ipa help <команда>
```

Например, вывести информацию о команде **ipa user-add**:

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

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

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

Например, вывести всех пользователей:

```
$ ipa user-find
```

Вывести все группы имя или описание которых содержит слово admin:

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

Вывести 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
```

Вывести подробную информацию о конкретной записи можно с помощью команд **ipa *-show**.
Например, вывести подробную информацию о узле comp01.example.test

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

Глава 8. Веб-интерфейс FreeIPA

8.1. Доступ к веб-интерфейсу

8.2. Использование билета Kerberos

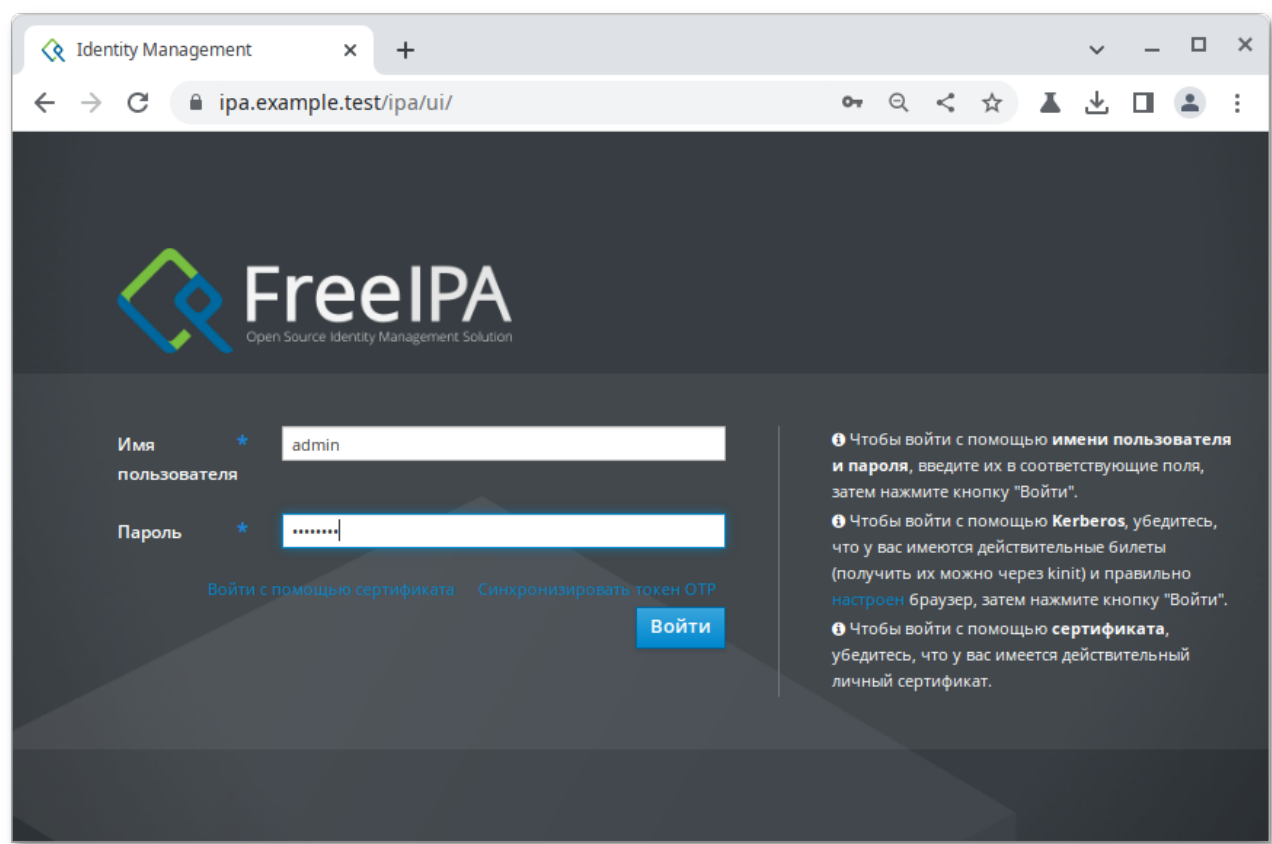
8.3. Использование одноразового пароля

Администрировать FreeIPA можно через веб-интерфейс. В веб-интерфейсе FreeIPA:

- администраторы — могут изменять все настройки сервера FreeIPA и настройки пользователей (полный доступ к серверу FreeIPA);
- пользователи FreeIPA — имеют ограниченный набор операций в зависимости от настроенных разрешений. По умолчанию активные пользователи FreeIPA могут настроить свою собственную учетную запись, но не могут изменять настройки других пользователей или настройки сервера FreeIPA.

8.1. Доступ к веб-интерфейсу

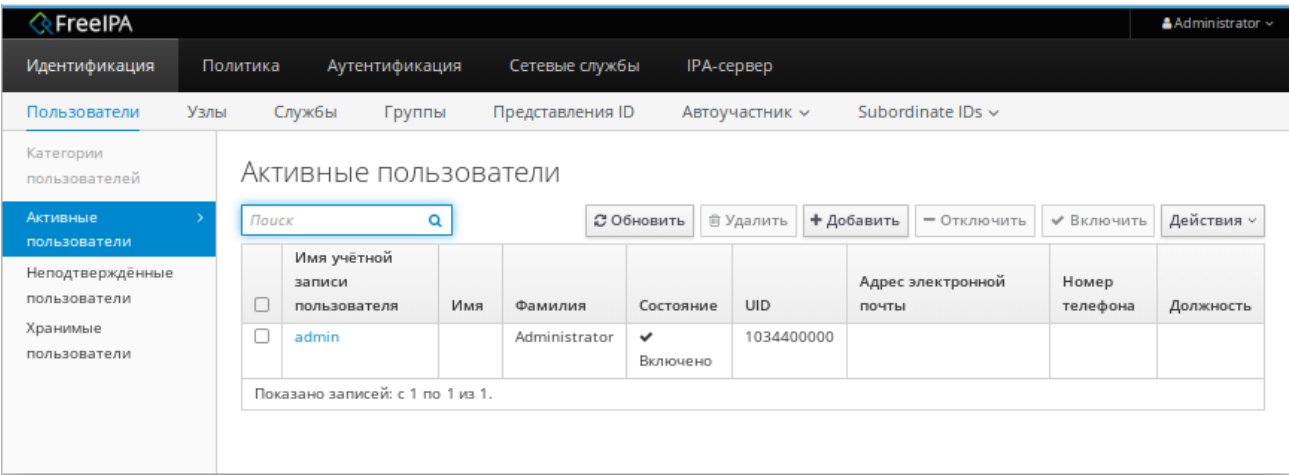
Веб-интерфейс FreeIPA доступен по адресу `https://<FQDN>`, например, `https://ipa.example.test`:



На сервере FreeIPA можно настроить следующие типы аутентификации:

- ▀ пароль (данный тип аутентификации настроен по умолчанию);
- ▀ билет Kerberos (см. [Использование билета Kerberos](#));
- ▀ смарт-карта;
- ▀ одноразовый пароль (см. [Использование одноразового пароля](#)) — его можно комбинировать с паролем и аутентификацией Kerberos.;

Администратор, войдя в систему, получает полный доступ к настройке сервера FreeIPA:



Пользователи FreeIPA могут настроить только свою собственную учетную запись:

The screenshot shows the FreeIPA web interface. At the top, there's a header with the FreeIPA logo and a user profile 'Илья Иванов'. Below the header, there are tabs for 'Пользователи' and 'Токены OTP'. The main content area is titled 'Активные пользователи » ivanov'. A sub-header indicates 'ivanov является участником:'. Below this, there are several tabs: 'Параметры' (selected), 'Группы пользователей (1)', 'Сетевые группы', 'Роли', 'Правила HBAC', 'Правила Sudo', and 'Subordinate ids'. There are also buttons for 'Обновить', 'Вернуть', 'Сохранить', and 'Действия'. The 'Параметры' tab is divided into two sections: 'Параметры идентификации' and 'Параметры учётной записи'. The 'Параметры идентификации' section includes fields for 'Должность', 'Имя *', 'Фамилия *', 'Полное имя *', 'Отображаемое имя', 'Инициалы', 'GECOS', and 'Класс'. The 'Параметры учётной записи' section includes fields for 'Имя учётной записи пользователя', 'Пароль', 'Окончание действия пароля', 'UID', 'ID группы', and 'Псевдоним учётной записи'.

Администратор FreeIPA 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 повторить новый пароль, ввести одноразовый пароль и нажать кнопку **Сбросить пароль и войти**:

The screenshot shows a password reset dialog box. At the top, there's a message: 'Срок действия вашего пароля истёк. Пожалуйста, введите новый пароль.' Below this, there are several input fields: 'Имя пользователя' (filled with 'ivanov'), 'Текущий пароль', 'Новый пароль *', 'Проверить пароль *', and 'ОТР' (with a placeholder 'One-Time Password'). At the bottom, there are two buttons: 'Отменить' and 'Сбросить пароль и войти'.

Примечание

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

8.2. Использование билета Kerberos

FreeIPA использует протокол Kerberos для поддержки единого входа. Это позволяет указать имя пользователя и пароль только один раз, после чего можно получить доступ к службам управления идентификацией без повторного запроса системой учётных данных.



Важно

Получать билет Kerberos нужно только в том случае, если первоначальный билет Kerberos был уничтожен или срок его действия истек.

Пользователь FreeIPA, пройдя процедуру аутентификацию на локальном компьютере, также автоматически входит в FreeIPA. Т.е. после входа в систему ему не требуется использовать утилиту **kinit** для доступа к ресурсам FreeIPA.

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 Kerberos:

- чтобы получить билет Kerberos для пользователя, который в данный момент вошел в систему в локальной системе, следует использовать **kinit** без указания имени пользователя:

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

- чтобы получить билет Kerberos для пользователя, который не соответствует локальному имени пользователя, следует передать имя пользователя утилите **kinit**. Например, чтобы войти в систему как администратор:

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

- чтобы убедиться, что вход в систему прошел успешно, можно воспользоваться утилитой **klist** для отображения кэшированного билета. В следующем примере кеш содержит билет для принцепала `ivanov`, что означает, что на этом хосте только пользователь `ivanov` в настоящее время имеет доступ к службам FreeIPA:

```
[ivanov@comp01 ~]$ klist
Ticket cache: KEYRING:persistent:1034400003:krb_ccache_fxAUUnBu
Default principal: ivanov@EXAMPLE.TEST

Valid starting          Expires                Service principal
01.09.2023 09:35:59    02.09.2023 09:31:20  krbtgt/EXAMPLE.TEST@EXAMPLE.TEST
```

Если проверка подлинности Kerberos работает правильно и у пользователя есть действительный билет, пользователь пройдёт автоматическую проверку подлинности (на странице <https://ipa.example.test>) и получит доступ к веб-интерфейсу.

Если срок действия билета Kerberos истёк, пользователю нужно пройти аутентификацию с помощью учётных данных. Но при повторном входе, веб-интерфейс FreeIPA откроется автоматически, без открытия диалогового окна входа в систему.

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

The screenshot shows the login page of the FreeIPA web interface. At the top, there is a red error message box that says: "Не удалось выполнить аутентификацию с Kerberos". Below this, there are two input fields: "Имя пользователя" (Username) and "Пароль" (Password). The password field has a placeholder text: "Password or Password+One-Time Password". Below the password field, there are two links: "Войти с помощью сертификата" (Login with certificate) and "Синхронизировать токен OTP" (Synchronize OTP token). At the bottom right, there is a blue button labeled "Войти" (Login). On the right side of the page, there is a sidebar with three informational messages: 1. "Чтобы войти с помощью имени пользователя и пароля, введите их в соответствующие поля, затем нажмите кнопку 'Войти'." (To login with username and password, enter them in the corresponding fields, then click the 'Login' button.) 2. "Чтобы войти с помощью Kerberos, убедитесь, что у вас имеются действительные билеты (получить их можно через kinit) и правильно настроен браузер, затем нажмите кнопку 'Войти'." (To login with Kerberos, ensure you have valid tickets (you can get them through kinit) and the browser is correctly configured, then click the 'Login' button.) 3. "Чтобы войти с помощью сертификата, убедитесь, что у вас имеется действительный личный сертификат." (To login with a certificate, ensure you have a valid personal certificate.)

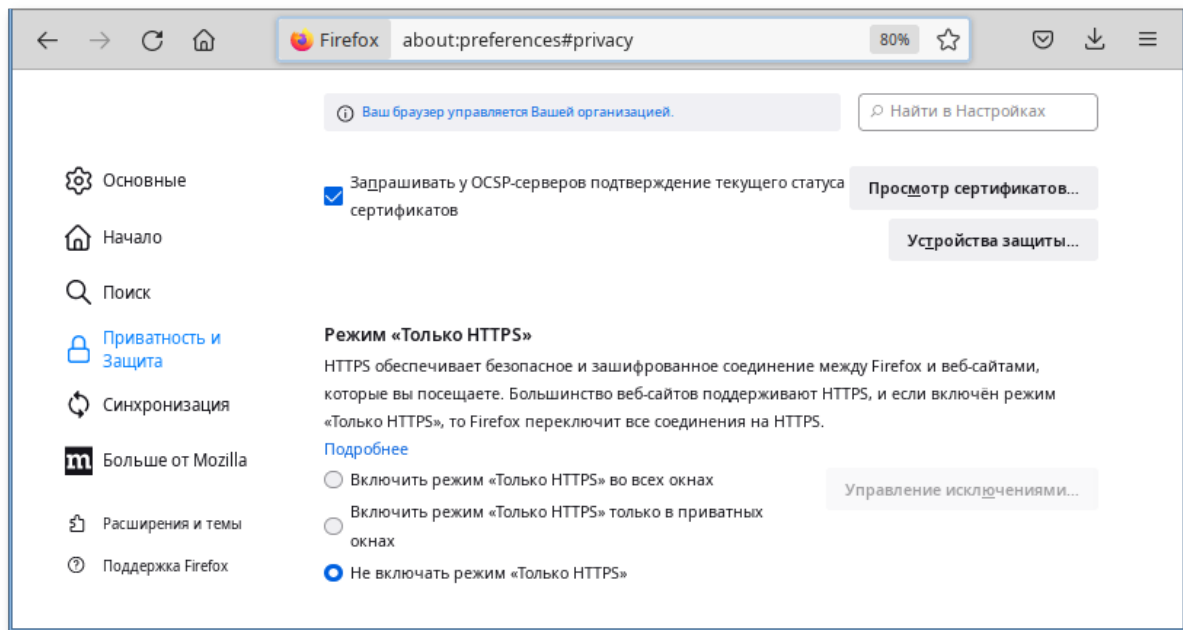
8.2.1. Настройка браузера для аутентификацию с Kerberos

Предварительно необходимо ввести компьютер в домен (см. [Разворачивание клиента FreeIPA](#)) и убедиться, что доменный пользователь получает билет Kerberos.

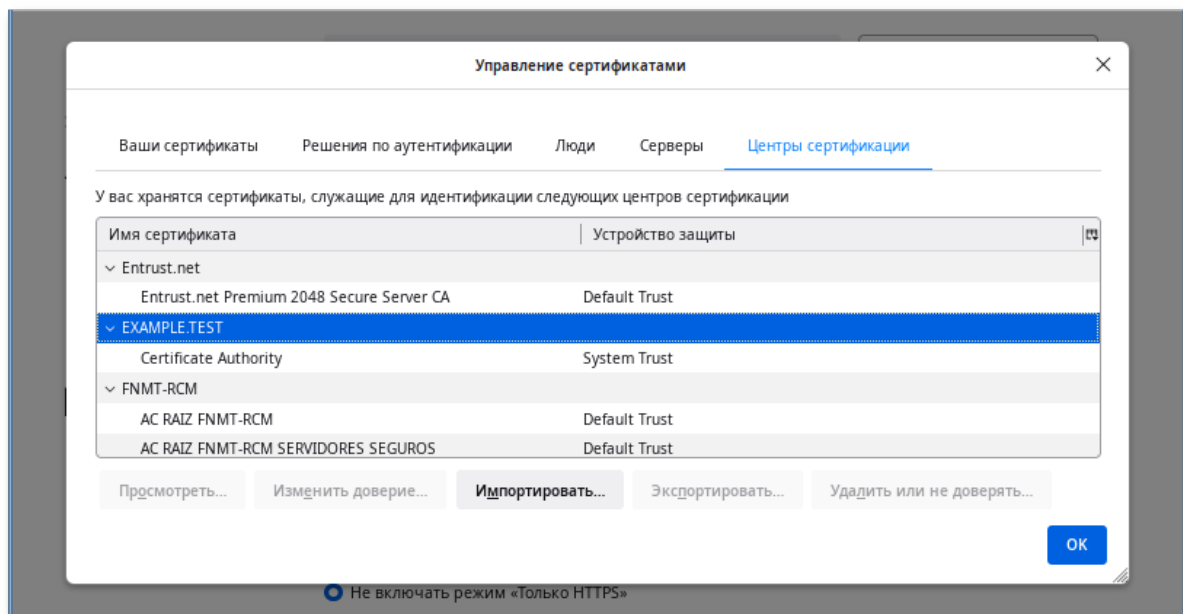
8.2.1.1. Настройка Mozilla Firefox

Порядок действий:

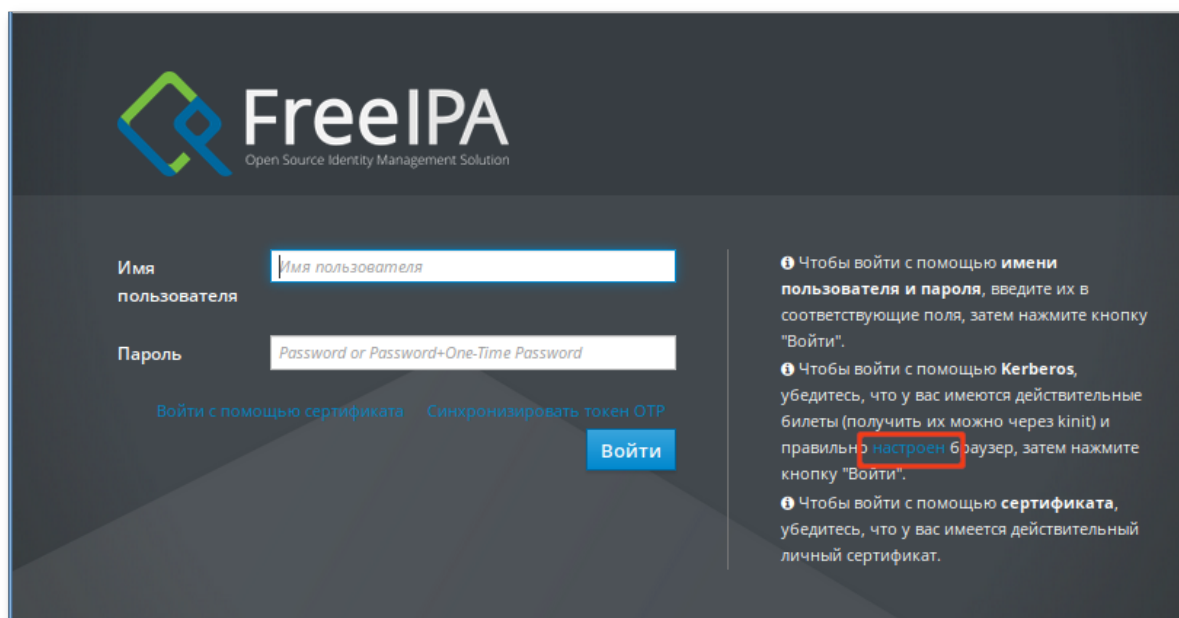
1. В настройках браузера на странице **Приватность и защита** (<about:preferences#privacy>) нажать кнопку **Просмотр сертификатов...**:



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



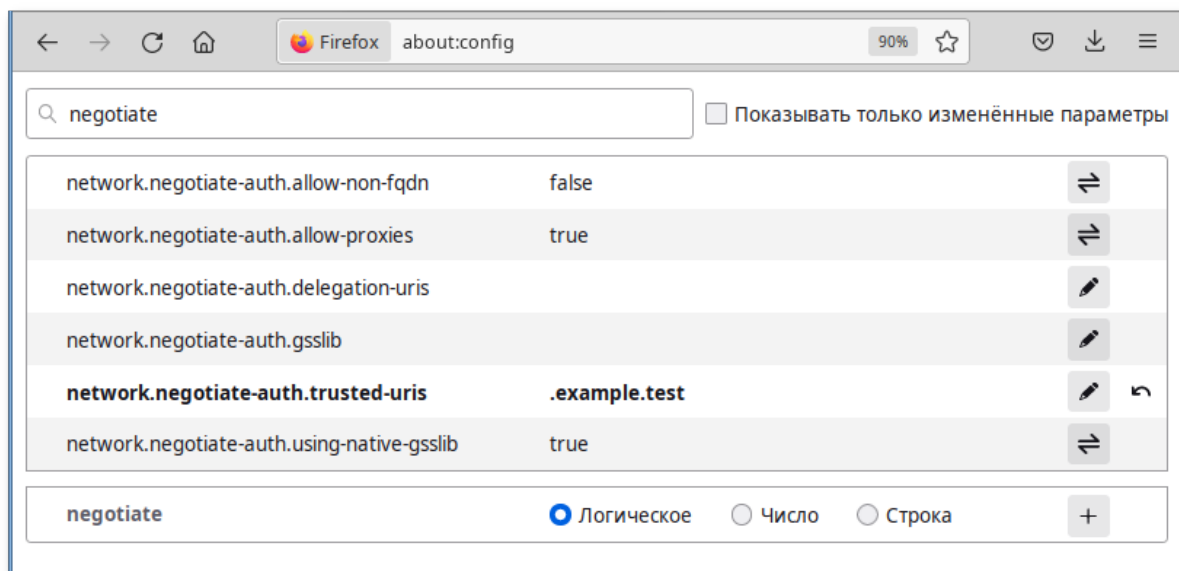
3. Если сертификат отсутствует, загрузить его по ссылке <https://ipa.example.test/ipa/config/ca.crt> и Импортировать полученный сертификат, нажав кнопку **Импорт**:



The image shows the FreeIPA login interface. At the top left is the FreeIPA logo with the text 'Open Source Identity Management Solution'. Below it are two input fields: 'Имя пользователя' (Username) with a placeholder 'Имя пользователя' and 'Пароль' (Password) with a placeholder 'Password or Password+One-Time Password'. There are two links below the password field: 'Войти с помощью сертификата' and 'Синхронизировать токен OTP'. A blue 'Войти' (Login) button is at the bottom right. To the right of the login fields is a list of instructions in Russian:

- ❗ Чтобы войти с помощью **имени пользователя и пароля**, введите их в соответствующие поля, затем нажмите кнопку "Войти".
- ❗ Чтобы войти с помощью **Kerberos**, убедитесь, что у вас имеются действительные билеты (получить их можно через kinit) и правильно **настроен** браузер, затем нажмите кнопку "Войти".
- ❗ Чтобы войти с помощью **сертификата**, убедитесь, что у вас имеется действительный личный сертификат.

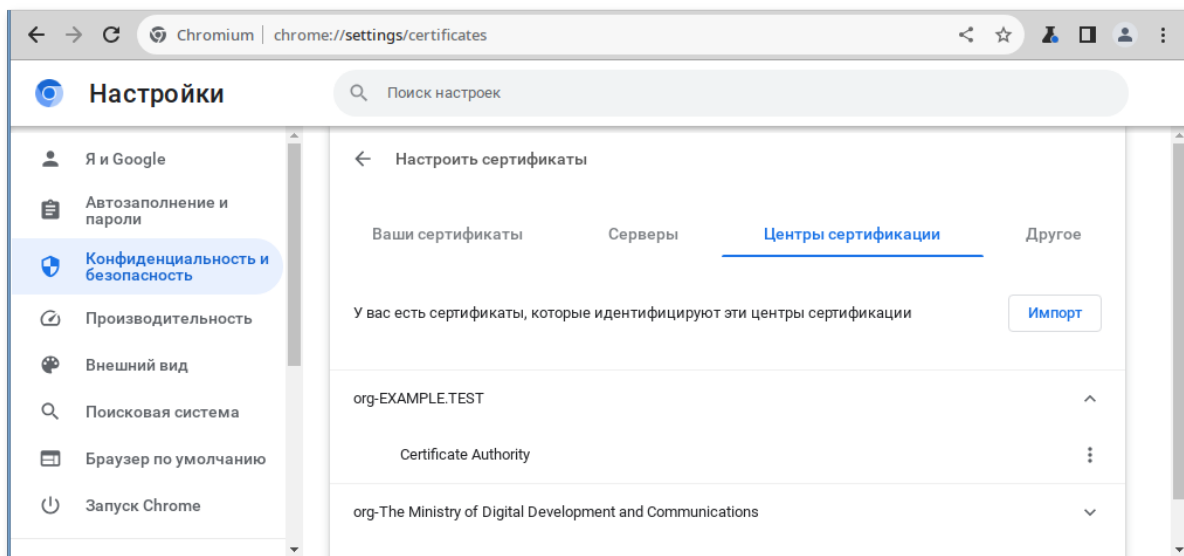
4. В адресной строке ввести **about:config**, чтобы отобразить список текущих параметров конфигурации (необходимо будет нажать кнопку **Принять риск и продолжить**).
5. В поле **Фильтр** ввести **negotiate**, чтобы ограничить список параметров.
6. Выбрать параметр **network.negotiate-auth.trusted-uris**.
7. Указать в этом параметре имя kerberos области (realm), включая предшествующую точку (.). Если нужно добавить несколько доменов, их необходимо указать через запятую.



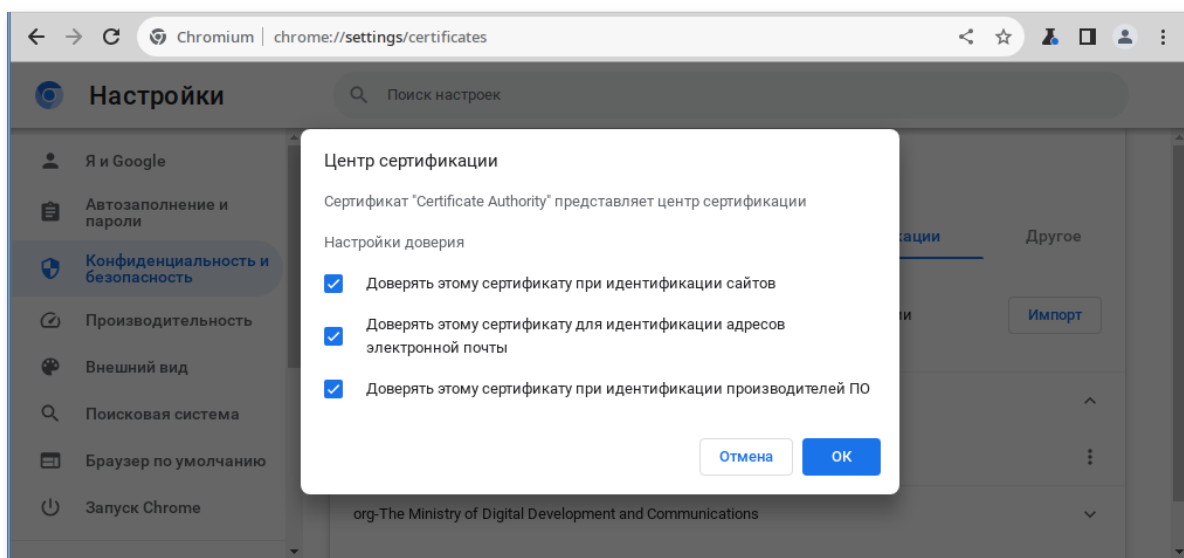
8.2.1.2. Настройка Chromium

Порядок действий:

1. В настройках браузера на странице **Конфиденциальность и безопасность** (**chrome://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. В файл `/etc/chromium/policies/managed/policies.json` добавить строку:

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

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

4. Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для Chromium можно проверить, указав в адресной строке URL: `"chrome://policy"`.



Примечание

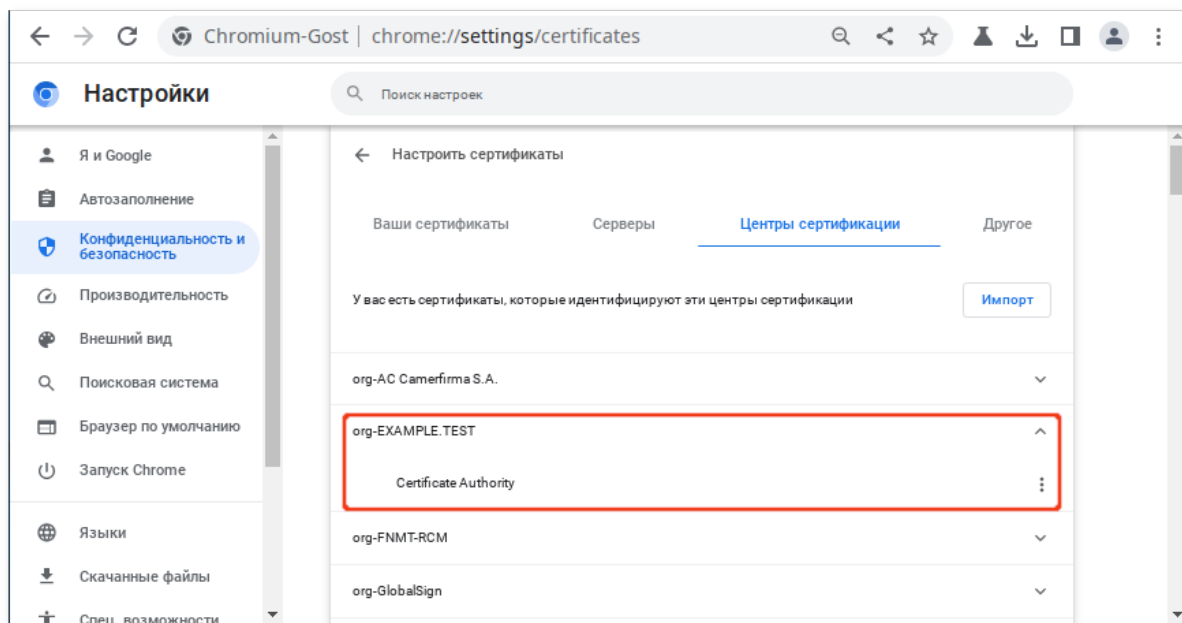
Для проверки работы аутентификации без изменения настроек браузера можно запустить браузер из командной строки, выполнив команду:


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

8.2.1.3. Настройка Chromium-Gost

Порядок действий:

1. В настройках браузера на странице **Конфиденциальность и безопасность** (`chrome://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. В файл `/etc/chromium/policies/managed/policies.json` добавить строку:

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

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

4. Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для Chromium-Gost можно проверить, указав в адресной строке URL: `"chrome://policy"`.



Примечание

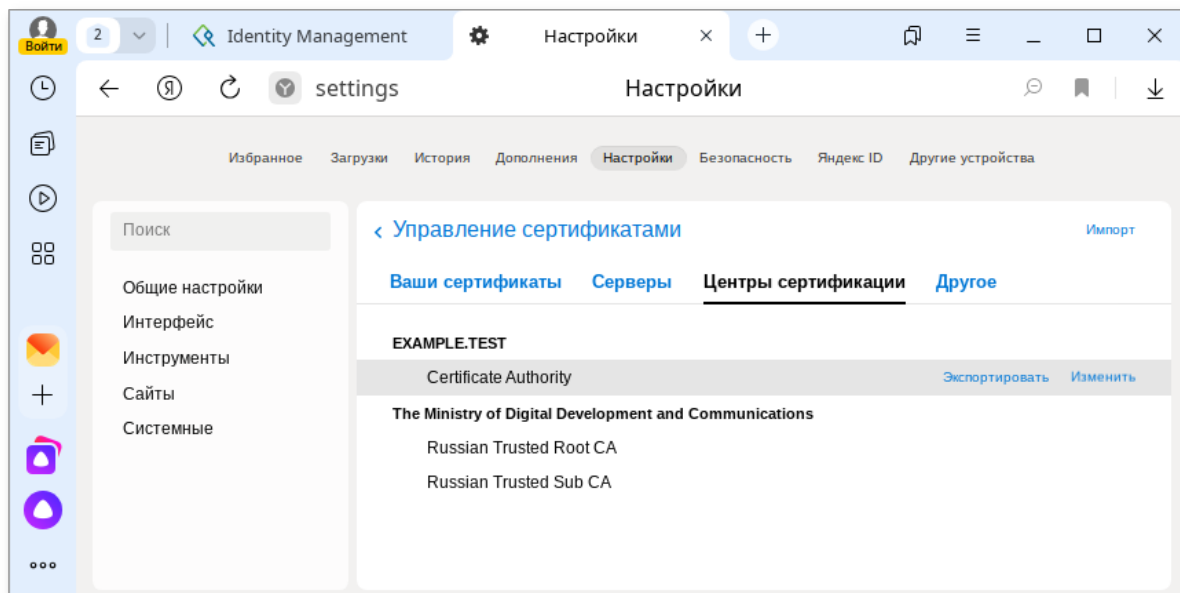
Для проверки работы аутентификации без изменения настроек браузера можно запустить браузер из командной строки, выполнив команду:

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

8.2.1.4. Настройка «Яндекс.Браузера»

Порядок действий:

1. В настройках браузера на странице **Конфиденциальность и безопасность** (<chrome://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. В файл `/etc/opt/yandex/browser/policies/managed/policies.json` добавить строку:

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

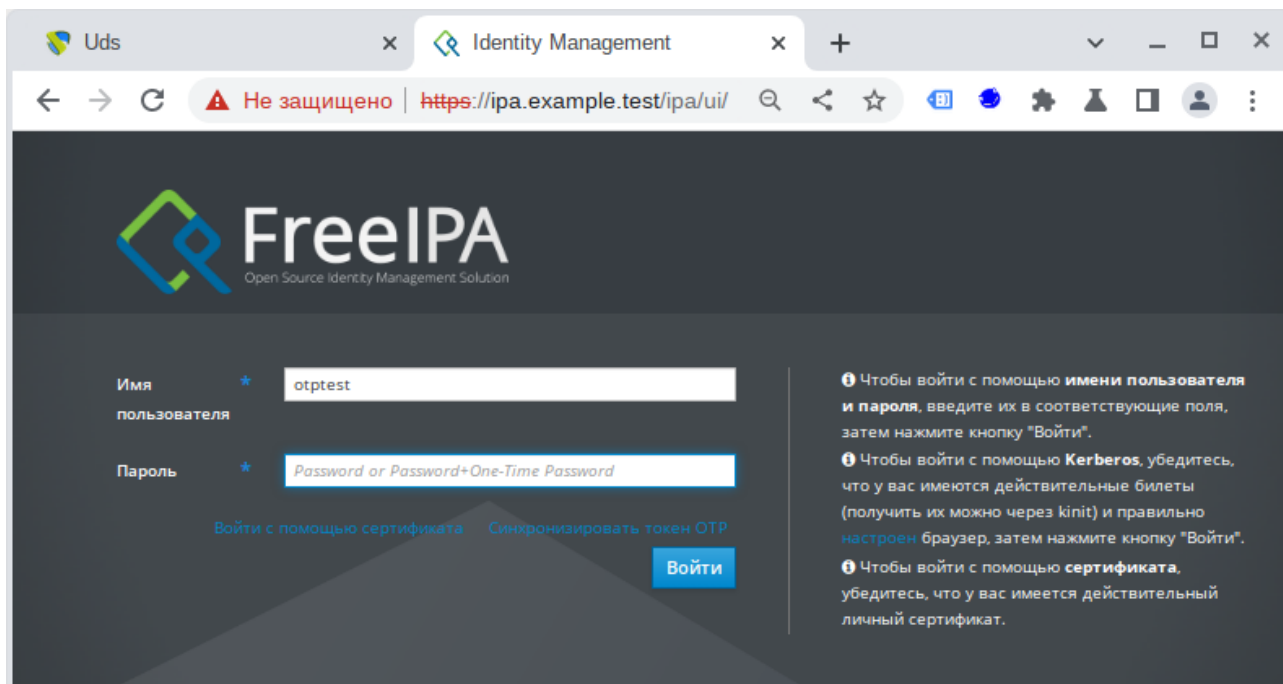
где `.example.test` — имя kerberos области (realm).

4. Для применения настроек необходимо перезапустить браузер. Результат применения параметров политики для «Яндекс.Браузера» можно проверить, указав в адресной строке URL: `"browser://policy"`.

8.3. Использование одноразового пароля

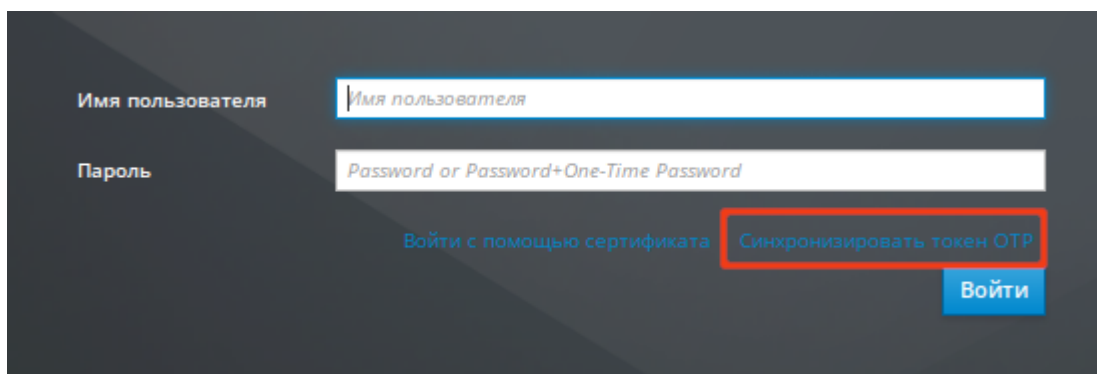
Настройка двухфакторной аутентификации рассмотрена в главе [Двухфакторная аутентификация](#).

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

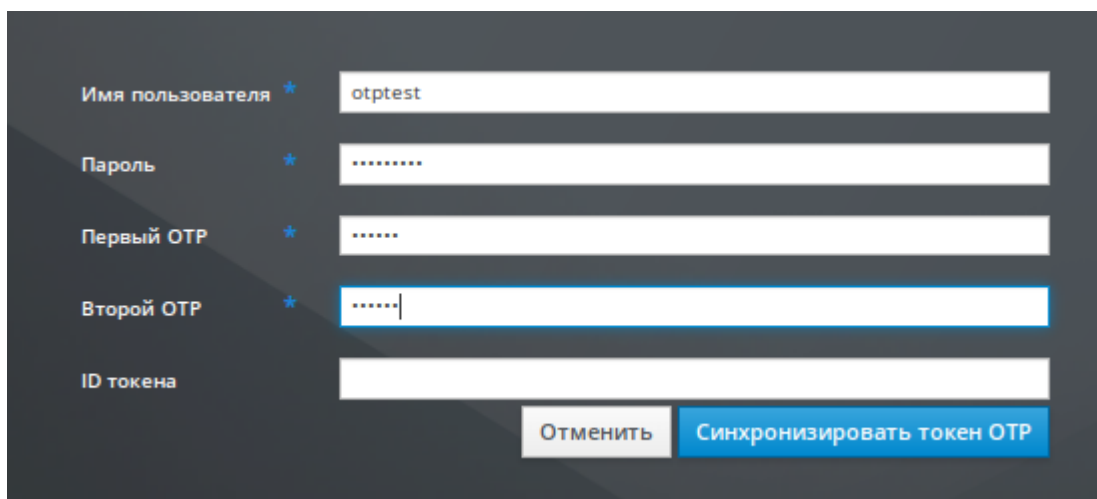


Если аутентификация не удалась, необходимо синхронизировать токены OTP:

1. На экране входа в веб-интерфейс FreeIPA нажать кнопку **Синхронизировать токен OTP**:



2. В открывшемся окне ввести имя пользователя и его пароль. Создать одноразовый пароль и ввести его в поле **Первый OTP**. Создать еще один одноразовый пароль и ввести его в поле **Второй OTP**. Ввести идентификатор токена, если это необходимо, и нажать кнопку **Синхронизировать токен OTP**:



Глава 9. Журналирование FreeIPA

9.1. Файлы журналов сервера и клиента FreeIPA

9.2. Файлы журналов сервера каталогов (Directory Service)

9.3. Файлы журналов сервера Apache

9.4. Файлы журналов системы сертификатов FreeIPA

9.5. Файлы журналов Kerberos

9.6. Файлы журналов DNS

9.1. Файлы журналов сервера и клиента FreeIPA

В следующей таблице представлены каталоги и файлы, которые сервер и клиент FreeIPA используют для регистрации информации.

Таблица 9.1. Файлы журналов сервера и клиента FreeIPA

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

9.2. Файлы журналов сервера каталогов (Directory Service)

В следующей таблице представлены каталоги и файлы, которые экземпляр сервера каталогов (DS) FreeIPA использует для регистрации информации.

Таблица 9.2. Файлы журналов сервера каталогов (Directory Service)

Файл/каталог	Описание
<code>/var/log/dirsrv/slapd-<REALM_NAME></code>	Файлы журналов, связанные с экземпляром DS, используемым сервером FreeIPA. Основная часть записанных здесь данных относятся к взаимодействиям сервера и реплики
<code>/var/log/dirsrv/slapd-<REALM_NAME>/audit</code>	Содержит журналы аудита всех операций DS, если аудит включен в конфигурации DS

Файл/каталог	Описание
/var/log/dirsrv/slapd-<REALM_NAME>/access	Содержит подробную информацию о попытках доступа к экземпляру DS домена
/var/log/dirsrv/slapd-<REALM_NAME>/errors	Содержит подробную информацию о неудачных операциях для экземпляра DS домена

9.3. Файлы журналов сервера Apache

В следующей таблице представлены каталоги и файлы, которые сервер Apache FreeIPA использует для регистрации информации.

Таблица 9.3. Файлы журналов сервера Apache

Файл/каталог	Описание
/var/log/httpd2/	Файлы журналов веб-сервера Apache
/var/log/httpd2/access_log	Стандартный журнал доступа веб-сервера Apache. Сообщения, специфичные для FreeIPA, записываются вместе с сообщениями Apache, поскольку веб-интерфейс FreeIPA и интерфейс командной строки используют Apache. В журналах доступа в основном регистрируются только субъект-пользователь и используемый URI, который часто является конечной точкой RPC.
/var/log/httpd2/error_log	Стандартный журнал ошибок веб-сервера Apache. Журнал ошибок содержит журналы сервера FreeIPA.

9.4. Файлы журналов системы сертификатов FreeIPA

В следующей таблице представлены каталоги и файлы, которые система сертификатов FreeIPA используют для регистрации информации.

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) FreeIPA
/var/log/pki/pki-kra-spawn.<time_of_installation>.log	Журнал установки центра восстановления ключей FreeIPA (KRA)
/var/log/pki/pki-tomcat/	Каталог верхнего уровня для журналов операций PKI. Содержит журналы CA и KRA.
/var/log/pki/pki-tomcat/ca/	Каталог с журналами, связанными с операциями над сертификатами. В FreeIPA эти журналы используются для субъектов-служб, узлов и других объектов, использующих сертификаты.

Файл/каталог	Описание
<code>/var/log/pki/pki-tomcat/kra/</code>	Каталог с журналами, относящимися к KRA

Сообщения об ошибках сертификата также добавляются в системный журнал.

9.5. Файлы журналов Kerberos

В следующей таблице представлены каталоги и файлы, которые Kerberos использует для регистрации информации.

Таблица 9.5. Файлы журналов Kerberos

Файл/каталог	Описание
<code>/var/log/krb5kdc.log</code>	Основной файл журнала для сервера Kerberos KDC
<code>/var/log/kadmind.log</code>	Основной файл журнала сервера администрирования Kerberos

Расположение этих файлов настраивается в файле `/etc/krb5.conf`.

9.6. Файлы журналов DNS

Сообщения об ошибках DNS добавляются в системный журнал.

Часть III. Настройка репликации

В этой части приводится общая информация по настройке репликации FreeIPA.

Содержание

- [10. Системные требования](#)
- [11. Системные требования](#)
- [12. Параметры утилиты ipa-replica-install](#)
- [13. Установка реплики](#)
- [14. Отладочная информация](#)
- [15. Удаление реплики](#)

Глава 10. Системные требования

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

Глава 11. Системные требования

11.1. Установка реплики на существующем клиенте FreeIPA

11.2. Установка реплики в системе, не зарегистрированной в домене FreeIPA

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

Новую реплику можно установить:

- на существующем клиенте FreeIPA путем преобразования клиента в реплику;
- на машине, которая еще не зарегистрирована в домене FreeIPA.

В обеих этих ситуациях можно настроить реплику, добавив нужные параметры в команду **ipa-replica-install**.

Для возможности установки реплики должны быть установлены те же пакеты, что и при установке сервера (см. [Установка сервера FreeIPA](#)):

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

11.1. Установка реплики на существующем клиенте FreeIPA

При установке реплики на существующем клиенте FreeIPA можно выбрать один из двух способов, чтобы авторизовать установку.

Способ 1. Использовать учетные данные привилегированного пользователя:

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

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

Способ 2. Включить узел в группу ipaservers. Членство в группе ipaservers предоставляет машине повышенные привилегии, аналогичные учетным данным администратора. Следовательно, на следующем этапе для запуска утилиты **ipa-replica-install** права администратора FreeIPA не потребуются.

11.2. Установка реплики в системе, не зарегистрированной в домене FreeIPA



Примечание

Перед настройкой репликации необходимо настроить систему на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки (см. [Подготовка системы к установке клиента FreeIPA](#)).

При установке реплики в системе, которая еще не зарегистрирована в домене FreeIPA, утилита **ipa-replica-install** сначала регистрирует систему в качестве клиента, а затем устанавливает компоненты реплики. Для этого сценария также можно выбрать один из двух способов, чтобы авторизовать установку реплики.

Способ 1. Использовать учетные данные привилегированного пользователя, указав их непосредственно во время установки реплики:

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

Способ 2. Использовать случайный пароль, сгенерированный на сервере FreeIPA.



Примечание

Сгенерированный пароль станет недействительным после регистрации машины в домене FreeIPA.

Глава 12. Параметры утилиты ipa-replica-install

По умолчанию реплика устанавливается на первый сервер FreeIPA, обнаруженный установщиком клиента. Чтобы установить реплику на определенный сервер, необходимо добавить следующие параметры в **ipa-replica-install**:

- » **--server** — для указания полного доменного имени сервера (FQDN);
- » **--domain** — для указания домена DNS FreeIPA.

При запуске без параметров **ipa-replica-install** настраивает только основные службы сервера. Чтобы установить дополнительные службы, например, DNS или центр сертификации (CA), следует добавить соответствующие параметры в **ipa-replica-install**:

- » **--setup-dns** и **--forwarder** — для установки реплики с DNS;
- » **--setup-ca** — для установки реплики с интегрированным CA;
- » **--dirsrv-cert-file**, **--dirsrv-pin**, **--http-cert-file** и **--http-pin** — для установки реплики без CA.

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

Глава 13. Установка реплики

13.1. Установка реплики на существующем клиенте FreeIPA, с использованием Host Keytab

13.2. Установка реплики с использованием случайного пароля

13.3. Установка реплики с использованием учётных данных привилегированного пользователя

13.4. С интегрированным DNS и без CA

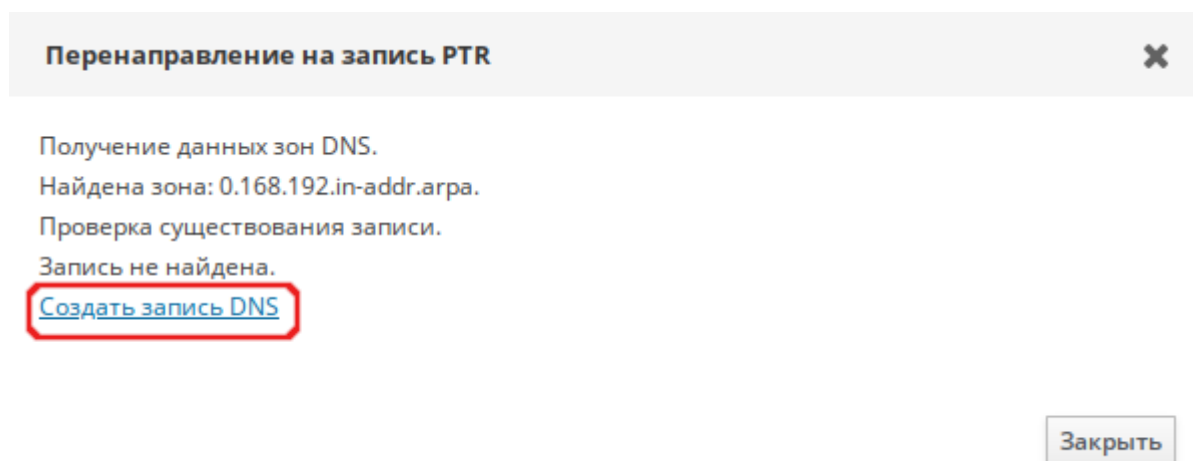
13.5. С интегрированными DNS и CA в системе, не зарегистрированной в домене FreeIPA

13.6. Проверка реплики

13.1. Установка реплики на существующем клиенте FreeIPA, с использованием Host Keytab

В данной процедуре клиент FreeIPA повышается до реплики с использованием собственной таблицы ключей хоста. Данная процедура не требует предоставления учетных данных администратора или диспетчера каталогов (DM), поэтому она более безопасна (т.к. в командной строке не отображается конфиденциальная информация).

Создать обратный адрес для реплики на DNS-сервере основного сервера. Для этого в веб-интерфейсе FreeIPA необходимо перейти в **Сетевые службы** → **DNS** → **Зоны DNS**, выбрать в таблице запись домена (например, example.test.), в открывшемся списке открыть запись реплики (например, ipabackup), нажать на IP-адрес в поле A записи и в открывшемся окне на ссылку **Создать запись DNS**:



Процедура установка реплики:

1. На любом узле FreeIPA получить билет Kerberos:

```
$ 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 утилиту **ipa-replica-install**:

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



Примечание

dbus может мешать проверке соединений при установке реплики, при появлении ошибок может помочь перезапуск сервиса:

```
# systemctl reload dbus
```

13.2. Установка реплики с использованием случайного пароля

В этой процедуре реплика устанавливается на машину, которая еще не является клиентом FreeIPA. Для авторизации регистрации используется случайный пароль, действительный только для одной регистрации этого клиента.

Данная процедура не требует предоставления учётных данных администратора или диспетчера каталогов (DM), поэтому она более безопасна (т.к. в командной строке не отображается конфиденциальная информация).

Процедура установка реплики:

1. На любом узле FreeIPA получить билет Kerberos:

```
$ kinit admin
```

2. Добавить внешнюю систему в качестве узла FreeIPA (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 систему в группу узлов 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 клиенте запустить утилиту **ipa-replica-install**, указав сгенерированный пароль в параметре **--password** (т.к. пароль часто содержит специальные символы, следует заключить его в одинарные кавычки):

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

Пример команды установки реплики с интегрированными DNS и CA:

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

13.3. Установка реплики с использованием учётных данных привилегированного пользователя

В этой процедуре реплика устанавливается на машину, которая еще не является клиентом FreeIPA. Для авторизации регистрации используются учётные данные привилегированного пользователя FreeIPA.

Процедура установка реплики:

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

The screenshot shows the FreeIPA web interface. The top navigation bar includes 'Идентификация', 'Политика', 'Аутентификация', 'Сетевые службы', and 'IPA-сервер'. The 'Сетевые службы' section is expanded, showing 'Автомониторинг' and 'DNS'. The 'DNS' page displays a table of DNS zones. The first zone, '0.168.192.in-addr.arpa.', is highlighted with a red box. The second zone is 'example.test.'. Both zones are in the 'Включено' (Enabled) state.

Имя зоны	Состояние
0.168.192.in-addr.arpa.	✓ Включено
example.test.	✓ Включено

Показано записей: с 1 по 2 из 2.

И в обратной зоне создана реверсивная запись для основного сервера 192.168.0.113:

FreeIPA Administrator

Идентификация Политика Аутентификация Сетевые службы IPA-сервер

Автомониторинг DNS

Зоны DNS > 0.168.192.in-addr.arpa.

Записи ресурсов DNS: 0.168.192.in-addr.arpa.

Записи ресурсов DNS Параметры

Поиск Обновить Удалить +Добавить

<input type="checkbox"/>	Имя записи	Тип записи	Данные
<input type="checkbox"/>	113	PTR	ipa.example.test.
<input type="checkbox"/>	@	NS	ipa.example.test.

Показано записей: с 1 по 2 из 2.

2. В реверсивной зоне создать реверсивную запись для сервера репликации (кнопка **Добавить**):

FreeIPA Administrator

Идентификация Автомониторинг Зоны DNS > Записи ресурсов DNS

Добавить запись ресурса DNS

Имя записи * 145

Тип записи PTR

Hostname * replica.example.test.

* Обязательное поле

Добавить Добавить и добавить ещё Добавить и изменить Отменить

Реверсивную запись можно также создать, выполнив команду:

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

3. На клиенте запустить утилиту **ipa-replica-install**:

```
# 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
```

13.4. С интегрированным DNS и без CA

Здесь предполагается, что первый сервер был установлен в режиме CA-less (см. [Установка сервера FreeIPA в режиме CA-less](#)). В этом случае можно предоставить необходимые сертификаты вручную.

На сервере, где создавались сертификаты для сервера:

1. Создать noise файл, заполненный случайными числами:

```
# 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=ipabackup.example.test,0=IPA -o /tmp/  
replicacert.req -k rsa -g 2048 -z ~/test_ca/noise.txt -f ~/test_ca/  
password.txt -a --extSKID
```

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=$((CERT_SERIAL + 1))  
# 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 -a
```

В ответ на запросы команды дать следующие ответы:

```
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 полученный 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 на будущую реплику.

Настройка репликации LDAP-каталога:

```
# 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
```

13.5. С интегрированными DNS и CA в системе, не зарегистрированной в домене FreeIPA

Пример, настройки репликации LDAP-каталога:

```
# ipa-replica-install --password='2AaT0Ix8itDsYugdDGoRtBt'  
Configuring client side components  
This program will set up IPA client.  
Version 4.9.11  
  
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 будет установлен клиент, а затем реплика.

13.6. Проверка реплики

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

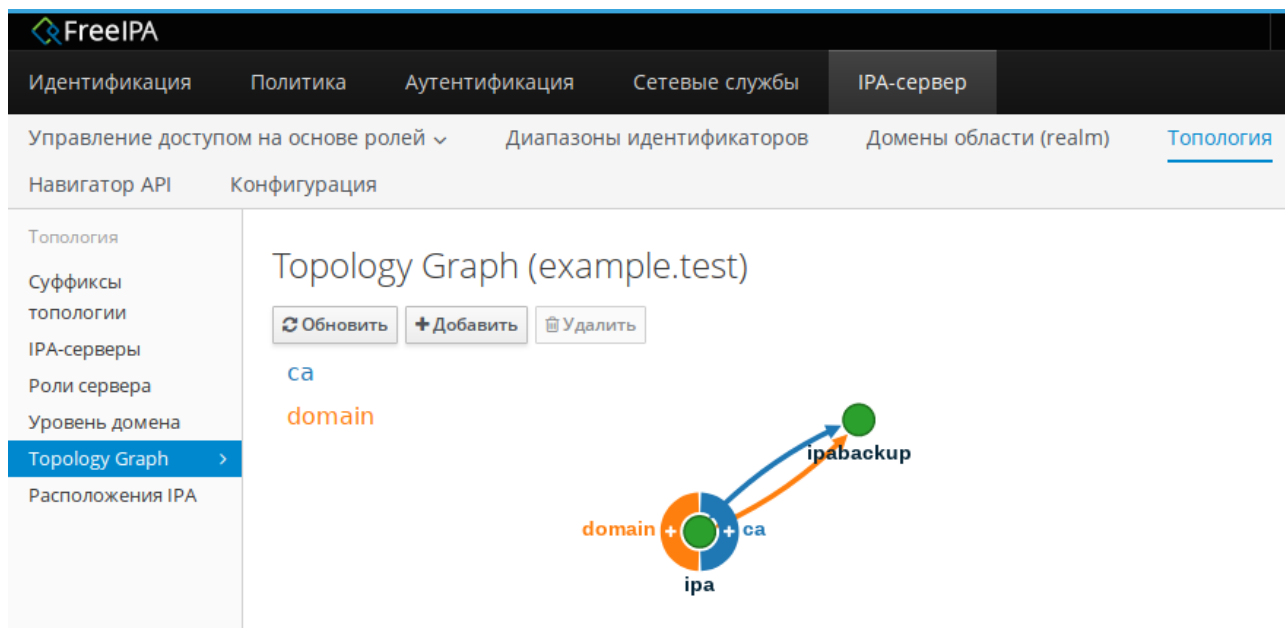
1. Создать пользователя на новой реплике:

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

2. Убедиться, что пользователь виден на другой реплике:

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

После настройки репликации посмотреть топологию можно в веб-интерфейсе FreeIPA (**IPA-сервер** → **Топология** → **Topology Graph**):



Глава 14. Отладочная информация

При установке реплики FreeIPA отладочная информация добавляется в следующие файлы журнала 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 следующие файлы журнала на сервере FreeIPA:

- » `/var/log/httpd2/error_log;`

» `/var/log/dirsrv/slapd-INSTANCE-NAME/access`

» `/var/log/dirsrv/slapd-INSTANCE-NAME/errors`

Глава 15. Удаление реплики

Администратор FreeIPA может удалить реплику FreeIPA из топологии. Дополнительные сведения см. [Удаление сервера FreeIPA](#)

Часть IV. Разворачивание клиента FreeIPA

В этой части приводится общая информация по разворачиванию FreeIPA.

Содержание

[16. Подготовка системы к установке клиента FreeIPA](#)

[17. Установка пакетов](#)

[18. Подключение к серверу](#)

[19. Проверка клиента FreeIPA](#)

[20. Отладочная информация](#)

[21. Повторная регистрация клиента FreeIPA](#)

[22. Удаление клиента FreeIPA](#)

Глава 16. Подготовка системы к установке клиента FreeIPA

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

Клиентские компьютеры должны быть настроены на использование DNS-сервера, который был сконфигурирован на сервере FreeIPA во время его установки. В сетевых настройках необходимо указать использовать сервер FreeIPA для разрешения имен. 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 FreeIPA сервера и в поле **Домены поиска** — домен для поиска:

Центр управления системой

Главная Режим эксперта Выход Справка

Имя компьютера:

Интерфейсы

enp0s3	Сетевая карта: Intel Corporation 82540EM Gigabit Ethernet Controller провод подсоединён MAC: 08:00:27:43:08:dc
--------	--

Версия протокола IP: ☒ Включить

Конфигурация:

IP-адреса:

Добавить ↑ IP: /24 (255.255.255.0)

Шлюз по умолчанию:

DNS-серверы:

Домены поиска:
(несколько значений записываются через пробел)



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
```

■ добавить DNS сервер, для этого необходимо создать файл **/etc/net/ifaces/eth0/resolv.conf** со следующим содержанием:

```
# nameserver 192.168.0.113
```

где 192.168.0.113 — IP-адрес FreeIPA сервера;

■ указать службе resolvconf использовать DNS FreeIPA и домен для поиска. Для этого в файле **/etc/resolvconf.conf** добавить/отредактировать следующие параметры:

```
interface_order='lo lo[0-9]* lo.* eth0'  
search_domains=example.test
```

где eth0 — интерфейс на котором доступен FreeIPA сервер, example.test — домен;

■ обновить DNS адреса:

```
# resolvconf -u
```

В результате выполненных действий в файле **/etc/resolv.conf** должны появиться строки:

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



Предупреждение

В строке *search* не должен присутствовать *localdomain*.



Примечание

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

Глава 17. Установка пакетов

Установить необходимые пакеты:

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

Глава 18. Подключение к серверу

18.1. Интерактивная установка

18.2. В пакетном режиме

18.3. В Центре управления системой

При настройке системы в качестве клиента FreeIPA она регистрируется в домене FreeIPA и позволяет системе использовать услуги FreeIPA на серверах FreeIPA.

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

- учетные данные привилегированного пользователя (параметр по умолчанию);
- одноразовый пароль (OTP);
- ключ (keytab) из предыдущей регистрации.

18.1. Интерактивная установка

Запустить скрипт настройки клиента в интерактивном режиме:

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

Можно добавить параметр **--enable-dns-updates**, чтобы обновить записи DNS с помощью IP-адреса клиентской системы, если выполняется одно из следующих условий:

- сервер FreeIPA, на котором будет зарегистрирован клиент, был установлен со встроенным DNS;
- DNS-сервер в сети принимает обновления записей DNS по протоколу GSS-TSIG.

Скрипт установки должен автоматически найти необходимые настройки на FreeIPA сервере, вывести их и спросить подтверждение для найденных параметров:

```
This program will set up IPA client.
Version 4.9.11

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
```

Затем запрашивается имя пользователя, имеющего право вводить машины в домен, и его пароль (можно использовать администратора по умолчанию, который был создан при установке сервера):

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

Далее сценарий установки настраивает клиент. Если установка прошла успешно, в конце вывода вы увидите:

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

18.1.1. С использованием одноразового пароля

На сервере FreeIPA добавить будущую клиентскую систему (следует использовать параметр **--random**, чтобы команда сгенерировала случайный одноразовый пароль):

```
# 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: 3Se0aJ5Gy0xbPcLmF5wpFQH
Пароль: True
Таблица ключей: False
Managed by: comp03.example.test
```



Примечание

Сгенерированный пароль станет недействительным после регистрации машины в домене FreeIPA. Он будет заменён соответствующей таблицей ключей узла после завершения регистрации.

Запустить утилиту **ipa-client-install** в системе, которая будет настроена в качестве клиента. Чтобы указать одноразовый случайный пароль, необходимо использовать параметр **--password**. Т.к. пароль часто содержит специальные символы, следует заключить его в одинарные кавычки:

```
# ipa-client-install --mkhomedir --password='3Se0aJ5Gy0xbPcLmF5wpFQH'
```

18.2. В пакетном режиме

Для установки в пакетном режиме утилите **ipa-client-install** с помощью параметров командной строки нужно предоставить всю необходимую информацию, как минимум:

1. Метод проверки пользователя:

- **-p PRINCIPAL, --principal=PRINCIPAL** и **-w PASSWORD, --password=PASSWORD** для указания учетных данных пользователя, уполномоченного регистрировать клиентов;
- **--password=PASSWORD** для указания одноразового случайного пароля, сгенерированный для клиента;
- **-k KEYTAB, --keytab=KEYTAB**, чтобы указать таблицу ключей из предыдущей регистрации.

2. Возможность автоматической установки:

- **--unattended, -U** — не запрашивать у пользователя информацию.

Скрипт настройки клиента в пакетном режиме:

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

Если записи SRV установлены правильно в зоне DNS FreeIPA, сценарий автоматически обнаруживает все остальные требуемые значения. Если сценарий не может обнаружить значения автоматически, можно указать их с помощью параметров командной строки, например:

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

Пример скрипта настройки клиента в пакетном режиме с дополнительными параметрами:

```
# ipa-client-install -U --password='3Se0aJ5Gy0xbPcLmF5wpFQH' --domain  
example.test --server ipa.example.test --realm EXAMPLE.TEST --mkhomedir
```



Примечание

Полный список параметров можно увидеть, запустив команду:

```
# ipa-client-install --help
```

18.3. В Центре управления системой



Примечание

Должен быть установлен пакет *task-auth-freeipa*:

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

Для ввода рабочей станции в домен FreeIPA, необходимо в Центре управления системой перейти в раздел **Пользователи** → **Аутентификация**. Здесь следует выбрать пункт **Домен FreeIPA**, заполнить поля **Домен** и **Имя компьютера**, затем нажать кнопку **Применить**:

Центр управления системой

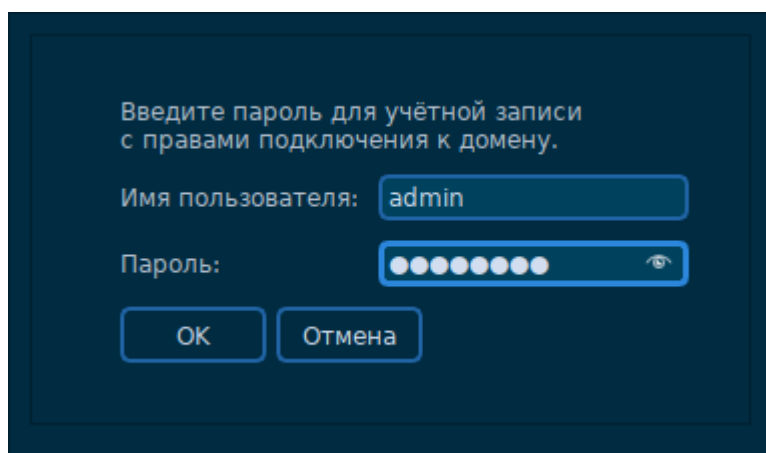
Главная Режим эксперта Выход Справка

- Локальная база пользователей
- Домен ALT Linux или Astra Linux Directory
Домен: example.test
☐ Кэшировать аутентификацию при недоступности сервера домена
- Домен Active Directory
Домен: example.test
Рабочая группа:
Имя компьютера: comp01
- Домен FreeIPA
Домен: example.test
Имя компьютера: comp01

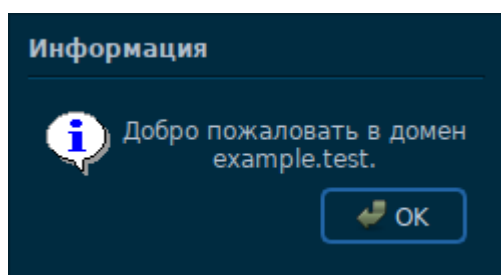
Внимание!
Изменение домена заработает только после перезагрузки компьютера

Применить

В открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, и его пароль и нажать кнопку **ОК**:



В случае успешного подключения, будет выведено соответствующее сообщение:



Перезагрузить рабочую станцию.

Глава 19. Проверка клиента FreeIPA

Проверить, может ли клиент FreeIPA получать информацию о пользователях, определенных на сервере:

```
# id admin
uid=465000000(admin) gid=465000000(admins) группы=465000000(admins)
```

Глава 20. 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, чтобы отменить любые изменения на узле. Причина сбоя установки может быть указана не в конце файла журнала, так как программа установки также записывает в журнал процедуру отката. Для устранения неполадок при неудачной установке клиента FreeIPA следует посмотреть строки с пометкой **ScriptError**.

Глава 21. Повторная регистрация клиента FreeIPA

21.1. В интерактивном режиме

21.2. В пакетном режиме, с использованием **keytab** клиентской системы

В этом разделе рассмотрена процедура повторной регистрации клиента в среде FreeIPA с тем же именем хоста. Повторная регистрация может потребоваться, если клиентский компьютер был уничтожен и потерял связь с серверами FreeIPA, например, из-за аппаратного сбоя клиента.

Во время повторной регистрации клиент создает новый ключ Kerberos и ключи SSH, но идентификатор клиента в базе данных LDAP остается неизменным. После повторной регистрации узел имеет свои ключи и другую информацию в том же объекте LDAP с тем же полным доменным именем, что и раньше, до потери связи машины с серверами FreeIPA.



Примечание

Повторно зарегистрировать можно только тех клиентов, запись о которых в домене все еще активна. Если клиент удалён (**ipa-client-install --uninstall**) или запись его узла отключена (**ipa host-disable**) его нельзя повторно зарегистрировать.

Нельзя повторно зарегистрировать клиента, если он был переименован. Единственный способ переименовать клиента — удалить узел из FreeIPA, изменить имя узла и установить его в качестве клиента FreeIPA с новым именем.

При повторной регистрации, FreeIPA:

- отменяет исходный сертификат хоста;
- создает новые ключи SSH;
- создает новый keytab.

21.1. В интерактивном режиме

Процедура повторной регистрации клиента FreeIPA в интерактивном режиме:

1. Повторно создать клиентский компьютер с тем же именем хоста.
2. Выполнить команду на клиентской машине:

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

3. Скрипт запросит имя пользователя, имеющего право вводить машины в домен, и его пароль (можно использовать администратора по умолчанию, который был создан при установке сервера):

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

21.2. В пакетном режиме, с использованием keytab клиентской системы

Повторная регистрация клиента FreeIPA в пакетном режиме:

1. Создать резервную копию исходного файла keytab.

2. Повторно создать (переустановить) клиентский компьютер, задав ему тоже имя узла.
3. Повторная регистрации клиента, с указанием местоположения файла keytab:

```
# ipa-client-install --keytab /tmp/krb5.keytab -U
This program will set up IPA client.
Version 4.9.11

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
Successfully retrieved CA cert
    Subject:      CN=Certificate Authority,O=EXAMPLE.TEST
    Issuer:       CN=Certificate Authority,O=EXAMPLE.TEST
    Valid From:   2023-08-28 14:28:44
    Valid Until:  2043-08-28 14:28:44

Enrolled in IPA realm EXAMPLE.TEST
Created /etc/ipa/default.conf
Configured /etc/sss/sss.conf
Systemwide CA database updated.
Adding SSH public key from /etc/openssh/ssh_host_rsa_key.pub
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_dsa_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
```



Примечание

Keytab, указанный в параметре **--keytab**, используется только при аутентификации для инициации регистрации. Во время повторной регистрации FreeIPA создаст новый keytab для клиента.

Глава 22. Удаление клиента FreeIPA

При удалении, клиент удаляется из домена FreeIPA вместе с конфигурацией системных служб FreeIPA, таких как демон System Security Services Daemon (SSSD).

Процедура удаления клиента FreeIPA:

1. На клиенте ввести 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
```

На клиенте удалить старые принципы Kerberos, кроме **/etc/krb5.keytab**:

```
# ipa-rmkeytab -k /path/to/keytab -r EXAMPLE.TEST
```

2. На сервере FreeIPA удалить все записи DNS для клиентского узла:

```
# 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 запись узла с сервера FreeIPA LDAP. При этом будут удалены все службы и отозваны все сертификаты, выданные для этого узла:

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



Примечание

Удаление записи узла клиента с сервера LDAP FreeIPA имеет решающее значение, если в будущем нужно будет зарегистрировать клиент с другим IP-адресом или другим именем узла.

Часть V. Ansible

В этой части приводится инструкция по разворачиванию FreeIPA с помощью Ansible.

Содержание

23. Предварительные настройки

24. Установка FreeIPA сервера с помощью Ansible

25. Установка FreeIPA клиентов с помощью Ansible

Глава 23. Предварительные настройки

23.1. Узел управления

23.2. Управляемые узлы

23.3. Роли ansible

23.1. Узел управления

На узле управления должна быть настроена среда Ansible.



Примечание

В Ansible необходимо указать пользователя, под которым будут запущены команды на управляемых узлах, и версию Python. Сделать это можно, добавив в конфигурационный файл Ansible (например, `/etc/ansible/ansible.cfg`) в секцию **[defaults]** строки:

```
remote_user = root
interpreter_python = /usr/bin/python3
```

или в inventory-файл:

```
[all:vars]
ansible_user=root
ansible_python_interpreter=/usr/bin/python3
```

Между узлом управления Ansible и клиентами должно быть настроен беспарольный доступ по ssh (см. [Настройка беспарольного доступа по ssh](#)). Управляемые узлы должны быть указаны в файле `~/.ssh/known_hosts` узла управления. Чтобы создать файл `known_hosts`, необходимо выполнить следующую команду со всеми именами узлов в качестве параметров:

```
$ ssh-keyscan <IP-узел1> <hostname-узел1> ... >> ~/.ssh/known_hosts
```



Примечание

Проверить доступность узлов можно, например, используя модуль **ping**:

```
$ ansible -i inventory/hosts -m ping ipaclients
comp02.example.test | SUCCESS => {
  "changed": false,
  "ping": "pong"
}
```

```
comp01.example.test | SUCCESS => {  
    "changed": false,  
    "ping": "pong"  
}
```

На узле управления Ansible необходимо установить пакет *ansible-freeipa*:

```
# apt-get install ansible-freeipa
```

Пакет *ansible-freeipa* содержит роли и сценарии Ansible для установки и удаления серверов, реплик и клиентов FreeIPA (а также модули для управления группами, узлами, пользователями и топологией).

23.2. Управляемые узлы

На управляемом узле должен быть настроен статический IP-адрес и должен быть доступен репозиторий пакетов.

Управляемые узлы должны быть доступны по протоколу SSH с узла управления.

23.3. Роли ansible

Структура пакета *ansible-freeipa*:

- в каталоге **/usr/share/ansible/roles/** хранятся роли для серверов, реплик и клиентов FreeIPA:

```
$ ls -l /usr/share/ansible/roles  
ipabackup  
ipaclient  
ipareplica  
ipaserver
```

Для каждой роли приводятся примеры, краткое описание и документация (в файле **README.md**):

```
$ ls -l /usr/share/ansible/roles/ipaclient  
action_plugins  
defaults  
library  
meta  
module_utils  
README.md  
tasks  
vars
```

- в каталоге **/usr/share/doc/ansible-freeipa-<версия>/** в файлах **README-*.md** находится документация для каждой роли:

```
$ ls -l /usr/share/doc/ansible-freeipa-1.5.0/  
playbooks  
README-automember.md  
README-automountlocation.md  
README-config.md  
README-delegation.md  
README-dnsconfig.md  
...
```

■ в каталоге `/usr/share/doc/ansible-freeipa-<версия>/playbooks/` находятся примеры playbook;

```
$ ls -l /usr/share/doc/ansible-freeipa-1.5.0/playbooks/  
...  
install-client.yml  
install-cluster.yml  
install-replica.yml  
install-server.yml  
location  
permission  
privilege  
pwpolicy  
remove-all-backups-from-server.yml  
remove-backup-from-server.yml  
...
```

Глава 24. Установка FreeIPA сервера с помощью Ansible

[24.1. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA](#)

[24.2. Установка FreeIPA с внешним DNS, с интегрированным CA в качестве корневого CA](#)

[24.3. Удаление сервера FreeIPA](#)

Развертывание управляется ролью `ipaclient`. По умолчанию роль использует режим автообнаружения для идентификации серверов FreeIPA, домена и других параметров. Роль можно изменить, чтобы playbook Ansible использовал параметры указанные, например, в `inventory`-файле.

24.1. Установка FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA

В данном разделе приведены параметры для `inventory`-файла для установки сервера FreeIPA с интегрированным DNS, с интегрированным CA в качестве корневого CA.

В `inventory`-файле, например, **`inventory/hosts`**, необходимо указать:

1. Полное имя узла (FQDN), который станет сервером FreeIPA. Имя узла должно быть написано строчными буквами. Разрешены только буквенно-цифровые символы и дефисы (-).

2. Домен FreeIPA и пространство Kerberos (realm).
3. Параметр **ipaserver_setup_dns=yes**, чтобы указать, что нужно использовать интегрированный DNS.
4. Настройки DNS. Можно выбрать один из следующих вариантов:
 - » параметр **ipaserver_auto_forwarders=yes**, чтобы установщик использовал DNS-серверы из настроек сети (из файла **/etc/resolv.conf**). Не следует использовать этот параметр, если сервер имен, указанный в файле **/etc/resolv.conf**, содержит адрес **localhost 127.0.0.1**;
 - » параметр **ipaserver_forwarders**, чтобы вручную указать дополнительные серверы;
 - » параметр **ipaserver_no_forwarders=yes**, чтобы настроить корневые DNS-серверы.
5. Параметры обратных зон DNS. Можно выбрать один из следующих вариантов:
 - » параметр **ipaserver_allow_zone_overlap=yes**, чтобы разрешить создание (обратной) зоны DNS, даже если зона уже существует;
 - » параметр **ipaserver_reverse_zones**, чтобы вручную указать обратные зоны;
 - » параметр **ipaserver_no_reverse=yes**, чтобы установщик не настраивал обратные зоны.



Примечание

Использование FreeIPA для управления обратными зонами не является обязательным. Для этой цели можно использовать внешнюю службу DNS.

6. Пароли для администратора FreeIPA и для Directory Manager:
 - » рекомендуется использовать Ansible Vault для хранения пароля и напрямую ссылаться на файл Vault из файла playbook, например:

```
- name: Playbook to configure IPA server
  hosts: ipaservers
  become: true
  vars_files:
    - playbook_sensitive_data.yml

  roles:
    - role: ipaserver
      state: present
```

- » можно указать пароли непосредственно в inventory-файле (менее безопасно, чем предыдущий способ):

```
[...]
[ipaservers:vars]
ipaadmin_password=12345678
ipadm_password=12345678
```

Пример Playbook, который использует principal и пароль из inventory-файла:

```
- name: Playbook to configure IPA server
  hosts: ipaservers
  become: true

  roles:
    - role: ipaserver
      state: present
```

7. Параметр **ipaserver_no_dnssec_validation=yes**, если необходимо выключить DNSSEC (например, если в дальнейшем планируется настраивать доверительные отношения с Active Directory и настраивать сервер пересылки DNS).

8. Параметр **ipaserver_setup_firewalld=no**, если не нужно устанавливать межсетевой экран.



Примечание

Установка пакетов по умолчанию включена. Если установка пакетов не требуется, необходимо установить переменную **ipaserver_install_packages** в значение **no**.

Пример inventory-файла с необходимой информацией о сервере (включая пароли):

```
[ipaservers]
ipa.example.test

[ipaservers:vars]
ipaserver_domain=example.test
ipaserver_realm=EXAMPLE.TEST
ipaserver_setup_dns=yes
ipaserver_auto_forwarders=yes
ipaserver_allow_zone_overlap=yes
ipaserver_no_dnssec_validation=yes
ipaadmin_password=12345678
ipadm_password=12345678
ipaserver_setup_firewalld=no
```



Примечание

Дополнительные параметры, принимаемые ролью ipaserver см. в **/usr/share/ansible/roles/ipaserver/README.md**.

Пример файла playbook **install-server.yml**, содержащего инструкции по развертыванию сервера FreeIPA:

```
---
- name: Playbook to configure IPA server
  hosts: ipaservers
  become: true

  roles:
    - role: ipaserver
      state: present
```

Здесь:

■Метод проверки пользователя:

- строка **hosts: ipaservers** указывает раздел файла **inventory/hosts**, где скрипт ansible ищет полные доменные имена узлов, на которых должен быть запущен скрипт **ipa-server-install**;
- строка **become: true** указывает, что скрипт **ipa-client-install** будет вызываться с правами суперпользователя (root);
- строка **role: ipaserver** указывает роль, которая будет установлена на узле (в данном случае это роль сервера FreeIPA);
- строка **state: present** указывает, что сервер должен быть установлен, а не удален (absent).

■Возможность автоматической установки:

- unattended, -U** — не запрашивать у пользователя информацию.

Установка сервера (уровень детализации указывается с помощью опций **-v**, **-vv** или **-vvv**):

```
$ ansible-playbook -v -i inventory/hosts install-server.yml
Using /etc/ansible/ansible.cfg as config file

PLAY [Playbook to configure IPA server]
*****

TASK [Gathering Facts]
*****
ok: [ipa.example.test]
...
PLAY RECAP
*****
ipa.example.test      : ok=36   changed=20   unreachable=0   failed=0
skipped=37   rescued=0   ignored=0
```

Если узел, определенный как сервер FreeIPA в inventory-файле, уже настроен, Ansible обнаружит это и проверит, соответствуют ли домен и область ожиданиям inventory-файла. Если домен и область совпадают, модуль успешно завершит работу и сообщит, что он не выполнял никаких изменений (changed=False). Если домен или область не соответствуют параметрам, настройка завершится с ошибкой.

24.2. Установка FreeIPA с внешним DNS, с интегрированным СА в качестве корневого СА

Для установки сервера FreeIPA с внешним DNS, с интегрированным СА в качестве корневого СА в inventory файле нужно указать параметр **ipaserver_setup_dns=no**.

24.3. Удаление сервера FreeIPA

Пример файла `playbook uninstall-server.yml`, содержащего инструкции по удалению сервера FreeIPA:

```
---
- name: Playbook to uninstall an IdM replica
  hosts: ipaservers
  become: true

  roles:
  - role: ipaserver
    ipaserver_remove_from_domain: true
    state: absent
```

Удаление сервера (уровень детализации указывается с помощью опций **-v**, **-vv** или **-vvv**):

```
$ ansible-playbook -v -i inventory/hosts uninstall-server.yml
```

Сначала проверяется, установлен ли сервер FreeIPA. Если сервер FreeIPA установлен, осуществляется вызов **ipa-server-install --uninstall -U**, чтобы удалить сервер FreeIPA. Если FreeIPA-сервер не установлен, никаких действий производится не будет (`changed=False`).

Глава 25. Установка FreeIPA клиентов с помощью Ansible

25.1. Настройка параметров в inventory-файле

25.2. Playbook

25.3. Развертывание клиентов FreeIPA

25.4. Удаление клиента FreeIPA

Развертывание клиентов управляется ролью `ipaclient`. По умолчанию роль использует режим автообнаружения для идентификации серверов FreeIPA, домена и других параметров. Роль можно изменить, чтобы `playbook Ansible` использовал параметры указанные, например, в `inventory-файле`.

25.1. Настройка параметров в inventory-файле

В `inventory-файле`, например, **`inventory/hosts`**, необходимо указать:

1. Полное имя узла (FQDN), который станет клиентом FreeIPA. Имя узла должно быть написано строчными буквами. Если записи SRV в зоне DNS FreeIPA установлены правильно, сценарий автоматически обнаружит все остальные требуемые значения.
2. Пароль пользователя, уполномоченного регистрировать клиентов:

■ рекомендуется использовать Ansible Vault для хранения пароля и напрямую ссылаться на файл Vault из файла `playbook`, например:


```
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true
  vars_files:
    - playbook_sensitive_data.yml

  roles:
    - role: ipaclient
      state: present
```

■ можно указать пароль пользователя admin, используя параметр **ipaadmin_password** в разделе **[ipaclients:vars]** файла **inventory/hosts** (менее безопасно, чем предыдущий способ). Если нужно указать другого пользователя (не admin), следует использовать параметр **ipaadmin_principal** для указания имени пользователя, например:

```
[...]
[ipaclients:vars]
ipaadmin_principal=my_admin
ipaadmin_password=Secret123
```

Пример Playbook, который использует principal и пароль из inventory-файла:

```
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true

  roles:
    - role: ipaclient
      state: present
```

■ client keytab из предыдущей регистрации, если он все ещё доступен. Этот параметр доступен, если система ранее уже была зарегистрирована как клиент FreeIPA. Чтобы использовать этот метод аутентификации, следует указать параметр **ipaclient_keytab** в разделе **[ipaclients:vars]** файла **inventory/hosts**, указав путь к файлу, в котором хранится keytab;



Примечание

Если в разделе **[ipaclients:vars]** указывается параметр **ipaclient_keytab**, то также должен быть указан параметр **ipaadmin_keytab**.

■ случайный одноразовый пароль (ОТР), который будет сгенерирован во время регистрации. Чтобы использовать этот метод аутентификации, следует использовать опцию **ipaclient_use_otp** в разделе **[ipaclients:vars]** файла **inventory/hosts**. Одновременно с ОТР также следует указать либо пароль пользователя, уполномоченного регистрировать клиентов (например, указав значение для **ipaadmin_password**), либо admin keytab (например, указав значение для **ipaadmin_keytab**).

3. При невозможности автообнаружения параметров домена, в inventory-файле, необходимо также указать:

- ▶ полное доменное имя сервера в разделе **[ipaservers]**;
- ▶ один из двух следующих параметров:
 - **ipaclient_domain** в разделе **[ipaclients:vars]** для указания DNS-имени FreeIPA, на котором будет зарегистрирован клиент;
 - **ipaclient_realm** в разделе **[ipaclients:vars]** для указания имени области Kerberos, контролируемой сервером FreeIPA.



Примечание

Для возможности использования одноразового пароля (OTP), на узле управления должен присутствовать **/usr/bin/kinit**.



Примечание

Установка клиентских пакетов по умолчанию включена. Если установка пакетов не требуется, необходимо установить переменную **ipaclient_install_packages** в значение **no**.

Пример inventory-файла:

```
[ipaclients]
comp01.example.test
comp02.example.test

[ipaservers]
ipa.example.test

[ipaclients:vars]
ipaclient_domain=example.test
ipaclient_realm=EXAMPLE.TEST
#ipaclient_use_otp=yes
ipaadmin_principal=admin
ipaadmin_password=12345678
```



Примечание

Дополнительные опции, принимаемые ролью ipaclient см. в **/usr/share/ansible/roles/ipaclient/README.md**.

25.2. Playbook

Пример файла playbook **install-client.yml**, содержащего инструкции по развертыванию клиента FreeIPA:

```

---
- name: Playbook to configure IPA clients with username/password
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: present

```

Здесь:

- Метод проверки пользователя:

- строка **hosts: ipaclients** указывает раздел файла **inventory/hosts**, где скрипт **ansible** ищет полные доменные имена узлов, на которых должен быть запущен скрипт **ipa-client-install**;
- строка **become: true** указывает, что скрипт **ipa-client-install** будет вызываться с правами суперпользователя (root);
- строка **role: ipaclient** указывает роль, которая будет установлена на узле (в данном случае это роль клиента FreeIPA);
- строка **state: present** указывает, что клиент должен быть установлен, а не удален (absent).

- Возможность автоматической установки:

- unattended, -U** — не запрашивать у пользователя информацию.

Роль ipaclient принимает параметр **state**, позволяющий настроить или отменить настройку клиента FreeIPA. Если роль вызывается с параметром **state: present** (или параметр **state** не определен) выполняется настройка клиента FreeIPA, а именно:

- установка клиентских пакетов *freeipa-client* (имя пакета зависит от ОС, установленной на управляемом узле);
- настройка клиента FreeIPA.

Пример файла **playbook uninstall-client.yml**, содержащего инструкции по удалению клиента FreeIPA:

```

---
- name: Playbook to unconfigure IPA clients
  hosts: ipaclients
  become: true

  roles:
  - role: ipaclient
    state: absent

```

25.3. Развертывание клиентов FreeIPA

Установка клиентов (уровень детализации указывается с помощью опций **-v**, **-vv** или **-vvv**):

```
$ ansible-playbook -v -i inventory/hosts install-client.yml
Using /etc/ansible/ansible.cfg as config file

PLAY [Playbook to unconfigure IPA clients]
*****

TASK [Gathering Facts]
*****
*****
ok: [comp02.example.test]
ok: [comp01.example.test]
...
PLAY RECAP *****
comp01.example.test      : ok=21    changed=11    unreachable=0    failed=0
skipped=20    rescued=0    ignored=0
comp02.example.test      : ok=21    changed=11    unreachable=0    failed=0
skipped=20    rescued=0    ignored=0
```

Если узел, определенный как клиент FreeIPA в inventory-файле, уже настроен, Ansible обнаружит это и проверит, соответствуют ли домен и область ожиданиям inventory-файла. Если домен и область совпадают, модуль успешно завершит работу и сообщит, что он не выполнял никаких изменений (`changed=False`). Если домен или область не соответствуют параметрам, настройка завершится с ошибкой.

Если узел, определенный как клиент FreeIPA в inventory-файле, еще не настроен как клиент FreeIPA, Ansible настроит клиент FreeIPA.

25.4. Удаление клиента FreeIPA

Удаление клиентов (уровень детализации указывается с помощью опций **-v**, **-vv** или **-vvv**):

```
$ ansible-playbook -v -i inventory/hosts uninstall-client.yml
```

Сначала проверяется, установлен ли клиент FreeIPA. Если клиент FreeIPA установлен, осуществляется вызов **ipa-client-install --uninstall -U**, чтобы отменить настройку клиента FreeIPA. Если FreeIPA-клиент не установлен, никаких действий производится не будет (`changed=False`).

При удалении клиента с узла удаляется только базовая конфигурация FreeIPA, но файлы конфигурации остаются на хосте на случай, если будет необходимо переустановить клиент. Кроме того, удаление имеет следующие ограничения:

- не удаляется запись узла-клиента с LDAP-сервера FreeIPA (выполняется только отмена регистрация узла);
- не удаляются какие-либо службы, находящиеся на клиенте, из FreeIPA;
- не удаляются DNS-записи клиента с сервера FreeIPA;
- не удаляются старые принципалы для keytab, кроме **/etc/krb5.keytab**.

При удалении клиента FreeIPA удаляются все сертификаты, выданные для узла CA.

Часть VI. Интеграция с AD

FreeIPA использует Samba для интеграции в Active Directory. Для работы Samba необходим работающий стек IPv6.

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 IPA домена — EXAMPLE;
- Домен AD — test.alt;
- Сервер AD — dc1.test.alt (192.168.0.122);
- NetBIOS имя AD домена — TEST.

Содержание

[26. Настройка DNS](#)

[27. Подготовка сервера FreeIPA к доверию](#)

[28. Настройка доверия](#)

[29. Удаление доверия](#)

Глава 26. Настройка DNS

[26.1. Настройка зоны перенаправления DNS на сервере FreeIPA](#)

[26.2. Настройка переадресации DNS в AD](#)

[26.3. Проверка конфигурации DNS](#)

Перед подключением FreeIPA и Active Directory (AD) к доверию необходимо убедиться, что серверы видят друг друга и правильно разрешают доменные имена. В этом сценарии описывается настройка DNS для разрешения доменных имен между:

- основным сервером FreeIPA, использующий интегрированный сервер DNS и CA;
- контроллером домена AD.

Для настройки DNS необходимо:

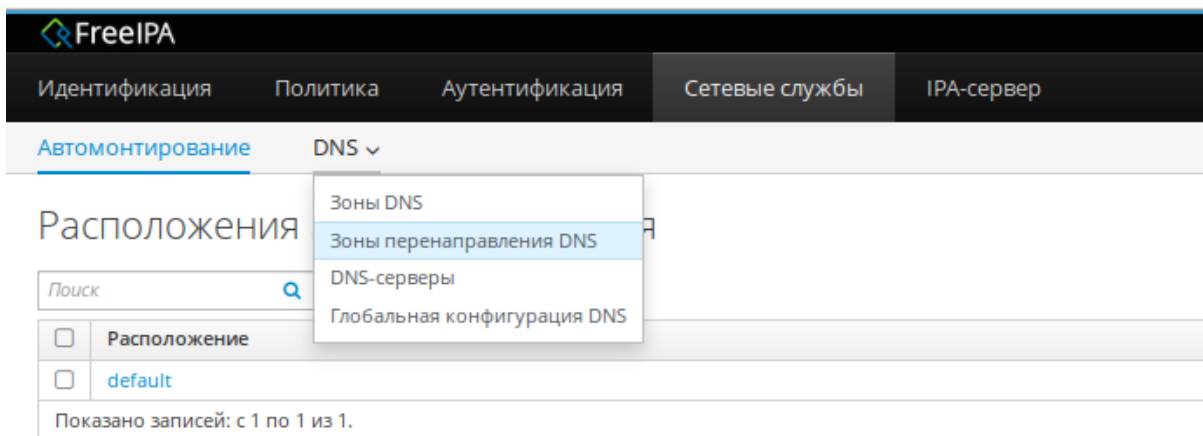
- настроить зоны DNS на сервере FreeIPA;
- настроить условную переадресацию DNS в AD;
- проверить правильность конфигурации DNS.

26.1. Настройка зоны перенаправления DNS на сервере FreeIPA

С помощью зон перенаправления DNS (forward zone) DNS-запросы для определенной зоны можно перенаправлять на другой DNS-сервер. Например, можно перенаправлять DNS-запросы для домена AD на DNS-сервер AD.

Настройка зоны перенаправления 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.
5. В строке **Перенаправители зон** нажать кнопку **Добавить**.
6. В поле **Перенаправители зон** добавить IP-адрес сервера, для которого создается новая зона перенаправления:

Добавить зону перенаправления DNS

Имя зоны *

test.alt

IP-сеть

обратной зоны

Перенаправители*

зон

192.168.0.122

Отменить

Добавить

Политика перенаправления

Сначала перенаправлять

Только перенаправлять

Перенаправление отключено

Пропустить проверку пересечения

* Обязательное поле

Добавить

Добавить и добавить ещё

Добавить и изменить

Отменить

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

FreeIPA

Administrator

Идентификация
Политика
Аутентификация
Сетевые службы
IPA-сервер

Автомониторинг
DNS

Зоны перенаправления DNS

Поиск

Обновить

Удалить

+ Добавить

- Отключить

✓ Включить

	Имя зоны	Состояние	Перенаправители зон	Политика перенаправления
<input type="checkbox"/>	test.alt	✓ Включено	192.168.0.122	first

Показано записей: с 1 по 1 из 1.

Создание зоны переадресации DNS для домена AD в командной строке (следует указать IP-адрес удаленного DNS-сервера с параметром **--forwarder**):

```
# kinit admin
# ipa dnsforwardzone-add test.alt --forwarder=192.168.0.122 --forward-policy=first
```

Сервер проверит DNS-перенаправитель (перенаправители).
 Это может занять некоторое время; пожалуйста, подождите...
 Имя зоны: test.alt.
 Активная зона: TRUE
 Перенаправители зон: 192.168.0.122
 Политика перенаправления: first



Примечание

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

Если включить проверку DNSSEC на удаленном DNS-сервере нельзя, можно отключить DNSSEC на сервере FreeIPA. Для этого в файле **/etc/bind/ipa-options-ext.conf** следует привести параметры **dnssec-validation** и **dnssec-enable** к виду:

```
dnssec-enable no;  
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    192.168.0.122
```

26.2. Настройка переадресации DNS в AD

В этом разделе описывается, как настроить переадресацию DNS в Active Directory для сервера FreeIPA.

26.2.1. Samba DC

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
```

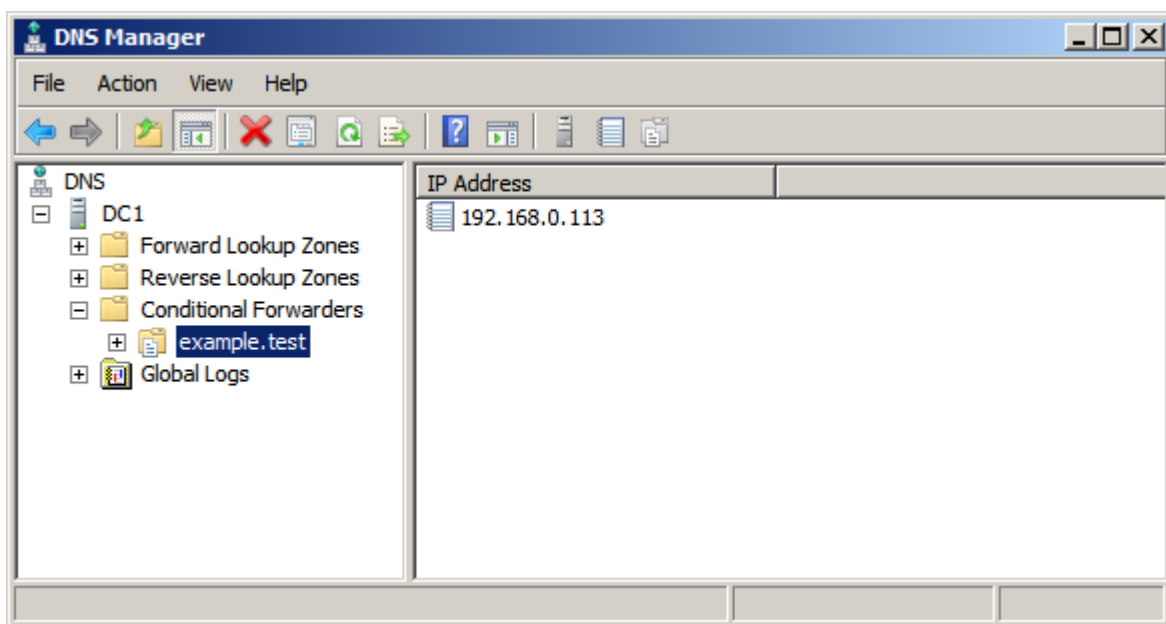
26.2.2. Windows Server с AD

На AD сервере создать сервер условной пересылки для зоны IPA домена.

В графическом интерфейсе:

1. Открыть **Диспетчер DNS (DNS Manager)**.

- В разделе **Серверы условной пересылки (Conditional Forwarders)** добавить новый сервер пересылки указав FQDN и IP-адрес сервера FreeIPA:



- 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
```

26.3. Проверка конфигурации DNS

Перед настройкой доверия необходимо убедиться, что серверы FreeIPA и AD могут разрешать себя и друг друга.

26.3.1. На сервере FreeIPA

Проверить наличие записей для работы сервисов IPA на DNS-сервере IPA:

- 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 IPA.

- Запись отвечающая за имя Kerberos realm IPA домена:

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

- Наличие записей для работы сервисов AD на DNS-сервере IPA:

```
# 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, обновите конфигурацию DNS, добавив недостающие записи:

»Если в среде FreeIPA используется встроенный DNS-сервер:

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

»Если в среде IPA не используется встроенный DNS-сервер. На сервере FreeIPA экспортировать записи DNS в файл:

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

Отправить запрос на обновление DNS на DNS-сервер с помощью утилиты **nsupdate** и файла **dns_records.nsupdate**. Или добавить DNS-записи на сервер другим способом.

26.3.2. На сервере AD

Проверить наличие записей DNS-сервере AD:

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 IPA домена:

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

"EXAMPLE.TEST"
```

Глава 27. Подготовка сервера FreeIPA к доверию

Установить необходимые пакеты:

```
# 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.

admin password:
```

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

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
```

Скрипт спросит необходимо ли конфигурировать плагин *slapi-nis* для поддержки работы старых клиентов (SSSD < 1.9) с пользователем из доверенного домена:

```
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
```

Перезапустить ipa:

```
# ipactl restart
Restarting Directory Service
Restarting krb5kdc Service
Restarting kadmind 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 -k
lpcfg_do_global_parameter: WARNING: The "domain logons" option is deprecated

  Sharename      Type      Comment
  -----
  IPC$           IPC       IPC Service (Samba 4.16.11)
...
```

Глава 28. Настройка доверия

[28.1. В командной строке](#)

[28.2. В веб-интерфейсе](#)

[28.3. Проверка конфигурации Kerberos](#)

28.4. Проверка конфигурации доверия в FreeIPA

28.5. Проверка конфигурации доверия в AD

28.6. Проверка пользователей доверенного домена

Сервер FreeIPA позволяет настроить три типа соглашений о доверии:

- **одностороннее доверие** — вариант по умолчанию. Одностороннее доверие позволяет пользователям и группам AD получать доступ к ресурсам в FreeIPA, но не наоборот. Домен FreeIPA доверяет лесу AD, но лес AD не доверяет домену FreeIPA;
- **двустороннее доверие** — позволяет пользователям и группам AD получать доступ к ресурсам в FreeIPA. Обратите внимание, что эта функция двустороннего доверия не позволяет пользователям FreeIPA входить в системы Windows, а двустороннее доверие в FreeIPA не дает пользователям никаких дополнительных прав по сравнению с решением одностороннего доверия в AD. Чтобы создать двустороннее доверие в команду следует добавить параметр **--two-way=true**;
- **внешнее доверие** — доверительные отношения между FreeIPA и доменом AD в разных лесах. В то время как доверие леса всегда требует установления доверия между FreeIPA и корневым доменом леса Active Directory, внешнее доверие может быть установлено от FreeIPA к домену в лесу. Рекомендуется только в том случае, если невозможно установить доверие леса между корневыми доменами леса по административным или организационным причинам. Чтобы создать внешнее доверие в команду следует добавить параметр **--external=true**.

28.1. В командной строке

Добавление двунаправленных доверительных отношений леса (Forest Trust) с AD:

```
# kinit admin
# ipa trust-add --type=ad test.alt --admin Administrator --password --two-way=true
Пароль администратора домена Active Directory:
...
```

При появлении запроса следует ввести пароль администратора домена Active Directory.



Важно

Учетная запись пользователя, используемая при создании доверия (аргумент опции **--admin**), должна быть членом группы Domain Admins. Имя учетной записи должно быть на английском языке.



Примечание

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

Получить список доверенных доменов леса со стороны AD:

```
# ipa trust-fetch-domains test.alt
```

```
-----  
Список надёжных доменов успешно обновлён. Используйте команду trustdomain-find  
для вывода этого списка.  
-----
```

```
-----  
Количество возвращённых записей 0  
-----
```

Чтобы увидеть список всех доверенных доменов из леса используйте следующую команду:

```
# ipa trustdomain-find test.alt
```

```
Имя домена: test.alt
```

```
Имя домена NetBIOS: TEST
```

```
Идентификатор безопасности домена: S-1-5-21-90931260-536030259-1550036695
```

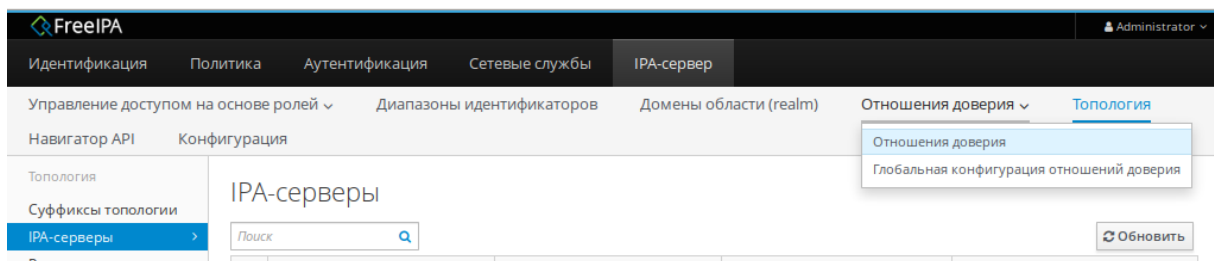
```
Домен включён: True  
-----
```

```
Количество возвращённых записей 1  
-----
```

28.2. В веб-интерфейсе

Настройка доверительных отношений:

1. В веб-интерфейсе 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 Active Directory. В поля **Учетная запись** и **Пароль** указать учетные данные администратора AD:

FreeIPA

Администратор

Идентификация Политика

Управление доступом на основе ролей

Навигатор API Конфигурация

Отношения доверия

Поиск

☐ Имя области (realm)

Отсутствуют записи.

Добавить отношение доверия

Домен * test.alt

Двустороннее отношение доверия ☐

Внешнее отношение доверия ☐

Установить с помощью

☒ Учётная запись администратора

Учётная запись * Administrator

Пароль *

☐ Общий пароль

Пароль

Проверить пароль

Тип диапазона

☒ Определить

☐ Домен Active Directory

☐ Домен Active Directory с атрибутами POSIX

Основной ID

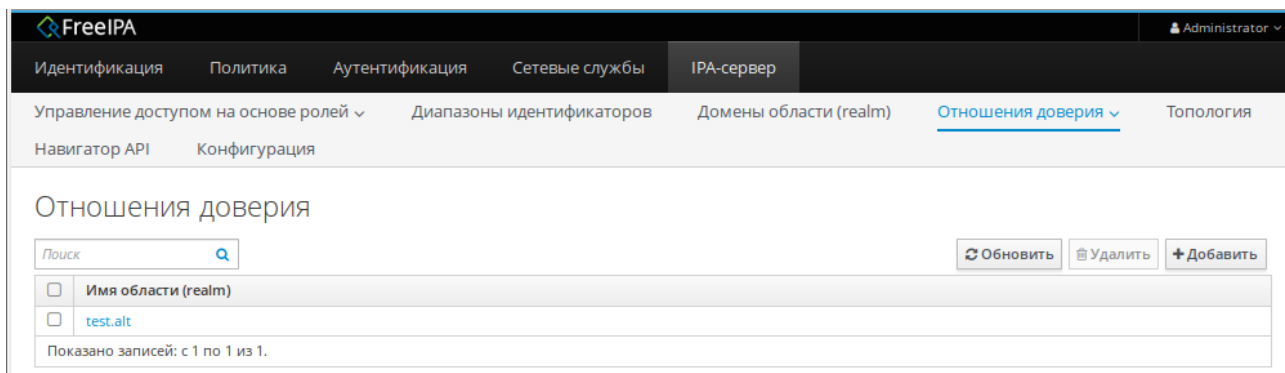
Размер диапазона

* Обязательное поле

Добавить Добавить и добавить ещё Добавить и изменить Отменить

5. (Необязательно) Отметить пункт **Двустороннее отношение доверия**, если нужно разрешить пользователям и группам AD доступ к ресурсам в FreeIPA. Однако двустороннее доверие в FreeIPA не дает пользователям никаких дополнительных прав по сравнению с односторонним доверием в AD. Оба решения считаются одинаково безопасными из-за настроек фильтрации SID доверия между лесами по умолчанию.
6. (Необязательно) Отметить пункт **Внешнее отношение доверия**, если настраивается доверие с доменом AD, который не является корневым доменом леса AD.
7. (Необязательно) По умолчанию сценарий установки доверия пытается определить соответствующий тип диапазона идентификаторов. Также можно явно задать тип диапазона идентификаторов.
8. Нажать кнопку **Добавить**.

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



28.3. Проверка конфигурации Kerberos

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

Запросить билет для пользователя AD:

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

Запросить service ticket для сервиса из FreeIPA домена:

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

Запросить service ticket сервиса из AD домена:

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

Если билет службы AD предоставлен, в списке билетов будет отображаться билет на предоставление билетов между областями (TGT) — krbtgt/IPA.DOMAIN@AD.DOMAIN (в примере: krbtgt/EXAMPLE.TEST@TEST.ALT):

```
# klist
Ticket cache: KEYRING:persistent:500:krb_ccache_QfXae5u
Default principal: ivanov@TEST.ALT

Valid starting    Expires          Service principal
07.09.2023 12:28:14 07.09.2023 22:27:51 cifs/dc1.test.alt@TEST.ALT
    renew until 08.09.2023 12:27:46
07.09.2023 12:27:33 07.09.2023 22:27:51 host/ipa.example.test@EXAMPLE.TEST
    renew until 08.09.2023 12:27:46
07.09.2023 12:28:05 07.09.2023 22:27:51 krbtgt/EXAMPLE.TEST@TEST.ALT
    renew until 08.09.2023 12:27:46
07.09.2023 12:27:51 07.09.2023 22:27:51 krbtgt/TEST.ALT@TEST.ALT
    renew until 08.09.2023 12:27:46
```


28.4. Проверка конфигурации доверия в 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.`

28.5. Проверка конфигурации доверия в AD



Примечание

Необходимо войти в систему с правами администратора.

Проверка конфигурации доверия в AD:

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

```
C:\> nslookup.exe
> set type=SRV
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.domc.testc internet address = 192.168.0.122
> _ldap._tcp.dc._msdcs.test.alt.
_ldap._tcp.dc._msdcs.test.alt.      SRV service location:
      priority = 0
      weight = 100
      port = 389
      svr hostname = dc1.dtest.alt.
dc1.domc.testc internet address = 192.168.0.122
```

28.6. Проверка пользователей доверенного домена

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

На рабочей станции FreeIPA выполнить команду:

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

где `ivanov` — это пользователь из AD домена.

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

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

Вывод команды должен стать таким:

```
# systemctl restart sssd
# getent passwd ivanov@test.alt
ivanov@test.alt:*:348001105:348001105:Иван Иванов:/home/test.alt/ivanov:/bin/bash
```

В результате пользователи AD получают возможность авторизоваться и входить на рабочие станции в домене под управлением FreeIPA. Для входа AD пользователя на рабочую станцию в домене под управлением FreeIPA, идентификатор пользователя должен быть указан 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 29. Удаление доверия

29.1. В командной строке

29.2. В веб-интерфейсе

29.3. Удаление диапазона ID после удаления доверия к AD

В этом разделе описывается, как удалить доверие FreeIPA/AD на стороне FreeIPA.

29.1. В командной строке

Удаление доверия:

1. Удалить конфигурацию доверия из FreeIPA:

```
# ipa trust-del test.alt
```

2. Удалить объект доверия из конфигурации Active Directory.
3. Проверить, что доверие удалено:

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



Примечание

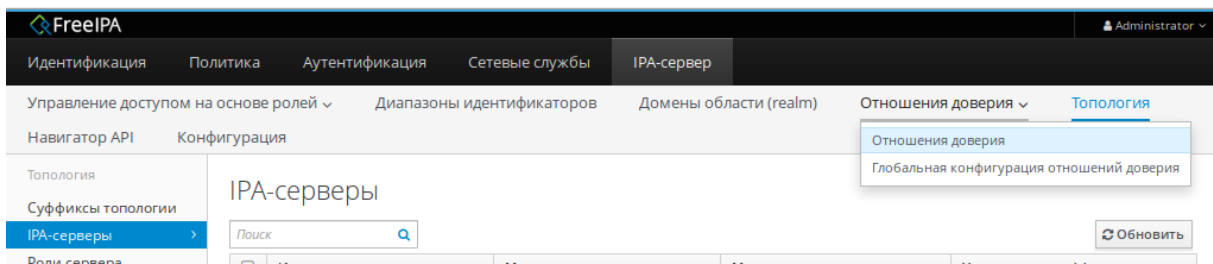
Удаление конфигурации доверия не приводит к автоматическому удалению диапазона идентификаторов, которые FreeIPA создал для пользователей AD. Таким образом, если доверие будет снова добавлено, существующий диапазон идентификаторов будет использоваться повторно.

Поэтому следует удалить диапазон идентификаторов пользователей AD (см. [Удаление диапазона ID после удаления доверия к AD](#)).

29.2. В веб-интерфейсе

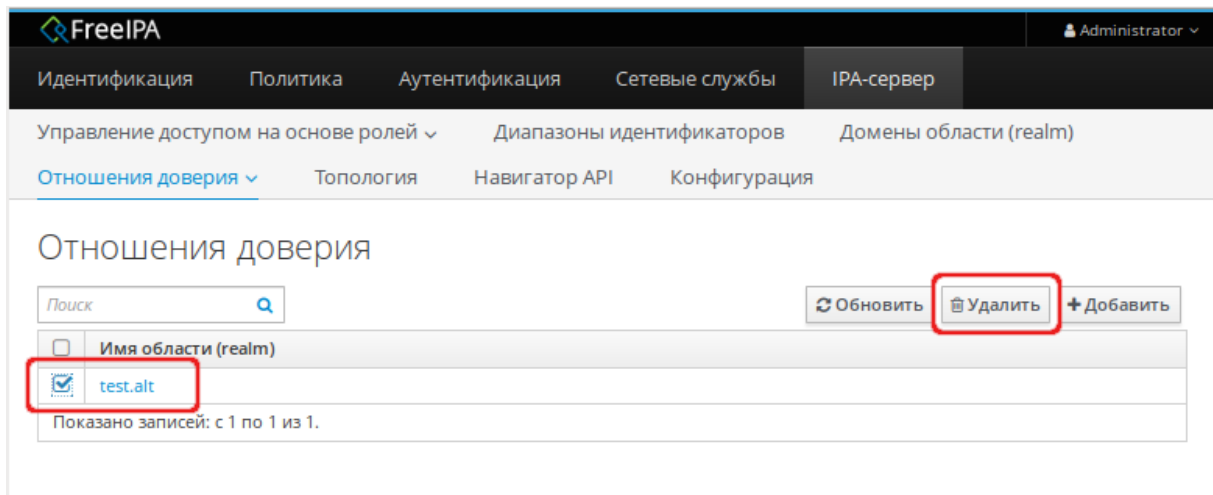
Удаление доверия:

1. В веб-интерфейсе перейти на вкладку **IPA-сервер**.
2. Выбрать пункт меню **Отношения доверия** → **Отношения доверия**:

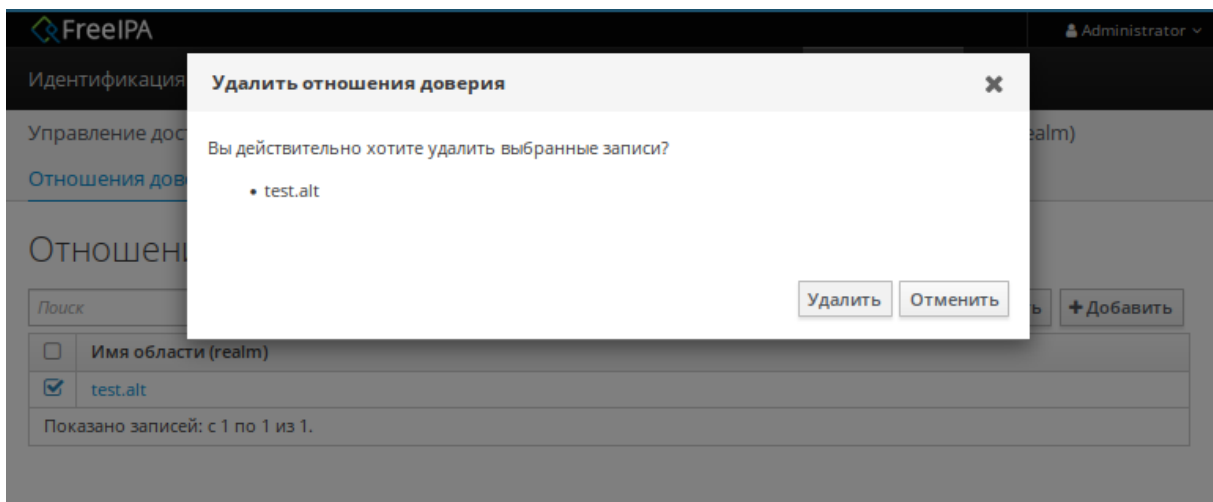


3. Выбрать объект доверия, которое требуется удалить.

4. Нажать кнопку **Удалить**:



5. В диалоговом окне **Удалить отношения доверия** нажать кнопку **Удалить**:



6. Удалить объект доверия из конфигурации Active Directory.

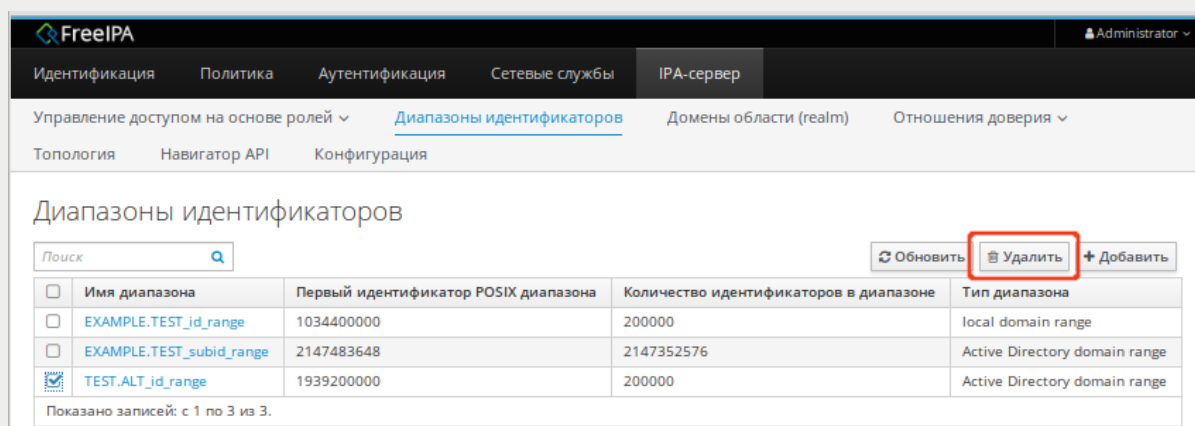
Если доверие было успешно удалено, сообщение об этом появится во всплывающем окне.



Примечание

Удаление конфигурации доверия не приводит к автоматическому удалению диапазона идентификаторов, которые FreeIPA создал для пользователей AD. Таким образом, если доверие будет снова добавлено, существующий диапазон идентификаторов будет использоваться повторно.

Удалить диапазон идентификаторов пользователей AD, после удаления конфигурации доверия и объекта доверия, можно на вкладке «Диапазоны идентификаторов»:



29.3. Удаление диапазона ID после удаления доверия к AD

Чтобы удалить всю информацию, связанную с доверием AD, после удаления конфигурации доверия и объекта доверия следует удалить диапазон идентификаторов пользователей AD.

Процедура удаления диапазонов 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. Определить диапазон идентификаторов, связанный с удалённым доверием. Первая часть имени диапазона идентификаторов — это имя доверия, например, TEST.ALT_id_range. Удалить диапазон:

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

3. Перезапустить службу SSSD, чтобы удалить ссылки на удаленный диапазон идентификаторов:

```
# systemctl restart sssd
```

Часть VII. Конфигурирование FreeIPA

Содержание

[30. Управление пользователями](#)

[31. Двухфакторная аутентификация](#)

Глава 30. Управление пользователями

[30.1. Управление пользователями в командной строке](#)

[30.2. Управление пользователями в веб-интерфейсе](#)

FreeIPA поддерживает три состояния учётной записи пользователя:

- **Неподтверждённые пользователи** — на этом этапе пользователям не разрешено проходить аутентификацию. Некоторые свойства учётной записи пользователя, необходимые для активных пользователей, например, членство в группе, не могут быть установлены. Данное состояние можно использовать, если нужно подготовить новые учетные записи пользователей, затем их можно будет активировать.
- **Активные пользователи** — это пользователи, которым разрешено проходить аутентификацию. В этом состоянии должны быть установлены все свойства учетной записи пользователя.
- **Хранимые пользователи** — это бывшие активные пользователи, которые считаются неактивными и не могут аутентифицироваться в FreeIPA. У сохранённых пользователей сохраняется большая часть свойств учётных записей, но они не входят ни в какие группы пользователей.

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

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

При сохранении FreeIPA переводит все символы имени учётной записи в нижний регистр (поэтому при входе пользователя используются только строчные буквы и нельзя создать пользователей, у которых имя учётной записи отличается только регистром букв).

Максимальная длина имени учётной записи по умолчанию составляет 32 символа. Для изменения длины используется команда **ipa config-mod --maxusername**. Например, увеличение максимальной длины имени учётной записи 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

Удаленные учетные записи пользователей не могут быть восстановлены. При удалении учетной записи пользователя вся информация, связанная с учетной записью, безвозвратно теряется.



Важно

Не удаляйте пользователя `admin`. Если вы хотите определить и использовать альтернативного пользователя-администратора, следует после того, как вы предоставили права администратора хотя бы одному другому пользователю, отключить предопределенного пользователя-администратора с помощью команды **`ipa user-disable admin`**.

30.1. Управление пользователями в командной строке

Команда **`ipa user-add`** используется для добавления активных пользователей. Для создания неподтвержденных учетных записей используется команда **`ipa stageuser-add`**.



Примечание

FreeIPA автоматически присваивает уникальный идентификатор пользователя (UID) новым учетным записям пользователей. Можно присвоить UID вручную, но так как сервер не проверяет уникальность номера UID, нескольким пользователям может быть назначен один и тот же UID.

Для возможности выполнения команд должны выполняться следующие условия:

- » пользователь должен обладать административными привилегиями или иметь роль **User Administrator**;
- » получен билет Kerberos.

Команда добавления нового пользователя:

```
$ ipa user-add <логин> --first=<имя> --last=<фамилия> --email=<email>
```

Пример добавления неподтвержденного пользователя:

```
$ ipa stageuser-add markov --first=Илья --last=Марков --email=markov@example.test
-----
Добавлен неподтвержденный 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
```

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

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

Просмотр списка всех пользователей с подробной информацией:

```
$ ipa user-find
```

Активация пользователя:

```
$ ipa stageuser-activate <логин>
```

Пример активации 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
```

Для сохранения возможности восстановить учётную запись после удаления, её можно сохранить.
Для сохранения учётной записи используется параметр **--preserve** команды **ipa user-del**:

```
$ ipa user-del --preserve <логин>
```

Например:


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

Для удаления пользователей используются команды:

- **ipa user-del <логин>** — удалить активного или хранимого пользователя;
- **ipa stageuser-del <логин>** — удалить неподтверждённого пользователя.

Чтобы удалить сразу нескольких пользователей используется параметр **--continue**:

```
$ ipa user-del --continue user1 user2 user3
-----
Preserved user "markov"
-----
```

Пример удаления пользователя:

```
$ ipa user-del markov
-----
Удален пользователь "markov"
-----
```

Для восстановления сохранённых пользователей используется команда **ipa user-undel <логин>**. При восстановлении учётной записи восстанавливаются не все предыдущие атрибуты учетной записи. Например, пароль пользователя не восстанавливается и должен быть установлен заново.

Пример восстановления активного пользователя:

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

30.2. Управление пользователями в веб-интерфейсе

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

Идентификация Политика Аутентификация Сетевые службы IPA-сервер								
Пользователи Узлы Службы Группы Представления ID Автоучастник Subordinate IDs								
Категории пользователей Активные пользователи Неподтверждённые пользователи Хранимые пользователи	Активные пользователи							
	Поиск <input type="text"/> <input type="button" value="Обновить"/> <input type="button" value="Удалить"/> <input type="button" value="+ Добавить"/> <input type="button" value="- Отключить"/> <input type="button" value="✓ Включить"/> Действия <input type="button" value="v"/>							
	<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона
	<input type="checkbox"/>	admin		Administrator	✓ Включено	948000000		
Показано записей: с 1 по 3 из 3.								

Для управления пользователями необходимо обладать административными привилегиями или иметь роль **User Administrator**.

30.2.1. 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**.

Добавить неподтверждённого пользователя

Имя учётной записи пользователя

markov

Имя *

Марков

Фамилия *

Илья

Класс

Новый пароль

.....

Проверить пароль

.....

* Обязательное поле

Добавить

Добавить и добавить ещё

Добавить и изменить

Отменить



Примечание

Если оставить поле **Имя учётной записи пользователя** пустым, FreeIPA попытается создать это имя (логин) таким образом: первая буква имени + фамилия. Но так как логин не может содержать символы кириллицы, поле логин можно не заполнять только, если **Имя** и **Фамилия** записываются на латинице.

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

Добавить пользователя

Имя учётной записи пользователя

isakova

Имя *

Ольга

Фамилия *

Исакова

Класс

Без личной группы

☐

ID группы

948000000

Новый пароль

.....

Проверить пароль

.....

* Обязательное поле

Добавить

Добавить и добавить ещё

Добавить и изменить

Отменить

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**):

Пользователи

Узлы

Службы

Группы

Представления ID

Автоучастник

Subordinate IDs

Категории пользователей

Активные пользователи

Неподтверждённые пользователи

Хранимые пользователи

Неподтверждённые пользователи

Поиск

Обновить

Удалить

Добавить

Активировать

<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	markov	Марков	Илья	-1	markov@example.test		

Показано записей: с 1 по 1 из 1.

Примечание

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

30.2.2. 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.

Для активации пользователя необходимо:

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

	Имя учётной записи пользователя	Имя	Фамилия	UID	Адрес электронной почты	Номер телефона	Должность
<input checked="" type="checkbox"/>	markov	Марков	Илья	-1	markov@example.test		

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

Подтверждение

Вы действительно хотите активировать выбранные записи пользователей?

ОК Отменить

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

30.2.3. Отключение/Включение учётной записи пользователя

Активную учётную запись можно отключить. Отключение пользователя деактивирует учетную запись, поэтому её нельзя будет использовать для аутентификации.

В отличие от сохранённых учётных записей, отключённые учётные записи остаются в активном состоянии и могут быть членами групп.



Примечание

После отключения учётной записи любые существующие подключения остаются в силе 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**:

Активные пользователи								
<input type="text" value="Поиск"/>		<input type="button" value="Обновить"/>		<input type="button" value="Удалить"/>		<input type="button" value="+ Добавить"/>		<input type="button" value="- Отключить"/> <input type="button" value="✓ Включить"/>
<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	948000000			
<input checked="" type="checkbox"/>	isakova	Ольга	Исакова	✓ Включено	948000007	isakova@example.test		
<input type="checkbox"/>	ivanov	Илья	Иванов	✓ Включено	948000003	ivanov@example.test		

4. В открывшемся диалоговом окне нажать кнопку **ОК**.

Убедиться, что процедура включения/отключения учётной записи прошла успешно можно в столбце **Состояние**:

Активные пользователи								
<input type="text" value="Поиск"/>		<input type="button" value="Обновить"/>		<input type="button" value="Удалить"/>		<input type="button" value="+ Добавить"/>		<input type="button" value="- Отключить"/> <input type="button" value="✓ Включить"/>
<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	948000000			
<input type="checkbox"/>	isakova	Ольга	Исакова	— Отключён	948000007	isakova@example.test		
<input type="checkbox"/>	ivanov	Илья	Иванов	✓ Включено	948000003	ivanov@example.test		

30.2.4. Сохранение учётной записи

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



Примечание

Список хранимых пользователей может предоставить историю прошлых учетных записей пользователей.

Для перевода учётной записи в статус хранимой необходимо:

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

Активные пользователи								
Поиск		Обновить		Удалить	+ Добавить	Отключить	Включить	Действия
<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	948000000			
<input checked="" type="checkbox"/>	isakova	Ольга	Исакова	✓ Включено	948000007	isakova@example.test		
<input type="checkbox"/>	ivanov	Илья	Иванов	✓ Включено	948000003	ivanov@example.test		

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

Удалить пользователей ✕

Вы действительно хотите удалить выбранные записи?

- isakova

Режим удаления ☐ удалить ☒ сохранить

Удалить

Отменить

Учётная запись будет перемещена в список хранимых пользователей.

30.2.5. Восстановление учётной записи

Сохранённую учётную запись можно перевести в активное или неподтверждённое состояние.

Для восстановления учётной записи необходимо:

1. Перейти на вкладку **Пользователи** → **Хранимые пользователи**;
2. Выбрать учётные записи, которые необходимо восстановить.

3. Нажать кнопку **Восстановить**:

Хранимые пользователи

Поиск

<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	UID	Адрес электронной почты	Номер телефона	Должность
<input checked="" type="checkbox"/>	isakova	Ольга	Исакова	948000007	isakova@example.test		

Показано записей: с 1 по 1 из 1.

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

Учётная запись будет перемещена в список активных пользователей.

30.2.6. Удаление учётной записи

Удаление пользователей является необратимой операцией, в результате которой учётные записи удаляются из базы данных FreeIPA (включая членство в группах и пароли). Любая внешняя конфигурация для пользователя, например, системная учетная запись, домашний каталог, не удаляется, но становится недоступной через FreeIPA.

Для удаления учётной записи необходимо:

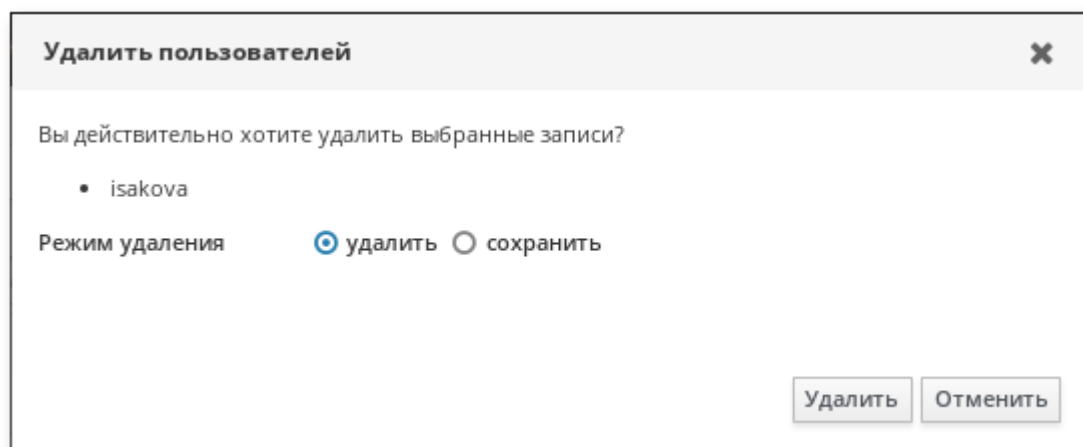
1. Перейти на вкладку **Пользователи** → **Активные пользователи** (или **Пользователи** → **Неподтверждённые пользователи**, **Пользователи** → **Хранимые пользователи**);
2. Выбрать учётные записи, которые необходимо удалить.
3. Нажать кнопку **Удалить**:

Активные пользователи

Поиск

<input type="checkbox"/>	Имя учётной записи пользователя	Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
<input type="checkbox"/>	admin		Administrator	✓ Включено	948000000			
<input checked="" type="checkbox"/>	isakova	Ольга	Исакова	✓ Включено	948000007	isakova@example.test		
<input type="checkbox"/>	ivanov	Илья	Иванов	✓ Включено	948000003	ivanov@example.test		

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



Учётная запись будет удалена из FreeIPA.

Глава 31. Двухфакторная аутентификация

31.1. Методы аутентификации

31.2. Разрешения (Permissions)

31.3. Управление функциями

31.4. Пример настройки двухфакторной аутентификации

31.5. Аутентификация

Использование двухфакторной аутентификации (2FA) — это один из способов повысить безопасность аутентификации. Одним из наиболее популярных вариантов является использование одноразовых паролей (OTP). Существуют открытые стандарты механизмов OTP:

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

31.1. Методы аутентификации

Во FreeIPA способы аутентификации пользователей могут быть установлены глобально или отдельно для каждого пользователя. Установка нескольких способов аутентификации позволяет использовать любой из указанных методов (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

- »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 установлено это значение, аутентификация только по паролю будет разрешена только в том случае, если у пользователя не определены токены.



Примечание

При выборе значения **Отключить переопределение на уровне пользователя** (может быть установлено только глобально), для всех пользователей, независимо от их собственных настроек, будет требоваться парольная аутентификация:

Добро пожаловать

.....

Первый фактор

Отмена Войти

Добро пожаловать

|

Второй фактор (необязательно)

Отмена Войти

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

31.2. Разрешения (Permissions)

У токена может быть либо ноль, либо один владелец. Если у токена нет владельца, он считается не назначенным. У владельца токена есть следующие права:

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

У токенов может быть ноль или более менеджеров. У менеджера токена есть следующие права:

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



Примечание

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

Администраторы могут создавать токены, которые либо не назначены/не управляемы, либо принадлежат и/или управляются любым пользователем. Пользователи могут создавать токены только себе (при этом они становятся владельцами и менеджерами созданного токена).

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**).

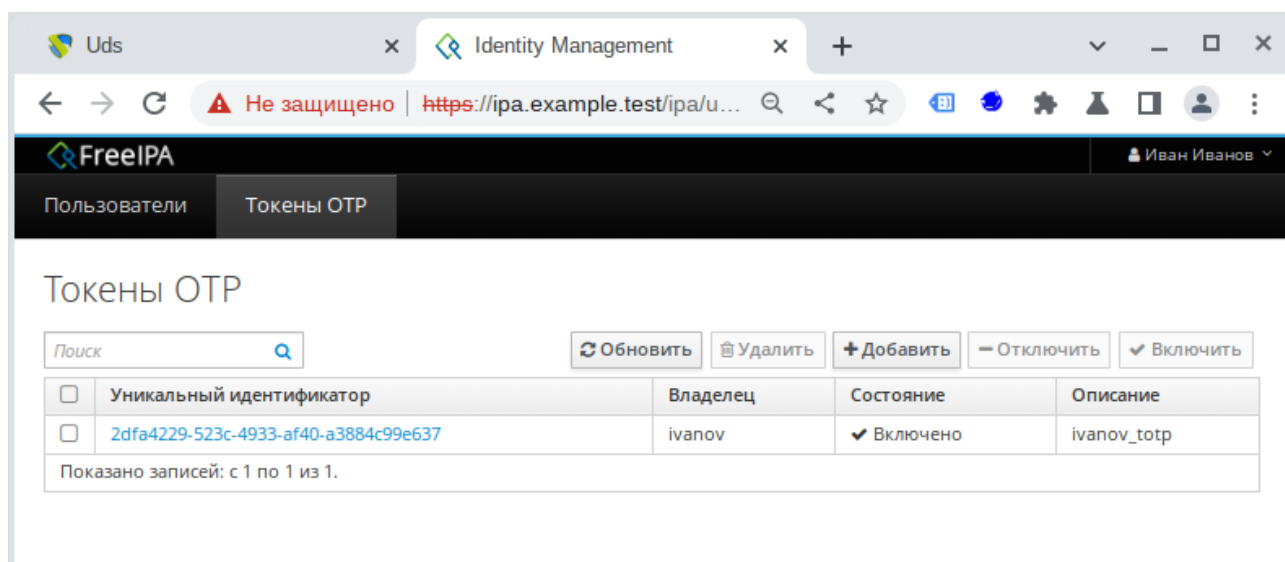
Методы аутентификации для каждого пользователя будут доступны на странице пользователя (**Идентификация** → **Пользователи** → **Пользователь** → **Типы аутентификации пользователей**).

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 страницу синхронизации предоставляется 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:

- установить глобально 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-qr-code
Добавить менеджера для токена	otptoken-add-managedby	--users=STR

Описание	Команда	Опции
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/JK0szbZGmTElSrIh70E3QruXqu+W4=
Алгоритм: sha1
Цифры: 6
Смещение времени: 0
Временной интервал: 30
Универсальный код ресурса (URI):
otppath://totp/ivanov@EXAMPLE.TEST:ivanov_otp?issuer=ivanov%40EXAMPLE.TEST
&secret=TFXYWBSYV3CKR4W46CN7ZEU0WM3NSGTEYSKSVYJCB32BG5BLXF5K56L0&digits=6&algor
ithm=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

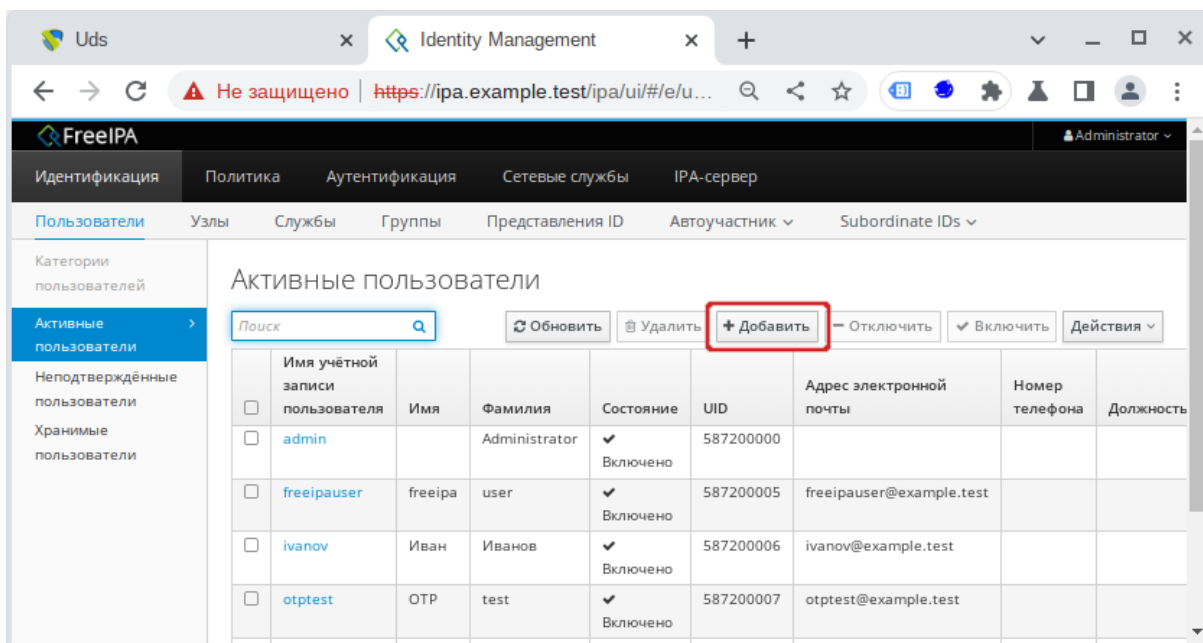
&secret=Q4ZUUJBjNGQG7ZYHI2PK7D6XIEL6D30XR0STR5CYVPMJVYZVACZP5JG&digits=6&algorit
  hm=SHA1&period=30
```


Отсканировать полученный QR-код с помощью FreeOTP.

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**:

Добавить пользователя

✕

Имя учётной записи пользователя

otpuser

Имя *

OTP

Фамилия *

user

Класс

Без личной группы

☐

ID группы

Новый пароль

.....

Проверить пароль

.....

* Обязательное поле

Добавить

Добавить и добавить ещё

Добавить и изменить

Отменить

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

FreeIPA Administrator

Идентификация Политика Аутентификация Сетевые службы IPA-сервер

Пользователи Узлы Службы Группы Представления ID Автоучастник Subordinate IDs

Активные пользователи > otpuser

✓ Пользователь: otpuser

otpuser является участником:

Параметры Группы пользователей (1) Сетевые группы Роли Правила HBAC Правила Sudo Subordinate ids

Обновить Вернуть Сохранить Действия

Параметры идентификации

Должность

Имя * OTP

Фамилия * user

Полное имя * OTP user

Отображаемое имя OTP user

Инициалы Ou

GECOS OTP user

Класс

Параметры учётной записи

Имя учётной записи пользователя otpuser

Пароль *****

Окончание действия пароля 2023-05-09 12:04:30Z

UID 587200004

ID группы 587200004

Псевдоним учётной записи otpuser@EXAMPLE.TEST Удалить

Добавить

Окончание действия учётной записи Kerberos YYYY-MM-DD hh : mi UTC

Типы аутентификации пользователей

- ☐ Пароль
- ☐ RADIUS
- ☒ Двухфакторная аутентификация (пароль + OTP)
- ☐ PKINIT
- ☐ Пароль с усиленной защитой (SPAKE или FAST)
- ☐ External Identity Provider

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

Identity Management

Не защищено | https://ipa.example.test/ipa/ui/...

FreeIPA OTP user

Пользователи Токены OTP

Токены OTP

Поиск

Обновить Удалить + Добавить Отключить Включить

<input type="checkbox"/> Уникальный идентификатор	Владелец	Состояние	Описание
Отсутствуют записи.			

Добавить токен OTP

✕

Тип

☒ На основе времени (TOTP)

☐ На основе счётчика (HOTP)

Описание

otpuser_token

* Обязательное поле

Добавить

Добавить и добавить ещё

Добавить и изменить

Отменить

6. Настроить токен, отсканировав полученный QR-код, например, с помощью FreeOTP.



Примечание

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

Добавить токен OTP

Тип

☒ На основе времени (TOTP)
☐ На основе счётчика (HOTP)

Уникальный идентификатор

Описание

otpuser_token

Владелец

otpuser

Начало срока действия

YYYY-MM-DD

hh

:

mm

UTC

Окончание срока действия

YYYY-MM-DD

hh

:

mm

UTC

Поставщик

Модель

Серийный номер

Ключ

Алгоритм

☒ sha1 ☐ sha256 ☐ sha384 ☐ sha512

Цифры

☒ 6 ☐ 8

Временной интервал (в секундах)

* Обязательное поле

Добавить

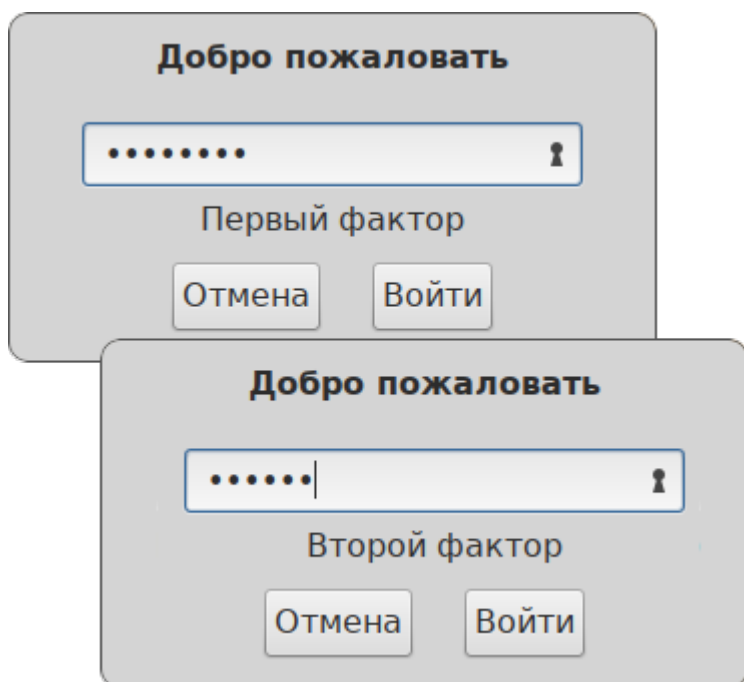
Добавить и добавить ещё

Добавить и изменить

Отменить

31.5. Аутентификация

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



Примечание

В ОС Альт Рабочая станция К 10.1 в качестве менеджера входа в систему по умолчанию используется SDDM. Чтобы иметь возможность использовать двухфактурную аутентификацию, следует перейти на LightDM.

Чтобы заменить менеджер входа в систему с SDDM на LightDM необходимо:

1. Установить пакет *lightdm-kde-greeter* и все его зависимости:

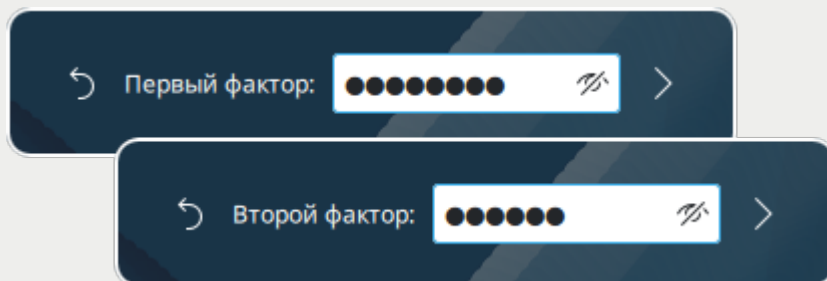
```
# apt-get install lightdm-kde-greeter
```

2. Отключить менеджер входа в систему по умолчанию и включить новый менеджер:

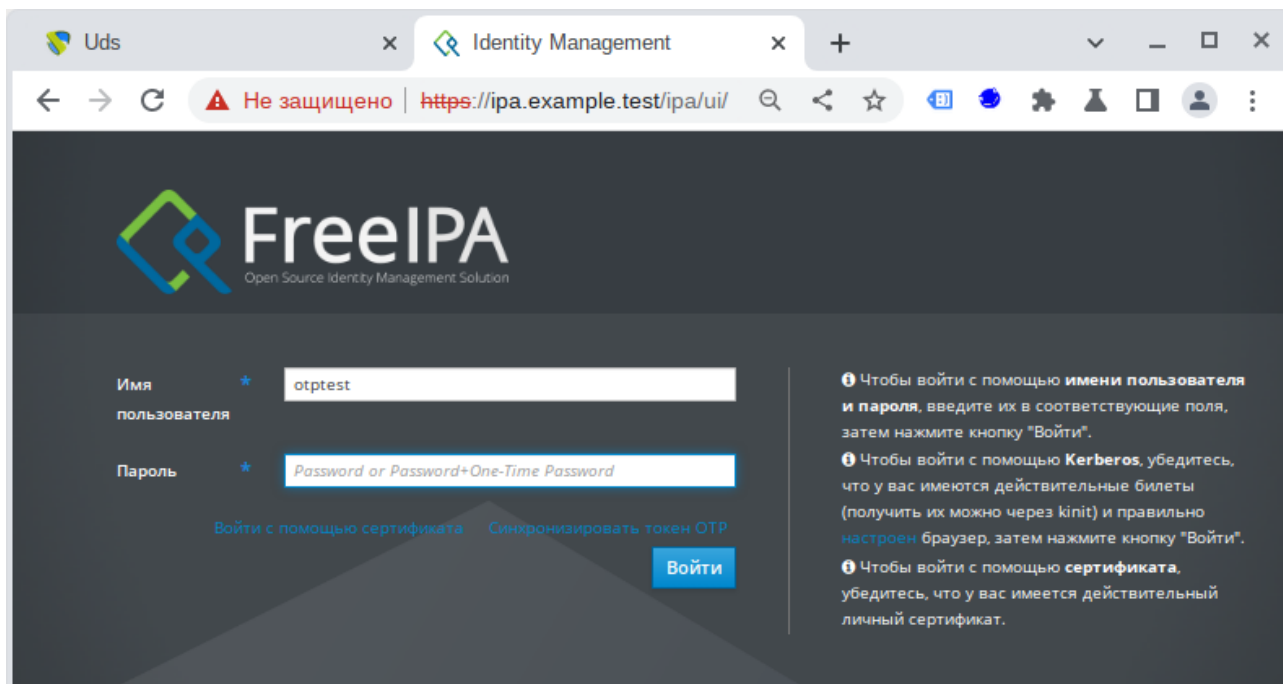
```
# systemctl disable --now display-manager && systemctl enable --now lightdm
```

3. Перезагрузить систему.

Двухфакторная аутентификация в LightDM:



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



Глава 32. Примечания

32.1. Настройка беспарольного доступа по ssh

32.2. Центр управления системой

32.1. Настройка беспарольного доступа по ssh

Генерация SSH-ключа (на узле управления):

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

На вопрос о файле для сохранения ключа нажать **Enter** (по умолчанию). На вопрос о пароле к ключу также нажать **Enter** (не указывать пароль)

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. Для этого подключиться к управляемому узлу и под root 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 есть возможность удалённо выполнять команды на управляемом узле с привилегиями администратора.

32.2. Центр управления системой

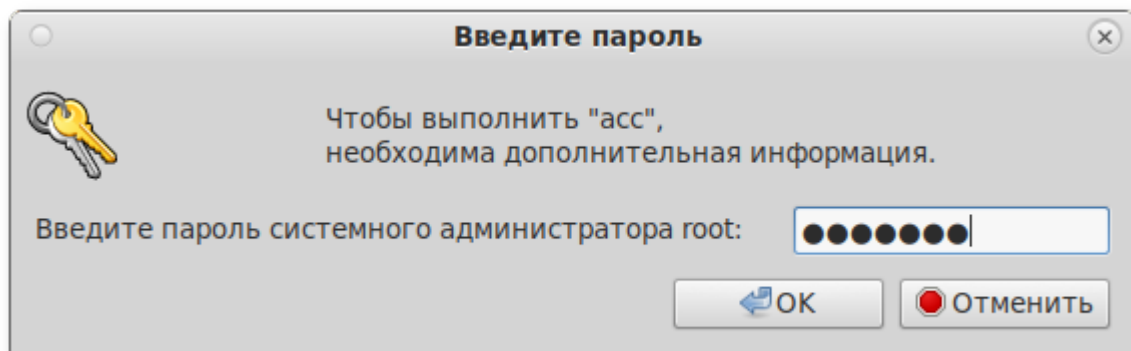
Центр управления системой (ЦУС, альтератор) представляет собой удобный интерфейс для выполнения наиболее востребованных административных задач: добавление и удаление пользователей, настройка сетевых подключений, просмотр информации о состоянии системы и т.п.

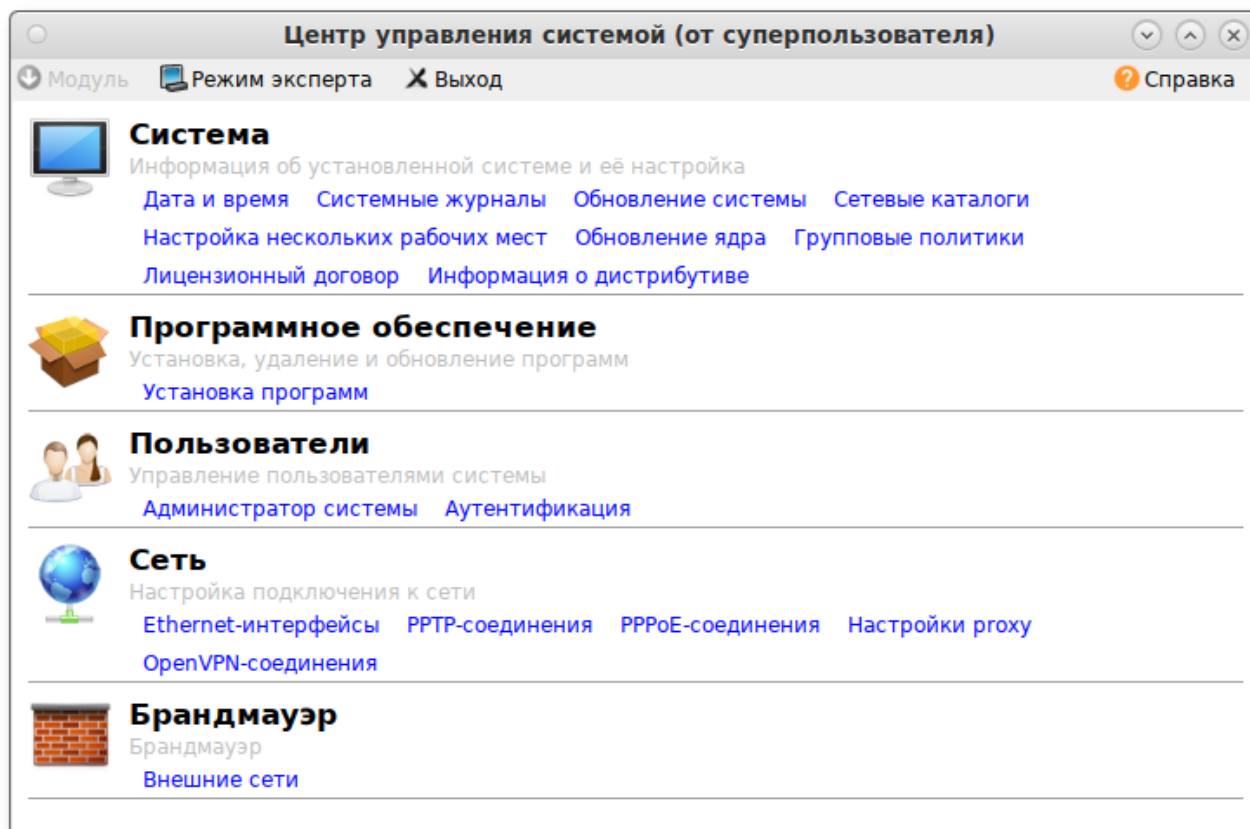
ЦУС состоит из независимых диалогов-модулей. Каждый модуль отвечает за настройку определённой функции или свойства системы.

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 **асс**.

Запуск ЦУС требует административных прав, и если запустить его от обычного пользователя, он запросит пароль администратора системы (root):





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

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

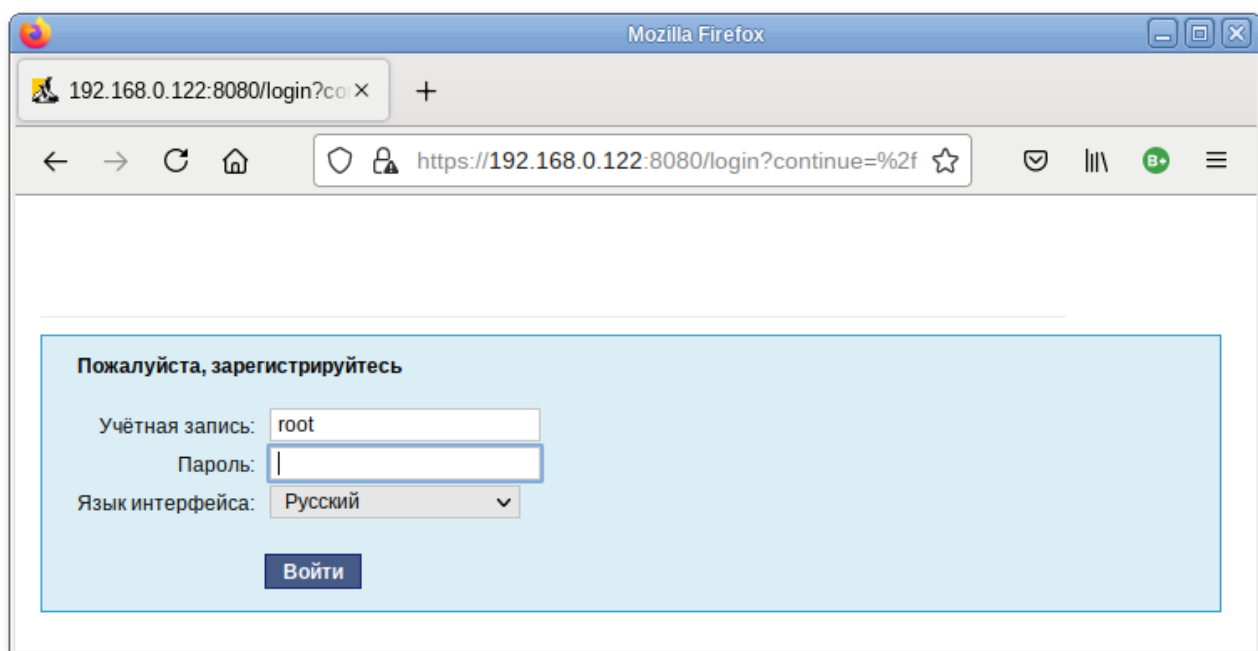
```
# apt-get install alterator-fbi
```

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

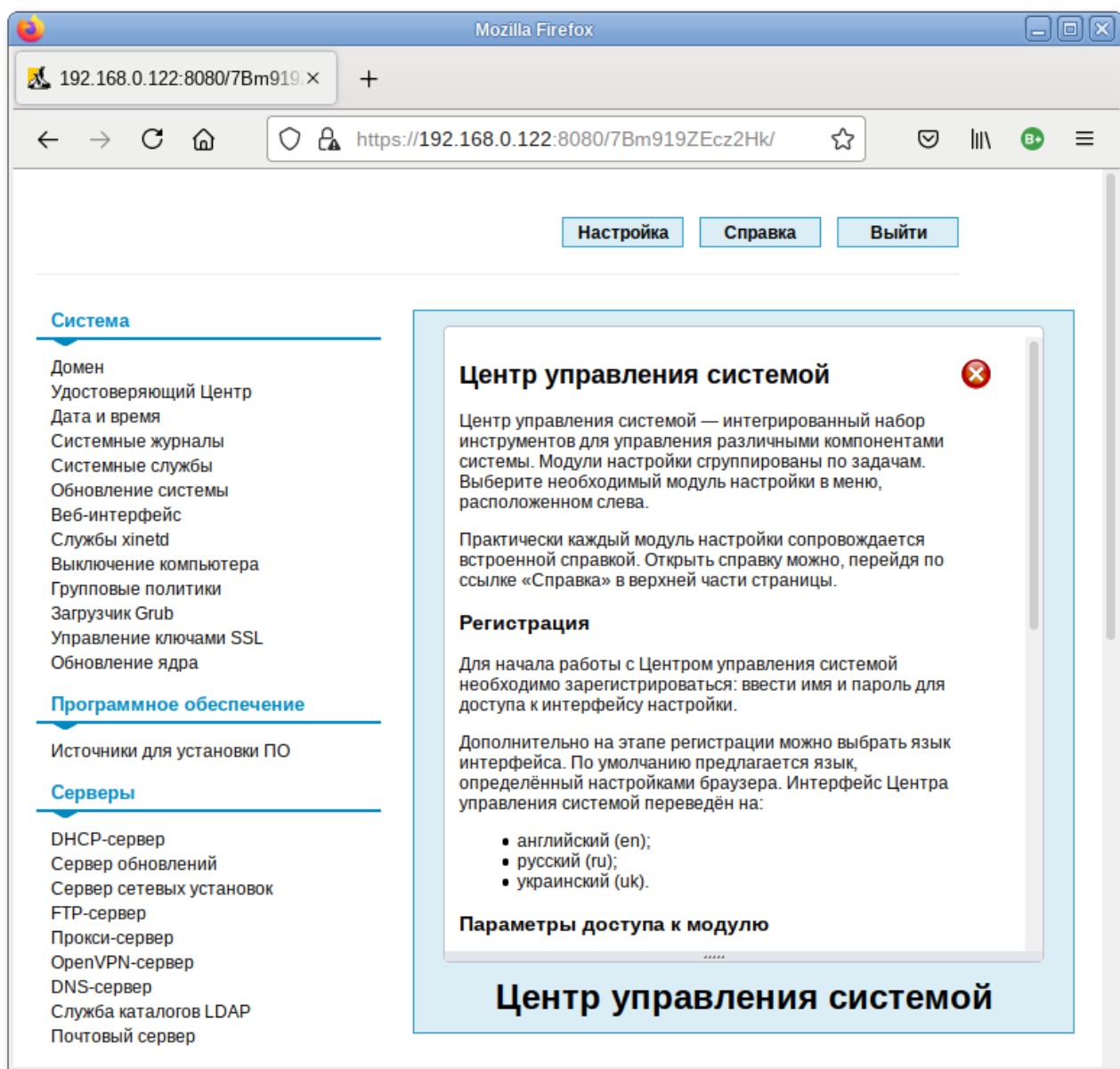
```
# systemctl enable --now ahttpd
# systemctl enable --now alteratord
```

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
```