

Домен на FreeIPA

Подготовка сервера

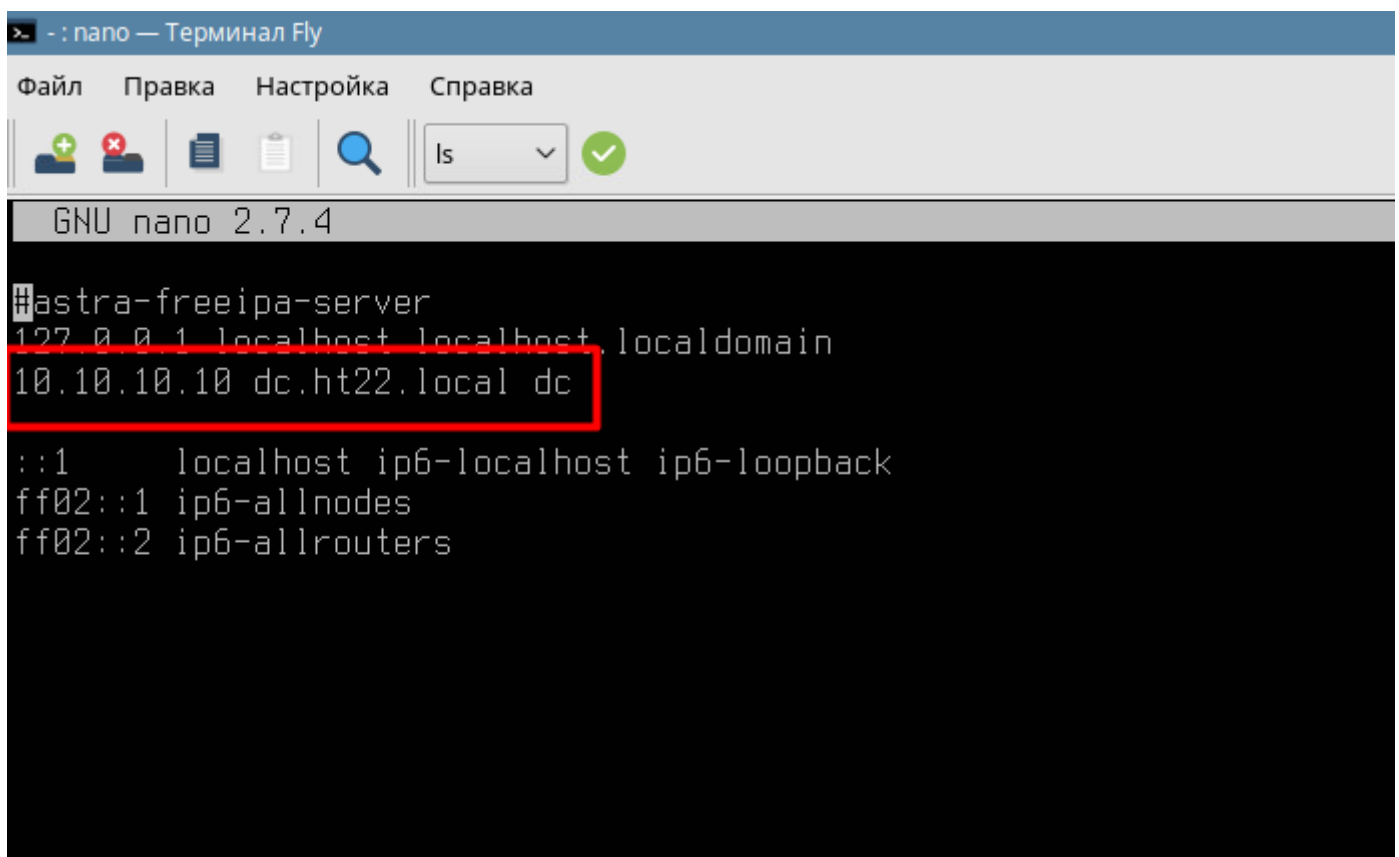
Перед установкой и настройкой FreeIPA необходимо выполнить подготовку сервера. Нужно настроить файл hosts, имя сервера, отключить и замаскировать службу NetworkManager, создать и настроить файл /etc/resolv.conf

Редактируем hostname:

```
hostnamectl set-hostname dc.ht22.local
```

Редактируем файл hosts в такой формат:

<ip сервера> <FQDN> <shortname>



```
> -: nano — Терминал Fly
Файл  Правка  Настройка  Справка
[Icons] [Search] [ls] [Checkmark]
GNU nano 2.7.4
#astra-freeipa-server
127.0.0.1 localhost localhost.localdomain
10.10.10.10 dc.ht22.local dc
::1      localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Также необходимо замаскировать службу NetworkManager и отключить её, иначе будут конфликты со службой networking:

```
systemctl mask NetworkManager
```

```
systemctl disable NetworkManager
```

После отключения службы создаем файл `resolv.conf` в `/etc` и пишем следующее:

```
search ht22.local
domain ht22.local
```

После этого перезагружаем сервер. Подготовка к установке и настройке FreeIPA успешно выполнена.

Установка и настройка astra-freeipa-server

Установка FreeIPA занимает несколько минут. В процессе нужно несколько раз подтвердить действия. Установка выполняется командой:

```
apt install -y astra-freeipa-server
```

После установки необходимо повысить сервер до контроллера домена. Сделать это можно, введя команду `astra-freeipa-server install` без параметров. Все нужные параметры он подберет сам. Либо можно воспользоваться командой `astra-freeipa-server install -d ht22.local -o -i 10.10.10.10` (-d - имя домена, -o - изолированная сеть, -i - ip-адрес интерфейса).

После этого проверяем конфигурацию и вводим пароль администратора `P@ssw0rd`. После 5 минут ожиданий выйдет сообщений об успешной настройке FreeIPA.

Вход в веб-интерфейс и работа с FreeIPA

Для входа в веб-интерфейс управления FreeIPA нужно открыть Firefox и ввести <https://dc.ht22.local>. Вылезет окно о том, что нет доверия сертификата. Это нормально, так как Firefox по умолчанию не умеет забирать сертификаты из корневого хранилища.

Имя	Фамилия	Состояние	UID	Адрес электронной почты	Номер телефона	Должность
admin	Administrator	Включено	584000			
immitkin	Ivan Mitkin	Включено	584001	immitkin@ht22.local		

Создание пользователей

У FreeIPA есть особенность при создании учетных записей пользователей через веб-интерфейс. Срок действия пароля заканчивается очень быстро. Скорее всего сделано с целью безопасности, чтобы пользователь сразу же менял свой пароль при входе в домен (команда login). Чтобы не логиниться под каждым юзером для смены пароля, можно создавать учетки с помощью терминала.

Для этого вводим следующую команду:

```
ipa user-add anivanov --first "Anton" --last "Ivanov" --cn "Anton Ivanov" --displayname "Anton Ivanov" --password-expiration=20221130000000Z --password
```

Будет предложено ввести пароль в интерактивном режиме с подтверждением. Вводим стандартный **P@ssw0rd**. В итоге получим такую картину:

```
root@dc:~# ipa user-add anivanov --first=Anton --last=Ivanov --cn="Anton Ivanov" --displayname="Anton Ivanov" --password-expiration 20221130000000Z --password
Пароль:
Введите Пароль ещё раз для проверки:
Добавлен пользователь "anivanov"
-----
Имя учётной записи пользователя: anivanov
Имя: Anton
Фамилия: Ivanov
Полное имя: Anton Ivanov
Отображаемое имя: Anton Ivanov
Инициалы: AI
Домашний каталог: /home/anivanov
GECOS: Anton Ivanov
Оболочка входа: /bin/bash
Имя учётной записи: anivanov@HT22.LOCAL
Псевдоним учётной записи: anivanov@HT22.LOCAL
Окончание действия пароля пользователя: 20221130000000Z
Адрес электронной почты: anivanov@ht22.local
UID: 584003
ID группы: 584003
Пароль: True
Участник групп: ipausers
Доступные ключи Kerberos: True
root@dc:~#
```

После этого в веб-интерфейсе можно посмотреть свойства учетной записи, где будет указано, когда истекает пароль УЗ:

The screenshot shows the 'Identity Management' web interface in a Mozilla Firefox browser. The URL is `https://dc.ht22.local/ipa/ui/#/e/user/details/anivanov`. The page displays details for the user 'anivanov'. On the left, under 'Параметры идентификации' (Identification parameters), fields include: Должность (empty), Имя (Anton), Фамилия (Ivanov), Полное имя (Anton Ivanov), Отображаемое имя (Anton Ivanov), Инициалы (AI), GECOS (Anton Ivanov), and Класс (empty). On the right, under 'Параметры учётной записи' (Account parameters), fields include: Имя учётной записи пользователя (anivanov), Пароль (masked with asterisks), Окончание действия пароля (2022-11-30 00:00:00Z, highlighted with a red box), UID (584003), ID группы (584003), Псевдоним учётной записи (anivanov@HT22.LOCAL), Окончание действия учётной записи Kerberos (YYYY-MM-DD), Оболочка входа (/bin/bash), Домашний каталог (/home/anivanov), and buttons to add SSH keys, certificates, and mappings.

Список пользователей FreeIPA

Можно вывести список пользовательских аккаунтов FreeIPA с помощью команды `ipa-user-find`.

Для вывода всех имеющихся аккаунтов можно использовать простую команду:

```
ipa user-find --all
```

Для вывода определенного аккаунта:

```
ipa user-find USERNAME
```

Пример:

```
ipa user-find jdoe
```

Дополнительно можно посмотреть в справке `ipa user-find --help`.

Редактирование учетных записей FreeIPA

Для изменения атрибутов пользователя необходимо использовать команду `ipa user-mod`

Например, можно вот так изменить параметр shell для пользователя:

```
ipa user-mod USERNAME --shell=/bin/bash
```

USERNAME это логин пользователя.

Для просмотра остальных атрибутов необходимо ввести команду `ipa user-mod --help`.

Для удаления пользователя можно использовать команду `ipa user-del`

```
ipa user-del USERNAME
```

Revision #2

Created 25 October 2022 07:38:53 by Иван Митькин

Updated 30 October 2022 13:18:12 by Иван Митькин