

1. Настройте сервер домена выбор, его типа обоснуйте, на базе HQ-SRV через web интерфейс, выбор технологий обоснуйте.

a. Введите машины BR-SRV и CLI в данный домен

b. Организуйте отслеживание подключения к домену

В качестве домена может быть выбраны один из двух вариантов, или SAMBA DC, или FREEIPA реализованная через DOCKER, т.к. экспериментальные версии freeipa-server больше не поддерживаются для системы DEBIAN, однако DOCKER позволяет реализовать freeipa-server для любой системы. ДЛЯ настройки будет выбрана именно FreeIpa.

Первым делом необходимо установить докер, воспользовавшись

скриптом, который есть в открытом доступе, однако для этого нам необходимо экспортировать переменные окружения относящиеся к Proxy (Если Proxy отсутствует т. е. Пакеты с не стандартных репозиториях устанавливаются сами, то первый шаг можно пропустить)

Первым шагом необходимо посмотреть переменные, которые необходимо экспортировать, перейдя по пути

nano /etc/apt/apt.conf.d/01proxy

и посмотреть находящиеся там значения, после чего посредством команд

export http_proxy=http(или https)://(адрес:порт)

export https_proxy=http(или https)://(адрес:порт)

Экспортировать переменные прокси для доступа в интернет

ПРИМЕР:



```
Acquire::http::Proxy "http://10.0.70.52:3128";
Acquire::https::Proxy "http://10.0.70.52:3128";
# END ANSIBLE MANAGED BLOCK
```

Рисунок 38 — пример файла 01proxy

Команды для экспортирования переменных для конфига из рисунка 38

export http_proxy=http://10.0.70.52:3128

export https_proxy=http://10.0.70.52:3128

Вторым шагом посредством скрипта необходимо установить сам DOCKER, для этого необходимо ввести следующую команду

wget -qO- https://get.docker.com | bash

Вся установка происходит автоматически, и не должна выдавать ошибок, если были выполнены все предыдущие шаги

Третьим шагом необходимо запустить готовый контейнер с образом freeipa для centos-8-4.8.4 Для этого создаём каталог для автоматического запуска служб докера (Необходимо если вы делали шаги с Proxy ранее), командой

mkdir -p /etc/systemd/system/docker.service.d

Далее заходим в файл

nano /etc/systemd/system/docker.service.d/http-proxy.conf

и заполняем в соответствии с рисунком 39

```
[Service]
Environment="HTTP_PROXY=http://10.0.70.52:3128"
Environment="HTTPS_PROXY=http://10.0.70.52:3128"
```

Рисунок 39 — настройка прокси для docker.service

После чего перезапускаем демона и сам докер командами в указанном порядке

systemctl daemon-reload

и

systemctl restart docker

После чего запускаем команду

docker pull freeipa/freeipa-server:centos-8-4.8.4

После окончания пула контейнера необходимо создать директорию, в которую будет монтироваться контейнер посредством команды

mkdir -p /var/lib/ipa-data

Также необходимо внести изменения в загрузчик системы для указания, необходимости использования обеих версий cgroup (механизм по ограничению ресурсов, начиная с 11 Debian по умолчанию включена только 2 версия)

Для этого посредством команды заходим в загрузчик ядра

nano /etc/default/grub

После чего вносятся изменения как показаны на рисунке 40

```
GRUB_CMDLINE_LINUX="quiet systemd.unified_cgroup_hierarchy=0"
```

Рисунок 40 — Изменение параметров cgroup

Для применения изменений необходимо использовать команду

grub-mkconfig -o /boot/grub/grub.cfg

После чего необходимо перезагрузить машину

Следующим шагом уже переходим к запуску контейнера с хранящейся там FreeIPA, в качестве параметров ключей, указывает имя, указываем доменную сеть, а так открываем все необходимые для работы порты, указываем путь и образ, разрешаем конфликт с IPv6. Все параметры показаны на рисунке 41.

```
root@HQ-SRV:~# docker run --name freeipa-server -ti -h hq-srv.hq.work -p 80:80 -p 443:443 -p 389:389
-p 636:636 -p 88:88 -p 464:464 -p 88:88/udp -p 464:464/udp -p 123:123/udp --read-only --sysctl net.
ipv6.conf.all.disable_ipv6=0 -v /sys/fs/cgroup:/sys/fs/cgroup:rw -v /var/lib/ipa-data:/data:Z freei
pa/freeipa-server:centos-8-4.8.4
```

Рисунок 41 — запуск контейнера с указанием всех параметров

Важное Примечание: В случае завершения выполняемых функций в контейнере в результате которых оболочка может перейти в состояние freezing, или при успешном завершении, для выхода из оболочки окружения необходимо последовательно нажать сочетание клавиш **ctrl + p**, а затем **ctrl + q**. В случае если вам необходимо остановить контейнер можно воспользоваться командой **docker stop имя контейнера**, для удаления контейнера **docker rm имя контейнера**, для просмотра существующих образов **docker images**

После успешного запуска необходимо заполнить форму:

На вопрос о интеграции DNS нажимаем **Enter**

На вопрос о задании имени сервера нажимаем **Enter**

На вопрос о подтверждение имени домена нажимаем **Enter**

На вопрос о подтверждение имени области нажимаем **Enter**

На запрос ввода пароля для менеджера директорий вводим **P@ssw0rd**

На запрос ввода пароля для IPA админа вводим **P@ssw0rd**

На вопрос синхронизации с службой Chrony нажимаем **Enter**

На вопрос о конфигурирование системы с текущими параметрами вводим **yes**

Процесс установки достаточно длительный и может занимать около 5-10 или более минут.

После завершения установки необходимо подготовить машины, которые будут присоединены к домену. Для этого первым делом переходим по пути:

Nano /etc/hosts

И конфигурируем файл на клиенте как указано на рисунке 42

```
127.0.0.1      localhost
127.0.1.1      cli.hq.work      cli
192.168.1.2    hq-srv.hq.work
```

Рисунок 42 – конфигурация хостов машины CLI

Для машины BR-SRV настройка будет выглядеть как показано на рисунке

127.0.0.1	localhost	
127.0.1.1	br-srv.branch.work	br-srv
192.168.1.2	hq-srv.hq.work	

Рисунок 43 – конфигурация файла хостов

машины BR-SRV Следующим шагом посредством команды:

apt install freeipa-client

Производим установку клиентской части FreeIPA для ввода машины в домен.

На все всплывающие окна во время установки **нажимаем Enter**

После установки клиента, для ввода машины в домен необходимо прописать команды:

НА CLI

ipa-client-install --mkhomedir --domain hq.work --server=hq-srv.hq.work -p admin -W

НА BR-SRV

ipa-client-install --mkhomedir --domain branch.work --server=hq-srv.hq.work -p admin -W

```
root@BR-SRV:~# ipa-client-install --mkhomedir --domain brach.work --server=hq-srv.hq.work -p admin
W
```

Рисунок 43 – пример команды по вводу в домен на BR_SRV

На сообщение о продолжении с фиксированными значения пишем **yes**

На вопрос о конфигурирование CHRONY нажимаем **ENTER**

На вопрос о конфигурировании с текущими значение пишем **yes**

Для проверки входа в FreeIPA, на клиентской машине необходимо открыть браузер и в адресной строке написать IP адрес машины HQ-SRV (192.168.1.2) логин и пароль для входа в вебку FreeIPA: admin и P@ssw0rd

Важное Примечание: если вы перезагрузите машину, то

контейнер выключится, для его запуска можно воспользоваться командой **docker start freeipa-server**