**Настройте доменный контроллер Samba на машине BR-SRV.**

• Создайте 5 пользователей для офиса HQ: имена пользователей

формата user№.hq. Создайте группу hq, введите в эту группу созданных

пользователей

• Введите в домен машину HQ-CLI

• Пользователи группы hq имеют право аутентифицироваться на

клиентском ПК

• Пользователи группы hq должны иметь возможность повышать

привилегии для выполнения ограниченного набора команд: cat, grep, id.

Запускать другие команды с повышенными привилегиями пользователи

группы не имеют права

**BR-SRV:**

**Для доступа к интернету в файл /etc/resolv.conf вводим строку:**

nameserver 8.8.8.8

* Установим необходимый пакет:

apt-get update && apt-get install task-samba-dc bind -y

* Настройка BIND9 для работы с Samba AD:
  + Отключаем chroot:

control bind-chroot disabled

* + Отключаем KRB5RCACHETYPE:

grep -q KRB5RCACHETYPE /etc/sysconfig/bind || echo 'KRB5RCACHETYPE="none"' >> /etc/sysconfig/bind

* Выполняем остановку службы **bind**:

systemctl stop bind

* Необходимо очистить базы и конфигурацию Samba:

rm -f /etc/samba/smb.conf

rm -rf /var/lib/samba

rm -rf /var/cache/samba

mkdir -p /var/lib/samba/sysvol

* Запускаем интерактивную установку контроллера домена:

samba-tool domain provision

Далее везде ставим энтер

Пароль: P@ssw0rd

* Запускаем службы **samba**:

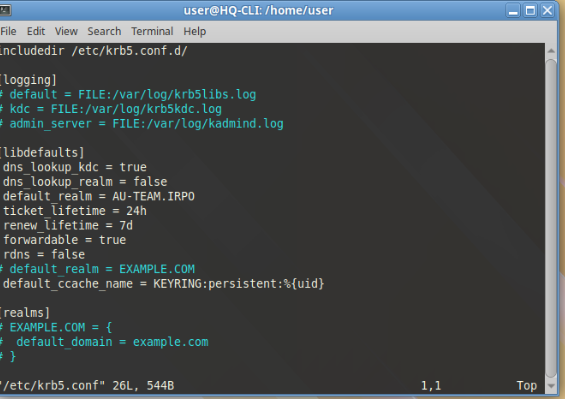
systemctl enable --now samba

Проверяем:

Samba-tool domain info 127.0.0.1

Переходим на **HQ-CLI**

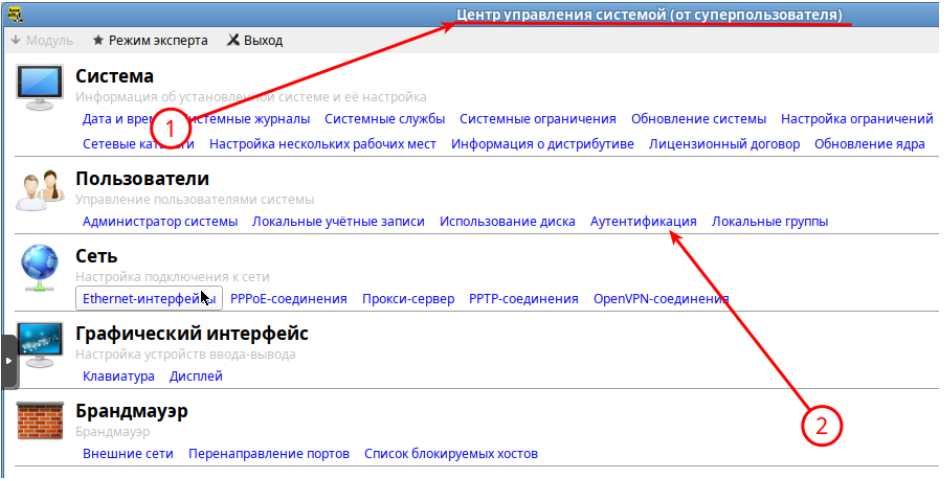
На HQ-CLI файл /etc/krb5.conf приводим к следующему виду:

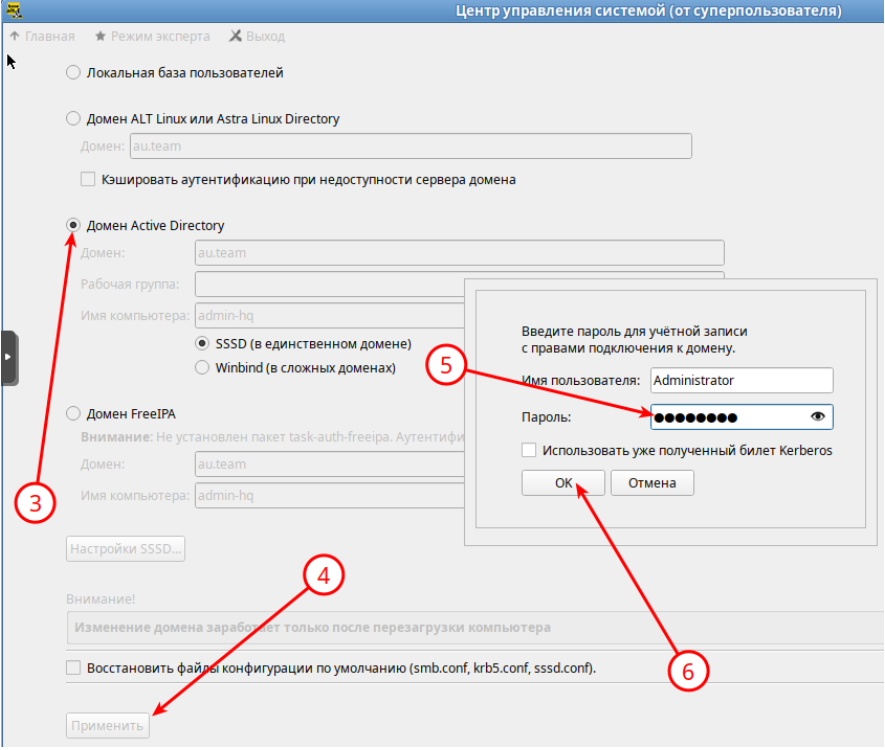


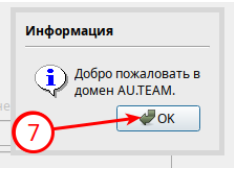
Добавляем в файл /etc/resolv.conf строку

nameserver 192.168.3.10

* Вводим клиента в домен:







**Перезагружаем машину**

**BR-SRV:**

* Проверяем наличие клиентов в домене:

samba-tool computer list

Создаём группу **hq:**

samba-tool group add hq

Создаём пользователей user1-user5 с паролем P@ssw0rd и добавляем их в группу **hq**

for i in {1..5}; do

samba-tool user add user$i.hq P@ssw0rd;

samba-tool user setexpiry user$i.hq --noexpiry;

samba-tool group addmembers "hq" user$i.hq;

done

На HQ-CLI логинимся под любым из созданных пользователей

Если при вводе user(1-5).hq пишет «incorrect password», проверьте что бы на hq-cli (Зайти можно под дефолтным «user») в файле /etc/resolv.conf присутствовала запись: nameserver 192.168.3.10 (адрес домена)