Задание:

Необходимо разработать и настроить инфраструктуру информационнокоммуникационной системы согласно предложенной топологии (см. Рисунок 1). Задание включает базовую настройку устройств:

• присвоение имен устройствам,

• расчет IP-адресации,

• настройку коммутации и маршрутизации.

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчет о своих действиях, включая таблицы и схемы, предусмотренные в задании. Итоговый отчет должен содержать одну таблицу и пять отчетов о ходе работы. Итоговый отчет по окончании работы следует сохранить на диске рабочего места

Изображение выглядит как текст, диаграмма

Автоматически созданное описание

Изображение выглядит как текст, число, меню, снимок экрана

Автоматически созданное описание

Чтобы зайти на стенд для 1 модуля. Логин m1 пароль modul1

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

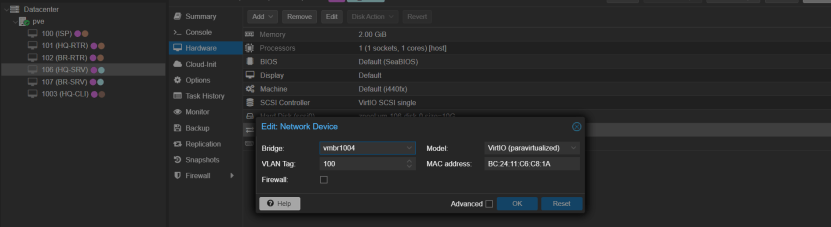
Перед включением виртуалок Настроем вланы. По заданию HQ-SRV в 100 влане, а HQ-CLI в 200 ЭТО НУЖНО ЗАНЕСТИ В ОТЧЕТ

Изображение выглядит как программное обеспечение, Мультимедийное программное обеспечение, Графическое программное обеспечение, снимок экрана

Автоматически созданное описание

Изображение выглядит как программное обеспечение, Мультимедийное программное обеспечение, текст, Графическое программное обеспечение

Автоматически созданное описание



Изображение выглядит как программное обеспечение, Мультимедийное программное обеспечение, текст, Графическое программное обеспечение

Автоматически созданное описание

ISP преднастроена, но включать ее надо

# Таблица IP-адресации:

|  |  |  |
| --- | --- | --- |
| Имя устройства | Ip address | iproute |
| ISP | DHCP |  |
|  | 172.16.4.1/28 |  |
|  | 172.16.5.1/28 |  |
| HQ-RTR | 172.16.4.2/28 | 172.16.4.1 |
|  | 192.168.100.1/26 |  |
|  | 192.168.10.1/28 |  |
| BR-RTR | 172.16.5.2/28 | 172.16.5.1 |
|  | 192.168.200.1/27 |  |
| HQ-SRV | 192.168.100.2/26 | 192.168.100.1 |
| HQ-CLI | 192.168.10.2/28 | 192.168.10.1 |
| BR-SRV | 192.168.200.2/27 | 192.168.200.1 |

## МОДУЛЬ 1

1. Сетевая связность - между HQ и BRANCH Выполение: HQ-R: Задаём сразу FQDN - выбор имени домена произвольный:

***Делай отчёт для практики***

Занеси в отчёт пароли от root’ов на машинах

### HQ-RTR



По такой же аналогии настройте остальные имена

Чтобы настроить адресацию переходим:



Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

Теперь сделаем из обычного дебиана роутер



Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

sysctl -p

Прокинем PAT для инета



Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание

Обязательно добавим в автозагрузку и активируем



Туннель мы допустим подняли, но просто по приколу пакеты через него не пойдут, нужна маршрутизация. Нечего нового установим frr.



 В файле **/etc/frr/daemons** - включим поддержку OSPFv2 (IPv4)

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Не забываем перезапускать, а то это линукс и он не поймет что вы что то изменили



Переходим к настройке frr

Изображение выглядит как текст, снимок экрана, Шрифт, черно-белый

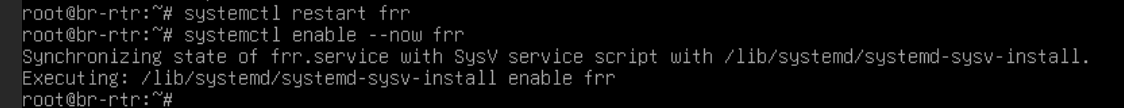
Автоматически созданное описание

Поставим пароль на фрр

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

Не забываем перезапустить



Перейдем к br-rtr

### BR-RTR

Произведем те же манипуляции





Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание





Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описаниеSysctl -p

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание





Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

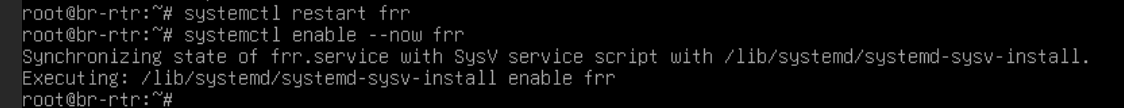


Изображение выглядит как текст, снимок экрана, Шрифт, черно-белый

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание



сетевая связность у РТР настроена

### HQ-SRV

Прокинем инет

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Перезапускаем сервис

Systemctl restart networking

Проверяем

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

### BR-SRV

Изображение выглядит как текст, снимок экрана, программное обеспечение, дисплей

Автоматически созданное описание



### Создание локальных учетных записей

Создайте пользователя sshuser на серверах **HQ-SRV(щас тут)**  **и BR-SRV**

Занеси в отчёт пароли

HQ-SRV

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

В дебиане нету судо поэтому скачаем





НА BR-SRV СДЕЛАЙТЕ ТОЖЕ САМОЕ

Создайте пользователя net\_admin на маршрутизаторах **HQ-RTR и BR-RTR**

Занеси в отчёт пароли

HQ-RTR





В дебиане нету судо поэтому скачаем





СДЕЛАЙТЕ ТОЖЕ САМОЕ НА BR-RTR

### Настройка ssh:

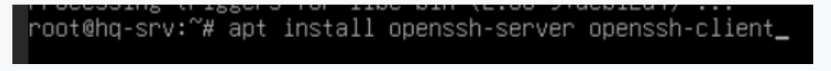
Настройка безопасного удаленного доступа на серверах HQ-SRV и BRSRV:

● Для подключения используйте порт 2024

● Разрешите подключения только пользователю sshuser ● Ограничьте количество попыток входа до двух

● Настройте баннер «Authorized access only»

HQ-SRV



Редактируем файл **/etc/ssh/sshd\_config**:

Меняем стандартный порт на порт в соответствие с заданием;

Разрешаем пользователю заходить

Ставим количество неудачных попытгок

И Баннер

Создаем файлик с баннером

Перезапускаем службу sshd

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание



Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

ДУБЛИРУЕМ ТОЖЕ САМОЕ НА BR-SRV

### DHCP

**HQ-RTR:**

Установим и настроим DHCP-сервер и зарезервируем адрес для HQ-SRV, чтобы потом на всех остальных оконечных устройствах задавая адреса сразу создавать пользователей

Apt install isc-dhcp-server

Первым делом нам необходимо указать, что наш DHCP сервер должен принимать запросы только с ens20 интерфейса.



Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

. Настройка протокола динамической конфигурации хостов.

● Настройте нужную подсеть

● Для офиса HQ в качестве сервера DHCP выступает маршрутизатор HQ-RTR.

● Клиентом является машина HQ-CLI.

● Исключите из выдачи адрес маршрутизатора

● Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR.

● Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV.

● DNS-суффикс для офисов HQ – au-team.irpo

● Сведения о настройке протокола занесите в отчёт



Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание



### DNS для офисов HQ и BR.

● Основной DNS-сервер реализован на HQ-SRV.

● Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2

● В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

Нам необходимо настроить DNS сервер. Будем использовать dnsmasq. Он проще в настройке, да и в целом есть в разы меньше ресурсов, нежели BIND. Для наших зон этого будет достаточно.

**HQ-SRV**

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Автоматически созданное описание

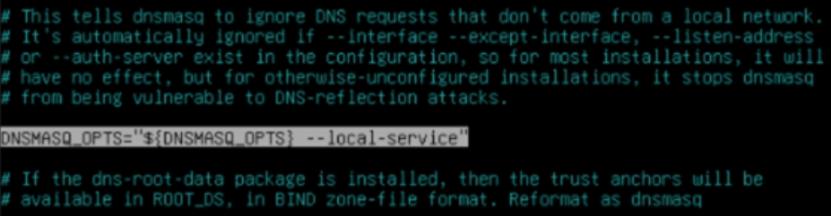
Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Теперь открываем скрипт-инициализации сервиса dnsmasq

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описаниеищем строчку DNSMASQ\_OPTS



Убираем оттуда **–local-service**

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание



**меняем везде домен на 192.168.100.2(попозже)** nano /etc/resolv.conf

### Настройка часового пояса

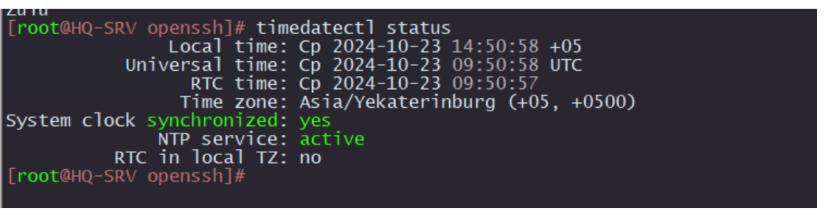
11. Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

НА всех машинах нужно прописать

**HQ-SRV, HQ-CLI, BR-SRV**

Проверяем какой часовой пояс установлен

timedatectl status



Если отличается, то устанавливаем

timedatectl set-timezone Asia/Yekaterinburg

## МОДУЛЬ 2

### Доменный контроллер Samba

• 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

• Выполните импорт пользователей из файла users.csv. Файл будет располагаться на виртуальной машине BR-SRV в папке /opt

**BR-SRV**

**Убери из resolv.conf фигню и поставь 10.0.1.4**

СКАЧИВАЙ ПАРАЛЛЕЛЬНО на СLI:[task](#Закладка2) [admc](#Закладка3) HQ-SRV: [mdadm](#Закладка4) [nfs](#Закладка5)

Появится синее окно, не пугайтесь, так и должно быть. В первом окне вводим имя домена **au-team.irpo**, а во втором — имя нашего сервера **br-srv**

Проверяем что установлено имя в формате FQDN;

Задаём domainname;

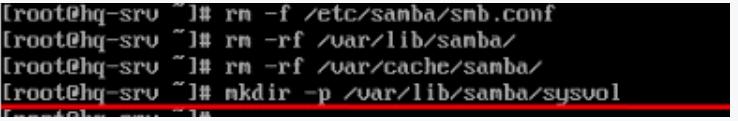
Очищаем конфигурацию samba;

Разворачиваем контроллер домена Active Directory на базе SambaDC с BIND9\_DLZ в качестве DNS

ip link delete docker0 && apt remove docker.io

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание



Подготовка домена Samba-tool --realm=au-team.irpo --domain=au-team –adminpass=”PAssw0rd” --dnsbackend=SAMBA\_INTERNAL --option=”dns forwrder=192.168.100.2” --server-role=dc

ВЫ МОЖЕТЕ НАПИСАТЬ ТОЛЬКО «samba-tool domain provision», А ОСТАЛЬНОЕ ОНО СПРОСИТ САМО

Занеси в отчёт пароль

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

надо перезапустить машинку



Проверяем

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

**меняем везде домен на 192.168.100.2**

### CLI: Ставим необходимые пакеты:

Установим пакет task-auth-ad-sssd:

apt-get update && apt-get install -y task-auth-ad-sssd

У вас возникнет ошибка, связанная с конфликтом с пакетом alterator-datetime, его необходимо удалить

apt-get remove alterator-datetime

После пропишем инсталл еще раз

apt-get install -y task-auth-ad-sssd

• Переходим к редактированию временного соединения и в качестве DNS-сервера прописываем адрес HQ-SRV, а также указываем поисковый домен:

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

переходим в Центр управления системой на вкладке Пользователи выбираем Аутентификация

Изображение выглядит как текст, программное обеспечение, веб-страница, Значок на компьютере

Автоматически созданное описаниеИзображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Изображение выглядит как текст, линия, Шрифт, снимок экрана

Автоматически созданное описание

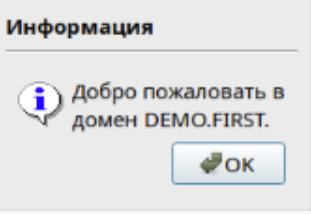
• Вводим пароль администратора домена:

Изображение выглядит как текст, Шрифт, линия, снимок экрана

Автоматически созданное описание

Занеси в отчёт пароль

• нажимаем ОК и перезагружаем систему:



• В качестве проверки после перезагрузки можно выполнить аутентификацию от имени доменного пользователя administrator:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Организуем отслеживание подключения к домену: CLI: На клиенте с граф. интерфейсом установим Модуль удаленного управления базой данных конфигурации (ADMC) • Установим пакет admc:

apt-get install -y admc

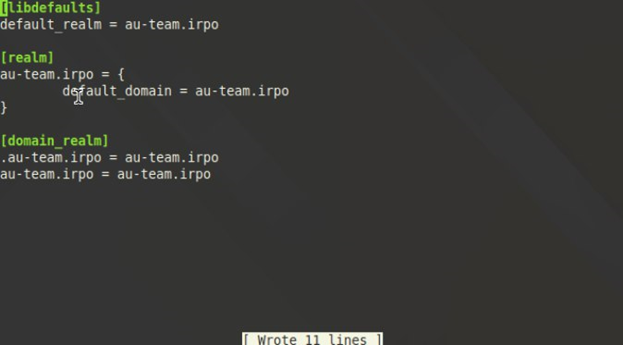
• Для использования ADMC необходимо предварительно получить ключ Kerberos для администратора домена. Получить ключ Kerberos можно, например, выполнив следующую команду:

из под обычного пользователя

kinit Administrator

• ADMC запускается из меню запуска приложений: пункт «Системные» → ADMC или из командной строки (команда admc).

Если admc долго не может запуститься(не выдает ошибок, но не запускается), то внесите изменения в файл /etc/krb5.conf



На вкладке «Компьютеры» в графическом режиме удобно отслеживать подключение к домену;

Создаем пять юзеров

Занеси в отчёт пароль

Изображение выглядит как текст, снимок экрана, чек, белый

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

**Создаем группу hq и в нее добавляем раннее созданных пользователей**

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

На **hq-CLI**

Настройте файл **/etc/sudoers** на рабочей станции Linux, как описано в предыдущем ответе, используя синтаксис для доменных групп

%hq ALL=(ALL) NOPASSWD: /bin/cat, /bin/grep, /usr/bin/id

### Сконфигурируйте файловое хранилище:

• При помощи трёх дополнительных дисков, размером 1Гб каждый, на HQ-SRV сконфигурируйте дисковый массив уровня 5

• Имя устройства – md0, конфигурация массива размещается в файле /etc/mdadm.conf

• Обеспечьте автоматическое монтирование в папку /raid5

• Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4

• Настройте сервер сетевой файловой системы(nfs), в качестве папки общего доступа выберите /raid5/nfs, доступ для чтения и записи для всей сети в сторону HQ-CLI

• На HQ-CLI настройте автомонтирование в папку /mnt/nfs

• Основные параметры сервера отметьте в отчёте

**HQ-SRV**

#### 1. Подготовка дисков

**Делай snapshot**

Убедитесь, что дополнительные диски распознаны системой. Список подключенных дисков можно проверить командой:

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Создайте RAID 5 массив из трех 1Гб дисков (предположим, они определены как /dev/sdb, /dev/sdc, и /dev/sdd):

Apt update && apt install mdadm

ПАРАЛЛЕЛЬНО СКАЧИВАЙ на BR-SRV: [mariadb](#Закладка6) и [docker](#Закладка9)



Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Проверяем

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Проверьте статус RAID массива:

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Сохраните конфигурацию массива в файл /etc/mdadm.conf:



Создание файловой системы и настройка монтирования

Создайте раздел и отформатируйте его в ext4:

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Создайте точку монтирования и настройте автоматическое монтирование в /etc/fstab:

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Смонтируйте файловую систему:

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

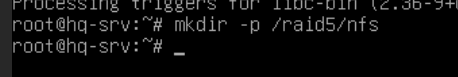
**Больше не перезагружай hq-srv(появиться ошибка с raid’ом)**

#### 2. Настройка NFS-сервера на HQ-SRV

Установите NFS-сервер



Создайте директорию для общего доступа:



Настройте права доступа для общей папки:



Настройте экспорт NFS для всей сети с разрешением на чтение и запись. Откройте файл **/etc/exports** и добавьте строку:

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Примените изменения в конфигурации NFS:

Изображение выглядит как текст, Шрифт, черный, снимок экрана

Автоматически созданное описание

Перезапустите NFS-сервер:



#### 3. Настройка автомонтирования на HQ-CLI (под ALT Workstation)

Создайте точку монтирования на **HQ-CLI**:

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Настройте автомонтирование в **/etc/fstab**, добавь след. строку:

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

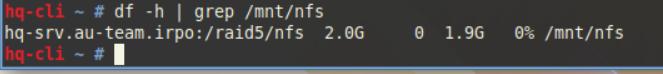
Автоматически созданное описание

Смонтируйте папку вручную или перезагрузите систему для применения настроек

Изображение выглядит как текст, Шрифт, снимок экрана, число

Автоматически созданное описание

Проверка подключения NFS на HQ-CLI:



### Настройте службу сетевого времени на chrony

• В качестве сервера выступает HQ-RTR

• На HQ-RTR настройте сервер chrony, выберите стратум 5 43

• В качестве клиентов настройте HQ-SRV, HQ-CLI, BR-RTR, BR-SRV

Установим пакет [chrony](https://chrony-project.org/):

apt install -y chrony • Приводим конфигурационный файл "[chrony.conf](https://manpages.ubuntu.com/manpages/impish/man5/chrony.conf.5.html)" к следующему виду:

**HQ-RTR:**

nano /etc/chrony/chrony.conf

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

где: server 127.0.0.1 iburst prefer - указываем сервером синхронизации самого себя,

опция «iburst» принудительно отправляет сразу несколько пакетов для точности синхронизации,

опция «prefer» говорит о том, что это будет предпочитаемый сервер;

hwtimestamp \* - опция, чтобы сетевой интерфейс считал собственный источник времени верным и синхронизировал клиентов с ним;

local stratum 5 - устанавливаем для себя значение по stratum = 5;

allow - кому разрешается подключаться к серверу и запрашивать время: чтобы не перечеслять все используемые в задании IPv4 и IPv6 сети, используется 0/0 и ::/0;

(закомментированный блок писать не надо, как пример описание всех используемых в задании сетей) • Запускаем и добавляем в автозагрузку службу chronyd: И не забываем рестартать сервис

systemctl enable --now chrony

systemctl restart chrony



Проверяем:

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Автоматически созданное описание

Настройка NTP клиентов: **HQ-SRV BR-SRV BR-RTR HQ-CLI:**

Установим пакет [chrony](https://chrony-project.org/):

apt install -y chrony

• Приводим конфигурационный файл "[chrony.conf](https://manpages.ubuntu.com/manpages/impish/man5/chrony.conf.5.html)" к следующему виду:

nano /etc/chrony/chrony.conf

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

где:

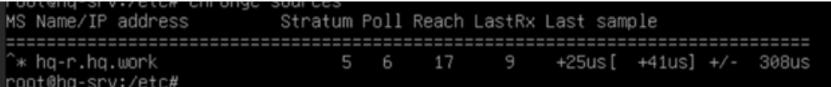
192.168.100.1 - IPv4 адрес HQ-R;

• Запускаем и добавляем в автозагрузку службу chronyd:

systemctl enable --now chrony

systemctl restart chrony

Проверяем: • с клиента HQ-SRV:



с сервера HQ-R:

Изображение выглядит как текст, снимок экрана, черный, Шрифт

Автоматически созданное описание

BR-R | BR-SRV | CLI: Настройка аналогична HQ-SRV - за исключением указания соответствующих адресов

### Сконфигурируйте ansible

**(должен работать DNS)**

• Сформируйте файл инвентаря, в инвентарь должны входить HQSRV, HQ-CLI, HQ-RTR и BR-RTR

• Рабочий каталог ansible должен располагаться в /etc/ansible

• Все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV

**BR-SRV**

#### 1 Установите Ansible (если он еще не установлен):

apt update

apt install ansible –y

СКАЧИВАЙ ОДНОВРЕМЕННО на HQ-SRV: [Apache2](#Закладка8) **и mariadb(пониже)**

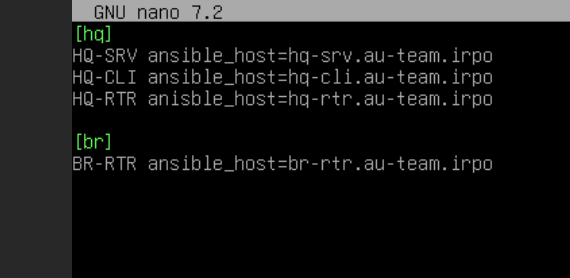
2 Создание рабочего каталога Ansible : Ansible обычно уже использует /etc/ansible как рабочий каталог, но если его нет, создайте его вручную:



#### Шаг 2: Создание файла инвентаря

Создайте инвентарь файла : /etc/ansible/hosts Откройте файл **/etc/ansible/hosts** для редактирования: (здесь у hq srv:sshuser@hq-srv.au-team.irpo ansible\_port=2024)





#### Шаг 3: Настройка SSH-доступа к машинам

Для того чтобы Ansible мог управлять машинами без необходимости ввода пароля, настройте SSH-доступ:



Скопируйте SSH-ключ на всех машинах в инвентаре : Выполните эту команду для каждой машины, чтобы разрешить безпарольный доступ:





**Для hq-srv:** ssh-copy-id –p 2024 sshuser@hq-srv.au-team.irpo



**Для hq-cli:** скачай openssh и systemctl restart sshd



создадим SSH-ключ на BR-SRV (если он еще не создан):

#### Шаг 4. Проверка подключения в Ansible

Выполните команду ping для проверки соединения : Выполните команду Ansible для проверки соединений со всеми хостами из инвентаря файла:

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

### Развертывание приложений в Docker

**BR-SRV**

**Делай snapshot**

• Создайте в домашней директории пользователя файл wiki.yml для приложения MediaWiki.

• Средствами docker compose должен создаваться стек контейнеров с приложением MediaWiki и базой данных.

• Используйте два сервиса

• Основной контейнер MediaWiki должен называться wiki и использовать образ mediawiki

• Файл LocalSettings.php с корректными настройками должен находиться в домашней папке пользователя и автоматически монтироваться в образ.

• Контейнер с базой данных должен называться mariadb и использовать образ mariadb.

• Разверните

• Он должен создавать базу с названием mediawiki, доступную по стандартному порту, пользователя wiki с паролем WikiP@ssw0rd должен иметь права доступа к этой базе данных

На маршрутизаторах сконфигурируйте статическую трансляцию портов

• Пробросьте порт 80 в порт 8080 на BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы сервиса wiki

• Пробросьте порт 2024 в порт 2024 на HQ-SRV на маршрутизаторе HQ-RTR

• Пробросьте порт 2024 в порт 2024 на BR-SRV на маршрутизаторе BR-RTR

apt install -y docker.io docker-compose

• Включаем и добавляем в автозагрузку службу docker:

systemctl enable --now docker.service

• В домашней директории пользователя root создаём файл wiki.yml со следующим содержимым:

nano ~/wiki.yml

ПАРОЛЬ – MYSQL\_PASSWORD ПОМЕНЯТЬ НА **WikiP@ssw0rd**

Изображение выглядит как текст, электроника, снимок экрана, дисплей

Автоматически созданное описание

Занеси в отчёт пароль от MYSQL\_PASSWORD

где: services — основной раздел, где мы будем создавать и описывать наши сервисы (контейнеры docker). В данном примере сервиса два: MediaWiki - для приложения mediawiki и database - для базы данных; container\_name — имя, которое получит созданный контейнер; image — имя образа, который будет использоваться для создания контейнера; restart — поведения контейнера при падении; ports (внешняя публикация). С помощью данной опции мы можем указывать, на каких портах должен слушать контейнер и на какие порты должны пробрасываться запросы environment — задаем переменные окружения; volumes - проброс папок; links - ссылайтесь на контейнеры в другом сервисе. Укажите либо имя сервиса, либо псевдоним ссылки (SERVICE:ALIAS), либо просто имя сервиса.

apt install –y mariadb-\*

P.S. После первоначальной настройки через Web-интерфейс с CLI загрузите LocalSettings.php в тот же каталог, что и эта wiki.yml и раскомментируйте следующую строку "# - ./LocalSettings.php:/var/www/html/LocalSettings.php" и используйте docker-compose для перезапуска службы mediawiki

• Чтобы отдельный volume для хранения базы данных имел правильное имя - создаём его средствами docker:

docker volume create dbvolume

• Выполняем сборку и запуск стека контейнеров с приложением MediaWiki и базой данных описанных в файле wiki.yml:

docker-compose -f wiki.yml up -d

Проверяем:

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, программное обеспечение, снимок экрана

Автоматически созданное описание

MediaWiki должна быть доступна извне через порт 8080 HQ-R:

**BR-RTR:**

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

**HQ-RTR**Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

**HQ-CLI**

su - echo 192.168.200.2 wiki.au-team.irpo mediawiki >> /etc/hosts • Переходим в браузер [http://wiki.au-team.irpo:8080/](http://mediawiki.au-team.irpo:8080/) для продолжения установки через веб-интерфейс - нажимаем set up the wiki:

Изображение выглядит как текст, снимок экрана, графический дизайн, визитная карточка

Автоматически созданное описание

• Выбираем необходимый Язык - нажимаем Далее:

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

• После успешной проверки внешней среды - нажимаем Далее:

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

• Заполняем параметры подключение к Базе Данных в соответствие с заданными переменными окружения в wiki.yml, которые соответствуют требованиям задания:

Хост базы данных: db

Имя базы данных: mediawiki

Пользователь: wiki

Пароль: wikiP@ssw0rd

Изображение выглядит как текст, Шрифт, линия, снимок экрана

Автоматически созданное описание

• Заполняем необходимые сведения:

Название вики: wiki

Имя участника: admin

Пароль: wikiP@ssw0rd

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

• После чего будет автоматически скачен файл LocalSettings.php - который необходимо передать на BR-SRV в домашнюю директорию пользователя root туда же где лежит wiki.yml:

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

**Сделай snapshot**

• Забираем файл LocalSettings.php

с **CLI**:

scp user@192.168.10.2:~/Downloads/LocalSettings.php ./(опционально)

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

• Передаём его на BR-SRV:

scp -P 2024 /home/AU-TEAM.IRP0/administrator/Downloads/LocalSettings.php sshuser@192.168.200.2:/tmp (или /home/sshuser)

**BR-SRV**

sudo mv /tmp/LocalSettings.php ~/

Измените владельца файла на root:

sudo chown root:root /root/LocalSettings.php

ls -l /root/LocalSettings.php

• Проверяем:

Если выдастся ошибка:



То убедитесь, что в /root уже есть каталог /root/LocalSettings.php:

Ls -l /root | grep LocalSettings.php

Если покажет что-то вроде: drwxr-xr-x…LocalSettings.php,(строка начинается на d) значит эта директория уже занята

Надо удалить файл:

Rm -rf /root/LocalSettings.php

Теперь перемещай файл:

Mv /tmp/LocalSettings.php ~/

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

Перезапускаем сервисы средствами docker-compose:

docker-compose -f wiki.yml stop

docker-compose -f wiki.yml up -d

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

**CLI**:

• Проверяем доступ к <http://wiki.au-team.irpo:8080>

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

• вход из под пользователя admin с паролем WikiP@ssw0rd:

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описаниеЗанеси в отчёт

Изображение выглядит как текст, снимок экрана, программное обеспечение, число

Автоматически созданное описаниеЗапустите сервис moodle

**HQ-SRV (не перезагружать)**

• Используйте веб-сервер apache

• В качестве системы управления базами данных используйте mariadb

• Создайте базу данных moodledb

• Создайте пользователя moodle с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных

• У пользователя admin в системе обучения задайте пароль P@ssw0rd

• На главной странице должен отражаться номер рабочего места в виде арабской цифры, других подписей делать не надо

• Основные параметры отметьте в отчёт

**Сделай snapshot**

Устанавливаем веб-сервер **Apache2** и необходимые пакеты:

apt install -y apache\* -y

ОДНОВРЕМЕННО СКАЧИВАЙ на HQ-RTR: [Nginx](#Закладка7)

Устанавливаем **PHP** и необходимые **модули**:

apt install -y php php8.2 php-curl php-zip php-xml libapache2-mod-php php-mysql php-mbstring php-gd php-intl php-soap -y

Установка СУБД **MySQL**:

apt install -y mariadb-\* -y

Включаем и добавляем в автозагрузку **MySQL**:

systemctl enable --now mariadb

systemctl enable --now apache2

Подключаемся к **MySQL**, создаём **базу данных** и **пользователя**:

имя базы даных - " **moodledb** ";

имя пользователя - "**moodle**", пароль "**P@ssw0rd**";

mysql

CREATE DATABASE moodledb DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4\_unicode\_ci;

CREATE USER 'moodle'@'localhost' IDENTIFIED BY 'P@ssw0rd';

GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, CREATE TEMPORARY TABLES, DROP, INDEX, ALTER ON moodledb.\* TO 'moodle'@'localhost';

FLUSH PRIVILEGES;

EXIT;

Устанавливаем **git**, чтобы можно было скачать проект **Moodle**:

apt install -y git

Загружаем **код** проекта **Moodle**:

git clone git://git.moodle.org/moodle.git

git clone https://github.com/moodle/moodle.git

Переходим в загруженный каталог **moodle**:

cd moodle

Извлекаем **список** **каждой** доступной **ветви**:

git branch -a

Сообщаем **git**, какую ветку отслеживать или использовать:

Изображение выглядит как снимок экрана, текст, дисплей, Мультимедийное программное обеспечение

Автоматически созданное описание

git branch --track MOODLE\_403\_STABLE origin/MOODLE\_403\_STABLE

• проверяем: git checkout MOODLE\_403\_STABLE

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

• Копируем локальный репозиторий в /var/www/html/:

cd /

cp -R /moodle /var/www/html/

• Создаём необходимую структуру каталагов для корректной установки и работы Moodle:

mkdir /var/moodledata

chown -R www-data /var/moodledata

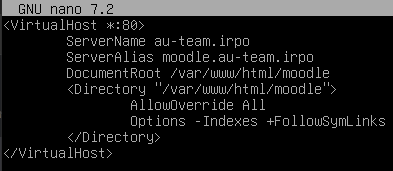
chmod -R 777 /var/moodledata

chmod -R 0755 /var/www/html/moodle

chown -R www-data:www-data /var/www/html/moodle

• Описываем конфигурационный файл для веб-сервера Apache:

nano /etc/apache2/sites-available/moodle.conf



где: ServerName - основное имя домена

ServerAlias - дополнительное имя, по которому будет доступен сайт

DocumentRoot - путь до проекта для этого домена AllowOverride All - когда сервер находит .htaccess файл (как определено AccessFileName) ему необходимо знать какие директивы, объявленные в том файле могут отменять ранее утановленную информацию доступа. Эта директива может быть установлена в None, т.е. чтобы сервер не читал файл .htaccess. Если она установленна в All - сервер будет допускать все директивы .htaccess файла.

Options -Indexes +FollowSymLinks - означает, что если каталог является символьной ссылкой, перейдите по ссылке

• Создаём символьную ссылку из sites-available на sites-enabled:

ln -s /etc/apache2/sites-available/moodle.conf /etc/apache2/sites-enabled/

• Проверяем синтаксис файла виртуального хоста: apachectl configtest

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

• Правим количество входных переменных, которые могут быть приняты в одном запросе, для работы Moodle - необходимо 5000, а значение в php.ini по умолчанию 1000:

sed -i "s/; max\_input\_vars = 1000/max\_input\_vars = 5000/g" /etc/php/8.0/apache2-mod\_php/php.ini **(заходим в файл “/etc/php…” tab’ами и изменяем, и нужно раскомментировать строчку)**

Перезагружаем apache:

Systemctl restart apache2

После можно переходить в браузер для установки Moodle

На **HQ-CLI:**

В etc/hosts

192.168.100.2 moodle.au-team.irpo moodle

Открываем firefox переходим на http://moodle.au-team.irpo(возможно: http://moodle.au-team.irpo/moodle) - выбираем Язык - нажимаем Далее:

Изображение выглядит как текст, снимок экрана, веб-страница, Веб-сайт

Автоматически созданное описание

• Подтверждаем пути - правим Каталог данных (в соответствии с созданной ранее директорией) - нажимаем Далее:

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

каталог: var/moodledata

• Выбираем драйвер баз данных MariaDB - нажимаем Далее:

Изображение выглядит как текст, Шрифт, веб-страница, Веб-сайт

Автоматически созданное описание

• Заполняем параметры ранее созданной Базы данных - пользователя БД, пароль и порт:

НАЗВАНИЕ БАЗЫ ДАННЫХ moodledb

ПОЛЬЗОВАТЕЛЬ moodle

ПАРОЛЬ P@ssw0rd

• нажимаем Продолжить:

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

• Нажимаем Продолжить: o к настройке HTTPS можно вернуться после настройки Центра Сертификации

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

• заполняем необходимые сведения и нажимаем Обновить профиль:

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, линия, диаграмма

Автоматически созданное описание

Заполняем необходимые сведения и нажимаем Сохранить изменения

Изображение выглядит как текст, снимок экрана, Шрифт

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

### 8. Настройка веб-сервера nginx как обратный прокси-сервер

**HQ-RTR**

• При обращении к HQ-RTR по доменному имени moodle.au-team.irpo клиента должно перенаправлять на HQ-SRV на стандартный порт, на сервис moodle

• При обращении к HQ-RTR по доменному имени wiki. au-team.irpo клиента должно перенаправлять на BR-SRV на порт, на сервис mediwiki

#### Шаг 1: Установите Nginx на HQ-RTR

apt update && apt install nginx -y

Запустите и активируйте Nginx:

systemctl start nginx

systemctl enable nginx

#### Шаг 2: Настройка Nginx как обратного прокси

**Сделай snapshot**

1. **Создадим конфигурационный файл для сайта в Nginx** :

Откройте новый файл конфигурации для настройки виртуальных хостов:



**Добавьте настройки для проксирования запросов** :

Добавьте конфигурацию в файл reverse-proxy.conf: **(полностью рукописный конфиг)**

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Автоматически созданное описание

 **Сохраните файл и закройте редактор**.

 **Создайте символическую ссылку на этот файл в папке sites-enabled** для активации конфигурации:



**Проверьте конфигурацию Nginx на наличие синтаксических ошибок**:

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

 Если конфигурация правильная, вы увидите сообщение syntax is ok.

 **Перезагрузите Nginx, чтобы применить изменения**:

systemctl reload nginx

### 9. Установите приложение Яндекс Браузере для организаций на HQ-CLI

• Установку браузера отметьте в отчёте

Изображение выглядит как текст, снимок экрана, программное обеспечение, веб-страница

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

# МОДУЛЬ 3

### Перенастройте ip-туннель с базового до уровня туннеля, обеспечивающего шифрование трафика

**HQ-RTR**

**apt update**

**apt install strongswan**

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

2. Конфигурация IPsec:  
  
   На обоих роутерах отредактируйте файл /etc/ipsec.conf, добавив следующее:

Изображение выглядит как текст, электроника, снимок экрана, компьютер

Контент, сгенерированный ИИ, может содержать ошибки.

Далее нужно настроить файл **ipsec.secrets**.

Вносим туда строку:

**172.16.4.2 172.16.5.2 : PSK “123qweR%”**

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Ещё один конфиг **charon.conf**, открываем его.

И редактируем в нём следующую строку, приводя к виду:

**install\_routes = no**

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

И осталось только перезагрузить службу **ipsec**:

**ipsec restart**

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

**BR-RTR**

Для начала необходимо установить пакет на наш роутер:

**apt update**

**apt install strongswan**

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

2. Конфигурация IPsec:  
  
   На обоих роутерах отредактируйте файл /etc/ipsec.conf, добавив следующее:

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Далее нужно настроить файл **ipsec.secrets**.

Вносим туда строку:

**172.16.5.2 172.16.4.2 : PSK “123qweR%”**

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Ещё один конфиг **charon.conf**, открываем его.

И редактируем в нём следующую строку, приводя к виду:

**install\_routes = no**

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

И осталось только перезагрузить службу **ipsec**:

**ipsec restart**

Также можно проверить передаются ли зашифрованные пакеты по сети, для этого нам пригодится утилита **tcpdump**:

**apt install tcpdump**

И теперь мы можем проверить это, пропишем на роутере **BR-RTR**команду:

**tcpdump -i ens18 -n -p esp**

А на роутере HQ-RTR отправим эхо-запрос:

**ping 192.168.200.2**

Как можно заметить, на правом роутере мы видим зашифрованные пакеты с меткой **ESP**.

Изображение выглядит как текст, снимок экрана, Мультимедийное программное обеспечение, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Если IPsec настроен правильно, вы должны видеть защищённый трафик между вашими серверами.

### 4 Настройте межсетевой экран на маршрутизаторах HQ-RTR и BR-RTR на сеть в сторону ISP

Для выполнения этого задания нам нужно обеспечить работу только нужных протоколов, а именно: HTTP, HTTPS, DNS, NTP, ICMP. А также запретить остальные подключения из сети Интернет во внутреннюю сеть.

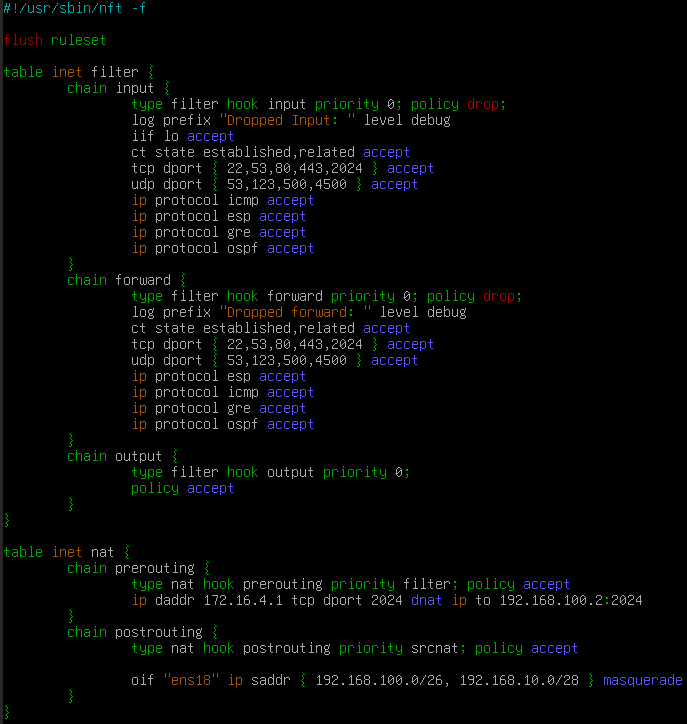
**HQ-RTR**

Отредактируем nftables под текст задания

Не забываем применять

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.



**BR-RTR**



Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

И проверим, не отвалился ли туннель ipsec после настройки правил на **HQ-RTR**:

**ipsec status**

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Контент, сгенерированный ИИ, может содержать ошибки.

Видим, что соединение установлено и всё хорошо!

Проверим также наличие связи между конечными устройствами, отправим эхо-запрос с **HQ-CLI** на **BR-SRV**:

**ping 192.168.200.2**

Изображение выглядит как текст, Шрифт, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Связь есть, всё отлично! Задание выполнено!

### 5 Настройте принт-сервер cups на сервере HQ-SRV.

Для начала необходимо установить пакеты cups и cups-pdf на **HQ-SRV:**

apt install cups cups-pdf

Теперь необходимо включить службу cups, чтобы она запускалась вместе с системой.

systemctl enable --now cups

Далее, необходимо отредактировать конфиг **/etc/cups/cupsd.conf**

Во всех блоках **Location**необходимо добавить строку **Allow all**, как на скриншоте:



Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

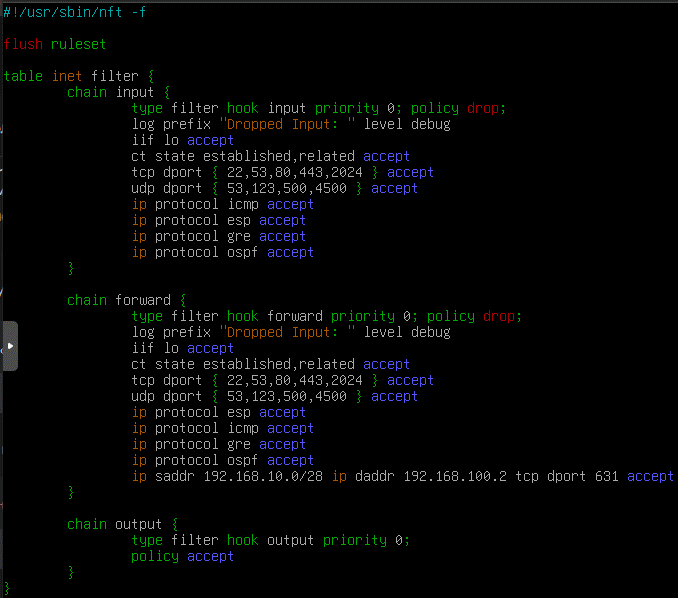
Перезапускаем службу **cups** для применения изменений:

systemctl restart cups

Переходим к подключению клиента **HQ-CLI**



Нужно добавить разрешающее правило в цепочку forward на маршрутизаторе **HQ-RTR**, чтобы разрешить трафик от HQ-CLI к HQ-SRV на порт 631: /etc/nftables.conf



На **HQ-CLI**выполняем следующую команду для подключения к принт-серверу:

lpadmin -p CUPS -E -v ipp://hq-srv.au-team.irpo:631/printers/PDF -m everywhere

Установим принтер CUPS, как принтер по умолчанию:

lpoptions -d CUPS

Изображение выглядит как текст, снимок экрана, Шрифт, информация

Контент, сгенерированный ИИ, может содержать ошибки.

Как можно заметить, принтер **CUPS**успешно подключен. Из-за того, что на **HQ-CLI**также установлен принт-сервер, можно отключить локальный принтер “**Cups-PDF**”, чтобы он не мешал.

**lpadmin -x Cups-PDF**

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь у нас остался один принтер. Проверим его работу. Откроем любой текстовый документ и попробуем его распечатать.

Изображение выглядит как программное обеспечение, текст, Значок на компьютере, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Перейдем в веб-интерфейс CUPS по адресу [https://hq-srv.au-team.irpo:631](https://www.google.com/url?q=https://www.google.com/url?q%3Dhttps://hq-srv.au-team.irpo:631%26amp;sa%3DD%26amp;source%3Deditors%26amp;ust%3D1746887455731527%26amp;usg%3DAOvVaw0ZWya3fI8n2ETgxyXRiOru&sa=D&source=docs&ust=1746887455948361&usg=AOvVaw2g6t0MMgeRytYp0EiSvZrO)

Вкладка **Принтеры**

Выбираем наш принтер.

Жмем кнопку **Показать все задания**

### 6 Реализуйте логирование при помощи rsyslog на устройствах HQ-RTR, BR-RTR, BR-SRV

Сперва необходимо настроить наш сервер для сбора логов.

Установим пакет **rsyslog**на **HQ-SRV:**

**apt install rsyslog**

Далее, отредактируем файл конфигурации, расположенный по пути

**/etc/rsyslog.conf**

Для передачи логов будем использовать протокол **TCP**, поэтому раскомментируем (уберем #) модуль **imtcp**, чтобы rsyslog мог получать логи с удаленных узлов.

Также необходимо в конец конфига добавить шаблон для сбора логов, чтобы rsyslog сохранял логи по пути, который указан в задании.

**$template RemoteLogs, "/opt/%HOSTNAME%/rsyslog.txt"**

**\*.\* ?RemoteLogs**

**& stop**

**Итоговый конфиг должен выглядеть так**

**Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

**Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.**

Включаем службу **rsyslog**, чтобы она запускалась вместе с системой и перезапускаем ее для применения изменений:

**systemctl enable rsyslog**

**systemctl restart rsyslog**

**Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.**

Сервер для приема логов настроен, переходим к настройке клиентов. Начнем с роутеров.

На **HQ-RTR** уже предустановлен пакет **rsyslog**, поэтому сразу перейдем к редактированию конфига **/etc/rsyslog.conf**





В блоке MODULES необходимо раскомментировать модули, которые обеспечивают поддержку логирования. (Все кроме модуля **imuxsock**, потому что вместо него будет использован модуль **imjournal**). Модуль **imjournal** придется дописать вручную.

**Изображение выглядит как текст, снимок экрана, программное обеспечение, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

Теперь опускаемся в самый низ конфига, там расположены правила.

Добавляем в самый конец строку, которая отвечает за отправку логов уровня предупреждения (warning) и выше:

**\*.warning @@192.168.100.2:514**

**Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.**

Теперь перезапускаем службу rsyslog, чтобы применить изменения.

**systemctl restart rsyslog**

На BR-RTR нужно повторить аналогично.

Переходим к **BR-SRV**, здесь настройка почти такая же.

Установим на **BR-SRV**пакет rsyslog:

**apt install rsyslog**



Далее, отредактируем файл конфигурации, расположенный по пути **/etc/rsyslog.conf**

Здесь также необходимо раскомментировать модули **imjournal**, **imklog**, **immark**. И добавить строку в конец конфига для того, чтобы логи отправлялись на сервер.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

Включаем службу **rsyslog**, чтобы она запускалась вместе с системой и перезапускаем ее для применения изменений:

**systemctl enable rsyslog**

**systemctl restart rsyslog**

За время пока выполнялась настройка клиентов уже должны появиться логи, проверим каталог **/opt HQ-SRV**

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

Как можно заметить, были автоматически созданы каталоги с именами клиентов. В каждом из них есть файл **rsyslog.txt**

Проверим, что логируются только сообщения уровня warning и выше.

Добавим несколько записей различного уровня в лог на любом из клиентов, например на **BR-SRV**, командами:

**logger -p user.info “Test info”**

Также добавим сообщения уровня **warning:**

**logger -p user.warning “Test warning”**

Также добавим сообщения уровня **error:**

**logger -p user.error “Test error”**

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь проверим на **HQ-SRV**содержимое файла **.txt**

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Контент, сгенерированный ИИ, может содержать ошибки.

Как можно заметить, здесь появились только сообщения уровня **warning**и **error**.

Перейдем к настройке ротации логов. На **HQ-SRV**создадим файл **/etc/logrotate.d/rsyslog**

Запишем в него следующее содержимое:

**/opt/\*/rsyslog.txt {**

**weekly**

**minsize 10M**

**compress**

**missingok**

**notifempty**

**create 0644 root root**

**rotate 4**

**dateext**

**}**

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Настройка ротации на этом закончена, каждую неделю будут проверяться логи и если какие-то из них больше 10МБ, они будут сжаты в архив.

### 8 Реализуйте механизм инвентаризации машин HQ-SRV и HQ-CLI через Ansible на BR-SRV

Для начала необходимо создать каталог, в котором будут размещены отчеты о рабочих местах:

**mkdir /etc/ansible/PC\_INFO**



Далее, создадим плейбук **/etc/ansible/inventory.yml**

****со следующим содержимым:

**---**

**- name: Инвентаризация машин HQ-SRV и HQ-CLI**

**hosts:**

**- HQ-SRV**

**- HQ-CLI**

**gather\_facts: yes**

**tasks:**

**- name: Создать отчёт с информацией рабочем месте**

**delegate\_to: localhost**

**copy:**

**dest: "/etc/ansible/PC\_INFO/{{ ansible\_hostname }}.yml"**

**content: |**

**---**

**Имя компьютера: "{{ ansible\_hostname }}"**

**IP-адрес компьютера: "{{ ansible\_default\_ipv4.address }}"**

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Проверим работу, командой:

**ansible-playbook /etc/ansible/inventory.yml**

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Ansible помечает результат как changed, так как фактическое состояние системы меняется. При первом запуске плейбука это ожидаемое поведение.

Если запустить плейбук ещё раз, то Ansible покажет для тех же задач статус ok, потому что требуемое состояние уже достигнуто и ничего менять не нужно.

Проверим наличие и содержимое, созданных отчетов:

**ls -la /etc/ansible/PC\_INFO**

**cat /etc/ansible/PC\_INFO/hq-cli.yml**

**cat /etc/ansible/PC\_INFO/hq-srv.yml**

Изображение выглядит как текст, снимок экрана, Шрифт, черный

Контент, сгенерированный ИИ, может содержать ошибки.

Как можно заметить, отчеты созданы и содержат необходимую информацию.

Задание выполнено.

### 9 Реализуйте механизм резервного копирования конфигурации для машин HQ-RTR и BR-RTR, через Ansible на BR-SRV

Спасибо за содействие подписчикам нашего канала, что предоставили плейбук для этого задания!

Создадим также каталог, в котором будут размещены резервные копии конфигураций маршрутизаторов:

**mkdir /etc/ansible/NETWORK\_INFO**



И создаём сам плейбук **/etc/ansible/backup.yml**

со следующим содержимым:

**ОБЯЗАТЕЛЬНО УСТАНОВИТЕ sudo НА HQ-RTR и BR-RTR**

**---**

**- name: Резервное копирование конфигурации маршрутизаторов HQ-RTR и BR-RTR**

**hosts:**

**- HQ-RTR**

**- BR-RTR**

**gather\_facts: no**

**tasks:**

**- name: Создание локальных папок для резервных копий**

**ansible.builtin.file:**

**path: "/etc/ansible/NETWORK\_INFO/{{ inventory\_hostname }}/{{ item }}"**

**state: directory**

**loop:**

**- "frr"**

**delegate\_to: localhost**

**- name: Копирование конфигурации FRR**

**ansible.builtin.fetch:**

**src: "/etc/frr/{{ item }}"**

**dest: "/etc/ansible/NETWORK\_INFO/{{ inventory\_hostname }}/frr/"**

**flat: yes**

**loop:**

**- "daemons"**

**- "frr.conf"**

**- "frr.conf.sav"**

**- "vtysh.conf"**

**become: yes**

**- name: Копирование сохранённых правил iptables**

**ansible.builtin.fetch:**

**src: /etc/iptablesRules**

**dest: /etc/ansible/NETWORK\_INFO/{{ inventory\_hostname }}/iptablesRules**

**flat: yes**

**become: yes**

**- name: Копирование конфигурации сетевых интерфейсов**

**ansible.builtin.fetch:**

**src: /etc/network/interfaces**

**dest: /etc/ansible/NETWORK\_INFO/{{ inventory\_hostname }}/interfaces**

**flat: yes**

**become: yes**

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Абсолютно также, как и в предыдущем задании, проверяем его работу, командой:

**ansible-playbook /etc/ansible/backup.yml**

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Как и в прошлом задании, Ansible помечает результат как **changed**, так как фактическое состояние системы меняется. При первом запуске плейбука так и должно быть.

И если запустить его ещё раз, то Ansible покажет для тех же задач статус **ok**, потому что требуемое состояние уже достигнуто и ничего менять не нужно.

Проверим наличие созданных отчетов:

**ls -la /etc/ansible/NETWORK\_INFO**

**ls -la /etc/ansible/NETWORK\_INFO/HQ-RTR**

**ls -la /etc/ansible/NETWORK\_INFO/BR-RTR**

Изображение выглядит как текст, снимок экрана, Шрифт, черно-белый

Контент, сгенерированный ИИ, может содержать ошибки.

А также их содержимое, если хотите убедиться, что действительно скопировалось, для примера покажем файл **interfaces** с маршрутизатора **HQ-RTR**, остальные можете сами:

**cat /etc/ansible/NETWORK\_INFO/HQ-RTR/interfaces**

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

По итогу все резервные копии конфигураций созданы и содержат необходимую информацию.

Задание выполнено.