Команда управления компетенции

Сетевое и системное администрирование

ПРАКТИКУМ.

Подготовка к Демонстрационному экзамену по 09.02.06 Сетевое и системное администрирование

УЧЕБНОЕ ПОСОБИЕ

2025

УДК 004
ББК 32.81я73
У36

У 36 Практикум. Подготовка к Демонстрационному экзамену по 09.02.06 Сетевое и системное администрирование / С.С. Дегтярев, Т.И. Ефименко, А.П. Золотарёв, И.М. Морозов, Д.И. Носенко, А.Г. Уймин, В.В. Шальнев. Практикум. Подготовка к Демонстрационному экзамену по 09.02.06 Сетевое и системное администрирование» – М.: РГУ нефти и газа (НИУ) имени И.М. Губкина, 2020. – Электрон.дан. - 1 электрон.опт.диск (CD-ROM); 12 см. – Систем.требования: компьютер IBM-PC совместимый; монитор, видеокарта, поддерживающ. разреш.1024x768; привод CD-ROM; программа для чтения pdf-файлов. – Загл.с этикетки диска. – Текст. Изображение : электронные.
ISBN 978-5-91961-583-5

Учебное пособие предназначено для преподавателей и студентов, осваивающих образовательные программы среднего профессионального образования по укрупненным группам «Информационная безопасность», «Информатика и вычислительная техника», «Электроника, радиотехника и системы связи» в целях повышения уровня знаний и умений в области профессиональной деятельности по направлению «Сетевое и системное администрирование» с применением ИТ-инфраструктуры на базе отечественных ИТ технологий.

Минимальные системные требования:
Тип компьютера, процессор, частота: IBM-PC совместимый
Видеосистема: монитор, видеокарта, поддерживающая разрешение1024x768
Дополнительное оборудование: привод CD-ROM
Дополнительное программное обеспечение: программа для чтения pdf-файлов.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

«Технологическая независимость в области ИТ критически важна в современном мире. Это стало очевидным после введения секторальных санкций в 2014 году, а затем после ухода с российского рынка зарубежных ИТ-фирм после 2022 года.

Сегодня отечественное ПО внедряют не только государственные структуры, но и предприятия различных отраслей — как крупные корпорации, так и малый бизнес.

При этом и российские разработчики, получая мощную государственную поддержку и обратную связь от реальных пользователей, постоянно совершенствуют свои программные продукты.

В этих условиях актуальным становится вопрос подготовки кадров, умеющих работать с современным отечественным софтом и оборудованием.

Сегодняшние выпускники завтра придут на производство: в госсектор, бизнес, образование и здравоохранение, поэтому крайне важно готовить студентов к реальным практическим задачам. ИТ-сфера меняется быстро: появляются новые технологии, а требования рынка растут. Для построения реальной технологической независимости страны необходимо постоянно повышать уровень технического образования, совершенствовать учебные программы, чтобы знания, полученные студентами, соответствовали актуальным потребностям рынка.

Ключевую роль в этом процессе играет совместная работа образовательных организаций и ИТ-компаний. Разработчики знают состояние ИТ-рынка, обладают экспертизой, могут сформировать актуальные требования к навыкам и знаниям сотрудников. Они готовы активно участвовать в разработке образовательных программ, учебных пособий, в то время как преподаватели могут методически грамотно и понятно реализовывать учебный процесс.

Важное преимущество дает и использование в обучении свободного программного обеспечения. Оно дает студентам доступ к исходному коду, позволяя не просто пользоваться программами, но и разбираться в их устройстве, изучать код и вносить в него изменения. В будущем такие студенты смогут не только администрировать системы, но и разрабатывать собственные программные продукты, тем самым укрепляя технологическую независимость страны.»

Смирнов А.В., председатель совета директоров, ООО «Базальт СПО»

Учебное пособие предназначено для практической подготовки студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования (далее – СПО) укрупненных групп специальностей «Информатика и вычислительная техника» и «Информационная безопасность» в целях содействия формированию профессиональных компетенций, необходимых в трудовой деятельности сетевого и системного администратора. В системе СПО основным инструментом объективной оценки уровня подготовки студентов является демонстрационный экзамен, который проводится независимыми экспертами по итогам обучения либо при промежуточной аттестации. Данное пособие включает рекомендации по выполнению заданий демонстрационного экзамена, организуемого в рамках государственной итоговой аттестации по завершении освоения образовательной программы СПО по специальности 09.02.06 «Сетевое и системное администрирование». Содержание пособия соответствует

требованиям Федерального государственного образовательного стандарта среднего профессионального образования (Федеральный государственный образовательный стандарт (ФГОС) по специальности 09.02.06 «Сетевое и системное администрирование» утверждён приказом Министерства образования и науки РФ от 09.12.2016 №1548 (ред. от 17.12.2020), Федеральный государственный образовательный стандарт (ФГОС) по специальности 09.02.06 «Сетевое и системное администрирование» утверждён приказом Министерства просвещения Российской Федерации от 10.07.2023 №519) и профессиональным квалификационным требованиям описанным в Профстандарт: 06.026 Системный администратор информационно-коммуникационных систем УТВЕРЖДЕН приказом Министерства труда и социальной защиты Российской Федерации от 29 сентября 2020 года N 680н Системный администратор информационно-коммуникационных систем, поддержано специалистами ФГБОУ ДПО «Институт развития профессионального образования».

Основными нормативными документами являются:

- МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИКАЗ от 8 ноября 2021 г. N 800 ОБ УТВЕРЖДЕНИИ ПОРЯДКА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ПО ОБРАЗОВАТЕЛЬНЫМ ПРОГРАММАМ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ (в ред. Приказов Минпросвещения РФ от 05.05.2022 N 311, от 19.01.2023 N 37, от 24.04.2024 N 272, от 22.11.2024 N 812)
- Приказ ФГБОУ ДПО ИРПО от 25 апреля 2024 г. № 01-09-139/2024 "Об утверждении Методических указаний по разработке оценочных материалов для проведения демонстрационного экзамена
- Приказ ФГБОУ ДПО ИРПО от 22 июня 2023 г. № П-291 «О введении в действие Методики организации и проведения демонстрационного экзамена»

Авторский коллектив:

ФИО	Должность, место работы
Дегтярев Сергей Сергеевич	г. Ростов-на-Дону, преподаватель, ГБПОУ РО "РКСИ", ведущий эксперт компетенции Сетевое и системное администрирование, разработчик КОД 09.02.06-5-2025 Специалист по администрированию сети
Ефименко Татьяна Ивановна	г. Санкт-Петербург, Колледж туризма и прикладных технологий Санкт-Петербурга, преподаватель, председатель ПЦК цифровых технологий, ведущий эксперт компетенции Сетевое и системное администрирование, разработчик КОД 09.02.06-2-2025 Системный администратор (Эксплуатация облачных сервисов) и КОД 09.02.06-3-2025 Системный администратор (Эксплуатация объектов сетевой инфраструктуры)
Золотарёв Андрей Петрович	г. Кировск, Ленинградская область, преподаватель, ГБОУ СПО ЛО "Кировский политехнический техникум", преподаватель, ведущий эксперт компетенции Сетевое и системное администрирование
Морозов Илья Михайлович	г. Москва, мастер производственного обучения, РГУ нефти и газа (НИУ) имени И.М. Губкина, ведущий эксперт компетенции Сетевое

	и системное администрирование, эксперт НОВОТЕХ, Менеджер компетенции Облачные технологии
Носенко Дмитрий Игоревич	г. Боровичи, преподаватель ОГА ПОУ "Боровичский Педагогический Колледж", ведущий эксперт компетенции Сетевое и системное администрирование, тренер Чемпиона России 2024 по Сетевому и системному администрированию
Уймин Антон Григорьевич	г. Москва, зав. лаб, РГУ нефти и газа (НИУ) имени И.М. Губкина, эксперт НОВОТЕХ, Менеджер компетенции Сетевое и системное администрирование, руководитель команды #au_team
Шальнев Владимир Валентинович	г. Ногинск, преподаватель высшей квалификационной категории по специальности 09.02.06 «Сетевое и системное администрирование», ГБПОУ МО «Ногинский колледж», ведущий эксперт компетенции Сетевое и системное администрирование

БЛАГОДАРНОСТИ

Коллективу компании "Базальт СПО" за предоставление возможности преподавателям и студентам изучать системное администрирование GNU/Linux-систем на примере ОС семейства «Альт», помощь и содействие в решении технических вопросов и выборе технологий при написании пособия и отдельно Губиной Татьяне Николаевне, к.п.н., руководителю направления по работе с образовательными организациями "Базальт СПО" за помощь в экспертной оценке материалов.

ООО "РДП Инновации" (бренд EcoRouter) за возможность изучать сетевые технологии на примере высокотехнологичного российского оборудования, которое формирует облик современной сетевой инфраструктуры и решает вопросы импортозамещения. Благодаря образовательным инициативам ООО "РДП Инновации" (бренд EcoRouter) у системы образования появляются сетевые инженеры, востребованные в промышленности, телеком секторе, банках и государственных организациях по всей стране.

Отдельно хотелось бы отметить вклад EcoRouter и Базальт СПО в поддержку чемпионатного движения по компетенции «Сетевое и системное администрирование», участники которого демонстрируют высокий уровень профессионального мастерства, наглядно демонстрирующий развитие российской отрасли ИТ.

ООО «Киберпротект» за активную поддержку компетенции Сетевое и системное администрирование в области резервного копирования и систем виртуализации.

ООО «Айдеко» за активную поддержку компетенции Сетевое и системное администрирование в области сетевой безопасности.

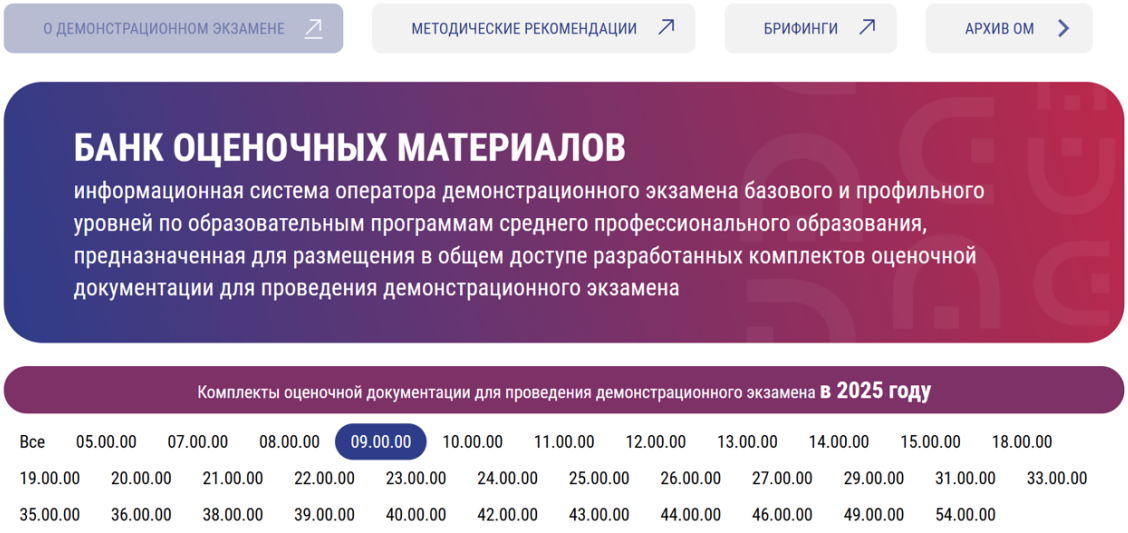
Барышниковой Алене Дмитриевне, за вклад в оформление и вычитку текста.

ВВЕДЕНИЕ

Проведение ГИА в 2025 году в форме демонстрационного экзамена регламентируется локальными актами образовательных организаций, нормативными актами Минпросвещения России и федеральными государственными образовательными стандартами среднего профессионального образования (далее – ФГОС СПО), в соответствии с которыми обучающиеся завершают обучение. Оценочные материалы для проведения ГИА в форме демонстрационного экзамена разработаны прошедшими конкурсный отбор экспертами и открыто размещены на следующих информационных ресурсах:

2025 г.– https://bom.firpo.ru/;

до 2023 г. – https://om.firpo.ru/archive.



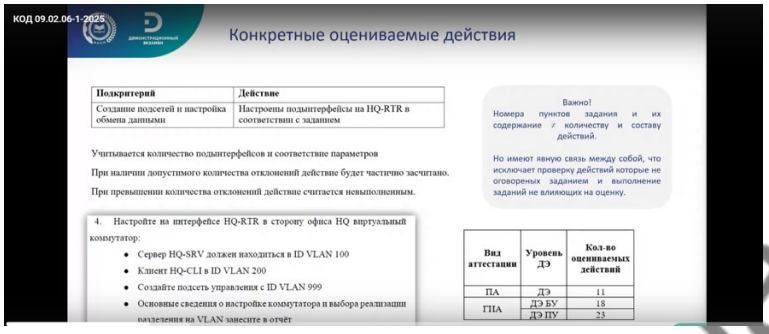
Информационная система оператора демонстрационного экзамена базового и профильного уровней по образовательным программам среднего профессионального образования, предназначенная для размещения в общем доступе разработанных комплектов оценочной документации для проведения демонстрационного экзамена:

ФГОС 09.02.06 Сетевое и системное администрирование (приказ №1548 от 09 декабря 2016) (https://spolab.firpo.ru/storage/NPD//0JLPhkk6Wi1rTWUlJWUDhifmY1EX5JLxyZAczvbA.docx)	

09.02.06-1-2025: Сетевой и системный администратор (https://bom.firpo.ru/Public/2359)	
09.02.06-5-2025: Специалист по администрированию сети (https://bom.firpo.ru/Public/2369)	
ФГОС 09.02.06 Сетевое и системное администрирование (приказ №519 от 10 июля 2023) (https://spolab.firpo.ru/npdv2/category-doc/get/3774)	
09.02.06-2-2025: Системный администратор (Эксплуатация облачных сервисов) (https://bom.firpo.ru/Public/2361)	
09.02.06-3-2025: Системный администратор (Эксплуатация объектов сетевой инфраструктуры) (https://bom.firpo.ru/Public/2363)	

09.02.06-4-2025: Системный администратор (Эксплуатация операционных систем) (https://bom.firpo.ru/Public/2365)	

Видеообзор комплекта оценочных материалов



https://vkvideo.ru/video-219561594_456239715?list=ln-dyXhMWQqd78jblZ1Ot&ref_domain=bom.firpo.ru

Видеообзор подготовки к ДЭ

Чат компетенции, структурированный по темам (https://t.me/+Sz-uToWW2zc5OWMy)	
ДЭ 2024 (https://vkvideo.ru/video/playlist/-228030577_1)	

Знакомство с технологиями EcoRouter в СиСА 2025 (https://vkvideo.ru/video/playlist/-228030577_4)	
Знакомство с технологиями IDECO FW в СиСА 2025 (https://vkvideo.ru/video/playlist/-228030577_6)	

КОД 09.02.06-1-2025 Сетевой и системный администратор

Модуль 1 Настройка сетевой инфраструктуры

Модуль № 1:

Настройка сетевой инфраструктуры

Вид аттестации/уровень ДЭ:

ПА, ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Задание:

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной 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.

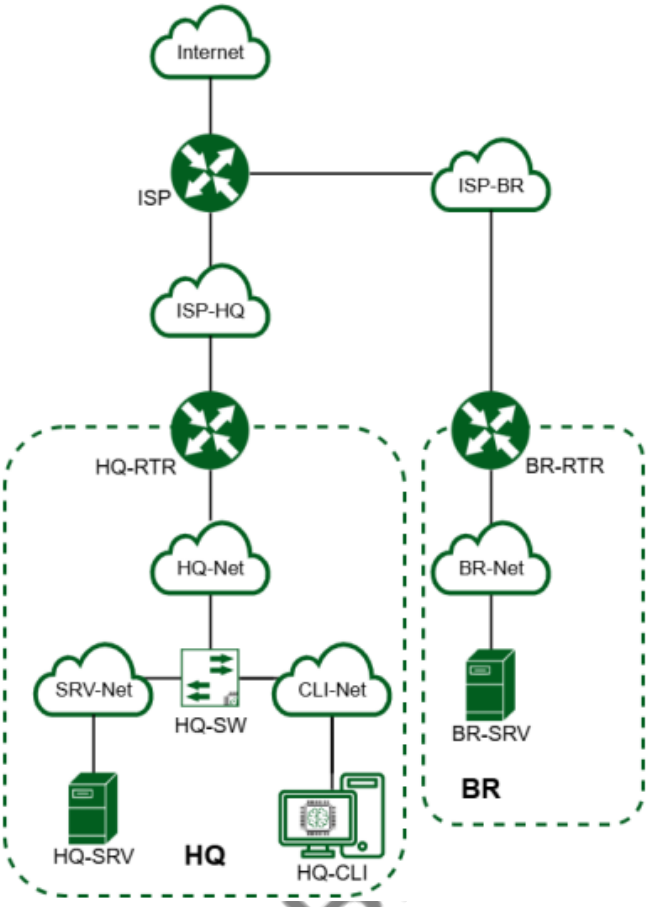


Рисунок 1. Топология сети

Таблица 1

Машина	RAM, ГБ	CPU	HDD/SSD, ГБ	ОС
ISP	1	1	10	ОС Альт JeOS/Linux или аналог
HQ-RTR	1	1	10	ОС EcoRouter или аналог
BR-RTR	1	1	10	ОС EcoRouter или аналог
HQ-SRV	2	1	10	ОС Альт Сервер/аналог
BR-SRV	2	1	10	ОС Альт Сервер/аналог
HQ-CLI	3	2	15	ОС Альт Рабочая Станция/аналог
Итого	10	7	65	-

1. Произведите базовую настройку устройств:
   - Настройте имена устройств согласно топологии. Используйте полное доменное имя;
   - На всех устройствах необходимо сконфигурировать IPv4;
   - IP-адрес должен быть из приватного диапазона в случае, если сеть локальная, согласно RFC1918;
   - Локальная сеть в сторону HQ-SRV (VLAN100) должна вмещать не более 64 адресов;
   - Локальная сеть в сторону HQ-CLI (VLAN200) должна вмещать не более 16 адресов;
   - Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов;
   - Локальная сеть для управления (VLAN999) должна вмещать не более 8 адресов;
   - Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3.
2. Настройка ISP
   - Настройте адресацию на интерфейсах:

- Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP;
- Настройте маршруты по умолчанию там, где это необходимо;
- Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28;
- Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28;
- На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет.

3. Создание локальных учетных записей:
   - Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV
     - Пароль пользователя sshuser с паролем P@ssw0rd;
     - Идентификатор пользователя 1010;
     - Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.
   - Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR
     - Пароль пользователя net_admin с паролем P@$$word;
     - При настройке на EcoRouter пользователь net_admin должен обладать максимальными привилегиями;
     - При настройке ОС на базе Linux, запускать sudo без дополнительной аутентификации.
4. Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:
   - Сервер HQ-SRV должен находиться в ID VLAN 100;
   - Клиент HQ-CLI в ID VLAN 200;
   - Создайте подсеть управления с ID VLAN 999;
   - Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт.
5. 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».
6. Между офисами HQ и BR необходимо сконфигурировать ip туннель:
   - Сведения о туннеле занесите в отчёт;
   - На выбор технологии GRE или IP in IP.
7. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.
   - Разрешите выбранный протокол только на интерфейсах в ip туннеле;
   - Маршрутизаторы должны делиться маршрутами только друг с другом;
   - Обеспечьте защиту выбранного протокола посредством парольной защиты;
   - Сведения о настройке и защите протокола занесите в отчёт.
8. Настройка динамической трансляции адресов.
   - Настройте динамическую трансляцию адресов для обоих офисов;
   - Все устройства в офисах должны иметь доступ к сети Интернет.
9. 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.

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

Таблица 2

Устройство	**Запись**	**Тип**
HQ-RTR	hq-rtr.au-team.irpo	A, PTR
BR-RTR	br-rtr.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A, PTR
HQ-CLI	hq-cli.au-team.irpo	A, PTR
BR-SRV	br-srv.au-team.irpo	A
HQ-RTR	moodle.au-team.irpo	CNAME
HQ-RTR	wiki.au-team.irpo	CNAME

Таблица 3

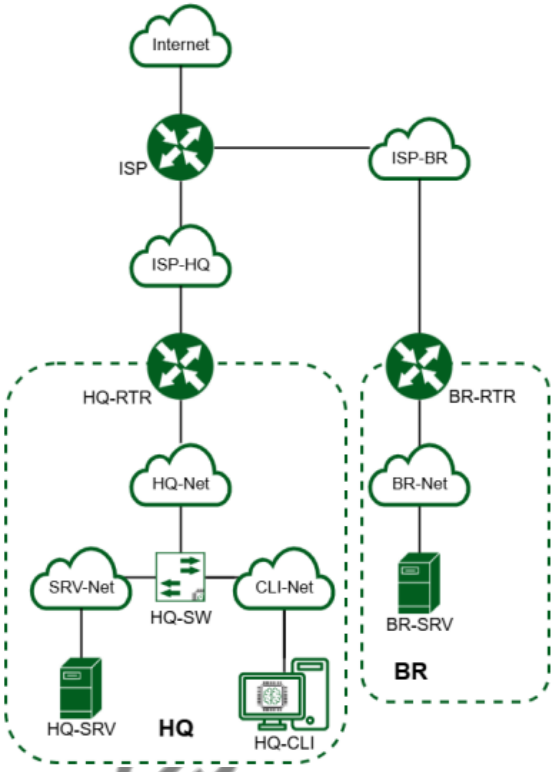
Имя устройства	**IP-адрес**	**Шлюз по умолчанию**
BR-SRV	192.168.0.2/24	192.168.0.1

Выполнение задания:

Базовая настройка устройств

Задание 1.

Настройте имена устройств согласно топологии. Используйте полное доменное имя.



Публичная схема экзаменационного задания

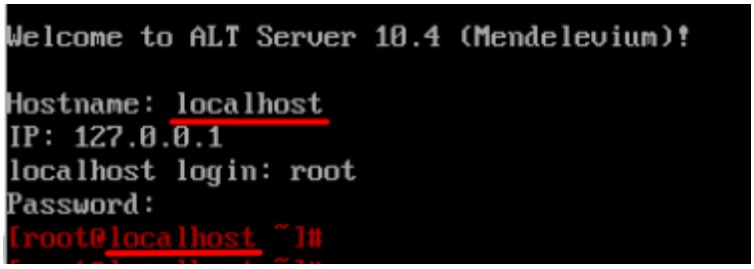
Где выполнять:

На машинах с ОС «Альт»

Как делать?

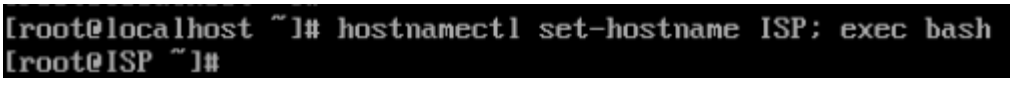
Переименования устройств с ОС «Альт»:

Изначально имя машины стандартное – localhost:



Для установки имени виртуальной машины необходимо воспользоваться утилитой HOSTNAMECTL (полное доменное имя прописывается везде, кроме ВМ ISP):

```
hostnamectl set-hostname <hostname>.<domain-name>; exec bash
```



Описание применяемых команд:

`hostnamectl` – программа для управления именем машины;

`set-hostname` – аргумент, позволяющий выполнить изменение хостнейма;

`<hostname>` – целевое имя машины;

`<domain-name>` – имя домена;

`exec bash` – перезапуск оболочки bash для отображения нового хостнейма.

Как проверить?

Перезагрузите компьютер с помощью команды `reboot`. После загрузки компьютера изменилось приглашение системы к вводу команд.

```
ISP login: root
Password:
Last login: Mon Apr  7 11:09:17 MSK 2025 on tty1
[root@ISP ~]# _
```

Команда `hostname` выведет текущее название машины.

```
[root@ISP ~]# hostname
ISP
[root@ISP ~]#
```

Где изучается?

2 курс: Операционные системы и среды, Компьютерные сети и далее.

Краткая справка:

– Общая информация о сетевых настройках системы ОС «Альт» (https://www.altlinux.org/Настройка_сети#Имя_компьютера).

Где выполнять:

На машинах с ОС «EcoRouterOS»

Как делать?

Для переименования устройств с ОС «EcoRouterOS», используются следующие команды:

```
enable
configure terminal
hostname <hostname>
ip domain-name <domain-name>
write memory
```

```
EcoRouterOS version Jasmine 26/12/2024 23:46:47
ecorouter>enable
ecorouter#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
ecorouter(config)#hostname hq-rtr
hq-rtr(config)#ip domain-name au-team.irpo
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

Описание применяемых команд:

`enable` – переход в привилегированный режим;

`configure terminal` – переход в режим конфигурирования;

`<hostname>` – целевое имя машины;

`ip domain-name` – установка доменного имени;

`<domain-name>` – имя домена;

`write memory` – сохранение изменений.

Как проверить?

Из привилегированного режима используется команда:

`show hostname` и `show running-config | include domain-name`.

```
hq-rtr#show hostname
hq-rtr
hq-rtr#show running-config | include domain-name
ip domain-name au-team.irpo
hq-rtr#
```

Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Дополнительно:

Имена устройств нужны для упрощения идентификации и управления ими. Они помогают пользователям легко находить, различать и взаимодействовать с множеством подключенных устройств. Хорошо подобранные имена делают взаимодействие более интуитивным и удобным. Кроме того, когда пользователь подключается удалённо, имя устройства даёт ему понимание, на каком устройство он работает прямо сейчас.

Где изучается?

2 курс:

– Операционные системы и среды;
– Компьютерные сети и далее.

Задание 2. На всех устройствах необходимо конфигурировать IPv4.

Подробное описание пункта задания

На всех устройствах необходимо сконфигурировать IPv4:

- Локальная сеть в сторону HQ-SRV (VLAN100) должна вмещать не более 64 адресов;
- Локальная сеть в сторону HQ-CLI (VLAN200) должна вмещать не более 16 адресов;
- Локальная сеть в сторону BR-SRV должна вмещать не более 32 адресов;
- Локальная сеть для управления (VLAN999) должна вмещать не более 8 адресов.

Где выполнять:

На машинах с ОС «Альт»: HQ-SRV, BR-SRV

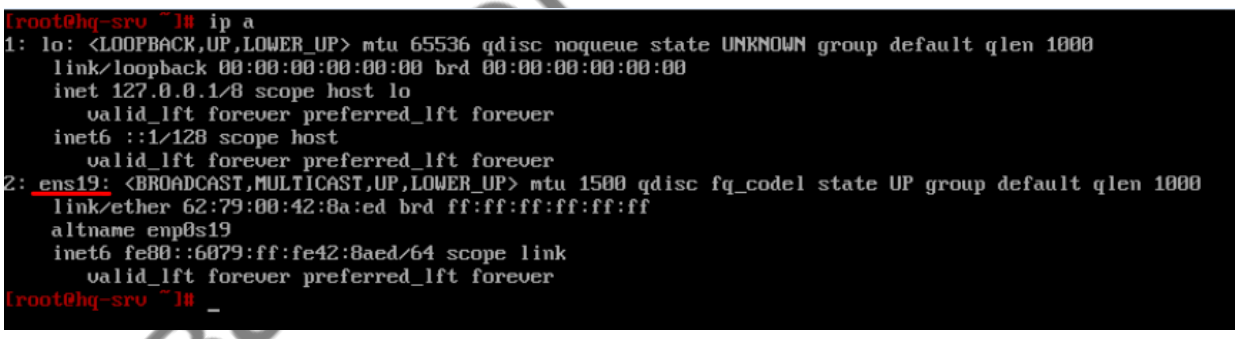
Как делать?

Для устройств с ОС «Альт»:

Базовая настройка сетевых параметров на ОС «Альт» будет осуществляться с использованием текстового редактора vim или nano, а также с использованием сетевой подсистемы `etcnet`. Для открытия файла для редактирования необходимо прописать vim и нужный путь (например: vim /etc/net/sysctl.conf) до файла, после чего, в открывшемся окне вписываются нужные параметры. **Внимание!** Для применения настроек, необходимо перезагрузить службу network, командой:

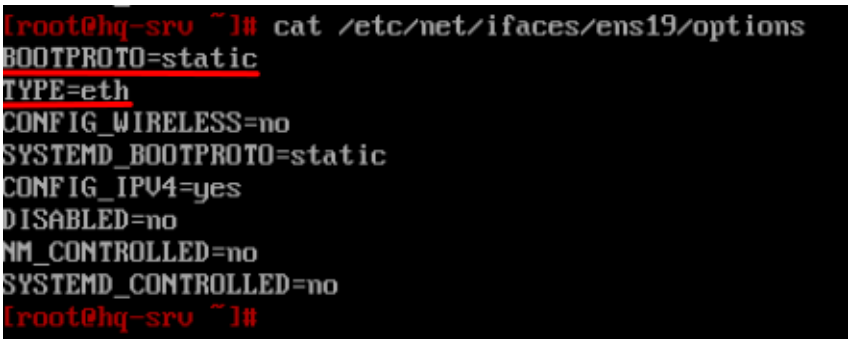
```
systemctl restart network
```

Просмотр существующих интерфейсов выполняется командой `ip a`



Красным цветом показано название интерфейса (в примере оно может отличаться!).

Для конфигурации IPv4 на устройствах, будут отредактированы файлы `options`, и созданы файлы `ipv4address`, `ipv4route`. В файле `/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/options`, должны быть заданы хотя бы два основных параметра. Параметр `TYPE=eth` указывает на тип интерфейса – ethernet, и параметр `BOOTPROTO=static` означает, что настройка статического IP-адреса и маршрутов будет взята из файлов `ipv4address` и `ipv4route`



Внимание! Для того, чтобы в качестве сетевой подсистемы корректно использовался `etcnet` и операционная система могла считывать и применять содержимое конфигурационных файлов: `ipv4address`, `ipv4route`, `resolv.conf` из директории `/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/`, необходимо, чтобы значение параметров `DISABLED,NM_CONTROLLED,SYSTEMD_CONTROLLED` были установлены в `no` или же указание данных параметров в файле `options` не является обязательным условием.

Далее опишем содержимое конфигурационных файлов: `ipv4address`, `ipv4route`, `resolv.conf`, обязательное к указанию в данных файлах, используя текстовый редактор `vim`.

Правила настройки

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ipv4address
```

<IP-адрес>/<Префикс>

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ipv4route
```

```
default via <IP-адрес шлюза>
```

```
vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/resolv.conf
```

```
search <ДОМЕН_ПОИСКА (ДОМЕННОЕ ИМЯ)>
```

```
nameserver <IP-адрес DNS-сервера>
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
[root@hq-srv ~]# ls /etc/net/ifaces/ens19/
ipv4address  ipv4route  options  resolv.conf
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/ipv4address
192.168.100.1/26
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/ipv4route
default via 192.168.100.62
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/resolv.conf
search au-team.irpo
nameserver 77.88.8.8
[root@hq-srv ~]#
```

Для применения настроек, необходимо перезагрузить службу network, командой:

```
systemctl restart network
```

Как проверить?

Проверка IP-адреса осуществляется командой: `ip a`

```
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 62:79:00:42:8a:ed brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.100.1/26 brd 192.168.100.63 scope global ens19
       valid_lft forever preferred_lft forever
    inet6 fe80::6079:ff:fe42:8aed/64 scope link
       valid_lft forever preferred_lft forever
[root@hq-srv ~]#
```

Проверка IP-адреса шлюза по умолчанию осуществляется командой: `ip r`

```
[root@hq-srv ~]# ip r
default via 192.168.100.62 dev ens19
192.168.100.0/26 dev ens19 proto kernel scope link src 192.168.100.1
[root@hq-srv ~]#
```

Проверка IP-адреса DNS-сервера осуществляется просмотром содержимого конфигурационного файла `/etc/resolv.conf`

```
[root@hq-srv ~]# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search au-team.irpo
nameserver 77.88.8.8
```

Краткая справка:

- Подсказки пользователю /etc/net (https://www.altlinux.org/Etcnet);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet (https://www.altlinux.org/Etcnet_start).

Где выполнять:

На машинах с ОС «EcoRouterOS»: HQ-RTR, BR-RTR.

Как делать?

Для устройств с ОС «EcoRouterOS»:

Просмотр существующих портов выполняется командой привилегированного режима: `show port` или `show port brief`

```
hq-rtr>enable
hq-rtr#show port brief
 Name             Physical   Admin   Lacp    Description
 ------------------------------------------------------------
 te0              UP         UP      *
 te1              UP         UP      *
hq-rtr#
```

Основные понятия касающиеся EcoRouter:

- `Порт (port)` – это устройство в составе EcoRouter, которое работает на уровне коммутации (L2);
- `Интерфейс (interface)` – это логический интерфейс для адресации, работает на сетевом уровне (L3);
- `Service instance` (Сабинтерфейс, SI, Сервисный интерфейс) является логическим сабинтерфейсом, работающим между L2 и L3 уровнями:
  - Данный вид интерфейса необходим для соединения физического порта с интерфейсами L3, интерфейсами bridge, портами;
  - Используется для гибкого управления трафиком на основании наличия меток VLANов в фреймах, или их отсутствия;
  - Сквозь сервисный интерфейс проходит весь трафик, приходящий на порт.

Для того чтобы назначить IPv4-адрес на EcoRouter, необходимо придерживаться следующего алгоритма в общем виде:

В режиме администрирование (`conf t`) создать интерфейс с произвольным именем и назначить на него IPv4:

`interface <ИМЯ_ИНТЕРФЕЙСА>`
`ip address <IP-адрес>/<Префикс>`

В режиме конфигурирования порта создать `service-instance` с произвольным именем, указать (инкапсулировать) что будет обрабатываться тегированный или не тегированный трафик, указать в какой интерфейс (ранее созданный) нужно отправить обработанные кадры:

Для не тегированного трафика:

```
port <ИМЯ_ПОРТА>
service-instance <ИМЯ>
encapsulation untagged
connect ip interface <ИМЯ_ИНТЕРФЕЙСА>
exit
```

Для того чтобы задать IP-адрес шлюза (маршрута) по умолчанию необходимо из режима администрирования (`conf t`) выполнить следующую команду:

```
ip route 0.0.0.0/0 <IP-адрес шлюза>
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

Создание интерфейса с последующим назначением IP-адреса, создание сервис-инстанса на порту с указанием не тегированного трафика и конкретного интерфейса:

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#interface ISP
hq-rtr(config-if)#ip address 172.16.4.14/28
hq-rtr(config-if)#exit
hq-rtr(config)#port te0
hq-rtr(config-port)#service-instance te0/ISP
hq-rtr(config-service-instance)#encapsulation untagged
hq-rtr(config-service-instance)#connect ip interface ISP

2025-04-07 09:43:31      INFO      Interface ISP changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

Как проверить?

Проверка осуществляется командой привилегированного режима:

```
show ip interface brief
```

```
hq-rtr#show ip interface brief
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 ISP              172.16.4.14/28      up                    default
hq-rtr#
```

Краткая справка:

- User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Дополнительно:

Знание IPv4 адресации необходимо для:

- Сетевой конфигурации: правильной настройки и управления устройствами в сети;
- Понимания сетевой архитектуры: формирования сетевых топологий и маршрутов;
- Устранения неполадок: диагностики и решения проблем с подключением;
- Безопасности: настройки брандмауэров и контроля доступа.

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

3 курс:

- Организация, принципы построение и функционирования компьютерных сетей;
- Программное обеспечение компьютерных сетей;
- Организация администрирования компьютерных систем и далее.

Задание 3. Сведения об адресах занесите в отчёт.

Подробное описание пункта задания:

Сделать таблицу, учитывая, что IP-адресация должна быть из приватного диапазона в случае, если сеть локальная, согласно RFC1918.

Как делать?

На локальной машине, с помощью табличного или текстового редактора.

Краткая справка:

– Распределение адресов для частных IP-сетей (https://protocols.ru/files/RFC/rfc1918.pdf).

Дополнительно:

Создание таблиц адресов устройств в сети с указанием имён, расположения версии операционной системы необходимо для:

- Упрощения управления: Легче отслеживать и управлять устройствами;
- Устранения неполадок: Быстрая диагностика проблем с конкретными устройства;
- Безопасности: Упрощение настройки доступа и мониторинг;
- Оптимизации сетевых ресурсов: Эффективное распределение нагрузки и планирование обновлений;
- Это повышает эффективность работы сети и облегчает администрирование.

Где изучается?

На учебной и производственной практике.

2 курс:

– Компьютерные сети.

3 курс:

– Эксплуатация объектов сетевой инфраструктуры.

Настройка ISP

Задание 1. Настройте адресацию на интерфейсах.

Подробное описание пункта задания

Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP.

Где выполнять:

На машинах: ISP.

Как делать?

Просмотр существующих интерфейсов выполняется командой `ip a`

```
[root@ISP ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 02:1e:1c:97:d1:5c brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet6 fe80::1e:1cff:fe97:d15c/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: ens20: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 96:56:6d:15:9b:49 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
4: ens21: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 6a:e0:74:76:3c:36 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
[root@ISP ~]# _
```

Красным цветом показано название интерфейса (в примере оно может отличаться!), желтым цветом – его MAC-адрес (в примере MAC-адрес может отличаться!). Для того чтобы понять, какой интерфейс куда настроен, необходимо ориентироваться по их MAC-адресам. В настройках виртуальной машины, в настройках сетевых интерфейсов можно увидеть MAC-адрес и сеть (Bridge), к которой подключен сетевой интерфейс.

Для того чтобы интерфейс, подключенный к магистральному провайдеру, получал адрес по DHCP, необходимо в конфигурационном файле, расположенном по пути `/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/options` в параметре `BOOTPROTO` указать значение `dhcp`:

```
[root@ISP ~]# cat /etc/net/ifaces/ens19/options
BOOTPROTO=dhcp
TYPE=eth
[root@ISP ~]# _
```

Для применения настроек, необходимо перезагрузить службу `network`, командой:

```
systemctl restart network
```

Как проверить?

Проверка IP-адреса осуществляется командой: `ip a`

```
ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
 link/ether 02:1e:1c:97:d1:5c brd ff:ff:ff:ff:ff:ff
 altname enp0s19
 inet 192.168.11.56/26 brd 192.168.11.63 scope global dynamic noprefixroute ens19
    valid_lft 5995sec preferred_lft 5245sec
 inet6 fe80::1e:1cff:fe97:d15c/64 scope link proto kernel_ll
    valid_lft forever preferred_lft forever
```

Проверка IP-адреса шлюза по умолчанию осуществляется командой: `ip r`

```
[root@ISP ~]# ip r
default via 192.168.11.62 dev ens19 proto dhcp src 192.168.11.56 metric 1002
192.168.11.0/26 dev ens19 proto dhcp scope link src 192.168.11.56 metric 1002
[root@ISP ~]# _
```

Проверка IP-адреса DNS-сервера осуществляется просмотром содержимого конфигурационного файла `/etc/resolv.conf`

```
[root@ISP ~]# cat /etc/resolv.conf
# Generated by dhcpcd from ens19.dhcp
# /etc/resolv.conf.head can replace this line
domain college.prof
nameserver 192.168.11.62
```

Проверка доступа в сеть Интернет осуществляется с помощью утилиты `ping`

```
[root@ISP ~]# ping -c3 ya.ru
PING ya.ru (77.88.44.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.44.242): icmp_seq=1 ttl=53 time=18.9 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=2 ttl=53 time=18.2 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=3 ttl=53 time=18.6 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 18.205/18.553/18.858/0.268 ms
[root@ISP ~]#
```

Краткая справка:

- Подсказки пользователю /etc/net (https://www.altlinux.org/Etcnet);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet (https://www.altlinux.org/Etcnet_start).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

Задание 2. Настройте адресацию на интерфейсах. Подключение к магистральному провайдеру.

Подробное описание пункта задания

Настройте маршруты по умолчанию, где это необходимо.

Где выполнять:

На машинах: ISP

Как делать?

Для устройства ISP маршрут по умолчанию настраивается автоматически, так как интерфейс, подключенный к магистральному провайдеру, получает все необходимые сетевые параметры по DHCP.

Краткая справка:

- Подсказки пользователю /etc/net (https://www.altlinux.org/Etcnet);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet (https://www.altlinux.org/Etcnet_start).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

Задание 3. Настройте адресацию на интерфейсах.

Подробное описание пункта задания

Интерфейс, к которому подключен HQ-RTR, подключен к сети 172.16.4.0/28.

Интерфейс, к которому подключен BR-RTR, подключен к сети 172.16.5.0/28.

Где выполнять:

На машинах: ISP

Как делать?

Для каждого интерфейса, необходимо в директории `/etc/net/ifaces/` создать директорию с именем данного интерфейса, для этого используется команда:

```
mkdir /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>
```

Для каждого интерфейса, необходимо в директории /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ создать конфигурационный файл `options` с минимально необходимыми параметрами, а именно: `TYPE=eth` указывает на тип интерфейса – `ethernet`, и параметр `BOOTPROTO=static` означает, что настройка статических параметров.

Далее опишем содержимое конфигурационного файла `ipv4address` для каждого интерфейса, используя текстовый редактор `vim` или `nano`.

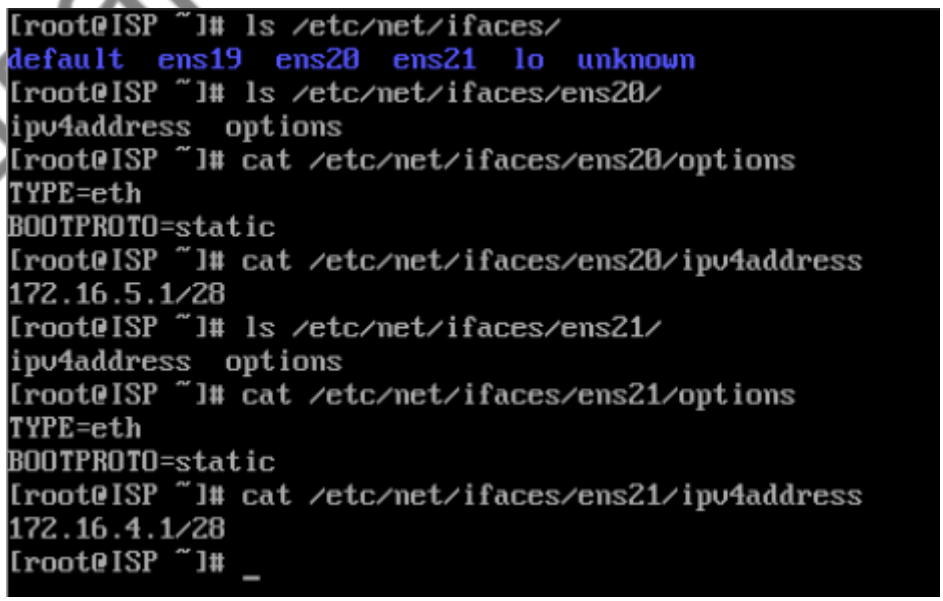
Правила настройки

`vim /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ipv4address`
`<IP-адрес>/<Префикс>`

Для применения настроек, необходимо перезагрузить службу `network`, командой:

```
systemctl restart network
```

Пример описания настроек на виртуальных машинах экзаменационного стенда



Как проверить?

Проверка IP-адреса осуществляется командой: `ip a`

```
3: ens20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 96:56:6d:15:9b:49 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
    inet 172.16.5.1/28 brd 172.16.5.15 scope global ens20
       valid_lft forever preferred_lft forever
    inet6 fe80::9456:6dff:fe15:9b49/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
4: ens21: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 6a:e0:74:76:3c:36 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
    inet 172.16.4.1/28 brd 172.16.4.15 scope global ens21
       valid_lft forever preferred_lft forever
    inet6 fe80::68e0:74ff:fe76:3c36/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Краткая справка:

- Подсказки пользователю /etc/net (https://www.altlinux.org/Etcnet);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet (https://www.altlinux.org/Etcnet_start).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

Задание 4. Настройте адресацию на интерфейсах.

Подробное описание пункта задания

На ISP настройте динамическую сетевую трансляцию в сторону HQ-RTR и BR-RTR для доступа к сети Интернет.

Где выполнять:

На машинах: ISP

Как делать?

Для того чтобы устройство ISP могло пересылать пакеты с интерфейса на интерфейс, необходимо включить пересылку пакетов (маршрутизацию/forwarding). Для этого следует в конфигурационном файле `/etc/net/sysctl.conf` в параметре `net.ipv4.ip_forward = 0` заменить значение с `0` на `1`. Для применения настроек, необходимо перезагрузить службу network, командой `systemctl restart network`.

```
# This file was formerly part of /etc/sysctl.conf
### IPV4 networking options.

# IPv4 packet forwarding.
#
# This variable is special, its change resets all configuration
# parameters to their default state (RFC 1122 for hosts, RFC 1812 for
# routers).
#
net.ipv4.ip_forward = 1
```

Для динамической сетевой трансляции можно использовать `iptables`. В случае использования в качестве ОС на ВМ ISP «Альт Jeos» – пакет `iptables` необходимо установить, выполнить установку можно с помощью команды `apt-get install iptables`, предварительно обновив список пакетов с помощью команды `apt-get update`.

```
[root@ISP ~]# apt-get update
Get:1 http://ftp.altlinux.org p11/branch/x86_64 release [4210B]
Get:2 http://ftp.altlinux.org p11/branch/x86_64-i586 release [1665B]
Get:3 http://ftp.altlinux.org p11/branch/noarch release [2831B]
Fetched 8706B in 0s (51.3kB/s)
Get:1 http://ftp.altlinux.org p11/branch/x86_64/classic pkglist [25.8MB]
Get:2 http://ftp.altlinux.org p11/branch/x86_64/classic release [137B]
Get:3 http://ftp.altlinux.org p11/branch/x86_64-i586/classic pkglist [17.6MB]
Get:4 http://ftp.altlinux.org p11/branch/x86_64-i586/classic release [142B]
Get:5 http://ftp.altlinux.org p11/branch/noarch/classic pkglist [7491kB]
Get:6 http://ftp.altlinux.org p11/branch/noarch/classic release [137B]
Fetched 50.8MB in 11s (4241kB/s)
Reading Package Lists... Done
Building Dependency Tree... Done
[root@ISP ~]# apt-get install iptables
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
  libnetfilter_conntrack  libnfnetlink  libpcap0.8
The following NEW packages will be installed:
  iptables  libnetfilter_conntrack  libnfnetlink  libpcap0.8
0 upgraded, 4 newly installed, 0 removed and 32 not upgraded.
Need to get 490kB of archives.
After unpacking 2446kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ftp.altlinux.org p11/branch/x86_64/classic libnfnetlink 1:1.0.1.0.8.5087-alt1:sisyphus+278100.3100.1.101626058838 [15.6kB]
Get:2 http://ftp.altlinux.org p11/branch/x86_64/classic libnetfilter_conntrack 1:1.0.9-alt1:sisyphus+295920.100.1.101645780453 [41.5kB]
Get:3 http://ftp.altlinux.org p11/branch/x86_64/classic libpcap0.8 2:1.10.5-alt1:p11+372203.33500.14.101739219647 [167kB]
Get:4 http://ftp.altlinux.org p11/branch/x86_64/classic iptables 1.8.10-alt1:sisyphus+343211.300.4.201713373128 [267kB]
Fetched 490kB in 0s (2054kB/s)
Committing changes...
Preparing...                    ################################################################################################################ [100%]
Updating / installing...
1: libnfnetlink-1:1.0.1.0.8.5087-alt1 ################################################################################################################ [ 25%]
2: libnetfilter_conntrack-1:1.0.9-alt1 ################################################################################################################ [ 50%]
3: libpcap0.8-2:1.10.5-alt1     ################################################################################################################ [ 75%]
4: iptables-1.8.10-alt1         ################################################################################################################ [100%]
Done.
[root@ISP ~]#
```

Реализация сетевой трансляции адресов с помощью `iptables` можно выполнить одной командой:

```
iptables -t nat -A POSTROUTING -o <ИМЯ_ВНЕШНЕГО_ИНТЕРФЕЙСА> -j MASQUERADE
```

где <ИМЯ_ВНЕШНЕГО_ИНТЕРФЕЙСА.> – внешний интерфейс, смотрящий сторону магистрального провайдера, `-t` – --table (от англ. таблица), идем по таблице (в данном случае это таблица `nat`), `-A` – --append (от англ. добавлять), добавление правила в конец списка, `-o` – -out-interface (от англ. наружу, вне, за пределами) – исходящий интерфейс, `-j` – -jump (от англ. прыжок), прописывается действие, которое будет выполняться этим правилом.

После сохраните все изменения:

```
iptables-save >> /etc/sysconfig/iptables
```

Далее необходимо запустить и добавить в автозагрузку службу `iptables`:

```
systemctl enable --now iptables
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
[root@ISP ~]# iptables -t nat -A POSTROUTING -o ens19 -j MASQUERADE
[root@ISP ~]# iptables-save >> /etc/sysconfig/iptables
[root@ISP ~]# systemctl enable --now iptables
Synchronizing state of iptables.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable iptables
Created symlink /etc/systemd/system/basic.target.wants/iptables.service → /usr/lib/systemd/system/iptables.service.
[root@ISP ~]# _
```

Как проверить?

Проверить включение функции пересылки пакетов:

```
sysctl net.ipv4.ip_forward
```

```
[root@ISP ~]# sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
[root@ISP ~]# _
```

Проверить наличие правила в таблице `nat` в цепочке `POSTROUTING`:

```
iptables -t nat -L -n -v
```

```
[root@ISP ~]# iptables -t nat -L -n -v
Chain PREROUTING (policy ACCEPT 32 packets, 2710 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain INPUT (policy ACCEPT 2 packets, 480 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 2 packets, 152 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain POSTROUTING (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    2   152 MASQUERADE  0    --  *      ens19   0.0.0.0/0            0.0.0.0/0
[root@ISP ~]# _
```

Краткая справка:

- Подсказки пользователю /etc/net (https://www.altlinux.org/Etcnet);
- На серверах, вместо Network Manager удобнее использовать сетевой менеджер Etcnet (https://www.altlinux.org/Etcnet_start);
- Конфигурирование файрвола при помощи iptables (https://www.altlinux.org/Iptables);
- Сетевой экран Iptables (https://www.altlinux.org/Firewall_start);
- Iptables – утилита командной строки для настройки встроенного в ядро Linux межсетевого экрана (https://wiki.archlinux.org/title/Iptables_(Русский)).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

Создание локальных учетных записей

Задание 1. Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV.

Подробное описание пункта задания:

Пароль пользователя sshuser с паролем P@ssw0rd.

Идентификатор пользователя 1010.

Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации.

Где выполнять:

На машинах: HQ-SRV и BR-SRV.

Как делать?

Во время создания учетных записей на ОС «Альт», создается пользователь `sshuser` с идентификатором `1010`, после чего задается пароль `P@ssw0rd`. Затем запускается файл редактирования `sudo`, где необходимо расскомментировать строку, позволяющую пользователям, входящим в группу `wheel` выполнять через `sudo` любую команду с любого компьютера, не запрашивая их пароль.

Создать пользователя с явным указанием UID можно с помощью команды:

```
useradd <ИМЯ_ПОЛЬЗОВАТЕЛЯ> -u <UID>
```

Задать пароль пользователю можно с помощью утилиты `passwd`:

```
passwd <ИМЯ_ПОЛЬЗОВАТЕЛЯ>
```

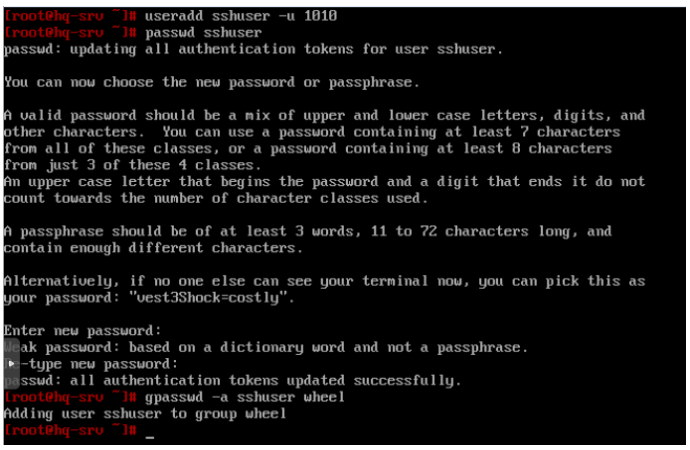
В результате запуска утилиты `passwd` необходимо будет задать пароль, а затем подтвердить заданный пароль.

Для редактирования `sudo` можно воспользоваться командой `visudo` или явно открыть файл `/etc/sudoers` в текстовом редакторе `vim` или `nano`, после чего следует найти и раскомментировать строку `WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL`.

Добавить пользователя в группу можно с помощью команды:

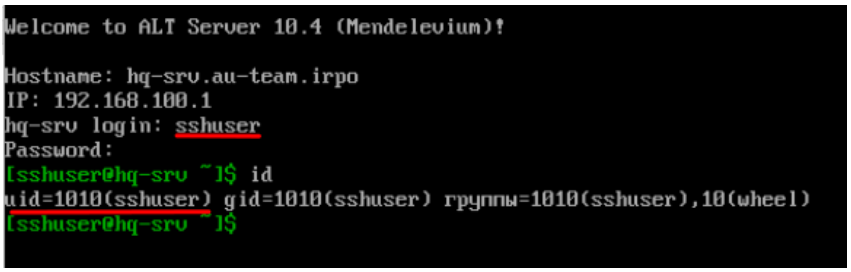
```
gpasswd -a <ИМЯ_ПОЛЬЗОВАТЕЛЯ> <ИМЯ_ГРУППЫ>
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

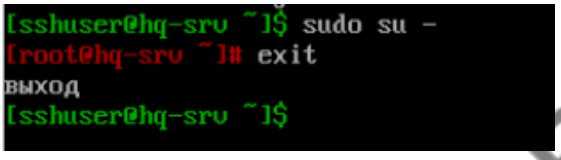


Как проверить?

Выполнить вход из-под пользователя `sshuser` с паролем `P@ssw0rd` и с помощью утилиты `id` посмотреть UID:



Попытаться перейти в режим суперпользователя используя `sudo` без ввода пароля:



Краткая справка:

- Особенности sudo в дистрибутивах ALT Linux (https://www.altlinux.org/Sudo);
- В дистрибутивах ALT Linux для управления доступом к важным службам используется подсистема control (https://www.altlinux.org/Control);
- Управление пользователями в ОС «Альт» (https://www.altlinux.org/Управление_пользователями).

Дополнительно:

Управление пользователями в Linux включает в себя несколько ключевых аспектов:

- Создание и удаление пользователей: для создания новых пользователей используется команда useradd, а для удаления – userdel. Эти команды позволяют задавать параметры, такие как домашний каталог и оболочка.
- Управление паролями: команда passwd используется для установки и изменения паролей пользователей. Это важный аспект безопасности системы.
- Группы пользователей: пользователи могут быть организованы в группы для упрощения управления правами доступа. Команды groupadd, groupdel и usermod позволяют создавать и изменять группы.
- Права доступа: в Linux используется модель прав доступа, основанная на владельцах, группах и других пользователях. Команды chmod, chown и chgrp позволяют управлять правами доступа к файлам и каталогам.
- Просмотр информации о пользователях: команды cat /etc/passwd и cat /etc/group позволяют просматривать информацию о пользователях и группах. Команда id показывает идентификаторы пользователя и группы.
- Управление сеансами: команды who, w и last позволяют отслеживать активные сеансы пользователей и историю входов.

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети

Задание 2. Создайте пользователя sshuser на маршрутизаторах HQ-RTR и BR-RTR.

Подробное описание пункта задания:

Пароль пользователя net_admin с паролем P@ssw0rd.

При настройке на EcoRouter пользователь net_admin должен обладать максимальными привилегиями.

Где выполнять:

На машинах: HQ-RTR и BR-RTR

Как делать?

Во время создания учетных записей на EcoRouterOS, создается пользователь `net_admin`, после чего задается пароль `P@ssw0rd`. Затем, созданному ранее пользователю присваиваются привилегии (роль) администратора.

Создать пользователя можно из режима администрирования (`conf t`) при помощи команды:

```
username <ИМЯ_ПОЛЬЗОВАТЕЛЯ>
```

Задать пароль для пользователя можно из режима конфигурирования пользователя (перейти в него можно использовав `username <ИМЯ_ПОЛЬЗОВАТЕЛЯ>`) с помощью команды:

```
password <ПАРОЛЬ>
```

Задать необходимую роль для пользователя можно из режима конфигурирования пользователя (перейти в него можно использовав `username <ИМЯ_ПОЛЬЗОВАТЕЛЯ>`) с помощью команды:

```
role <РОЛЬ>
```

Доступные роли:

`admin` – права администратора;

`helpdesk` – привилегия поддержки;

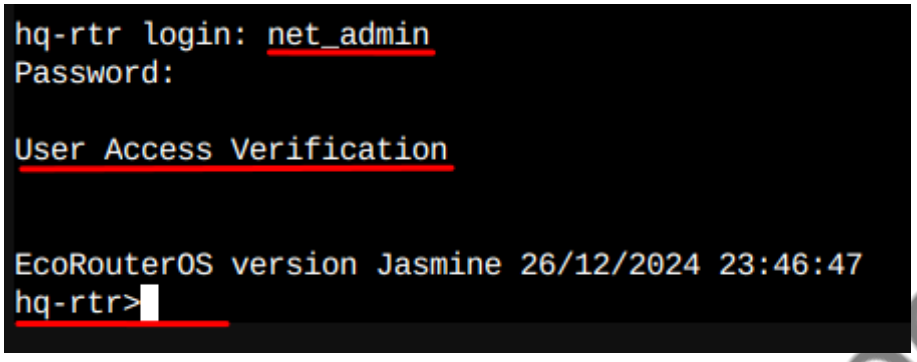
`noc` – привилегии оператора.

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#username net_admin
hq-rtr(config-user)#password P@ssw0rd
hq-rtr(config-user)#role admin
hq-rtr(config-user)#exit
hq-rtr(config)#write memory
Building configuration...
```

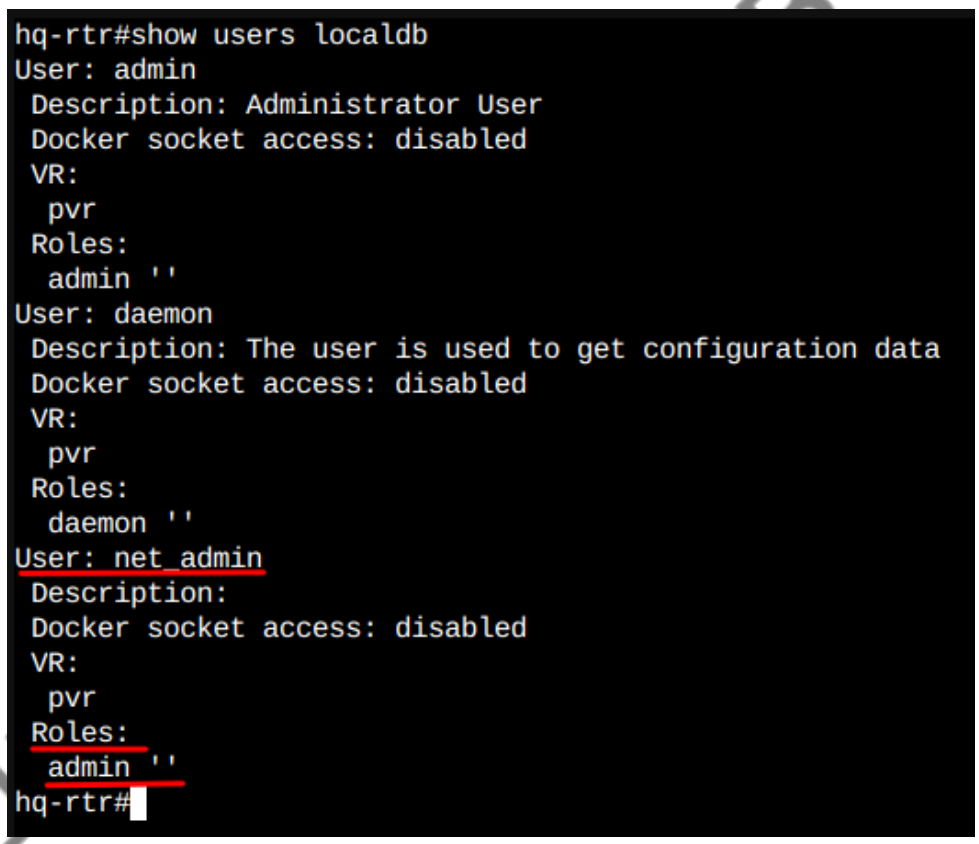
Как проверить?

Выполнить вход из-под пользователя `net_admin` с паролем `P@ssw0rd`



Проверить роль, заданную для пользователя `net_admin` можно использовав команду привилегированного режима:

```
show users localdb
```



Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

– Операционные системы и среды;
– Компьютерные сети

Коммутация – если HQ-SW виртуальная машина

Подробное описание пункта задания:

Настройте на интерфейсе HQ-RTR в сторону офиса HQ виртуальный коммутатор:

- Сервер HQ-SRV должен находиться в ID VLAN 100
- Клиент HQ-CLI в ID VLAN 200
- Создайте подсеть управления с ID VLAN 999
- Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт

Где выполнять:

На HQ-SW

Как делать?

Убедитесь, что служба `ovs-vswitchd` и `ovsdb-server` запущены, и интерфейсы ovs включены и переведены в режим `manual`. Сверку соответствия сетям рекомендуется проводить по mac адресам.

```
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host proto kernel_lo
       valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 02:00:b1:39:25:3d brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 fe80::b1ff:fe39:253d/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 02:00:df:31:8a:b9 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
    inet6 fe80::dfff:fe31:8ab9/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
4: ens5: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP grou
p default qlen 1000
    link/ether 02:00:e5:72:ad:52 brd ff:ff:ff:ff:ff:ff
    altname enp0s5
    inet6 fe80::e5ff:fe72:ad52/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@ovsSW ifaces]#
```

На конкретном стенде интерфейс ens3 подключен к HQ-RTR, ens4 к HQ-SRV, интерфейс ens5 к HQ-CLI. Таким образом, очевидно, что интерфейс ens3 будет выполнять роль trunk, ens4 тегировать vlan 100, ens5 тегировать vlan 200

Создаём мост:

```
ovs-vsctl add-br SW
```

Добавляем в мост транковый интерфейс:

```
ovs-vsctl add-port SW ens3 trunk=100,200,999
```

Добавляем в мост интерфейс доступа, трафик которого будет тегироваться:

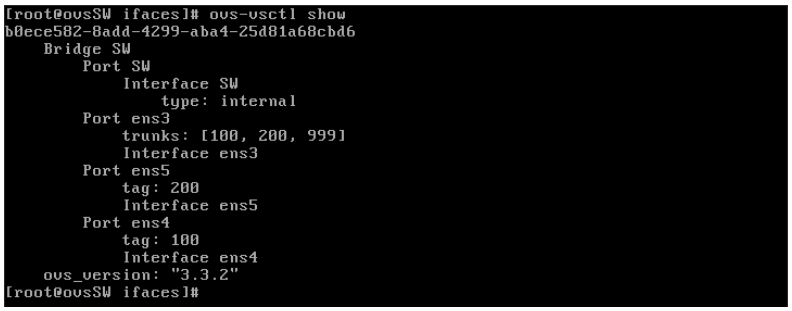
```
ovs-vsctl add-port SW ens4 tag=100
```

Добавляем в мост интерфейс доступа, трафик которого будет тегироваться:

```
ovs-vsctl add-port SW ens5 tag=200
```

Как проверить:

```
ovs-vsctl show
```



Дополнительно:

Преимущества Open vSwitch:

- Масштабируемость: Open vSwitch (OVS) поддерживает большое количество виртуальных машин и сетевых интерфейсов, что делает его идеальным для облачных и виртуализированных сред;
- Гибкость и расширяемость: OVS можно настраивать и расширять с помощью различных плагинов и модулей, что позволяет адаптировать его под специфические требования сети;
- Поддержка виртуальных сетей: OVS позволяет создавать сложные виртуальные сетевые топологии, включая VLAN, VXLAN и GRE, что упрощает управление сетевыми ресурсами;
- Мониторинг и диагностика: OVS предоставляет мощные инструменты для мониторинга трафика и диагностики сетевых проблем, что облегчает администрирование и оптимизацию сети;
- Интеграция с контейнерами: OVS хорошо работает с контейнерными технологиями, такими как Docker и Kubernetes, обеспечивая эффективное управление сетевыми ресурсами в контейнеризованных приложениях;
- Поддержка QoS: Open vSwitch позволяет настраивать политику качества обслуживания (QoS), что помогает управлять пропускной способностью и приоритизировать трафик;
- Безопасность: OVS поддерживает различные механизмы безопасности, включая фильтрацию трафика и контроль доступа, что повышает уровень защиты сети.

Эти преимущества делают Open vSwitch мощным инструментом для управления виртуальными сетями в современных IT-инфраструктурах.

Краткая справка:

- Официальная документация Open vSwitch (https://docs.openvswitch.org/en/latest/);
- Настройка openvswitch из etcnet (https://www.altlinux.org/Etcnet/openvswitch);
- О настройке Open vSwitch непростым языком (https://habr.com/ru/articles/325560/).

Где изучается?

На учебной и производственной практике.

2 курс:

- Компьютерные сети.

3 курс:

- Организация, принципы построения и функционирования компьютерных сетей.

Коммутация – если HQ-SW не является виртуальной машиной

Подробное описание пункта задания:

Настройте на интерфейсе HQ-RTR в сторону офиса HQ коммутатор:

- Сервер HQ-SRV должен находиться в ID VLAN 100
- Клиент HQ-CLI в ID VLAN 200
- Создайте подсеть управления с ID VLAN 999
- Основные сведения о настройке коммутатора и выбора реализации разделения на VLAN занесите в отчёт

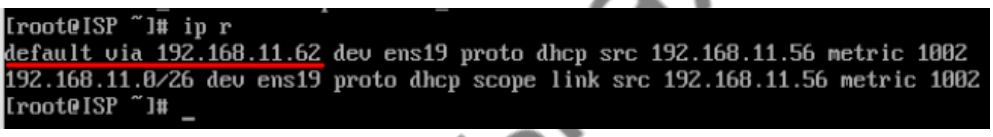
Где выполнять:

На машинах: HQ-RTR, гипервизор (порты доступа).

Как делать?

Для устройства с ОС «EcoRouterOS»:

Просмотр существующих портов выполняется командой привилегированного режима: `show port` или `show port brief`



Основные понятия касающиеся EcoRouter:

- `Порт (port)` – это устройство в составе EcoRouter, которое работает на уровне коммутации (L2);
- `Интерфейс (interface)` – это логический интерфейс для адресации, работает на сетевом уровне (L3);
- `Service instance` (Сабинтерфейс, SI, Сервисный интерфейс) является логическим сабинтерфейсом, работающим между L2 и L3 уровнями:
  - Данный вид интерфейса необходим для соединения физического порта с интерфейсами L3, интерфейсами bridge, портами;
  - Используется для гибкого управления трафиком на основании наличия меток VLANов в фреймах, или их отсутствия;
  - Сквозь сервисный интерфейс проходит весь трафик, приходящий на порт.

Для того чтобы назначить IPv4-адрес на EcoRouter, необходимо придерживаться следующего алгоритма в общем виде:

В режиме администрирование (`conf t`) создать интерфейс с произвольным именем и назначить на него IPv4:

```
interface <ИМЯ_ИНТЕРФЕЙСА>
ip address <IP-адрес>/<Префикс>
```

В режиме конфигурирования порта создать `service-instance` с произвольным именем, указать (инкапсулировать) что будет обрабатываться тегированный или не тегированный трафик, указать в какой интерфейс (ранее созданный) нужно отправить обработанные кадры:

Для тегированного трафика:

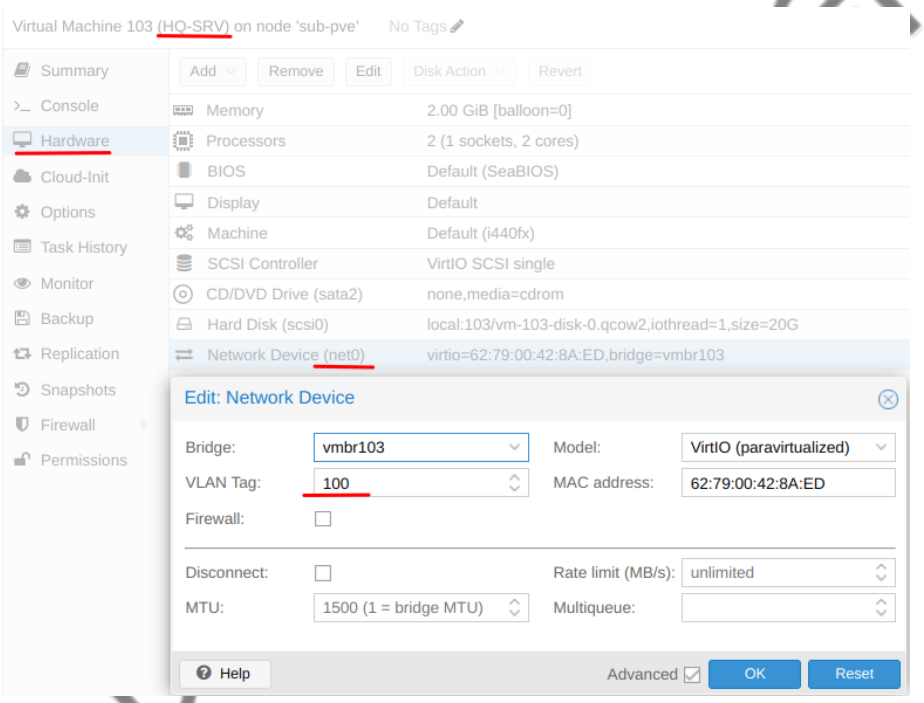
```
port <ИМЯ_ПОРТА>
```

`service-instance <ИМЯ>`
`encapsulation dot1q <VID – идентификатор VLAN>`
`rewrite pop 1 (операция снятия метки)`
`connect ip interface <ИМЯ_ИНТЕРФЕЙСА>`
`exit`

Для того чтобы задать IP-адрес шлюза (маршрута) по умолчанию необходимо из режима администрирования (`conf t`) выполнить следующую команду:

```
ip route 0.0.0.0/0 <IP-адрес шлюза>
```

Поскольку данный вариант не подразумевает использование в качестве HQ-SW выделенной виртуальной машины, необходима на оконечных устройствах настроить порты доступа на уровне гипервизора, например Альт Виртуализация PVE:



Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#interface vl100
hq-rtr(config-if)#ip address 192.168.100.62/26
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl200
hq-rtr(config-if)#ip address 192.168.100.78/28
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl999
hq-rtr(config-if)#ip address 192.168.100.86/29
hq-rtr(config-if)#exit
hq-rtr(config)#
```

```
hq-rtr(config)#port te1
hq-rtr(config-port)#service-instance te1/vl100
hq-rtr(config-service-instance)#encapsulation dot1q 100
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl100
```

```
2025-04-07 13:11:19      INFO      Interface vl100 changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#service-instance te1/vl200
hq-rtr(config-service-instance)#encapsulation dot1q 200
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl200

2025-04-07 13:11:35      INFO      Interface vl200 changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#service-instance te1/vl999
hq-rtr(config-service-instance)#encapsulation dot1q 999
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl999

2025-04-07 13:11:54      INFO      Interface vl999 changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

Как проверить?

Проверка осуществляется командой привилегированного режима:

```
show ip interface brief
```

```
hq-rtr#show ip interface brief
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 ISP              172.16.4.14/28      up                    default
 vl100            192.168.100.62/26   up                    default
 vl200            192.168.100.78/28   up                    default
 vl999            192.168.100.86/29   up                    default
hq-rtr#
```

Средствами утилиты `ping` проверить связность с HQ-SRV до HQ-RTR:

```
[root@hq-srv ~]# ip r
default via 192.168.100.62 dev ens19
192.168.100.0/26 dev ens19 proto kernel scope link src 192.168.100.1
[root@hq-srv ~]# ping -c3 192.168.100.62
PING 192.168.100.62 (192.168.100.62) 56(84) bytes of data.
64 bytes from 192.168.100.62: icmp_seq=1 ttl=64 time=7.73 ms
64 bytes from 192.168.100.62: icmp_seq=2 ttl=64 time=7.15 ms
64 bytes from 192.168.100.62: icmp_seq=3 ttl=64 time=7.40 ms

--- 192.168.100.62 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 7.146/7.423/7.729/0.238 ms
[root@hq-srv ~]# _
```

Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

– Компьютерные сети.

3 курс:

– Организация, принципы построение и функционирования компьютерных сетей;
– Программное обеспечение компьютерных сетей;
– Организация администрирования компьютерных систем и далее.

Настройка безопасного удаленного доступа

Подробное описание пункта задания:

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

- Для подключения используйте порт 2024;
- Разрешите подключения только пользователю sshuser;
- Ограничьте количество попыток входа до двух;
- Настройте баннер «Authorized access only».

Где выполнять:

На машинах: HQ-SRV и BR-SRV.

Как делать?

Редактируем конфигурационный файл `openssh`, расположенный по пути `/etc/openssh/sshd_config`, текстовым редактором `vim` или `nano`. Находим следующие параметры и приводим их к следующему виду:

`Port 2024` – Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию – 22;

`AllowUsers sshuser` – список имён пользователей через пробел. Если параметр определён, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов;

`MaxAuthTries 2` – ограничение на число попыток идентифицировать себя в течение одного соединения;

`PasswordAuthentication yes` – допускать аутентификацию по паролю;

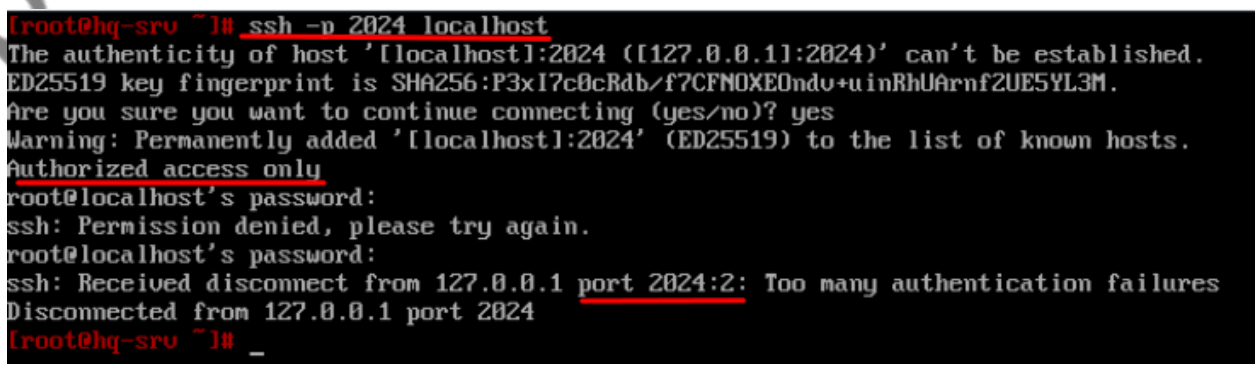
`Banner /etc/openssh/banner` – содержимое указанного файла будет отправлено удалённому пользователю прежде, чем будет разрешена аутентификация.

Редактируем баннер, а именно файл по пути `/etc/openssh/banner` текстовым редактором `vim` или `nano` и добавляем в него следующее содержимое: `Authorized access only`. Для применения всех изменений необходимо перезапустить службу `sshd`, для этого можно использовать команду:

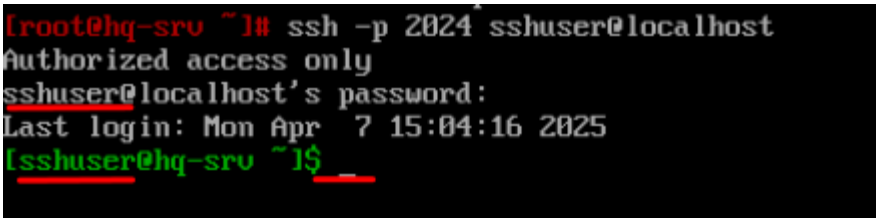
```
systemctl restart sshd
```

Как проверить?

Попытаться не из-под пользователя `sshuser`:



Попытаться подключить под пользователем `sshuser`:



Дополнительно:

ssh (secure shell) – это сетевой протокол, который обеспечивает безопасный доступ к удалённым системам. Вот несколько ключевых преимуществ SSH:

- Безопасность: SSH шифрует данные, передаваемые между клиентом и сервером, защищая их от перехвата;
- Аутентификация: поддержка как парольной аутентификации, так и аутентификации с помощью ключей, что повышает уровень безопасности;
- Удалённое управление: позволяет администраторам безопасно управлять серверами и другими устройствами из любого места;
- Создание туннелей: возможность перенаправления сетевого трафика (SSH-туннели) обеспечивает безопасность для других протоколов;
- Поддержка сценариев: SSH позволяет автоматизировать задачи через скрипты, что упрощает администрирование SSH является важным инструментом для безопасного управления системами и передачи данных в сетевой среде.

Краткая справка:

- Создание и настройка входа через ssh (https://www.altlinux.org/SSH);
- Доступ по SSH (https://www.altlinux.org/Доступ_по_SSH);
- man sshd (https://www.opennet.ru/man.shtml?topic=sshd_config&category=5&russian=0).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети и далее.

Настройка IP-туннеля между офисами

Подробное описание пункта задания:

Между офисами HQ и BR необходимо сконфигурировать ip туннель.

Где выполнять:

На машинах: HQ-RTR и BR-RTR.

Как делать?

Для создания интерфейса GRE-туннеля на ОС «EcoRouterOS» создаётся интерфейс tunnel.<№>, для этого из режима администрирования (`conf t`) используется команда:

```
interface tunnel.<№>
```

После чего интерфейсу назначается IP-адрес, для этого используется команда (в режиме конфигурирования туннельного интерфейса):

```
ip address <IP-адрес>.<Префикс>
```

Затем выставляется параметр ip tunnel, в котором необходимо указать адрес источника и назначения, а также режим работы туннеля:

```
ip tunnel <IP-адрес_ИСТОЧНИКА> <IP-адрес_НАЗНАЧЕНИЯ> mode <ТУННЕЛЬНЫЙ_РЕЖИМ>
```

Туннельный режим может быть выбран как `gre` так и `ipip`.

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#ip address 10.10.10.1/30
hq-rtr(config-if-tunnel)#ip tunnel 172.16.4.14 172.16.5.14 mode gre

2025-04-07 13:54:55      INFO      Interface tunnel.0 changed state to up
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

Как проверить?

Выполнить команду (из привилегированного режима): `show interface tunnel.<№>`

```
hq-rtr#show interface tunnel.0
 Interface tunnel.0 is up
  Snmp index: 9
  Ethernet address: (port not configured)
  MTU: 1476
  Tunnel source: 172.16.4.14
  Tunnel destination: 172.16.5.14
  Tunnel mode: GRE
  Tunnel keepalive: disabled
  NAT: no
  ARP Proxy: disable
  ICMP redirects on, unreachables on
  IP URPF is disabled
  Label switching is disabled
  <UP,BROADCAST,RUNNING,NOARP,MULTICAST>
  inet 10.10.10.1/30 broadcast 10.10.10.3/30
  total input packets 0, bytes 0
  total output packets 0, bytes 0
hq-rtr#
```

Средствами утилиты `ping` проверить связность с противоположенной стороной туннеля:

```
hq-rtr#show ip interface brief
 Interface        IP-Address          Status                  VRF
 ------------------------------------------------------------------
 ISP              172.16.4.14/28      up                      default
 vl100            192.168.100.62/26   up                      default
 vl200            192.168.100.78/28   up                      default
 vl999            192.168.100.86/29   up                      default
 tunnel.0         10.10.10.1/30       up                      default
hq-rtr#ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=77.3 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=76.0 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=75.6 ms

--- 10.10.10.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 75.582/76.306/77.327/0.742 ms
hq-rtr#
```

Дополнительно:

Применение GRE:

- Связывание удалённых сетей: GRE часто используется для создания соединений между офисами, находящимися в разных местах;
- Виртуальные частные сети (VPN): можно использовать в сочетании с IPsec для создания защищённых VPN-соединений;
- Тестирование и лабораторные сценарии: GRE может быть использован для имитации различных сетевых топологий и конфигураций. Таким образом, GRE-туннели являются эффективным способом инкапсуляции и передачи данных в различных сетевых сценариях.

Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

– Компьютерные сети и далее.

Настройка динамической маршрутизации

Подробное описание пункта задания:

Ресурсы одного офиса должны быть доступны из другого офиса.

Для обеспечения динамической маршрутизации используйте link state протокол на ваше усмотрение.

Разрешите выбранный протокол только на интерфейсах в ip туннеле:

- Маршрутизаторы должны делиться маршрутами только друг с другом;
- Обеспечьте защиту выбранного протокола посредством парольной защиты;
- Сведения о настройке и защите протокола занесите в отчёт.

Где выполнять:

На машинах: HQ-RTR и BR-RTR.

Как делать?

Создать процесс OSPF можно используя следующу команду из режима администрирования (`conf t`):

```
router ospf <№>
```

Объявить сети для динамической марщрутизации в созданном процессе OSPF можно следующей командой из режима конфигурирования процесса OSPF:

```
network <IP-АДРЕС_СЕТИ>/<ПРЕФИКС> area <№>
```

Исключить все интерфейсы из процесса OSPF, можно следующей командой из режима конфигурирования процесса OSPF:

```
passive-interface default
```

Добавить исключение, чтобы интерфейс использовался в процессе OSPF, можно следующей командой из режима конфигурирования процесса OSPF:

```
no passive-interface <ИМЯ_ИНТЕРФЕЙСА>
```

Включить аутентификацию для всех интерфейсов определенной области, можно следующей командой из режима конфигурирования процесса OSPF:

```
area <№> authentication
```

Для обеспечения парольной защиты OSPF, можно указать ключ аутентификации на конкретном интерфейсе, для этого необходимо выполнить команды из режима администрирования (`conf t`):

```
interface <ИМЯ_ИНТЕРФЕЙСА>
ip ospf authentification-key <ПАРОЛЬ>
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr>enable
hq-rtr#configure termina
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#router ospf 1
hq-rtr(config-router)#passive-interface default
hq-rtr(config-router)#no passive-interface tunnel.0
hq-rtr(config-router)#network 10.10.10.0/30 area 0
hq-rtr(config-router)#network 192.168.100.0/26 area 0
hq-rtr(config-router)#network 192.168.100.64/28 area 0
hq-rtr(config-router)#network 192.168.100.80/29 area 0
hq-rtr(config-router)#area 0 authentication
hq-rtr(config-router)#exit
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#ip ospf authentication-key P@ssw0rd
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

Как проверить?

Проверить установление соседских отношений можно из привилегированного режима с помощью команды:

```
show ip ospf neighbor
```

```
hq-rtr#show ip ospf neighbor

Total number of full neighbors: 1
OSPF process 1 VRF(default):
Neighbor ID     Pri   State           Dead Time   Address         Interface           Instanc
192.168.200.30    1   Full/Backup     00:00:30    10.10.10.2      tunnel.0              0
hq-rtr#
```

Проверить таблицу маршрутизации (маршруты по ospf) можно из привилегированного режима с помощью команды:

```
show ip route ospf
```

```
hq-rtr#show ip route ospf
IP Route Table for VRF "default"
O       192.168.200.0/27 [110/2] via 10.10.10.2, tunnel.0, 00:02:35

Gateway of last resort is not set
hq-rtr#
```

```
br-rtr#show ip route ospf
IP Route Table for VRF "default"
O       192.168.100.0/26 [110/2] via 10.10.10.1, tunnel.0, 00:03:18
O       192.168.100.64/28 [110/2] via 10.10.10.1, tunnel.0, 00:03:18
O       192.168.100.80/29 [110/2] via 10.10.10.1, tunnel.0, 00:03:18

Gateway of last resort is not set
br-rtr#
```

Средствами утилиты `ping` проверить связность между BR-SRV и HQ-SRV:

```
[root@br-srv ~]# ip -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens19            UP             192.168.200.1/27 fe80::34f5:adff:fe82:1b21/64
[root@br-srv ~]# ping -c3 192.168.100.1
PING 192.168.100.1 (192.168.100.1) 56(84) bytes of data.
64 bytes from 192.168.100.1: icmp_seq=1 ttl=62 time=89.6 ms
64 bytes from 192.168.100.1: icmp_seq=2 ttl=62 time=80.0 ms
64 bytes from 192.168.100.1: icmp_seq=3 ttl=62 time=78.2 ms

--- 192.168.100.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 78.227/82.601/89.561/4.975 ms
[root@br-srv ~]#
```

Дополнительно:

OSPF (Open Shortest Path First) – это протокол динамической маршрутизации, который используется для передачи данных в IP-сетях.

OSPF является одним из наиболее распространённых протоколов маршрутизации в корпоративных сетях благодаря своей эффективности, надежности и адаптивности к изменяющимся условиям.

Вот несколько ключевых преимуществ OSPF:

- Быстрое converging: OSPF быстро адаптируется к изменениям в сети, что позволяет ему быстро находить новые маршруты и обеспечивать высокую доступность;
- Поддержка больших сетей: OSPF эффективно работает в крупных сетях, поддерживая иерархическую структуру с использованием областей (areas), что позволяет оптимизировать процесс маршрутизации и уменьшить нагрузку на маршрутизаторы;
- Адаптивность к изменениям: OSPF использует алгоритмы SPF (Shortest Path First), которые позволяют ему находить кратчайший путь к каждой цели, учитывая текущие условия в сети;
- Поддержка многоадресной рассылки: OSPF может эффективно использовать многоадресную рассылку для обновления маршрутов, что уменьшает количество дублирующего трафика;
- Поддержка аутентификации: OSPF обеспечивает возможность настройки аутентификации, что повышает уровень безопасности при обмене маршрутной информацией между маршрутизаторами;
- Интеграция с IPv6: OSPFv3 поддерживает маршрутизацию для IPv6, что делает его актуальным в современных сетевых инфраструктурах;
- Управляемый трафик: OSPF имеет механизмы, позволяющие управлять маршрутным трафиком и обеспечивать балансировку нагрузки;
- Гибкость: позволяет настраивать различные параметры, такие как приоритеты интерфейсов и стоимости маршрутов, что делает его очень гибким инструментом для администраторов сетей.

Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

– Компьютерные сети

Далее на других курсах.

Настройка динамической трансляции адресов

Подробное описание пункта задания:

Настройте динамическую трансляцию адресов для обоих офисов.

Все устройства в офисах должны иметь доступ к сети Интернет.

Где выполнять:

На машинах: HQ-RTR и BR-RTR.

Как делать?

Определить «внутренний интерфейс NAT» (`inside`) и «внешний интерфейс NAT» (`outside`), можно в режиме конфигурирования интерфейса:

```
interface <ИМЯ_ИНТЕРФЕЙСА>
ip nat <inside | outside>
```

Определить пул адресов для дальнейшего использования данного пула в правилах трансляции, можно из режима администрирования (`conf t`) при помощи команды:

```
ip nat pool <ИМЯ_ПУЛА> <IP-АДРЕС_НАЧАЛА_ДИАПАЗОНА>-<IP-АДРЕС_ОКОНЧАНИЯ_ДИАПАЗОНА>
```

Создать правило динамической трансляции адресов, можно из режима администрирования (`conf t`) при помощи команды:

```
ip nat source dynamic inside-to-outside pool <ИМЯ_ПУЛА> overload interface <ИМЯ_ВНЕШНЕГО_ИНТЕРФЕЙСА>
```

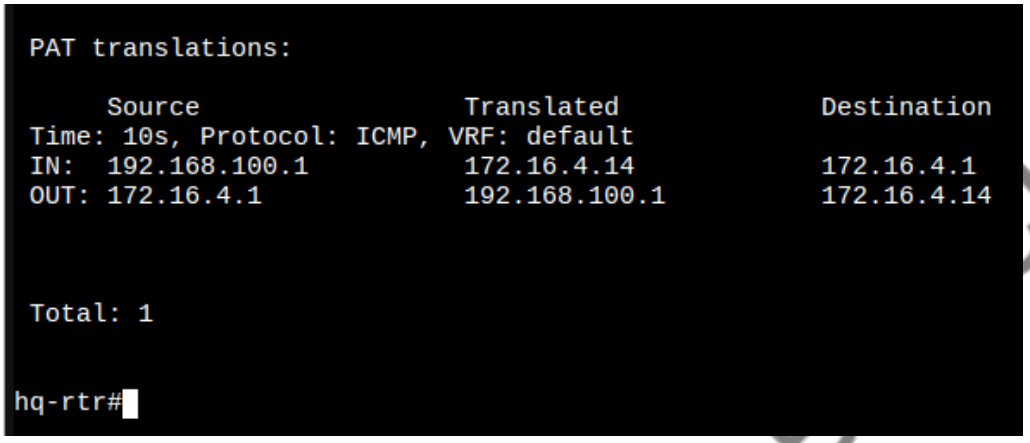
Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#interface ISP
hq-rtr(config-if)#ip nat outside
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl100
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl200
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl999
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#exit
hq-rtr(config)#ip nat pool HQ 192.168.100.1-192.168.100.254
hq-rtr(config)#ip nat source dynamic inside-to-outside pool HQ overload interface ISP
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

Как проверить?

Средствами утилиты `ping` с HQ-SRV попытать проверить связность с ISP, после чего на HQ-RTR из привилегированного режима просмотреть таблицу NAT, при помощи команды:

```
show ip nat translations
```



Дополнительно:

NAT (Network Address Translation) – это технология, используемая для преобразования частных IP-адресов в публичные и обратно. Вот несколько ключевых преимуществ NAT:

- Экономия IP-адресов: NAT позволяет многим устройствам в частной сети использовать один публичный IP-адрес, что экономит ресурсы адресного пространства.
- Улучшение безопасности: NAT скрывает внутреннюю структуру сети, что делает её менее уязвимой к внешним атакам. Внешние устройства не могут напрямую обращаться к внутренним адресам;
- Гибкость и управляемость: легко управлять внутренними IP-адресами, изменяя их без необходимости в переадресации или изменении публичного адреса;
- Поддержка различных протоколов: NAT может работать с различными протоколами и типами трафика, обеспечивая совместимость.

Таким образом, NAT является полезным инструментом для управления адресами, улучшения безопасности и оптимизации использования IP-ресурсов в сети.

Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

– Операционные системы и среды;
– Компьютерные сети.

Далее на других курсах.

Настройка протокола динамической конфигурации хостов

Подробное описание пункта задания:

- 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.

Где выполнять:

На машине: HQ-RTR.

Как делать?

Создать пул с произвольным именем и указать диапазон раздаваемых IP-адресов можно из режима администрирования (`conf t`) при помощи следующей команды:

```
ip pool <ИМЯ_ПУЛА> <IP-АДРЕС_НАЧАЛА_ДИАПАЗОНА>-<IP-АДРЕС_ОКОНЧАНИЯ_ДИАПАЗОНА>
```

Для настройки DHCP-сервера необходимо из режима администрирования (`conf t`) перейти в режим конфигурирования dhcp-сервера, присвоив ему произвольный номер в системе маршрутизатора, для этого используется команда:

```
dhcp-server <№>
```

Далее в режиме конфигурирования dhcp-сервера, необходимо привязать созданный ранее пул раздаваемых адресов с указанием номера dhcp-сервера в системе маршрутизатора, сделать это можно при помощи команды:

```
pool <ИМЯ_ПУЛА> <№>
```

В результате чего можно из режима настройки конкретного пула dhcp задавать все необходимые параметры, например:

```
mask <СЕТЕВАЯ_МАСКА>
gateway <IP-АДРЕС_ШЛЮЗА>
dns <IP-АДРЕС_DNS-СЕРВЕРА>
domain-name <DNS-СУФФИКС>
```

После настройки сервера необходимо указать, на каком интерфейсе маршрутизатор будет принимать пакеты DHCP Discover и отвечать на них предложением с IP-настройками, сделать это можно из режима конфигурирования определённого интерфейса при помощи следующей команды:

```
interface <ИМЯ_ИНТЕРФЕЙСА>
dhcp-server <№>
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#ip pool HQ-Clients 192.168.100.65-192.168.100.77
hq-rtr(config)#dhcp-server 1
hq-rtr(config-dhcp-server)#pool HQ-Clients 1
hq-rtr(config-dhcp-server-pool)#mask 255.255.255.240
hq-rtr(config-dhcp-server-pool)#gateway 192.168.100.78
hq-rtr(config-dhcp-server-pool)#dns 192.168.100.1
hq-rtr(config-dhcp-server-pool)#domain-name au-team.irpo
hq-rtr(config-dhcp-server-pool)#exit
hq-rtr(config-dhcp-server)#exit
hq-rtr(config)#interface vl200
hq-rtr(config-if)#dhcp-server 1
hq-rtr(config-if)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

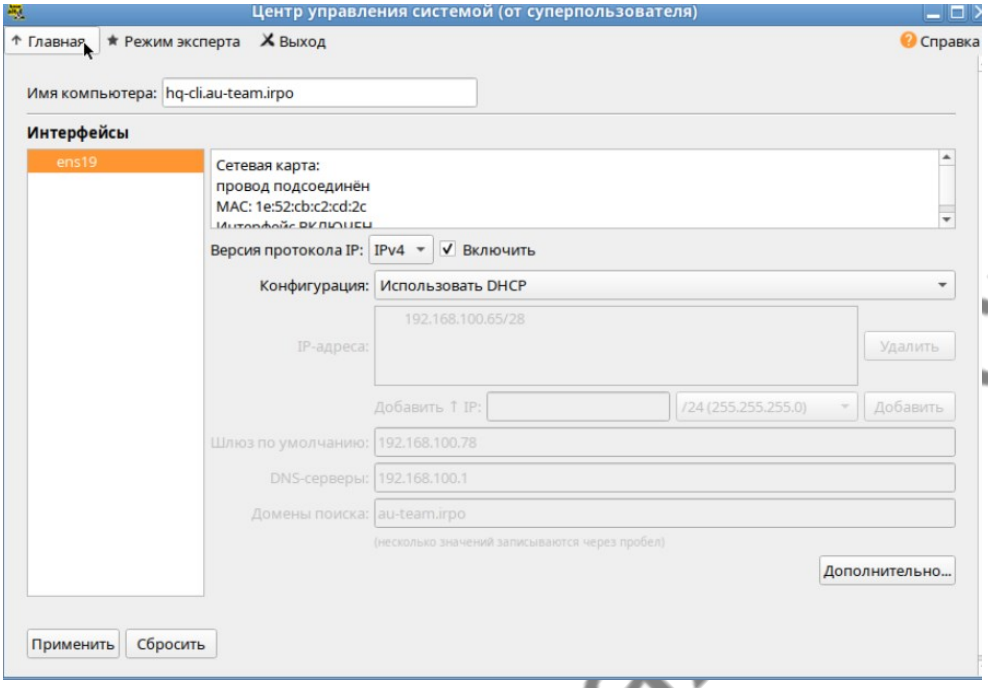
Как проверить?

Из привилегированного режима можно проверить информацию о созданном DHCP-пуле, используя команду:

```
show dhcp-server <№> detailed
```

```
hq-rtr#show dhcp-server 1 detailed
DHCP-server 1:

* Global options:
   Lease-time: 86400 sec
   Netmask: 255.255.255.0


* Static entries:

* Framed-ip pool entries:

* Pool entries:
** pool HQ-Clients 1
    Gateway:                    192.168.100.78
    DNS-servers:                192.168.100.1
    Domain-name:                au-team.irpo
    Netmask: 255.255.255.240
hq-rtr#
```

На виртуальной машине HQ-CLI должен быть получен IP-адрес и все необходимые сетевые параметры автоматически:



Также на DHCP-сервере можно просмотреть информацию о клиентах (выданных адресах) на определённом интерфейсе, для этого используется команда из привилегированного режима:

```
show dhcp-server clients <ИМЯ_ИНТЕРФЕЙСА>
```

```
hq-rtr#show dhcp-server clients vl200
 Total DHCP clients count: 1
 Client          Client          Server     Server
 IP Address      MAC Address     ACK Time   Lease Time
 ------------------------------------------------------
 192.168.100.65  1e52.cbc2.cd2c  25          86400
hq-rtr#
```

Дополнительно:

DHCP (Dynamic Host Configuration Protocol) – это протокол, который автоматизирует процесс назначения IP-адресов и других параметров конфигурации сетевых устройств. Вот несколько основных преимуществ DHCP:

- Автоматизация: упрощает управление сетью, автоматически назначая IP-адреса и настройки (например, шлюз, DNS) устройства при подключении к сети;
- Снижение ошибок: минимизирует вероятность ошибок, связанных с ручной конфигурацией адресов, таких как дублирование IP-адресов;
- Централизованное управление: позволяет администраторам управлять настройками сети из одного места, упрощая внесение изменений;
- Гибкость: поддерживает динамическое (временное) и статическое (постоянное) назначение IP-адресов, а также резервирование адресов для определённых устройств;
- Оптимизация использования ресурсов: эффективно распределяет адресное пространство, освобождая IP-адреса, которые не используются DHCP значительно упрощает администрирование сетей и улучшает их управляемость.

Краткая справка:

- User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети

Далее на других курсах.

Настройка DNS

Подробное описание пункта задания:

- 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.

Устройство	Запись	Тип
HQ-RTR	hq-rtr.au-team.irpo	A, PTR
BR-RTR	br-rtr.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A, PTR
HQ-CLI	hq-cli.au-team.irpo	A, PTR
BR-SRV	br-srv.au-team.irpo	A
HQ-RTR	moodle.au-team.irpo	CNAME
HQ-RTR	wiki.au-team.irpo	CNAME

Где выполнять:

На машине: HQ-SRV.

Как делать?

Для установки и дальнейшей настройки DNS-сервера, необходимо выполнить установку пакета BIND, сделать это можно при помощи команды:

```
apt-get update && apt-get install bind -y
```

Далее выполняется редактирование конфигурационного файла `/var/lib/bind/etc/options.conf` согласно скриншоту, используя текстовый редактор `vim` или `nano`:

```
options {
        version "unknown";
        directory "/etc/bind/zone";
        dump-file "/var/run/named/named_dump.db";
        statistics-file "/var/run/named/named.stats";
        recursing-file "/var/run/named/named.recursing";
        secroots-file "/var/run/named/named.secroots";

        // disables the use of a PID file
        pid-file none;

        /*
         * Oftenly used directives are listed below.
         */

        listen-on { 192.168.100.1; };
        listen-on-v6 { none; };

        /*
         * If the forward directive is set to "only", the server will only
         * query the forwarders.
         */
        //forward only;
        forwarders { 77.88.8.8; };
```

```
        /*
         * Specifies which hosts are allowed to ask ordinary questions.
         */
        allow-query { any; };

        /*
         * This lets "allow-query" be used to specify the default zone access
         * level rather than having to have every zone override the global
         * value. "allow-query-cache" can be set at both the options and view
         * levels.  If "allow-query-cache" is not set then "allow-recursion" is
         * used if set, otherwise "allow-query" is used if set unless
         * "recursion no;" is set in which case "none;" is used, otherwise the
         * default (localhost; localnets;) is used.
         */
        //allow-query-cache { localnets; };

        /*
         * Specifies which hosts are allowed to make recursive queries
         * through this server.  If not specified, the default is to allow
         * recursive queries from all hosts.  Note that disallowing recursive
         * queries for a host does not prevent the host from retrieving data
         * that is already in the server's cache.
         */
        allow-recursion { any; };
```

`listen-on` параметр определяет адреса и порты, на которых DNS-сервер будет слушать запросы.

В параметре `forwarders` указываются сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне.

`allow-query` – IP-адреса и подсети от которых будут обрабатываться запросы.

Далее необходимо добавить зоны прямого и обратного просмотра в файл `/var/lib/bind/etc/rfc1912.conf`, используя текстовый редактор `vim` или `nano`:

```
zone "au-team.irpo" {
        type master;
        file "au-team.irpo";
};

zone "100.168.192.in-addr.arpa" {
        type master;
        file "100.168.192.in-addr.arpa";
};
```

Необходимо перейти в директорию `/var/lib/bind/etc/zone` и путем копирования создать файлы зон:

```
[root@hq-srv ~]# cd /var/lib/bind/etc/zone/
[root@hq-srv zone]# cp empty au-team.irpo
[root@hq-srv zone]# cp empty 100.168.192.in-addr.arpa
[root@hq-srv zone]#
```

Необходимо сконфигурировать файл `au-team.irpo`, который является прямой зоной следующим образом:

```
[root@hq-srv zone]# cat au-team.irpo
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it and use that copy.
;
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025020600      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
        IN      A       192.168.100.1
hq-rtr  IN      A       192.168.100.62
hq-rtr  IN      A       192.168.100.78
hq-rtr  IN      A       192.168.100.86
br-rtr  IN      A       192.168.200.30
hq-srv  IN      A       192.168.100.1
hq-cli  IN      A       192.168.100.65
moodle  IN      CNAME   hq-rtr.au-team.irpo.
wiki    IN      CNAME   hq-rtr.au-team.irpo.
[root@hq-srv zone]#
```

Далее необходимо настроить обратную зону и привести файл `100.168.192.in-addr.arpa` к следующему виду:

```
[root@hq-srv zone]# cat 100.168.192.in-addr.arpa
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it and use that copy.
;
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025020600      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
62      IN      PTR     hq-rtr.au-team.irpo.
78      IN      PTR     hq-rtr.au-team.irpo.
86      IN      PTR     hq-rtr.au-team.irpo.
1       IN      PTR     hq-srv.au-team.irpo.
65      IN      PTR     hq-cli.au-team.irpo.
[root@hq-srv zone]#
```

Для DNS-сервиса важно обеспечить непрерывный аптайм, не допуская даже минутных простоев. Если вы попытаетесь перезапустить systemd-юнит обычной командой systemctl, а в конфигурации будут ошибки, то BIND не запустится. Чтобы избежать столь неприятных последствий, всего-то надо правильно настроить утилиту rndc, которая позволяет обойти эти сложности. После того, как конфигурация зон была завершена, для корректной работы службы bind необходимо выполнить команду:

```
rndc-confgen > /etc/bind/rndc.key
```

Затем выполнить команду:

```
sed -i '6,$d' rndc.key
```

```
[root@hq-srv zone]# rndc-confgen > /var/lib/bind/etc/rndc.key
[root@hq-srv zone]# sed -i '6,$d' /var/lib/bind/etc/rndc.key
[root@hq-srv zone]# cat /var/lib/bind/etc/rndc.key
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-sha256;
        secret "rgTaO7nHHh1XZj4/Shpz4CwY1E54BLIbM+tGS/wv18U=";
};
[root@hq-srv zone]#
```

Перед запуском службы остается поменять группу у файлов зон, которые были созданы ранее, на named, а также проверить конфигурационные файлы и файлы зон командами `named-checkconf` и `named-checkconf -z` соответственно:

```
[root@hq-srv etc]# chgrp -R named /var/lib/bind/etc/zone/
[root@hq-srv etc]# named-checkconf
[root@hq-srv etc]# named-checkconf -z
zone localhost/IN: loaded serial 2025020600
zone localdomain/IN: loaded serial 2025020600
zone 127.in-addr.arpa/IN: loaded serial 2025020600
zone 0.in-addr.arpa/IN: loaded serial 2025020600
zone 255.in-addr.arpa/IN: loaded serial 2025020600
zone au-team.irpo/IN: loaded serial 2025020600
zone 100.168.192.in-addr.arpa/IN: loaded serial 2025020600
[root@hq-srv etc]# _
```

После этого можно запустить службу bind командой `systemctl enable --now bind.service`. Проверить статус службы можно при помощи команды `systemctl status bind`:

```
[root@hq-srv etc]# systemctl enable --now bind
Synchronizing state of bind.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable bind
Created symlink /etc/systemd/system/multi-user.target.wants/bind.service → /lib/systemd/system/bind.service.
[root@hq-srv etc]# systemctl status bind.service
● bind.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/lib/systemd/system/bind.service; enabled; vendor preset: disabled)
     Active: active (running) since Tue 2025-04-08 09:34:10 MSK; 4s ago
    Process: 19285 ExecStartPre=/etc/init.d/bind rndc_keygen (code=exited, status=0/SUCCESS)
    Process: 19289 ExecStartPre=/usr/sbin/named-checkconf $CHROOT -z /etc/named.conf (code=exited, status=0/SUCCESS)
    Process: 19290 ExecStart=/usr/sbin/named -u named $CHROOT $RETAIN_CAPS $EXTRAOPTIONS (code=exited, status=0/SUCCESS)
      Tasks: 8 (limit: 2339)
     Memory: 18.5M
        CPU: 64ms
     CGroup: /system.slice/bind.service
             └─ 19291 /usr/sbin/named -u named

Apr 08 09:34:10 hq-srv.au-team.irpo named[19291]: REFUSED unexpected RCODE resolving './NS/IN': 192.58.128.30#53
Apr 08 09:34:10 hq-srv.au-team.irpo named[19291]: REFUSED unexpected RCODE resolving './NS/IN': 199.7.91.13#53
```

Как проверить?

Проверить доступ в сеть Интернет средствами утилиты `ping`, учитывая, что в качестве DNS-сервера используется HQ-SRV:

```
[root@hq-srv etc]# cat /etc/resolv.conf
# Generated by resolvconf
# Do not edit manually, use
# /etc/net/ifaces/<interface>/resolv.conf instead.
search au-team.irpo
nameserver 192.168.100.1
[root@hq-srv etc]# ping -c3 ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=241 time=90.2 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=241 time=75.1 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=241 time=73.7 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2891ms
rtt min/avg/max/mdev = 73.708/79.671/90.234/7.489 ms
[root@hq-srv etc]#
```

Используя утилиту `host` или `nslookup` проверить записи типа A, PTR и CNAME:

```
[root@hq-srv etc]# host hq-rtr.au-team.irpo
hq-rtr.au-team.irpo has address 192.168.100.62
hq-rtr.au-team.irpo has address 192.168.100.78
hq-rtr.au-team.irpo has address 192.168.100.86
[root@hq-srv etc]# host 192.168.100.78
78.100.168.192.in-addr.arpa domain name pointer hq-rtr.au-team.irpo.
[root@hq-srv etc]# nslookup wiki.au-team.irpo
Server:         192.168.100.1
Address:        192.168.100.1#53

wiki.au-team.irpo       canonical name = hq-rtr.au-team.irpo.
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.62
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.78
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.86

[root@hq-srv etc]# _
```

Дополнительно:

DNS (Domain Name System) – это система, которая переводит доменные имена, понятные человеку, в IP-адреса, которые понимают компьютеры. Вот несколько ключевых моментов, которые делают DNS замечательным:

- Удобство использования: позволяет пользователям обращаться к сайтам по запоминающимся именам (например, www.example.com), вместо сложных числовых IP-адресов;
- Иерархическая структура: DNS имеет иерархическую архитектуру, что позволяет распределять управление доменными именами и облегчает масштабирование;
- Кэширование: DNS-серверы кэшируют результаты запросов, что ускоряет доступ к часто запрашиваемым доменным именам и снижает нагрузку на сеть;

- Распределенность: DNS работает на основе распределенной базы данных, что делает его устойчивым к сбоям и атакам;
- Поддержка различных записей: DNS поддерживает различные типы записей (A, AAAA, CNAME, MX и др.), что позволяет управлять не только адресами, но и другими аспектами сетевой инфраструктуры.

BIND (Berkeley Internet Name Domain) – это одна из самых популярных реализаций DNS-сервера. Вот несколько его особенностей:

- Широкое распространение: BIND является стандартом де-факто для DNS-серверов в Unix-подобных системах и используется многими интернет-провайдерами и организациями;
- Гибкость и настраиваемость: BIND предлагает множество опций для настройки, включая поддержку различных типов записей и возможность настройки зон;
- Поддержка безопасности: BIND поддерживает расширенные функции безопасности, такие как DNSSEC (DNS Security Extensions), что позволяет защитить данные DNS от подделки.

Таким образом, DNS и его реализация BIND играют ключевую роль в функционировании интернета, обеспечивая удобный и надежный способ разрешения доменных имен.

Краткая справка:

- Служба DNS (Bind) (https://docs.altlinux.org/ru-RU/archive/2.4/html-single/master/alt-docs-master/ch06s13.html);
- Безграничный DNS (https://www.altlinux.org/Безграничный_DNS).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети и далее.

3 курс:

- Организация, принципы построения и функционирования компьютерных сетей.

Настройка часовых поясов

Подробное описание пункта задания:

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

Где выполнять:

На всех машинах.

Как делать?

На устройствах с ОС «Альт» необходимо выполнить следующую команду:

```
timedatectl set-timezone <ЧАСОВАЯ_ЗОНА>
```

Например:

```
timedatectl set-timezone Europe/Moscow
```

На устройствах с ОС «EcoRouterOS» необходимо выполнить следующую команду из режима администрирования (`conf t`):

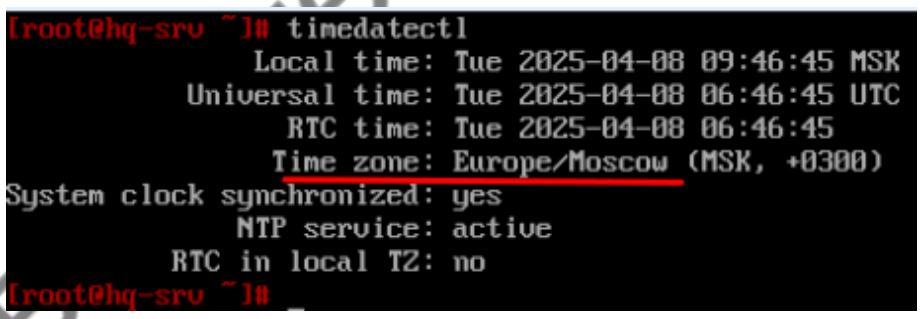
```
ntp timezone utc+<ЦИФРА>
```

Например:

```
ntp timezone utc+3
```

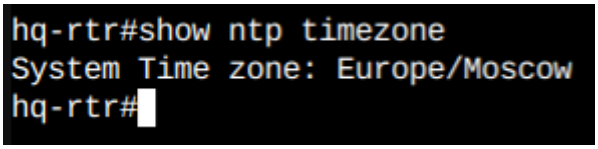
Как проверить?

На устройствах с ОС «Альт» воспользоваться утилитой `timedatectl`:



На устройствах с ОС «EcoRouterOS» воспользоваться командой из привилегированного режима:

```
show ntp timezone
```



Дополнительно:

Настройка временной зоны (timezone) важна по нескольким причинам:

- Корректное отображение времени: правильная настройка временной зоны обеспечивает отображение актуального времени для пользователей и систем, что особенно важно для приложений, работающих с временными метками.

- Синхронизация событий: временные зоны помогают синхронизировать события и действия, происходящие в разных регионах, что критично для распределенных систем и приложений.
- Логирование: правильная временная зона в логах позволяет точно отслеживать и анализировать события, что упрощает диагностику и устранение проблем.
- Планирование задач: многие системы используют время для планирования задач (например, cron в Linux). Неправильная временная зона может привести к выполнению задач в нежелательное время.
- Соответствие законодательству: в некоторых странах существуют законы, касающиеся времени работы и отчетности, поэтому правильная настройка временной зоны помогает соблюдать эти требования.

В целом, настройка временной зоны способствует улучшению работы систем и приложений, обеспечивая точность и согласованность во времени, а в некоторых задач это критически важно.

Краткая справка:

– Синхронизация времени (https://www.altlinux.org/Синхронизация_времени#Пакет_systemd-timesyncd).

Где изучается?

2 курс:

– Операционные системы и среды
– Компьютерные сети

Далее на других курсах.

Модуль 2 Организация сетевого администрирования операционных систем

Модуль № 2:

Организация сетевого администрирования операционных систем

Вид аттестации/уровень ДЭ:

ГИА ДЭ БУ, ГИА ДЭ ПУ (инвариантная часть)

Задание:

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной системы согласно предложенной топологии (см. Рисунок 2).

Для модуля 2 используется отдельный стенд. В стенде преднастроены:

- IP-адреса, маски подсетей и шлюзы по умолчанию;
- Сетевая трансляция адресов;
- IP туннель;
- Динамическая маршрутизация;
- Созданы пользователи sshuser на серверах и net_admin на маршрутизаторах;
- DHCP-сервер;
- DNS-сервер.

Задание Модуля 2 содержит развёртывание доменной инфраструктуры, механизмов инвентаризации, внедрения и настройки ansible как инфраструктуры на основе открытых ключей, установку и настройку файловых служб и служб управления правами и службы сетевого времени, настройки веб серверов.

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчеты (пять отчетов) о своих действиях, включая таблицы и схемы, предусмотренные в задании. Отчеты по окончании работы следует сохранить на диске рабочего места.

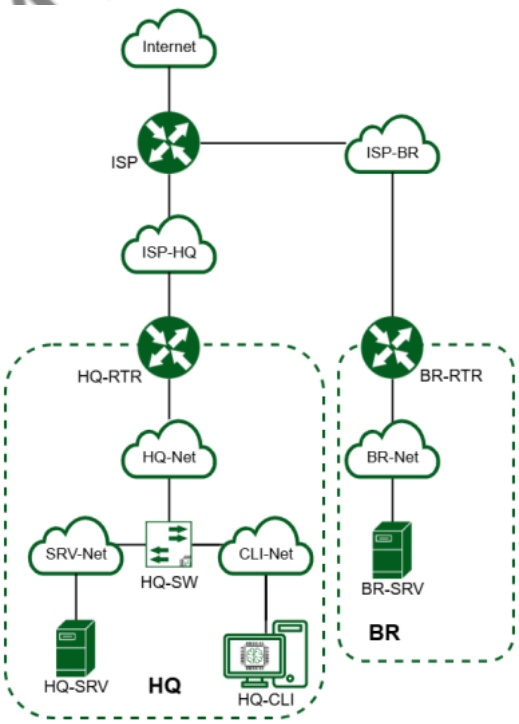


Рисунок 2 – Топология сети

Таблица 1

Машина	**RAM, ГБ**	**CPU**	**HDD/SSD, ГБ**	**ОС**
ISP	1	1	10	ОС Альт JeOS/Linux или аналог
HQ-RTR	1	1	10	ОС EcoRouter или аналог
BR-RTR	1	1	10	ОС EcoRouter или аналог
HQ-SRV	2	1	10	ОС Альт Сервер/аналог
BR-SRV	2	1	10	ОС Альт Сервер/аналог
HQ-CLI	3	2	15	ОС Альт Рабочая Станция/аналог
Итого	10	7	65	-

1. 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;
   - Выполните импорт пользователей из файла users.csv. Файл будет располагаться на виртуальной машине BR-SRV в папке /opt.
2. 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.
3. Настройте службу сетевого времени на базе сервиса chrony:
   - В качестве сервера выступает HQ-RTR;
   - На HQ-RTR настройте сервер chrony, выберите стратум 5;
   - В качестве клиентов настройте HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.
4. Сконфигурируйте ansible на сервере BR-SRV:
   - Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, 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.
5. Развертывание приложений в Docker на сервере BR-SRV:
   - 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;
- 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;
- MediaWiki должна быть доступна извне через порт 8080.

6. На маршрутизаторах сконфигурируйте статическую трансляцию портов:
   - 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;
7. Запустите сервис moodle на сервере HQ-SRV:
   - 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 отчёте.
8. Настройте веб-сервер nginx как обратный прокси-сервер на 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.
9. Удобным способом установите приложение Яндекс Браузере для организаций на HQ-CLI:
   - Установку браузера отметьте в отчёте.

Выполнение задания:

Настройка файлового хранилища

Подробное описание пункта задания:

- 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.

Где выполнять:

На машинах: HQ-SRV, HQ-CLI.

Как делать?

Для просмотра всех подключённых блочных устройств можно воспользоваться утилитой `lsblk`:

```
[root@hq-srv ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0   20G  0 disk
├─sda1   8:1    0    2G  0 part [SWAP]
└─sda2   8:2    0   18G  0 part /
sdb      8:16   0    1G  0 disk
sdc      8:32   0    1G  0 disk
sdd      8:48   0    1G  0 disk
sr0     11:0    1 1024M  0 rom
[root@hq-srv ~]# _
```

Не размеченные диски должны быть одного размера – 1Гб, не смонтированы и не размечены. Для создания raid массива необходимо установить пакет `mdadm`, если он не установлен, для этого можно воспользоваться командой:

```
apt-get install -y mdadm
```

Создание RAID-массива с использованием утилиты `mdadm` происходит при использовании следующей команды:

```
mdadm --create /dev/md0 -l5 -n 3 /dev/sdb /dev/sdc /dev/sdd
```

Описание применяемых команд:

`/dev/md0` – устройство RAID, которое появится после сборки;

`-l5` – уровень RAID;

`-n 3` – количество дисков, из которых собирается массив;

`/dev/sdb /dev/sdc /dev/sdd` – сборка выполняется из дисков sdb, sdc и `sdd`.

Далее необходимо создать файловую систему на созданном RAID-массиве используя утилиту `mkfs` следующей командой:

```
mkfs.ext4 /dev/md0
```

Создаем папку и редактируем файл `mdadm.conf`, в котором находится информация о RAID-массивах и компонентах, которые в них входят:

```
mkdir /etc/mdadm
echo "DEVICE partitions" > /etc/mdadm/mdadm.conf
mdadm --detail --scan >> /etc/mdadm/mdadm.conf
```

Для реализации автоматического монтирование созданного RAID-массива в директорию `/raid5`, первым делом следует создать данную директорию используя команду:

```
mkdir /raid5
```

В конфигурационный файл `/etc/fstab` в конец файла удобным текстовым редактором `vim` или `nano` дописываем следующую строку:

```
/dev/md0        /raid5  ext4    defaults        0       0
```

Для применения монтирования, можно воспользоваться утилитой `mount`, выполнив команду:

```
mount -av
```

```
[root@hq-srv ~]# mount -av
/proc                      : already mounted
/dev/pts                   : already mounted
/tmp                       : already mounted
/                          : ignored
swap                       : ignored
/raid5                     : successfully mounted
[root@hq-srv ~]# _
```

Для реализации сервера NFS необходимо установить пакеты `nfs-server` и `nfs-utils`, для этого можно воспользоваться командой:

```
apt-get install -y nfs-server nfs-utils
```

Для того чтобы реализовать общий доступ средствами NFS до директории `/raid5/nfs`, данную директорию необходимо создать, воспользовавшись следующей командой:

```
mkdir /raid5/nfs
```

Также стоит выдать права для созданной директории:

```
chmod 777 /raid5/nfs
```

Настроить общий доступ средствами NFS можно отредактировав конфигурационный файл `/etc/exports` и добавить в него следующую запись:

```
/raid5/nfs 192.168.100.64/28(sync,rw,no_root_squash)
```

где `/raid5/nfs` – общий ресурс, `192.168.100.64/28` – клиентская сеть, которой разрешено монтирование общего ресурса, `rw` – разрешение на чтение и запись, `no_root_squash` – отключение ограничения прав root, `sync` – синхронный режим доступа.

Для того чтобы запустить NFS-сервер можно воспользоваться командой:

```
systemctl enable --now nfs-server
```

Для того чтобы на виртуальной машине HQ-CLI реализовать монтирование общего ресурса с NFS-сервера необходимо установить пакет `nfs-utils`, сделать это можно воспользовавшись командой:

```
apt-get update && apt-get install -y nfs-utils
```

После чего создать директорию, в которую будет происходить монтирование общего ресурса:

```
mkdir /mnt/nfs
```

Выдать соответствующие права на созданную директорию:

```
chmod -R 777 /mnt/nfs
```

В конфигурационный файл /etc/fstab в конец файла удобным текстовым редактором vim или nano дописываем следующую строку:

```
hq-srv.au-team.irpo:/raid5/nfs  /mnt/nfs        nfs     defaults        0       0
```

Для применения монтирования, можно воспользоваться утилитой `mount`, выполнив команду:

```
mount -av
```

```
[root@hq-cli ~]# mount -av
/proc                    : already mounted
/dev/pts                 : already mounted
/tmp                     : already mounted
/                        : ignored
swap                     : ignored
/media/ALTLinux          : ignored
mount.nfs: timeout set for Tue Apr  8 11:01:19 2025
mount.nfs: trying text-based options 'vers=4.2,addr=192.168.100.1,clientaddr=192.168.100.65'
/mnt/nfs                 : successfully mounted
[root@hq-cli ~]#
```

Как проверить?

Средствами утилиты `lsblk`:

```
[root@hq-srv ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda      8:0    0   20G  0 disk
├─sda1   8:1    0    2G  0 part  [SWAP]
└─sda2   8:2    0   18G  0 part  /
sdb      8:16   0    1G  0 disk
└─md0    9:0    0    2G  0 raid5 /raid5
sdc      8:32   0    1G  0 disk
└─md0    9:0    0    2G  0 raid5 /raid5
sdd      8:48   0    1G  0 disk
└─md0    9:0    0    2G  0 raid5 /raid5
sr0     11:0    1 1024M  0 rom
[root@hq-srv ~]#
```

Средствами утилиты `blkid`:

```
[root@hq-srv ~]# blkid /dev/md0
/dev/md0: UUID="d08c31ee-ca02-4369-950e-312161d27be9" BLOCK_SIZE="4096" TYPE="ext4"
[root@hq-srv ~]#
```

Средствами утилиты `showmount`:

```
[user@hq-cli ~]$ showmount -e hq-srv.au-team.irpo
Export list for hq-srv.au-team.irpo:
/srv/public *
/raid5/nfs  192.168.100.64/28
[user@hq-cli ~]$
```

Средствами утилиты `df`:

```
user@hq-cli ~]$ df -h
Файловая система            Размер Использовано  Дост Использовано% Смонтировано в
udevfs                        5,0M          100K  5,0M             2% /dev
runfs                         984M         1000K  983M             1% /run
/dev/sda2                      28G          7,1G   20G            28% /
tmpfs                         984M             0  984M             0% /dev/shm
tmpfs                         984M          8,0K  984M             1% /tmp
tmpfs                         197M           68K  197M             1% /run/user/500
hq-srv.au-team.irpo:/raid5/nfs  2,0G             0  1,9G             0% /mnt/nfs
[user@hq-cli ~]$
```

Дополнительно:

NFS (Network File System) – это протокол, который позволяет пользователям и приложениям на одном компьютере получать доступ к файлам на другом компьютере через сеть. Вот несколько основных преимуществ NFS:

- Простота использования: позволяет пользователям работать с удалёнными файлами так же, как с локальными, что упрощает доступ к данным.
- Совместный доступ: обеспечивает возможность совместного использования файлов и каталогов между несколькими пользователями и системами, что улучшает сотрудничество.
- Кроссплатформенная поддержка: работает на различных операционных системах, включая UNIX, Linux и Windows, что делает его универсальным решением для сетевого хранения.
- Гибкость: позволяет монтировать удалённые файловые системы в локальную файловую систему, что упрощает организацию и доступ к данным.
- Эффективность: поддерживает кэширование, что может улучшить производительность при доступе к часто используемым файлам.

NFS является мощным инструментом для организации сетевого хранения и совместного доступа к файлам.

Краткая справка:

- NFS (https://www.altlinux.org/NFS);
- RAID – технология виртуализации данных (https://www.altlinux.org/CreateRAID).

Где изучается?

2 курс:

- Операционные системы и среды;
- Компьютерные сети.

3 курс:

- Организация, принципы построение и функционирования компьютерных сетей;
- Программное обеспечение компьютерных сетей;
- Организация администрирования компьютерных систем.

Далее на других курсах.

Настройка служб сетевого времени на базе сервиса chrony

Подробное описание пункта задания:

- В качестве сервера выступает ISP.
- На ISP настройте сервер chrony, выберите стратум 5.
- В качестве клиентов настройте HQ-SRV, HQ-CLI, HQ-RTR, BR-RTR, BR-SRV.

Где выполнять:

На машинах: ISP, HQ-SRV, HQ-CLI, HQ-RTR, BR-RTR, BR-SRV.

Как делать?

На виртуальной машине ISP, которая будет выступать в роли сервера времени необходимо привести конфигурационный файл `/etc/chrony.conf` удобным текстовым редактором `vim` или `nano` к следующему виду:

```
server 127.0.0.1 iburst
local stratum 5
allow 0.0.0.0/0
```

Для применения изменений, необходимо перезагрузить службу `chronyd` следующей командой:

```
systemctl restart chronyd
```

На всех остальных виртуальных машинах с ОС «Альт», которые будут выступать клиентами с точки зрения сервера времени необходимо добавить в конфигурационный файл `/etc/chrony.conf` следующую строку:

```
#pool pool.ntp.org iburst
pool 172.16.4.1 iburst
```

Для применения изменений, необходимо перезагрузить службу `chronyd` следующей командой:

```
systemctl restart chronyd
```

На всех остальных виртуальных машинах с ОС «EcoRouterOS», из режима администрирования (`conf t`) необходимо выполнить следующую команду:

```
ntp server 172.16.5.1
```

Как проверить?

При помощи утилиты `chronyc`:

```
[root@ISP ~]# chronyc tracking
Reference ID    : 7F7F0101 ()
Stratum         : 5
```

```
[root@ISP ~]# chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^? localhost.localdomain         0   8   377     -     +0ns[   +0ns] +/-
[root@ISP ~]#
```

Дополнительно:

Chronyd – это демон для синхронизации системного времени с использованием протокола NTP (Network Time Protocol). Вот несколько основных преимуществ и причин, почему он нужен:

- Точная синхронизация времени: Chronyd обеспечивает высокую точность синхронизации системного времени с удалёнными NTP-серверами, что важно для многих приложений и служб;
- Быстрая корректировка времени: Chronyd может быстро корректировать время, даже если оно значительно отклонено от реального, что делает его полезным для систем, которые часто отключаются от сети;
- Работа в условиях нестабильной сети: Chronyd хорошо справляется с изменениями в сетевых условиях, такими как высокая задержка или временные разрывы соединения;
- Низкое потребление ресурсов: Chronyd требует меньше системных ресурсов по сравнению с другими NTP-демонами, что делает его подходящим для использования на устройствах с ограниченными ресурсами;
- Поддержка виртуальных и мобильных сред: Chronyd хорошо работает в виртуализированных и мобильных средах, где время может быть нестабильным.

Chronyd является эффективным инструментом для обеспечения точного и надежного времени в компьютерных системах.

Краткая справка:

– Синхронизация времени (https://www.altlinux.org/Синхронизация_времени).

Где изучается?

3 курс:

– Организация, принципы построение и функционирования компьютерных сетей,
– Программное обеспечение компьютерных сетей,
– Организация администрирования компьютерных систем.

Далее на других курсах.

Настройка ansible

Подробное описание пункта задания:

- Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI.
- 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.

Где выполнять:

На машине: BR-SRV.

Как делать?

Необходимо установить пакет `ansible` и `sshpass` выполнить это можно следующей командой:

```
apt-get update && apt-get install -y ansible sshpass
```

Приведём файл инвентаря Ansible к следующему виду, отредактировав конфигурационный файл по пути `/etc/ansible/hosts` любым удобным текстовым редактором, например `vim` или `nano`:

```
[hq]
hq-srv ansible_port=2024 ansible_ssh_user=sshuser ansible_ssh_pass=P@ssw0rd
hq-cli ansible_ssh_user=user ansible_ssh_pass=resu
```

Редактируем файл `/etc/ansible/ansible.cfg`, приводя его к следующему виду (для того, чтобы ansible не писал ошибки интерпретатора python3):

```
[defaults]
inventory      = /etc/ansible/hosts
host_key_checking = False
interpreter_python = /usr/bin/python3
```

Как проверить?

Проверяем, ответы от машин должны быть зелёного цвета и содержать поле pong:

```
ansible all -m ping
```

```
[root@br-srv ~]# ansible -m ping all
hq-srv | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
hq-cli | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

Дополнительно:

Ansible – это инструмент для автоматизации управления конфигурацией, развертывания приложений и оркестрации. Вот несколько основных преимуществ Ansible:

- Простота использования: Ansible использует простой и понятный синтаксис на основе YAML, что облегчает написание и чтение сценариев (плейбуков);

- Безагентная архитектура: Ansible не требует установки агентов на управляемых узлах, что упрощает развертывание и управление;
- Масштабируемость: Ansible может управлять большим количеством серверов одновременно, что делает его подходящим для работы в масштабируемых средах;
- Кроссплатформенность: Ansible поддерживает множество операционных систем и платформ, включая Linux, Windows и облачные сервисы;
- Идемпотентность: Ansible гарантирует, что выполнение плейбука приведет к одному и тому же результату, независимо от того, сколько раз он будет запущен, что упрощает управление конфигурацией;
- Расширяемость: Ansible позволяет создавать собственные модули и плагины, что дает возможность адаптировать его под специфические нужды;
- Сообщество и поддержка: Ansible имеет активное сообщество и множество доступных модулей и ролей, что облегчает поиск решений и примеров.

Ansible является мощным инструментом для автоматизации и управления инфраструктурой, что позволяет повысить эффективность и снизить вероятность ошибок.

Краткая справка:

– Ansible – система управления конфигурациями (https://www.altlinux.org/Ansible).

Где изучается?

2 курс:

– Операционные системы и среды.

3,4 курс:

– Организация администрирования компьютерных систем

Далее на других курсах.

Развертывание приложений в Docker

Подробное описание пункта задания:

- 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.
- 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.
- MediaWiki должна быть доступна извне через порт 8080.

Где выполнять:

На машинах: BR-SRV, HQ-CLI.

Как делать?

Установить необходимые пакеты для работы с Docker и Docker Compose можно воспользовавшись следующей командой:

```
apt-get install –y docker-engine docker-compose
```

После установки необходимых пакетов стоит запустить службу `docker`:

```
systemctl enable --now docker.service
```

Создаем файл `wiki.yml` для приложения MediaWiki в директории `/root` и удобным текстовым редактором добавляем в него следующее содержимое:

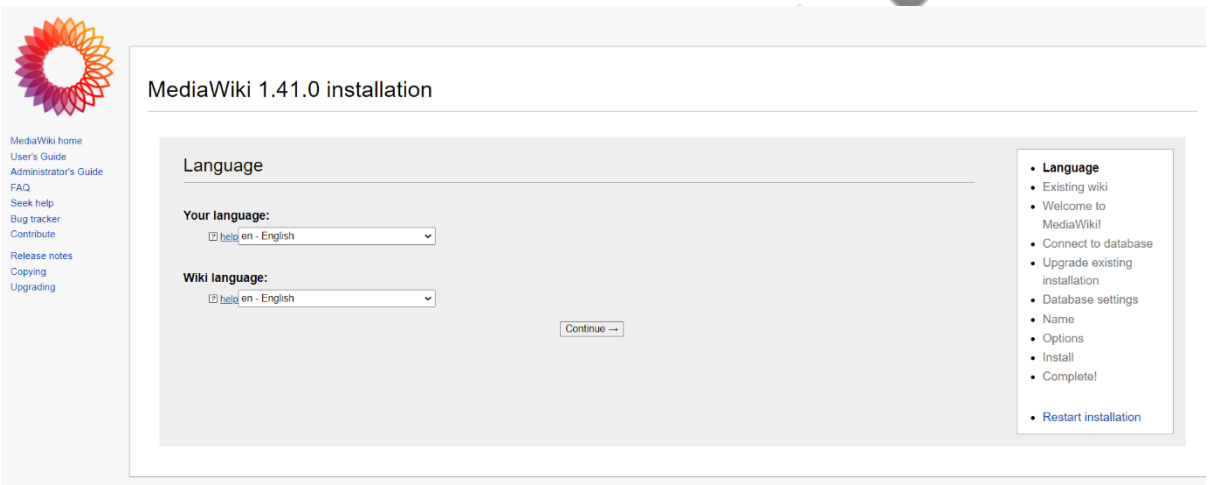
```
services:
  mariadb:
    image: mariadb:latest
    environment:
      - MYSQL_ROOT_PASSWORD=toor
      - MYSQL_DATABASE=mediawiki
      - MYSQL_USER=wiki
      - MYSQL_PASSWORD=WikiP@ssw0rd
  mediawiki:
    image: mediawiki:latest
    ports:
      - "8080:80"
    environment:
```

```
      - MEDIAWIKI_DB_TYPE=mysql
      - MEDIAWIKI_DB_HOST=mariadb
      - MEDIAWIKI_DB_USER=wiki
      - MEDIAWIKI_DB_PASSWORD=WikiP@ssw0rd
      - MEDIAWIKI_DB_NAME=mediawiki
    # volumes: [/root/mediawiki/LocalSettings.php:/var/www/html/LocalSettings.php]
volumes:
  mediawiki_data:
  mariadb_data:
```

Запустить сборку с последующим запуском контейнеров можно воспользовавшись командой:

```
docker compose –f /root/wiki.yml up -d
```

Далее необходимо произвести установку mediawiki с клиента HQ-CLI, используя веб-интерфейс, создав пользователь wiki с паролем WikiP@ssw0rd:



По результатам установки средствами веб-интерфейса должен быть скачан файл `LocalSettings.php` который необходимо передать на BR-SRV в директорию `/root/mediawiki`.

В файле `wiki.yml` необходимо убрать символ комментария перед строкой `[/root/mediawiki/LocalSettings.php:/var/www/html/LocalSettings.php]`. После чего выполнить перезапуск контейнеров:

```
docker compose -f wiki.yml stop
docker compose -f wiki.yml up -d
```

Дополнительно:

Docker – это платформа для автоматизации развертывания, масштабирования и управления приложениями в контейнерах. Вот несколько основных преимуществ использования Docker:

- Изоляция приложений: контейнеры Docker обеспечивают изоляцию приложений и их зависимостей, что позволяет избежать конфликтов между различными версиями библиотек и программного обеспечения;
- Портативность: контейнеры могут работать на любой системе, поддерживающей Docker, что делает приложения легко переносимыми между различными средами;

- Упрощенное развертывание: Docker позволяет быстро и легко развертывать приложения, используя образы, что сокращает время на настройку и конфигурацию;
- Масштабируемость: Docker упрощает масштабирование приложений, позволяя быстро создавать и удалять контейнеры в зависимости от нагрузки;
- Эффективное использование ресурсов: контейнеры используют меньше ресурсов по сравнению с виртуальными машинами, так как они разделяют ядро операционной системы, что позволяет запускать большее количество приложений на одном хост;
- Управление зависимостями: Docker позволяет упаковывать все зависимости приложения в один контейнер, что упрощает управление и развертывание;
- Поддержка микросервисной архитектуры: Docker идеально подходит для разработки и развертывания микросервисов, позволяя каждому сервису работать в своем контейнере;
- Сообщество и экосистема: Docker имеет активное сообщество и множество доступных образов в Docker Hub, что облегчает поиск готовых решений и ускоряет разработку.

Краткая справка:

– MediaWiki-Docker (https://www.mediawiki.org/wiki/MediaWiki-Docker/ru);
– Разворачиваем Mediawiki (https://habr.com/ru/articles/491030/).

Где изучается?

3,4 курс:

– Организация администрирования компьютерных систем.

Далее на других курсах.

Настройка трансляции портов

Подробное описание пункта задания:

- 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.

Где выполнять:

На машинах: HQ-RTR, BR-RTR.

Как делать?

Из режима администрирования (`conf t`) выполнить следующую команду:

```
ip nat source static tcp <IP-АДРЕС_УСТРОЙСТВА_ЛОКАЛЬНОЙ_СЕТИ>
<ПОРТ_УСТРОЙСТВА_ЛОКАЛЬНОЙ_СЕТИ> <ВНЕШНИЙ_IP-АДРЕС_УСТРОЙСТВА>
<ПОРТ_ДЛЯ_ОБРАЩЕНИЯ_ИЗ_ВНЕШНЕЙ_СЕТИ>
```

Например:

Проброс порта 2024 в порт 2024 на HQ-SRV:

```
ip nat source static tcp 192.168.100.1 2024 172.16.4.14 2024
```

Проброс порта 80 в порт 8080 на BR-SRV, для работы сервиса mediawiki:

```
ip nat source static tcp 192.168.200.1 80 172.16.5.14 8080
```

Проброс порта 2024 в порт 2024 на BR-SRV:

```
ip nat source static tcp 192.168.200.1 2024 172.16.5.14 2024
```

Дополнительно:

Статический NAT (проброс портов) – это метод, используемый для сопоставления внутреннего IP-адреса и порта с внешним IP-адресом и портом, позволяющий устройствам из внешней сети (например, из сети Интернет) получить доступ к определённым сервисам, запущенным в локальной сети.

Краткая справка:

– User Guide Руководство по установке и конфигурированию (https://rdp.ru/wp-content/uploads/ER_UserGuide.pdf).

Где изучается?

2 курс:

– Операционные системы и среды;
– Компьютерные сети.

3,4 курс:

– Организация, принципы построения и функционирования компьютерных систем,
– Организация администрирования компьютерных систем

Далее на других курсах.

Настройка сервиса Moodle

Подробное описание пункта задания:

- 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 отчёте.

Где выполнять:

На машинах: HQ-SRV, HQ-CLI.

Как делать?

Установка необходимых пакетов выполняется при помощи команды:

```
apt-get install –y apache2 php8.2 apache2-mods apache2-mod_php8.2 php8.2-libs mariadb-server php8.2-opcache php8.2-curl php8.2-gd php8.2-intl php8.2-mysqlnd-mysqli php8.2-xmlrpc php8.2-zip php8.2-soap php8.2-mbstring php8.2-xmlreader php8.2-fileinfo php8.2-sodium
```

Включение и добавление в автозагрузку служб `httpd2` и `mysql`:

```
systemctl enable --now httpd2 mariadb
```

Зайти в консоль mariadb:

```
mariadb -u root
```

Создать базу данных:

```
create database moodle;
```

Создать пользователя с паролем:

```
create user moodle identified by 'P@ssw0rd';
```

Предоставить максимальные привилегии пользователю к базе данных:

```
grant all privileges on moodle.* to moodle;
flush privileges;
```

Выйти из консоли mariadb:

```
exit;
```

Скачиваем moodle, распаковываем и перемещаем в директорию `/var/www/html/`:

```
wget https://download.moodle.org/download.php/direct/stable405/moodle-latest-405.tgz
tar -xf moodle-latest-405.tgz
mv moodle /var/www/html/
```

Создание каталога moodledata с изменением владельца на каталогах html и moodledata:

```
mkdir /var/www/moodledata
chown -R apache2:apache2 /var/www/html
```

Удаляем стандартную страницы apache:

```
rm /var/www/html/index.html
```

В конфигурационном файле /etc/httpd2/conf/sites-available/default.conf добавьте каталог moodle в секции DocumentRoot:

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot "/var/www/html/moodle"
```

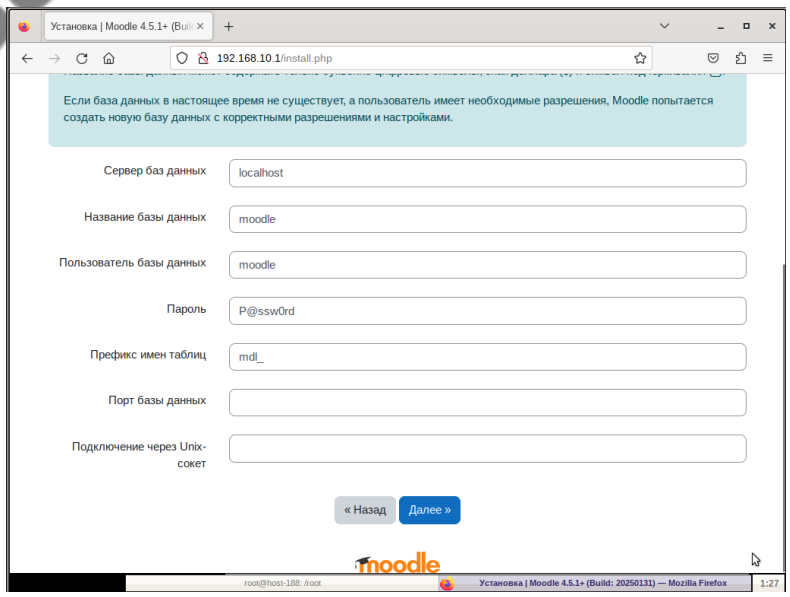
В файле `/etc/php/8.2/apache2-mod_php/php.ini` переменную `max_input_vars` выставляем равной 5000:

```
; Development Value: 60 (60 seconds)
; Production Value: 60 (60 seconds)
; http://php.net/max-input-time
max_input_time = 240

; Maximum input variable nesting level
; http://php.net/max-input-nesting-level
;max_input_nesting_level = 64

; How many GET/POST/COOKIE input variables may be accepted
max_input_vars = 5000

; Maximum amount of memory a script may consume (128MB)
; http://php.net/memory-limit
memory_limit = 128M

;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
; Error handling and logging ;
;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;;
```

Перезапуск службы httpd2:

```
systemctl restart httpd2
```

С клиента HQ-CLI в браузере зайдите на страницу `http://<IP-АДРЕС_HQ-SRV>/install.php` и начните установку moodle в графическом режиме, заполнив параметры из предыдущих шагов:

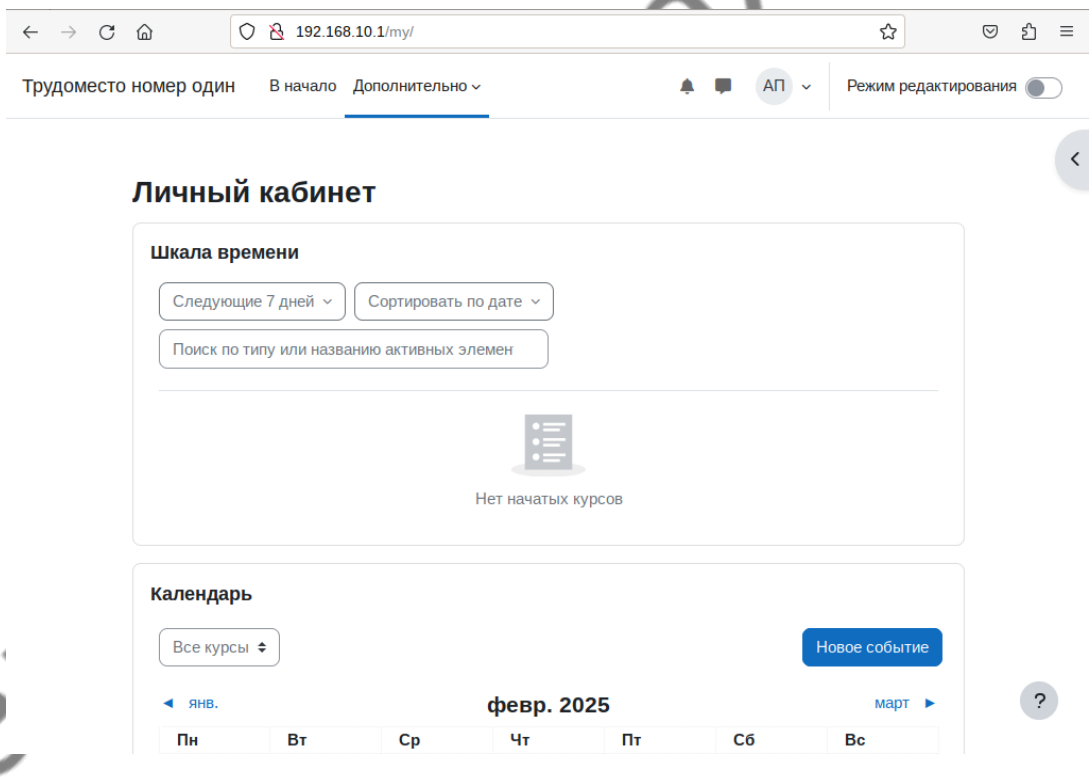


При установке также инсталлятор попросит выставить параметр `$CFG->dbtype='mariadb';` вместо `'mysql'` в файле `/var/www/html/moodle/config.php`:

```
<?php  // Moodle configuration file

unset($CFG);
global $CFG;
$CFG = new stdClass();

$CFG->dbtype    = 'mariadb';
$CFG->dblibrary = 'native';
$CFG->dbhost    = 'localhost';
$CFG->dbname    = 'moodle';
$CFG->dbuser    = 'moodle';
$CFG->dbpass    = 'P@ssw0rd';
$CFG->prefix    = 'mdl_';
$CFG->dboptions = array (
  'dbpersist' => 0,
  'dbport' => '',
  'dbsocket' => '',
  'dbcollation' => 'utf8mb4_general_ci',
);
```

После всех манипуляций сервер moodle установлен, осталось только сделать настройку стартовой страницы с номер рабочего места участника ДЭ

Задайте полное название сайта, в кратком названии сайта укажите номер вашего рабочего места.



Дополнительно:

Moodle – это популярная платформа для управления обучением (LMS), обладающая рядом преимуществ:

- Открытый исходный код: Moodle является бесплатным и открытым программным обеспечением, что позволяет пользователям настраивать и модифицировать платформу под свои нужды;
- Гибкость и масштабируемость: платформа поддерживает различные форматы курсов и может быть адаптирована для учебных заведений любого размера – от небольших школ до крупных университетов;

- Интерактивные инструменты: Moodle предлагает множество инструментов для взаимодействия, включая форумы, чаты, опросы и задания, что способствует активному обучению;
- Поддержка различных форматов контента: платформа позволяет загружать и использовать различные типы материалов, включая текст, видео, аудио и интерактивные элементы;
- Мобильная доступность: Moodle имеет мобильное приложение, что позволяет учащимся получать доступ к курсам и материалам с любых устройств.

Краткая справка:

– Установить Moodle используя apache2 (https://www.altlinux.org/Moodle).

Где изучается?

2 курс:

– Операционные системы и среды;
– Основы проектирования баз данных.

3 курс:

– Организация администрирования компьютерных систем

Далее на других курсах.

Настройка веб-сервера nginx, как обратный прокси-сервер

Подробное описание пункта задания:

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.

Где выполнять:

На машине: HQ-SRV.

Как делать?

Установить пакет `nginx`:

```
apt-get install -y nginx
```

Настроить nginx как реверсивный прокси сервер, дописав в файл `/etc/nginx/nginx.conf` следующую информацию:

```
http {
    server {
        listen 80;  # Слушаем на 80 порту для HTTP
        server_name moodle.au-team.irpo;  # Указываем первое доменное имя
        location / {
            proxy_pass http://192.168.10.1:80;  # Перенаправление на указанный адрес
и порт
            proxy_set_header Host $host;  # Пробрасываем заголовок Host
            proxy_set_header X-Real-IP $remote_addr;  # Пробрасываем IP клиента
            proxy_set_header      X-Forwarded-For      $proxy_add_x_forwarded_for;
#Пробрасываем заголовок X-Forwarded-For
            proxy_set_header X-Forwarded-Proto $scheme;  #Пробрасываем схему запроса
        }
    }
    server {
        listen 80;  # Слушаем на 80 порту для HTTP
        server_name wiki.au-team.irpo;  # Указываем второе доменное имя
        location / {
            proxy_pass  http://192.168.5.1:8080;   # Перенаправление на указанный
адрес и порт
            proxy_set_header Host $host;  # Пробрасываем заголовок Host
            proxy_set_header X-Real-IP $remote_addr;  # Пробрасываем IP клиента
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
#Пробрасываем заголовок X-Forwarded-For
            proxy_set_header  X-Forwarded-Proto  $scheme;    #  Пробрасываем  схему
запроса
        }
    }
}
```

Запустить и активировать службу nginx:

```
systemctl enable --now nginx
```

Дополнительно:

Реверсивный прокси Nginx обладает рядом замечательных характеристик и преимуществ, которые делают его популярным выбором для веб-разработчиков и системных администраторов. Вот некоторые из основных достоинств:

- Балансировка нагрузки: Nginx может распределять входящие запросы между несколькими серверами, что позволяет улучшить производительность и отказоустойчивость.
- Кэширование: Nginx может кэшировать статические файлы и результаты выполнения запросов, что снижает нагрузку на серверы приложений и ускоряет ответ пользователям
- Безопасность: Реверсивный прокси может служить дополнительным уровнем безопасности, скрывая внутреннюю инфраструктуру и предоставляя защиту от атак, таких как DDoS
- Сжатие данных: Поддержка сжатия ответов (например, с использованием gzip) помогает уменьшить объем трафика и ускорить время загрузки страниц.
- Легкость в использовании и высокая производительность: Nginx известен своей высокой производительностью и эффективно использует ресурсы, что делает его пригодным для обработки большого объема одновременных соединений.
- Масштабируемость: Nginx легко масштабируется, позволяя добавлять дополнительные серверы в инфраструктуру без значительных изменений в конфигурации.
- Отладка и мониторинг: Nginx предоставляет различные возможности для логирования и мониторинга, что помогает в диагностике проблем и оптимизации производительности.

Краткая справка:

– Использование nginx (https://www.altlinux.org/Nginx/php-fpm).

Где изучается?

2 курс:

– Операционные системы и среды.

3 курс:

– Организация администрирования компьютерных систем

Далее на других курсах.

Установка Яндекс.Браузера

Подробное описание пункта задания:

Установите браузер отметьте в отчёте.

Как делать?

От имени суперпользователя выполнить:

```
apt-get install -y yandex-browser-stable
```

Где выполнять:

На виртуальной машине HQ-CLI.

Дополнительно:

Yandex.Browser (Яндекс.Браузер) – это веб-браузер, для просмотра Всемирной Паутины. Он основан на движке ChromiumYandex.Browser доступен для различных платформ, включая Linux и даже Windows.

Существует две основные версии браузера:

1. Стандартная (красный Yandex.Browser) — версия для домашнего использования.

2. Корпоративная (синий Yandex.Browser для бизнеса) — версия с дополнительными инструментами для организаций, включая управление через групповые политики (GPO) и Active Directory.

Краткая справка:

– Яндекс.Браузер (https://www.altlinux.org/ЯндексБраузер).

Где изучается?

2 курс:

– Операционные системы и среды

Начало работы с Кибер Инфраструктурой

Установка системы

О Кибер Инфраструктуре

На следующей схеме показаны основные вычислительные компоненты продукта Кибер Инфраструктура:

Кибер Инфраструктура – гиперконвергентное решение, состоящее из ресурсов хранилища, вычислительных и сетевых ресурсов, обеспечивающих:

- Файловое хранилище, объектное хранилище S3, и блочное хранилище для ВМ или баз данных;
- Частные и публичные облака;
- Виртуальные машины (ВМ) и программно-определяемые сети (SDN) и управление ими;
- Сервис SaaS, включая «Kubernetes как услуга», «Балансировщик нагрузки как услуга» и постоянное хранилище для Kubernetes;
- Высокую доступность для критически важных приложений.

Кибер Инфраструктура, устанавливаемая на выделенные физические серверы без ПО, объединяет их в единый кластер, который можно легко масштабировать путем добавления дисков или узлов. Кластер управляется через веб-панель администрирования с высокой доступностью и через интерфейс командной строки.

Панель администрирования обеспечивает всесторонний мониторинг всех компонентов. Обзорные панели мониторинга интегрируются в решения Prometheus, Grafana, SNMP и Zabbix, обеспечивая предоставление полезной информации о состоянии инфраструктуры. Кроме того, система оповещений позволяет администратору быть в курсе неправильных конфигураций, сбоев и других проблем.

Требования к системе

Кибер Инфраструктура работает на стандартном оборудовании, поэтому можно создать кластер, используя обычные серверы, диски и сетевые карты. Тем не менее для оптимальной производительности необходимо соблюдение некоторых условий и рекомендаций.

Для промышленных сред можно запускать продукт Кибер Инфраструктура на физическом сервере или внутри виртуальной машины, чтобы использовать хранилище резервных копий в публичном облаке. Требования к оборудованию и рекомендуемое количество серверов в кластере зависят от развертываемых сервисов.

Кластер можно создать поверх различного оборудования, использование серверов со сходной аппаратной конфигурацией обеспечит лучшую производительность, мощность и балансировку кластера.

Даже в минимальной конфигурации рекомендуется три сервера, можно начать тестировать продукт Кибер Инфраструктура всего с одним сервером и добавить остальные серверы позже.

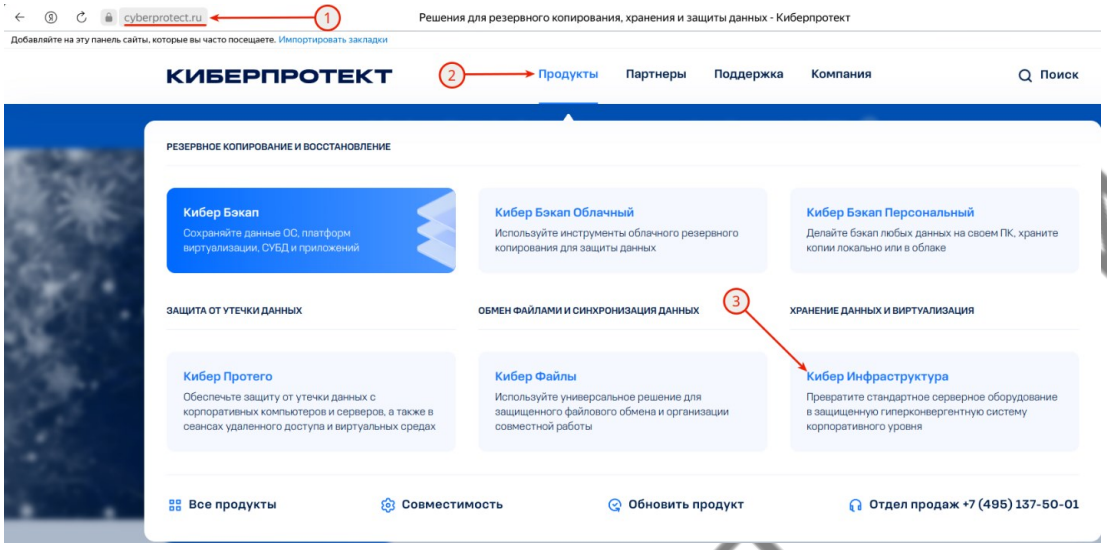
Минимальные аппаратные требования к узлу:

Поддерживаются 64-разрядные процессоры x86 с включенными AMD-V или Intel VT.

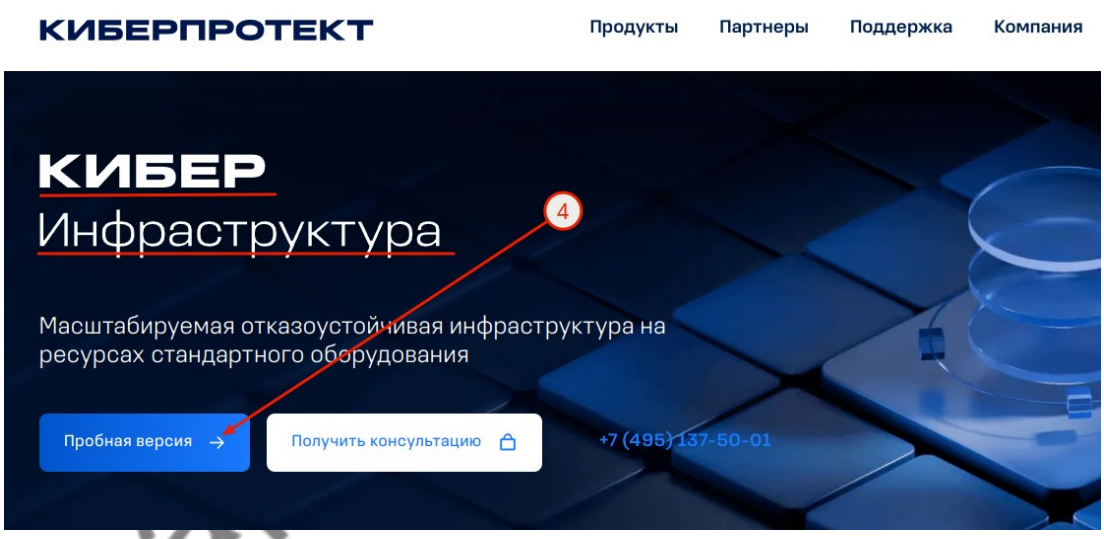
Тип	Узел управления с функциями хранения и вычислений	Подчиненный узел с функциями хранения и вычислений	Сервер управления с хранилищем и Backup Gateway
ЦП	16 ядер*	8 ядер*	4 ядра*
ОЗУ	32 ГБ	32 ГБ	32 ГБ
Хранилище	1 диск: система + метаданные, жесткий диск SATA 100+ ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости	1 диск: система, жесткий диск SATA 100 ГБ 1 диск: метаданные, жесткий диск SATA 100 ГБ (только на первых трех узлах в кластере) 1 диск: хранилище, жесткий диск SATA, размер по необходимости	1 диск: система + метаданные, жесткий диск SATA 120 ГБ 1 диск: хранилище, жесткий диск SATA, размер по необходимости
Сеть	10 GbE для частной сети 1 GbE для публичной сети	10 GbE для частной сети 1 GbE для публичной сети	10 GbE для частной сети 1 GbE для публичной сети
*Ядро ЦП здесь означает физическое ядро в многоядерном процессоре (Hyper-Threading не учитывается)			

Как получить дистрибутив

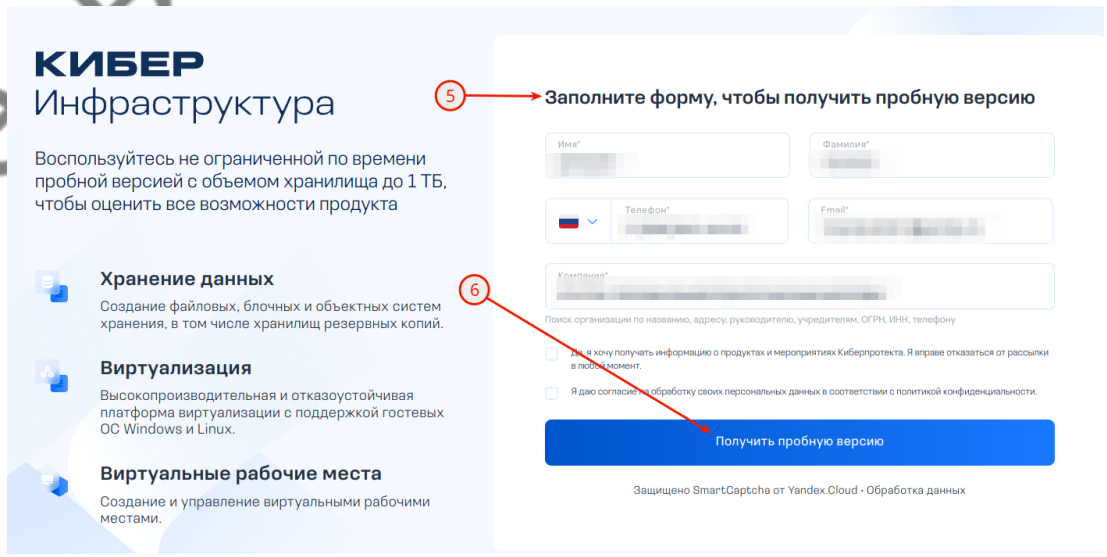
Перейти на сайт киберпротекта (https://cyberprotect.ru/), затем в разделе «Продукты» выбрать решение «Кибер Инфраструктура»:



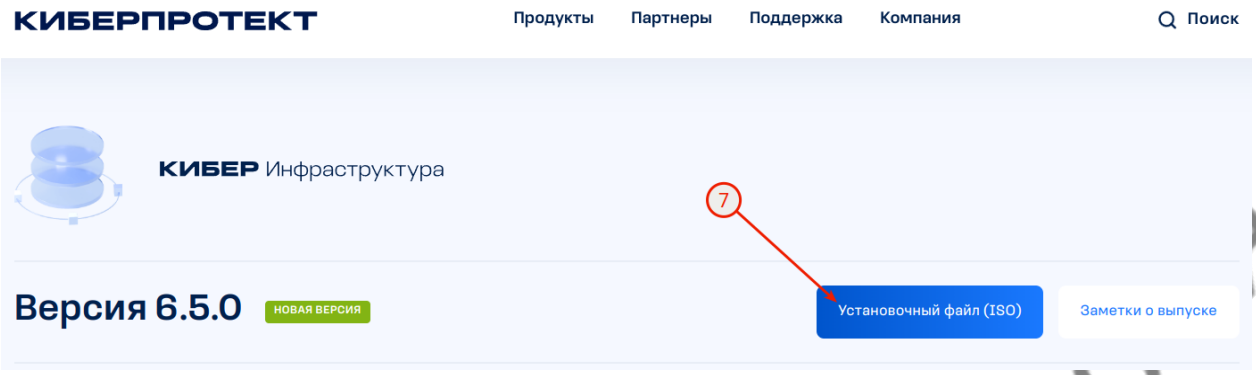
Выбрать «Пробная версия»:



Заполнить форму и нажать «Получить пробную версию»:



Выбрать «Установочный файл (ISO)»:

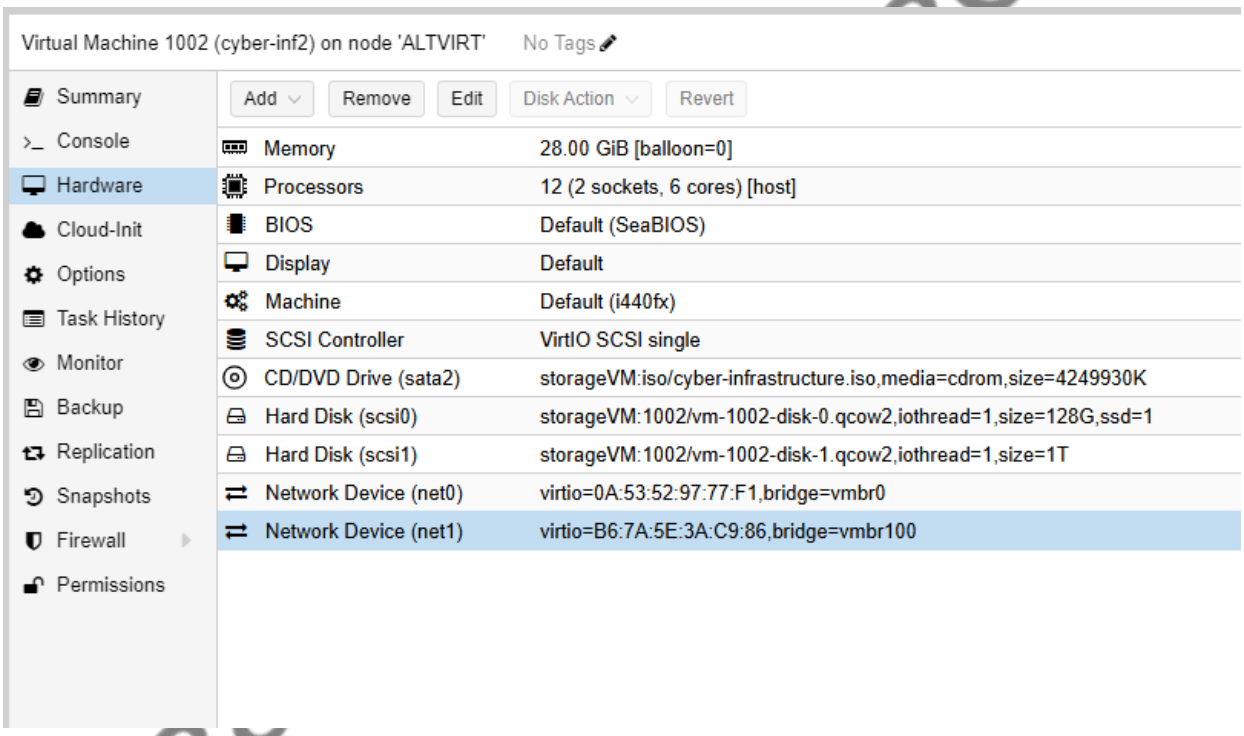


Свойства стенда

Стенд с Кибер Инфраструктурой развернут в среде виртуализации Альт Виртуализация. Однако, настоятельно советуем устанавливать Кибер Инфраструктуру на «голое» железо (bare metal).

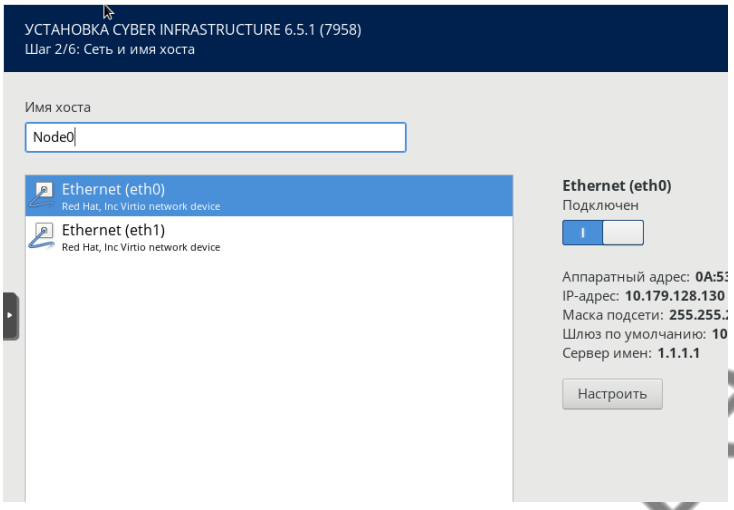
Были выделены следующие ресурсы:

- Процессор Intel(R) Xeon(R) CPU E5620 @ 2.40GHz – 12 ядер;
- ОЗУ – 28 Gb;
- HDD:
  - 128Gb – на систему
  - 1Tb – на хранилище;
- Network:
  - сетевой адаптер, подключенный общей сети, доступ в Интернет (сеть 10.179.128.0/23);
  - сетевой адаптер во внутренней изолированной сети (192.168.1.0/24).



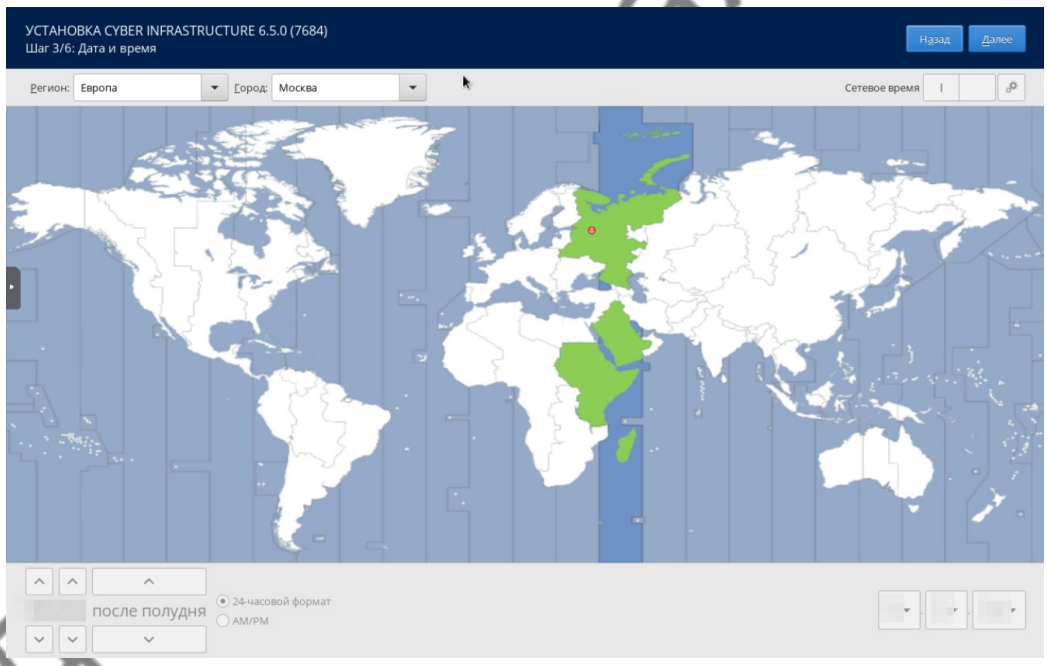
Установка системы

После конфигурирования и запуска ВМ подтверждаем установку, принимаем лицензионное соглашение, и попадаем на экран настройки «Сети и имени хоста»:

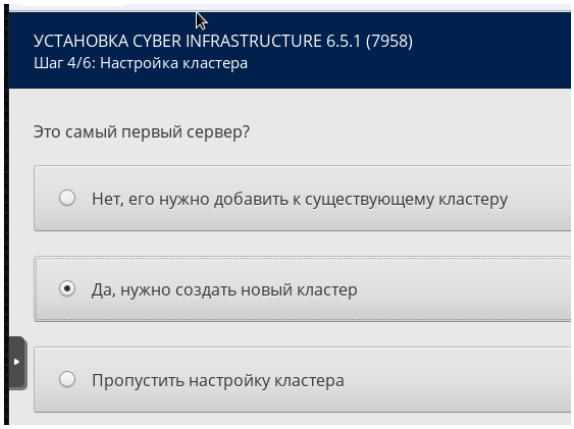


Вводим данные. Не забудьте включить и настроить **ВСЕ** интерфейсы!

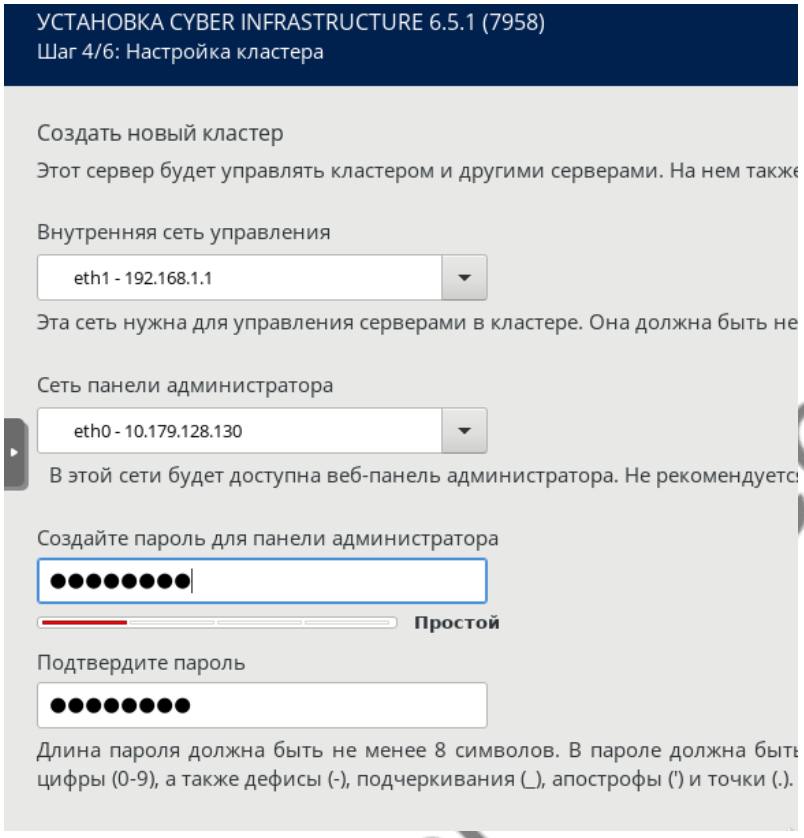
Далее на следующем шаге настраиваем часовой пояс:



На следующем экране устанавливаем значение на «Да, нужно создать новый кластер»:

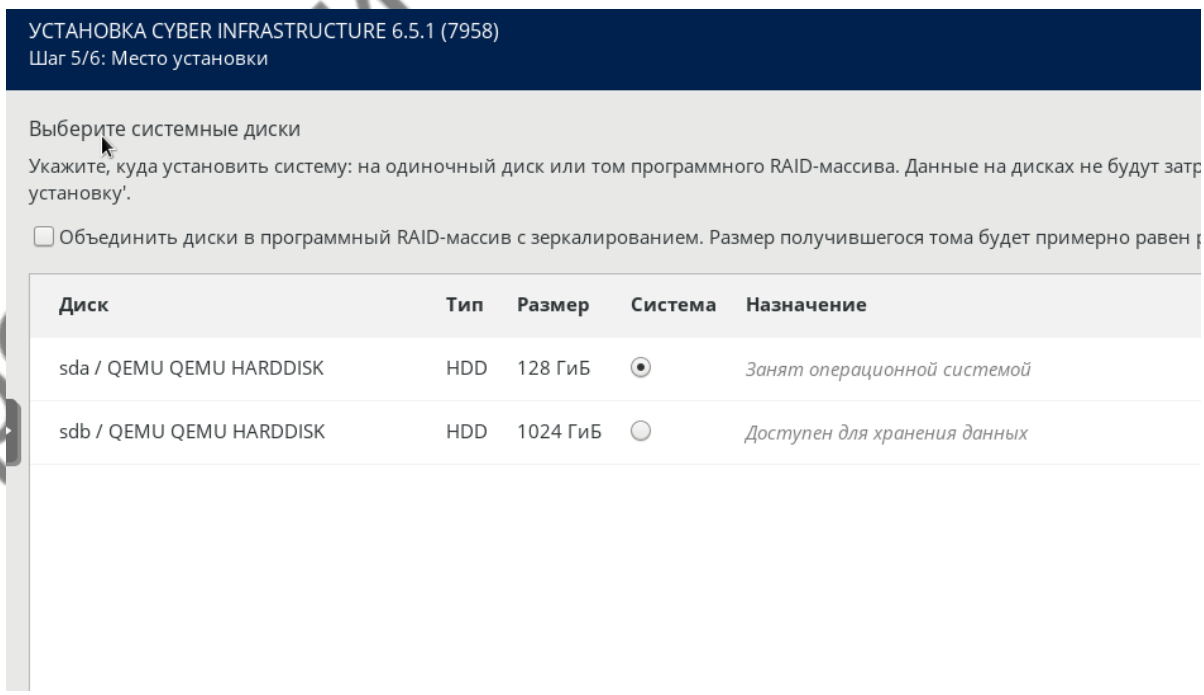


Следующий шаг – настройка сетей кластера:



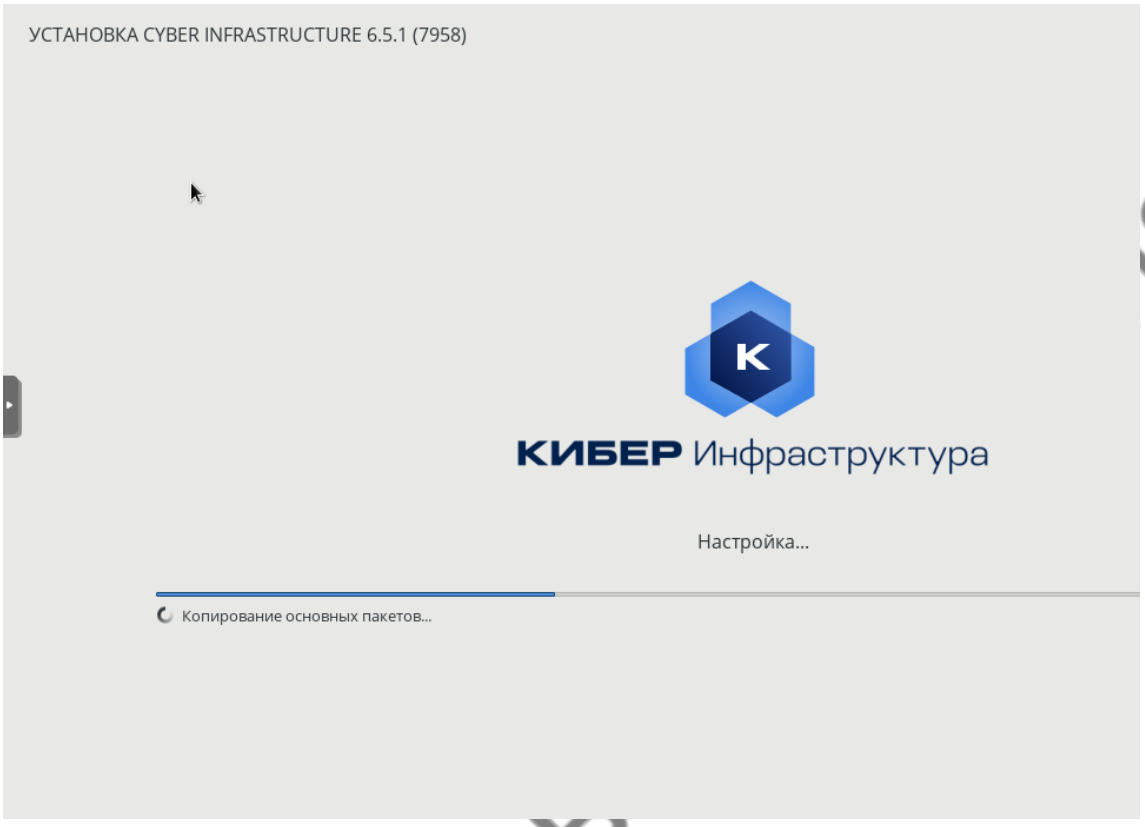
Обратите внимание! Сеть **управления** – это внутренняя сеть, а сеть **администрирования** – внешняя, с доступом в интернет. В пароле нельзя использовать специальные символы (" № ; % и тп.). Можно использовать простые и словарные пароли, например "Passw0rd", конечно, только для экспериментальных и учебных стендов. В таком случае, требуется дважды нажать «далее».

На следующем шаге – настройка дисковой подсистемы:



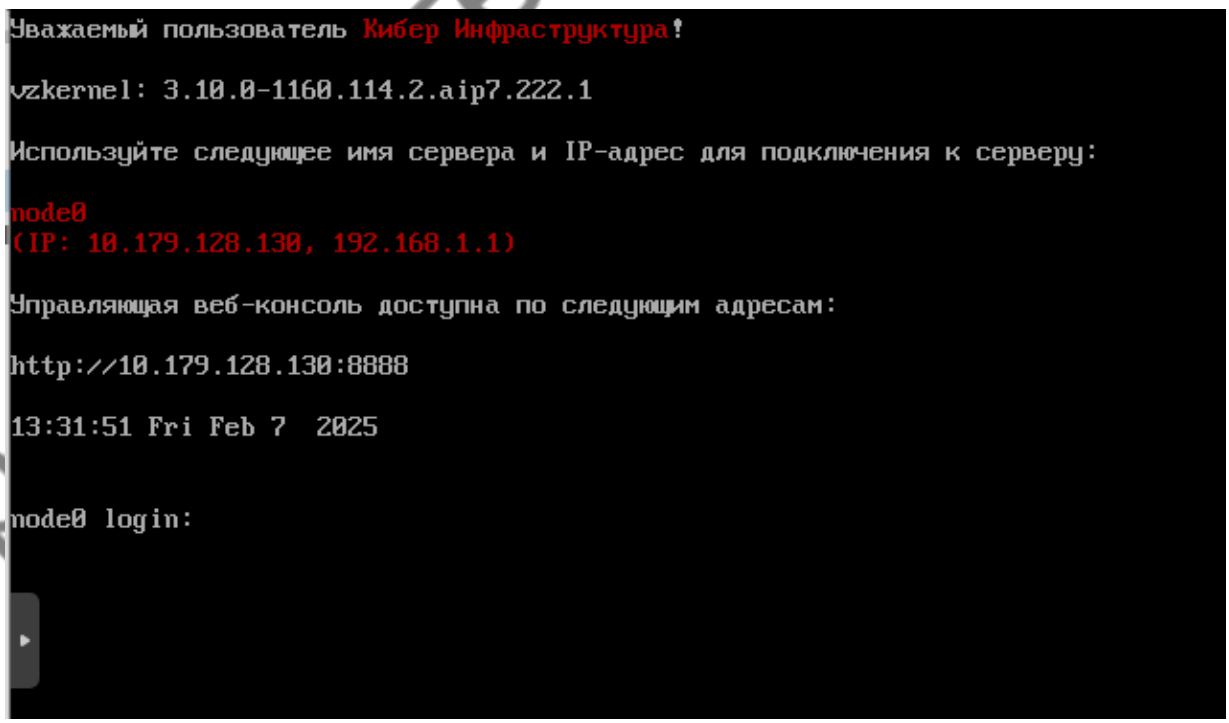
Должен быть выделен диск под операционную систему. В дальнейшем мы настроим диск под хранилище. После подтверждения операции нажимаем далее.

Начинается установка системы. В зависимости от производительности аппаратного обеспечения (особенно дисков) может занять в достаточно длительное время, до 1 часа:



В это время индикация может на некоторое время замирать на одном месте, это **нормально**.

После установки машина самостоятельно перезагрузится, и в консоли отобразится параметры подключения к веб-консоли:

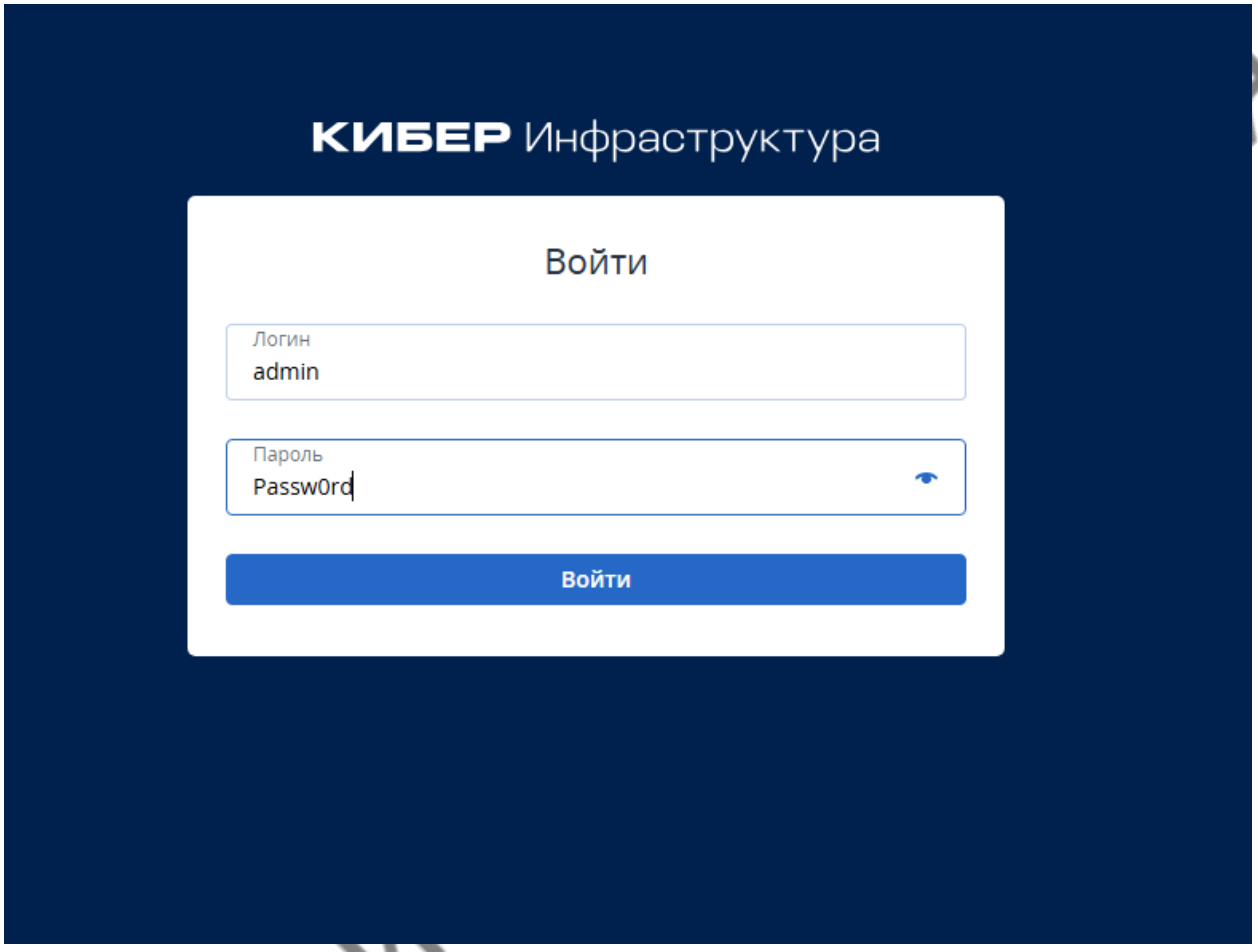


Система установлена.

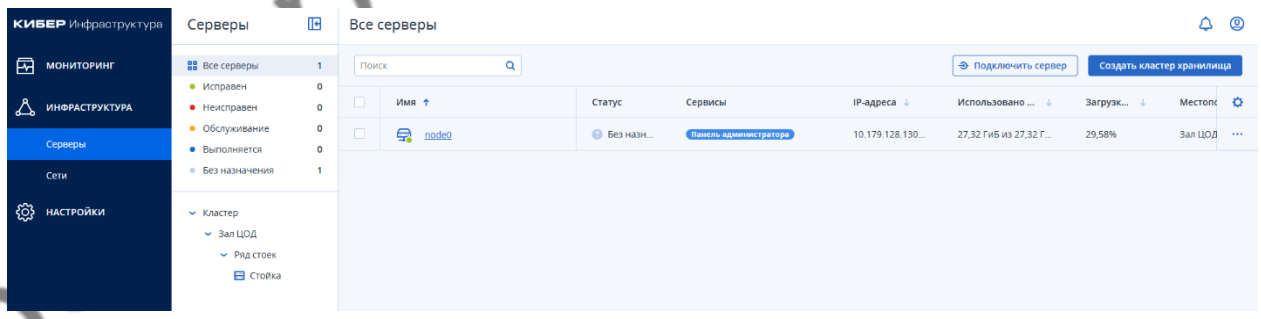
Настройка системы

Начало настройки

После ввода параметров веб-консоли и предупреждения о самоподписаном сертификате попадаем в окно аутентификации:



Далее, попадаем в панель администратора:



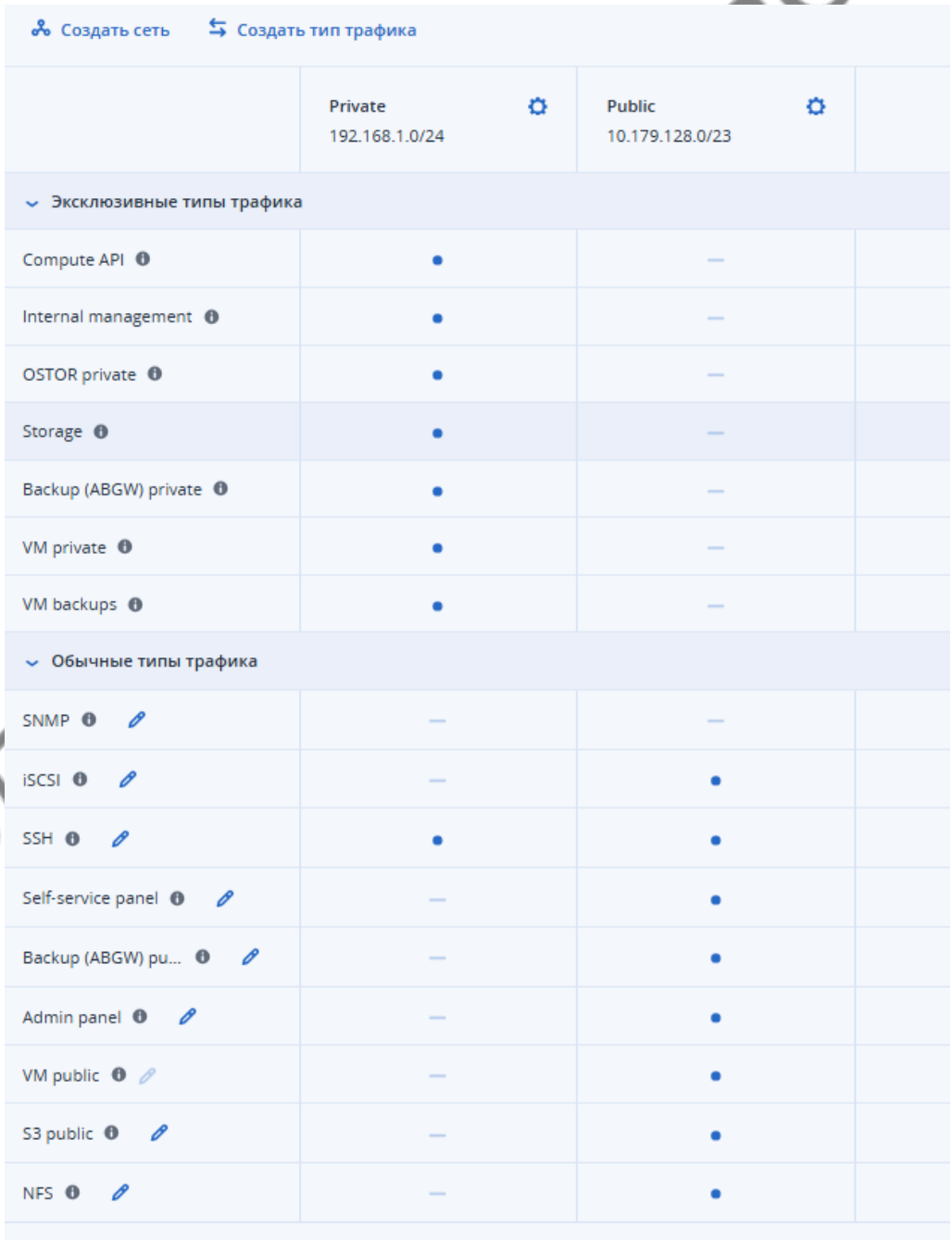
Напоминаем вам, что решение Кибер инфраструктура является полноценной гиперконвергентной инфраструктурой, объединяющую **вычислительные** ресурсы, **системы хранения** данных и **сетевые технологии** в единую единицу управления. Поэтому, для успешной работы необходимо предварительно настроить сетевую подсистему и настроить кластер хранилища. Далее, появится возможность настроить вычислительный кластер (пусть и состоящий из одной ноды), загрузить образы и шаблоны дисков и создавать экземпляры виртуальных машин.

Настройка сети

Переходим к пункт меню «Сети». Меню разделено на два вида трафика: **эксклюзивный** и **обычный**.

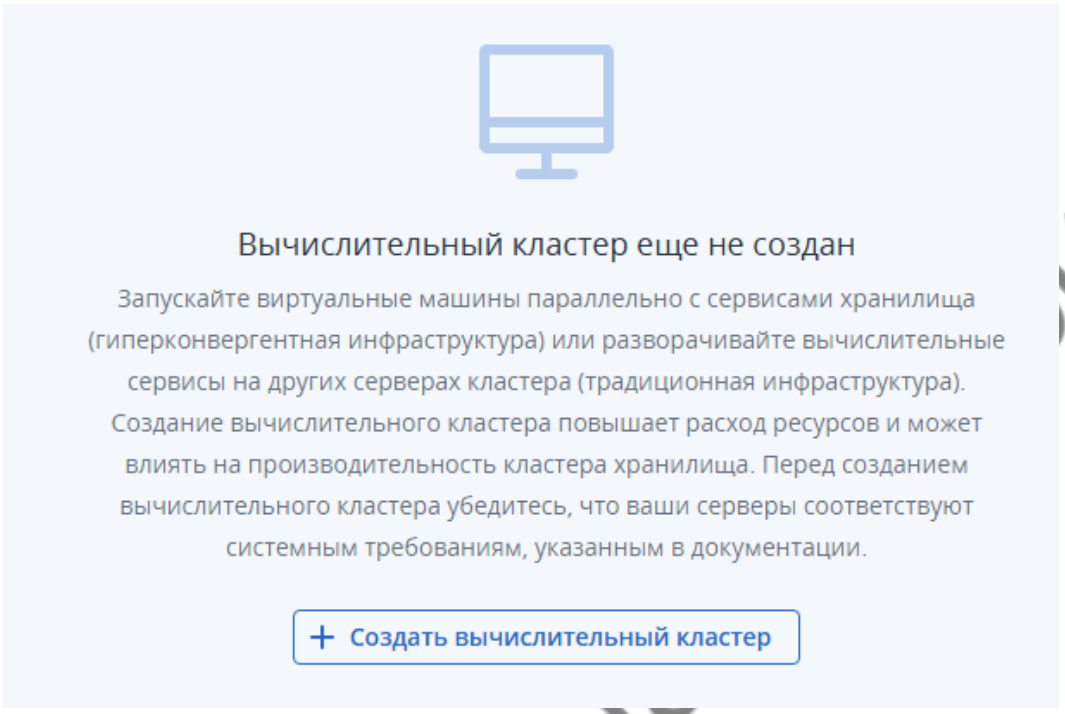
Эксклюзивные типы трафика характерны для виртуальных машин, например для обмена данными между ВМ (VM private: VXLAN) и хранилищ, например дисковых массивов кластера. Следует назначать внутренним сетям. Для этого выбираем пункт справа «Назначить сети», выбираем тип трафика, выбираем сеть и подтверждаем действие.

Типы трафика определяют обычный сетевой трафик и сети управления. Здесь трафик может быть разрешен в обеих сетях. Для настройки используем пункт «Назначить сетям». Кроме этого, вверху есть пункты «Создать сеть» и «Создать тип трафика». Первый создает сеть, с отдельным адресным пространством, в которой можно выполнить отдельные настройки обоих видов трафика, а второй создает пользовательский тип трафика, связанный с определенным портом. Кроме этого, на оба пункта можно настроить правила доступа к сетям и портам:



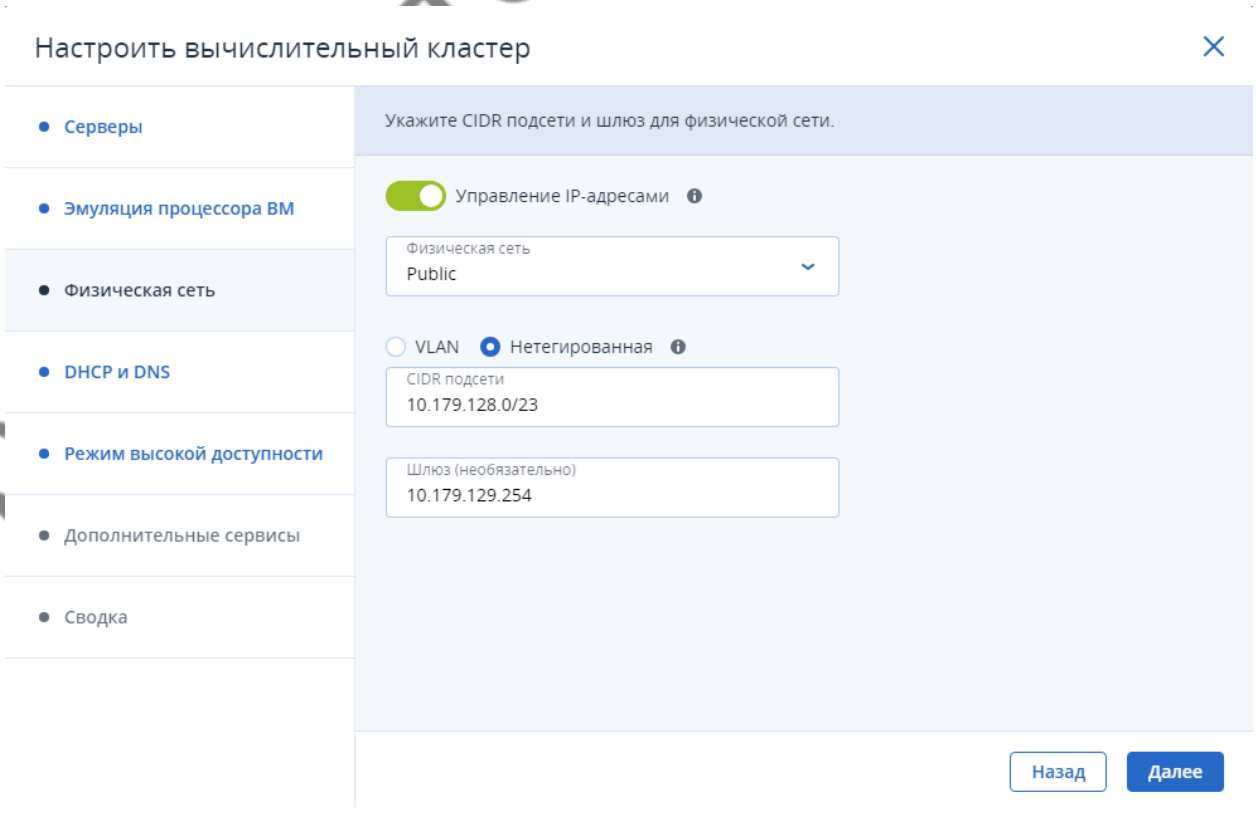
Настройка вычислительного кластера

Переходим в пункт «Вычисления»:

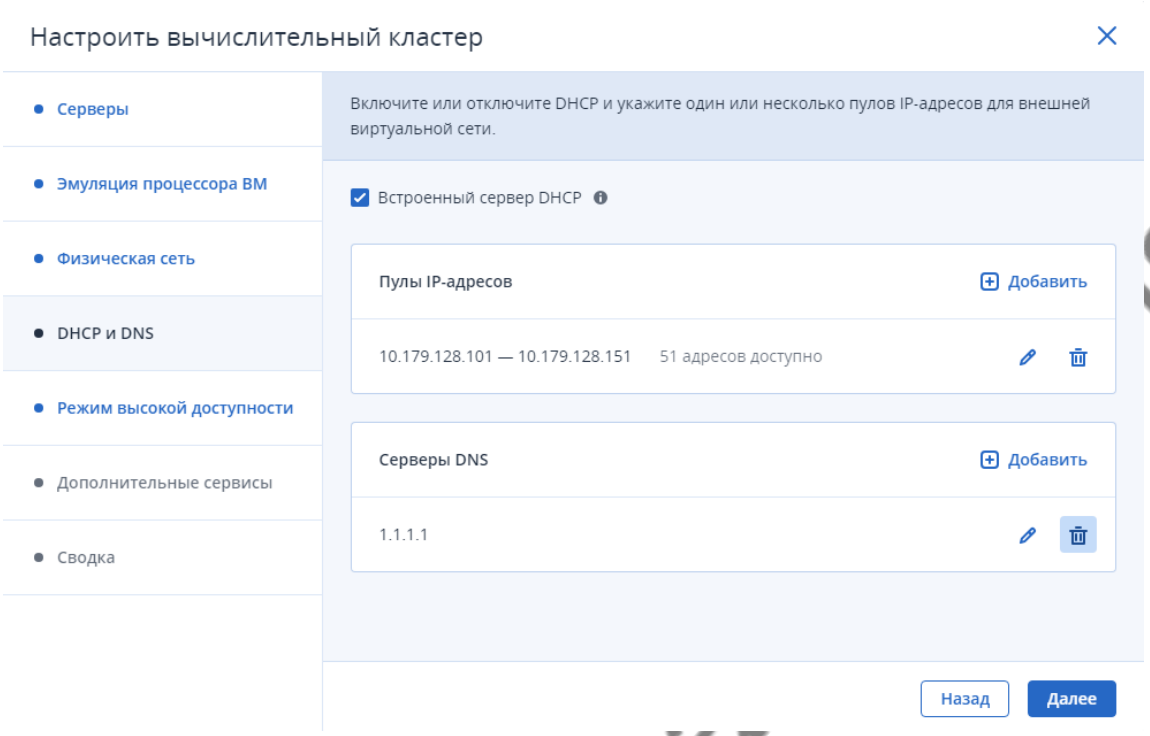


Нажимаем «Создать вычислительный кластер». Выбираем сервер (единственный). Выбираем тип виртуализации. При наличии нескольких серверов разных моделей и поколений можно выбрать разную стратегию виртуализации. В нашем случае де-факто все варианты одинаковы. Оставляем по умолчанию «Host-Model». Далее.

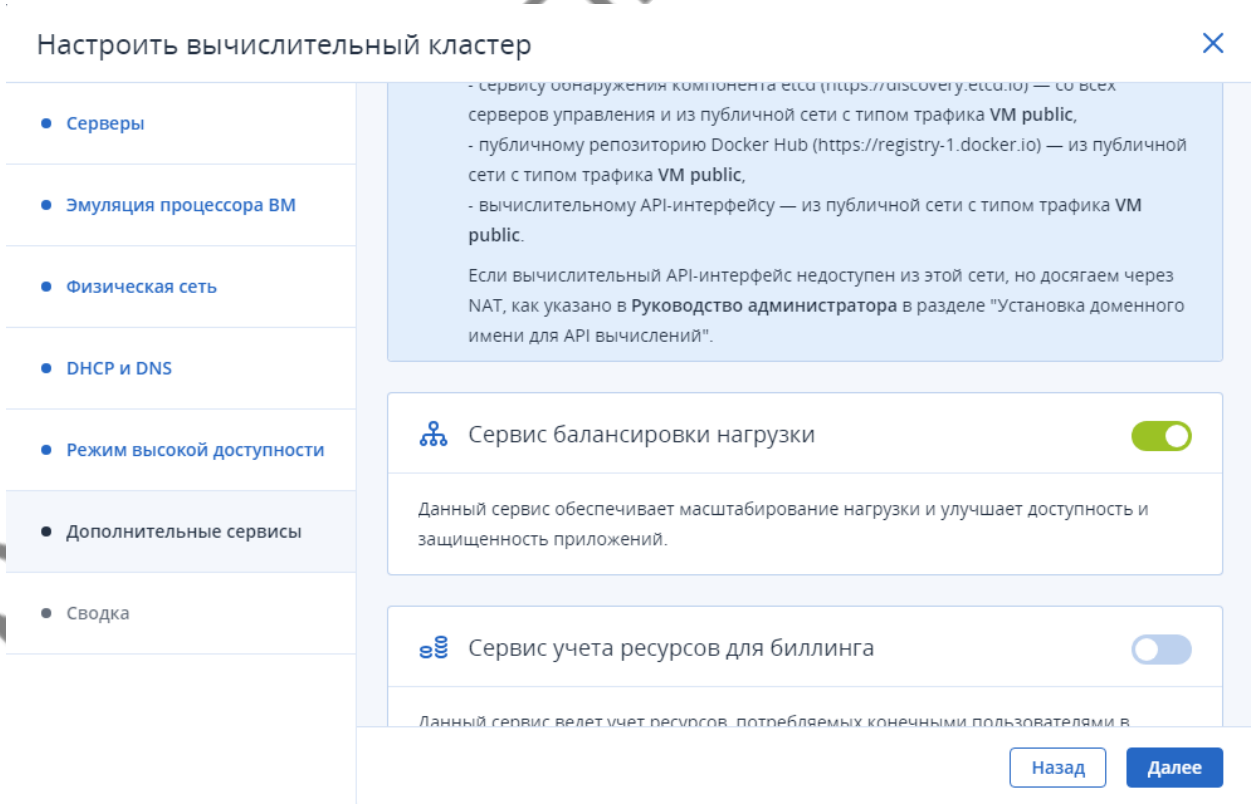
Настроим физическую сеть, с возможностью выдавать виртуальным машинам «белые» IP адреса для реализации прямого доступа в интернет:



Затем настроим внутренний DHCP сервер на выдачу адресов и параметров:



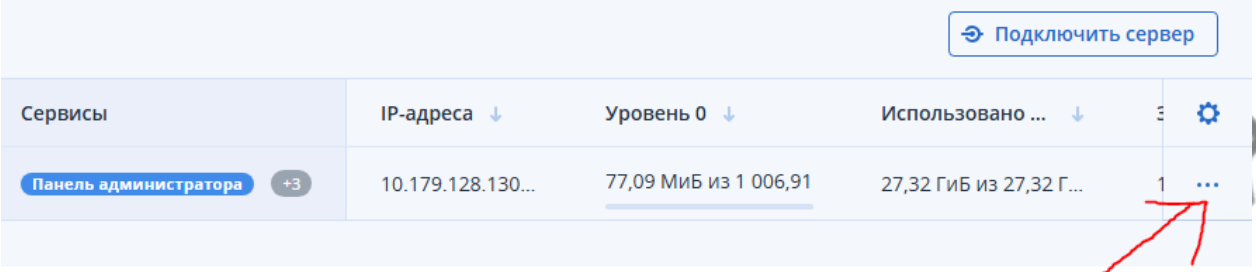
Далее режим «Высокой доступности» для нас не имеет смысла, поскольку только один сервер. Значение по умолчанию. Далее «Дополнительные сервисы». Сервис Kubernetes в данный момент мы рассматривать не будем, а вот сервис балансировки нагрузки нам понадобится. Впрочем, эти сервисы можно будет установить позже:



На последнем пункте отображена сводка, где мы можем проверить правильность выбранных параметров. После проверки нажимаем «Создать кластер» Эта операция может также занять, в зависимости от производительности "железа" некоторое время.

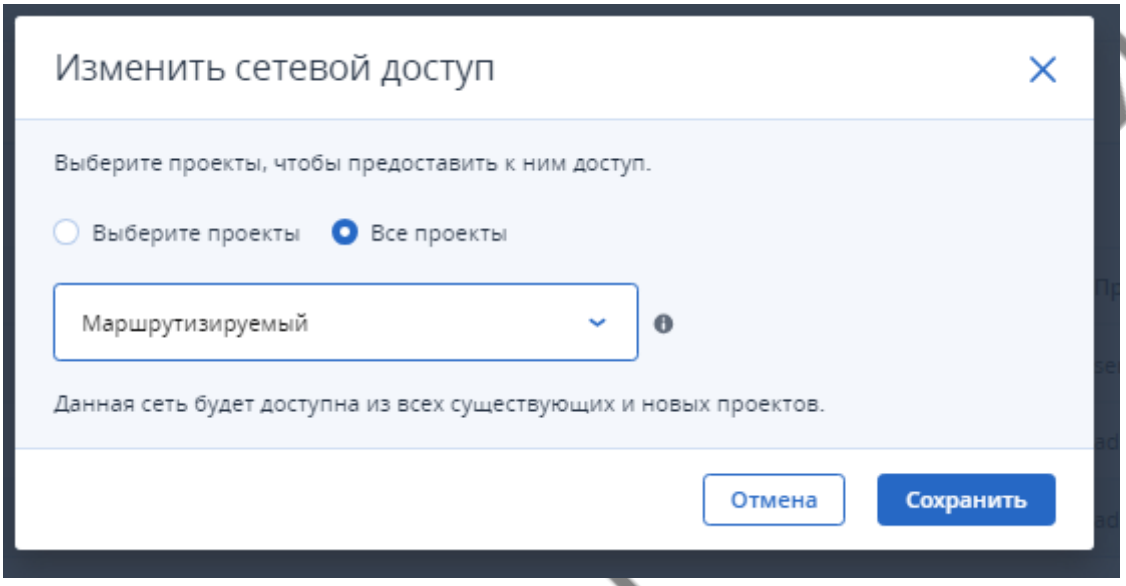
Подключение сервера

Теперь необходимо подключить к кластеру нашу ноду (сервер). Переходим «Инфраструктура» – «Серверы», выбираем наш сервер, три точки, подключить сервер:

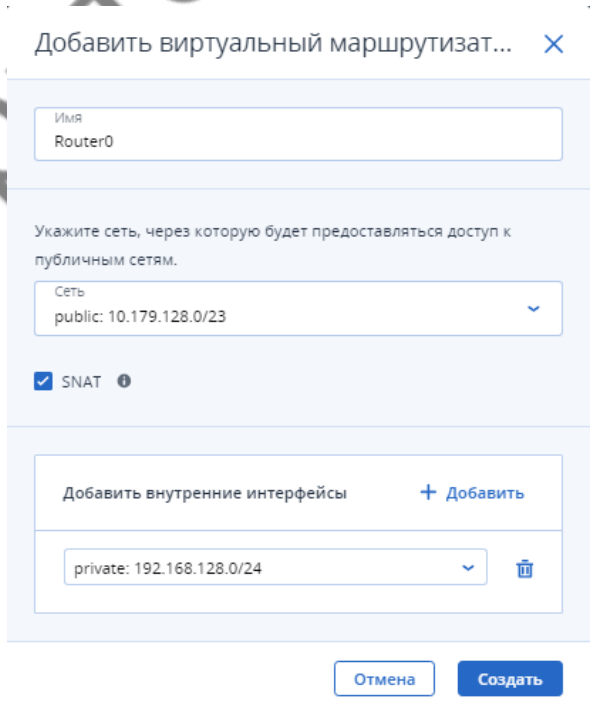


Настройка сети ВМ

Необходимо настроить сетевые параметры для виртуальных машин и пользователей проектов. Это необходимо для ограничения бесконтрольного доступа к физической сети. Они будут получать доступ к физической сети на основе маршрутизаторов и плавающего IP. Для этого идем «Вычисления» – «Сеть» выбираем сеть «public» – в открывшемся окне справа внизу – «Сетевой доступ» – «Изменить». Настраиваем для всех проектов маршрутизируемый доступ – «Сохранить».



Теперь настроим сеть «private». Нажимаем дважды на название, в открывшемся окне справа внизу «Подсети». Изменяем, выбираем подходящее нам параметры пула, DNS сервера, устанавливаем адрес шлюза, я выбрал последний адрес в сети. Шлюз нужен обязательно, иначе не удастся создать маршрутизатор. Сохраняем параметры. Далее, возвращаемся, и находим пункт меню - Маршрутизаторы, создаем новый маршрутизатор:



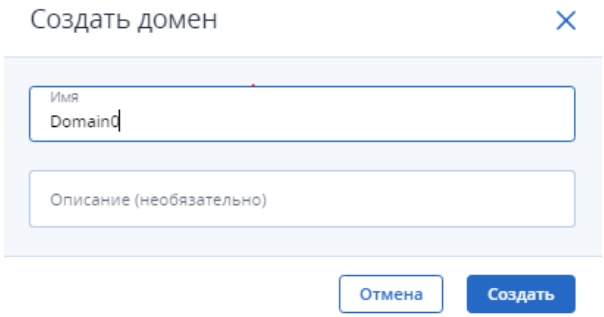
В дальнейшем мы настроим плавающие IP, когда создадим пользователей. На этом базовая настройка системы закончена.

Домен. Проект. Пользователи.

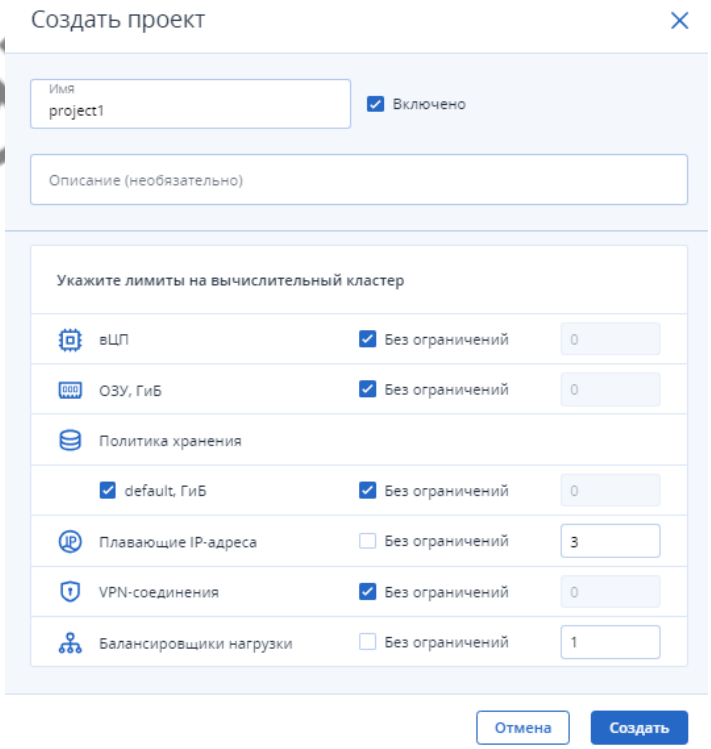
Создание домена и проекта

Корневым объектом для управления проектам, учетными данными пользователей, предоставлением ресурсов является домен. В рамках домена создается проекты и пользователи, устанавливается связь между ними. При создании пользователя выбирается его роль. Пользователю можно назначить одну из следующих ролей:

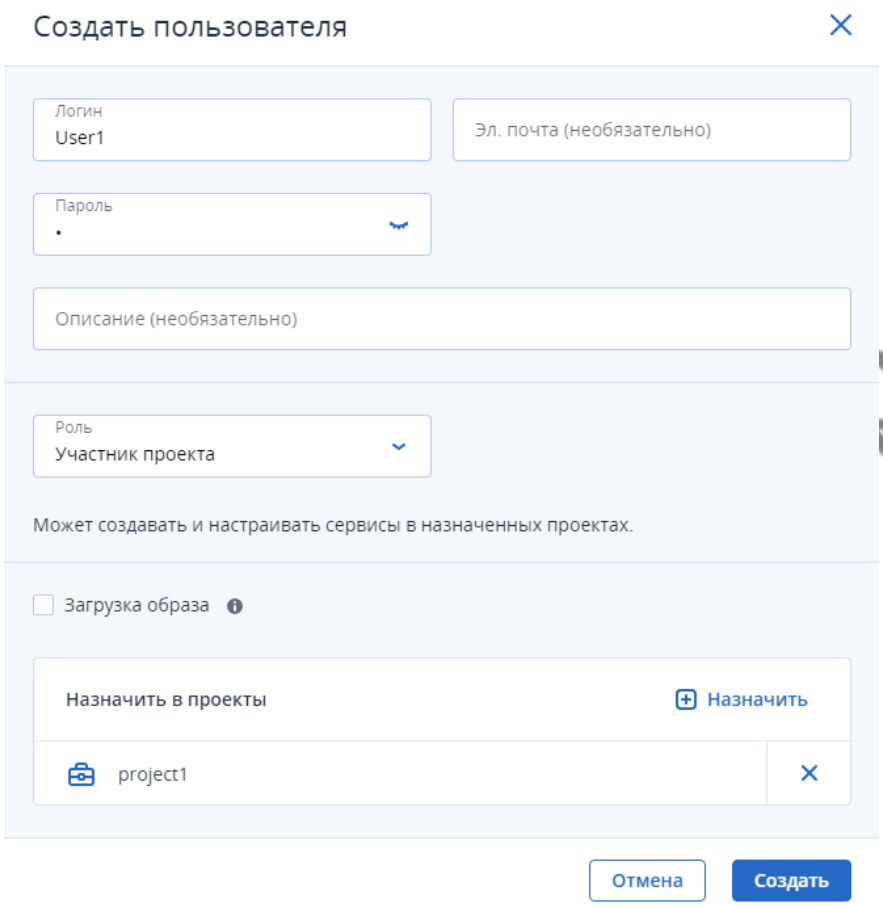
- **Администратор** домена может управлять виртуальными объектами во всех проектах внутри назначенного домена, а также назначением проектов и пользователей на панели самообслуживания.
- **Участник проекта** играет роль администратора проекта в определенном домене на панели самообслуживания. Участника проектов можно назначить на несколько проектов, тогда он будет управлять виртуальными объектами во всех этих проектах. С проектами можно выполнить следующие действия:
    - **Просмотреть и назначить** квоты проектов.
    - Назначить **участников** на проекты начнём с создания домена. Переходим в «Настройки» – «Проекты и пользователи» – «Создать домен».



Далее, выбираем наш домен, и создаем в нем проект, даем ему имя и указываем лимиты на ресурсы. Укажем 3 плавающих IP и один балансировщик нагрузки. Лимиты впоследствии можно изменить:



Далее, создадим пользователя и назначим его в проект. Роль у пользователя будет «Участник проекта». Назначим пользователя в созданный только что проект:



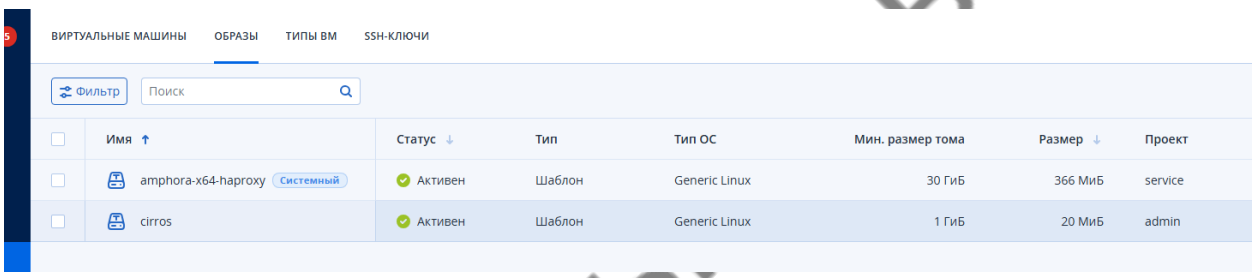
Кроме того, можно разрешить пользователям загружать образы ОС. Поскольку мы сами загрузим все необходимые образы, этот пункт отмечать не будем.

Загрузка образов

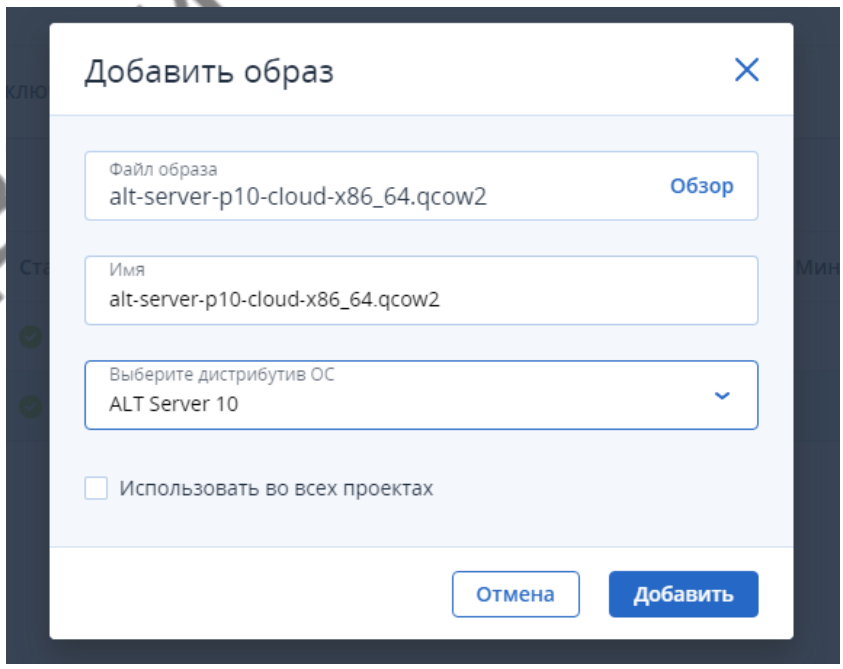
Теперь необходимо загрузить образ. Образы бывают двух типов:

- ISO-образ – это стандартный формат дистрибутивов ОС, которые необходимо устанавливать на диск. ISO-образ можно загрузить в вычислительный кластер.
- Шаблон – это готовый загрузочный том с установленной операционной системой и приложениями. Многие поставщики ОС предлагают шаблоны своих операционных систем, называя их облачными образами в формате .img, .qcow2, .raw.

Напоминаем вам, что можно дать право скачивать образы и дистрибутивы ОС пользователям. Настройку образов можно проводить по пути «Вычисления» – «Виртуальные машины», вкладка «Образы». В системе, в зависимости от конфигурации могут уже присутствовать образы, по крайней мере один – CirrOS. Это тестовый минимальный образ на ядре Linux. Поскольку Кибер Инфраструктура является "близким родственником" такого популярного решения, как OpenStack, то и тестовый образ наследуется оттуда. Обратите внимание, образы, помеченные как "системные" удалить нельзя:



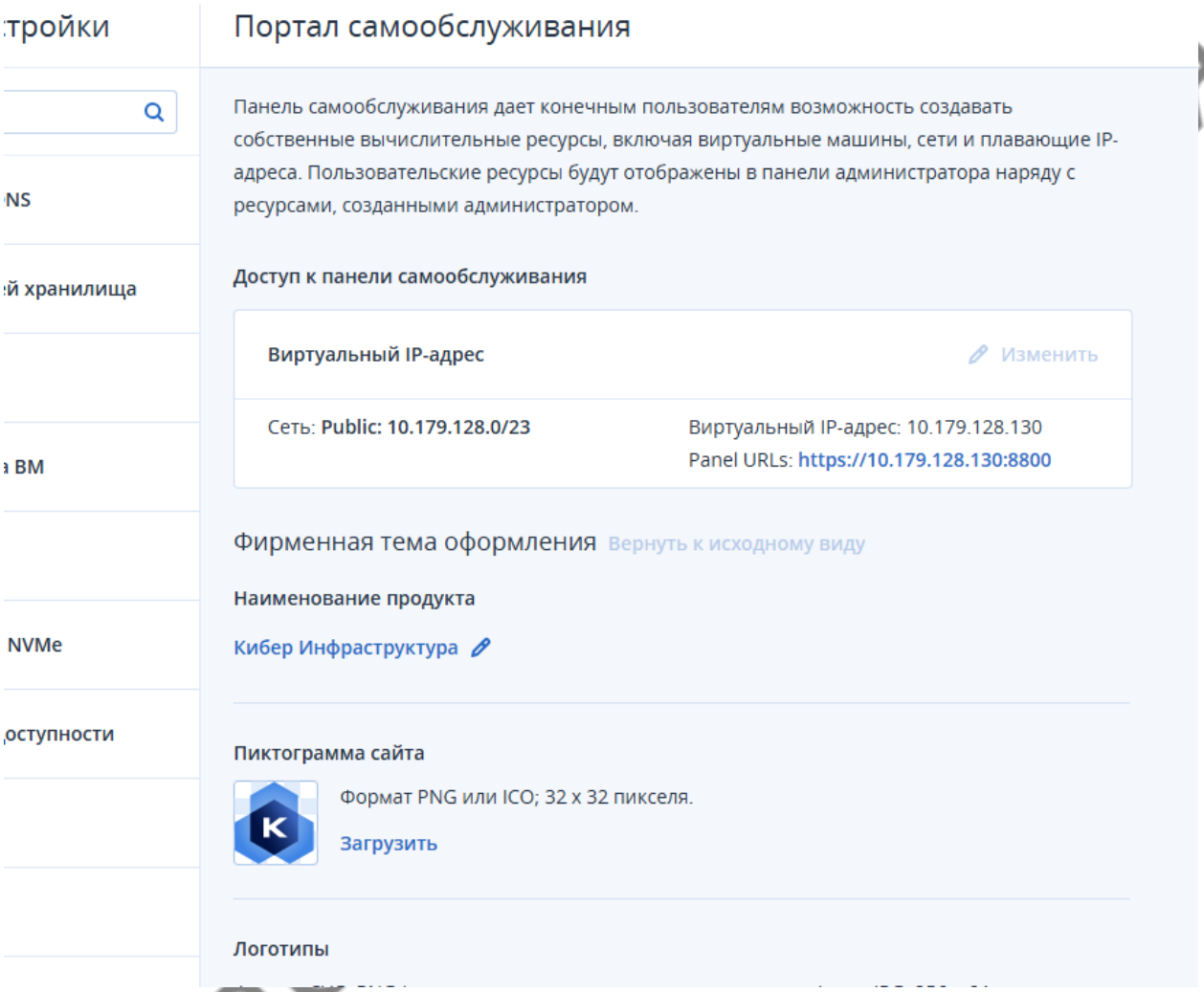
Давайте добавим образ ОС Альт Сервер 10, поскольку компания Базальт СПО подготовила удобный образ специально для облачной среды, уже с интегрированными сервисами Cloudbase-Init и OpenSSH Server. Также, он входит в список поддерживаемых гостевых операционных систем стр. 16 Официального Руководства по самообслуживанию. Для этого нажмем «Добавить образ» и загрузим предварительно скачанный образ ОС из одного из репозиториев:



После загрузки образа можно перейти в режим пользователя и переключится в панель самообслуживания.

Вход в портал самообслуживания

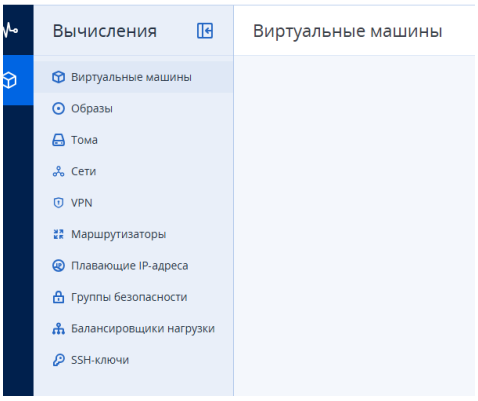
Портал самообслуживания нужен конечным пользователям для создания собственных вычислительных ресурсов, включая виртуальные машины, сети и плавающие IP-адреса. Параметры портала самообслуживания можно посмотреть и настроить по пути: Настройки - Системные настройки - Портал самообслуживания (последний пункт меню):



Тут мы видим адрес IP панели, в нашем случае совпадающий с IP адресом ноды. Порт по умолчанию - 8800. Перейдя по ссылке, попадаем в окно аутентификации, вводим данные. (если добавить в адресной строке имя домена, например https://10.179.128.130:8800/login/Domain0, то вводить домен не нужно). Все параметры чувствительны к регистру.

Портал самообслуживания

Интерфейс портала самообслуживания состоит из двух базовых элементов, раскрывающийся в подменю – МОНИТОРИНГ (пока пустой) и Вычисления. Вычисления, в свою очередь дают возможность создавать и управлять всеми доступными пользователю ресурсами:



Давайте кратко рассмотрим пункты меню:

Виртуальные машины (ВМ) - независимая система с независимым набором виртуального оборудования. Виртуальная машина представляет собой подобие обычного компьютера и работает аналогичным образом. Программные приложения могут работать в виртуальных машинах без каких-либо изменений или специальных настроек. Конфигурацию виртуальной машины можно легко изменить, например добавив новые виртуальные диски или память. Хотя виртуальные машины совместно используют одни физические аппаратные ресурсы, они полностью изолированы друг от друга (имеют отдельные файловые системы, процессы, переменные sysctl) и от вычислительного сервера. На виртуальной машине может работать любая поддерживаемая гостевая операционная система.

Образы - ISO-файлы и шаблоны, которые можно использовать для создания томов ВМ.

Тома - виртуальный дисковый накопитель, который можно присоединить к виртуальной машине.

Сети — это доступные физические и виртуальные сети, к которым можно подключать ВМ. Можно создать свою виртуальную сеть с собственным изолированным адресным пространством

VPN (VPN as a Service) – это возможность, с помощью которой пользователи могут соединять виртуальные сети через общедоступные сети, такие как Интернет.

Маршрутизаторы – сервисы L3, такие как маршрутизация и преобразование исходных сетевых адресов (SNAT), между виртуальными и физическими сетями либо различными виртуальными сетями.

Плавающий IP-адрес предназначен для доступа к ВМ из внешних сетей. Гостевая операционная система ВМ не имеет сведений о назначенном плавающем IP-адресе.

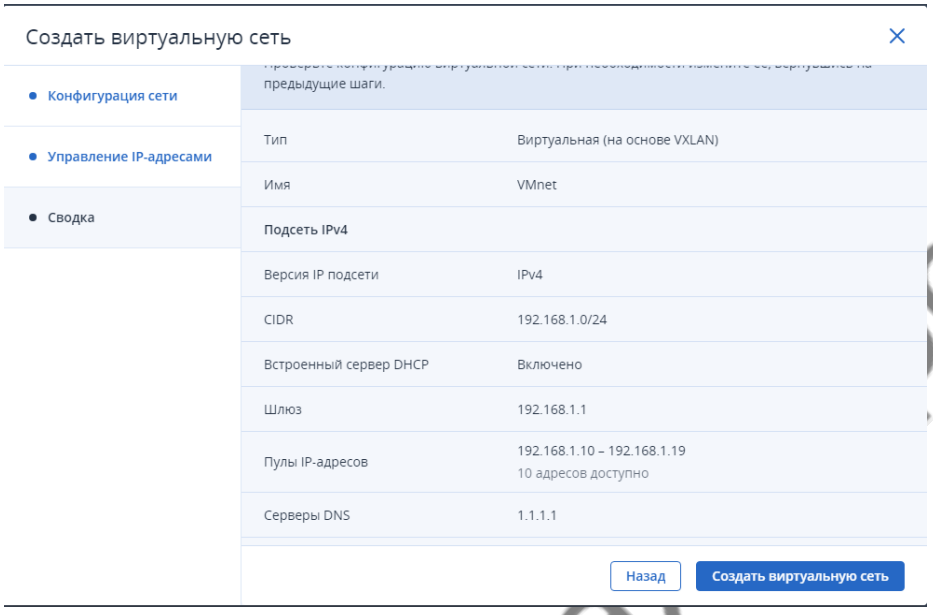
Группы безопасности – это наборы правил сетевого доступа, которые контролируют входящий и исходящий трафик виртуальных машин, назначенных в эту группу.

Балансировщики нагрузки обеспечивают отказоустойчивость и повышают производительность веб-приложений путем распределения входящего сетевого трафика по виртуальным машинам из пула балансировки

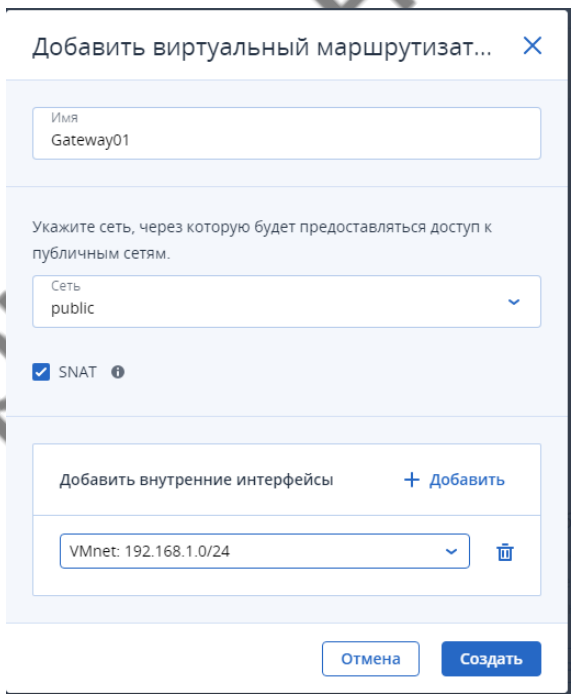
SSH-ключи применяются для защищенного SSH-доступа к виртуальным машинам.

Создание виртуальной машины

Первое, что нам необходимо сделать – создать внутреннюю виртуальную сеть, в которую мы поместим ВМ:



Далее, необходимо создать маршрутизатор, через который ВМ будут получать доступ в интернет:



Теперь, можно приступить к созданию ВМ. Выбираем меню Виртуальные машины – Создать виртуальную машину:

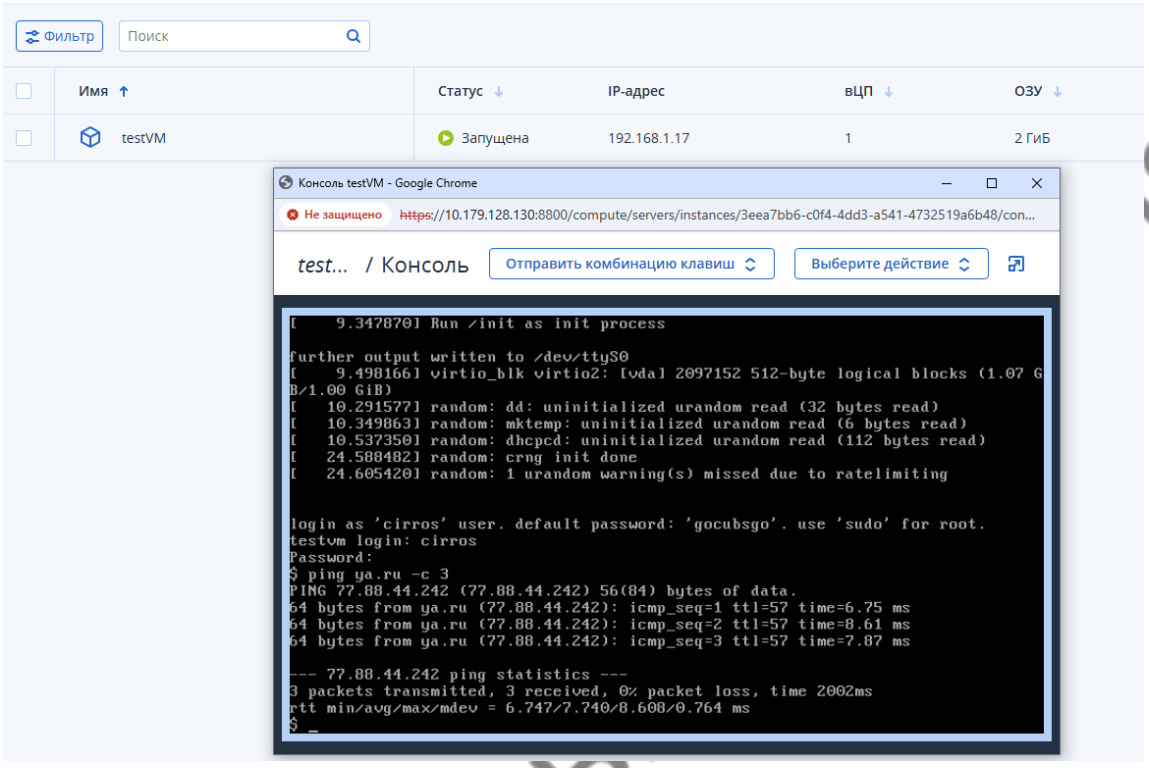
1. Даем имя ВМ. Указываем, что будем разворачивать ее из образа.

2. Выбираем образ cirros.

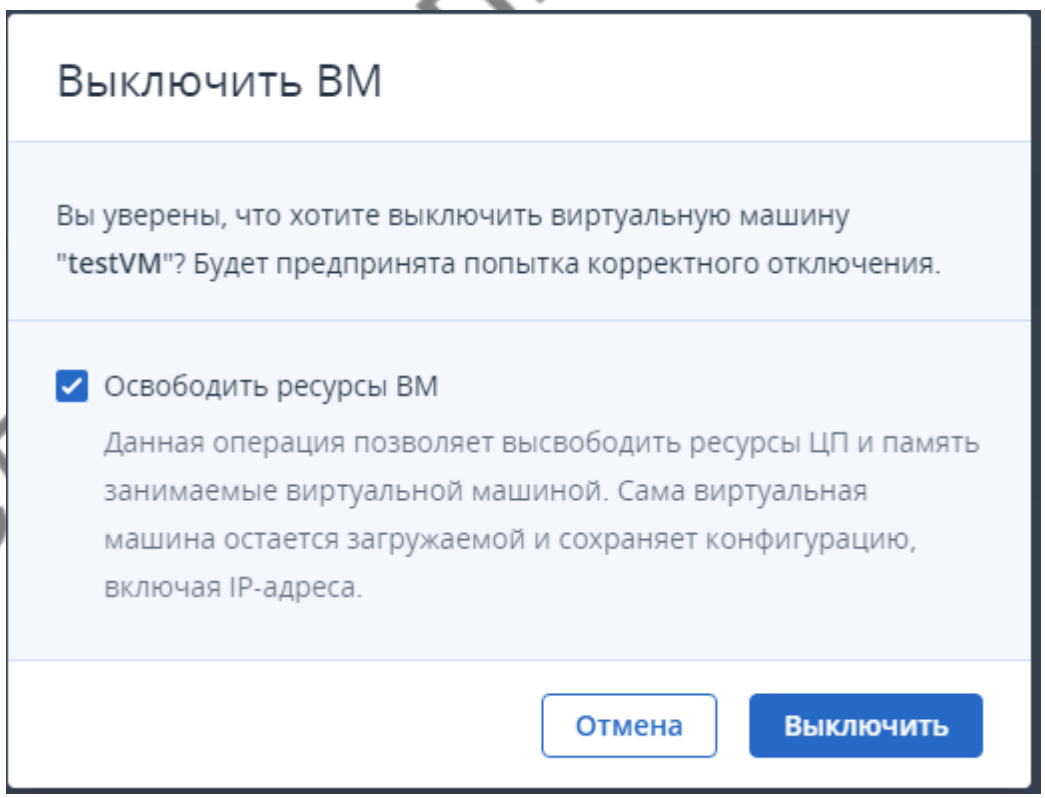
3. Тип — это "размер" нашей ВМ, то есть количество ресурсов, которое будет выдано данной машине. Выберем small.

4. Добавим сетевой интерфейс, из нашей только что созданной виртуальной сети Остальные параметры пока указывать не будем. Нажимаем Развернуть. Спустя некоторое время

виртуальная машина будет создана. Выбрав её, мы сможем войти в консоль, и введя дефолтные логин/пароль (cirros/gocubsgo) сможем войти в интерфейс ВМ и проверить доступ в интернет:

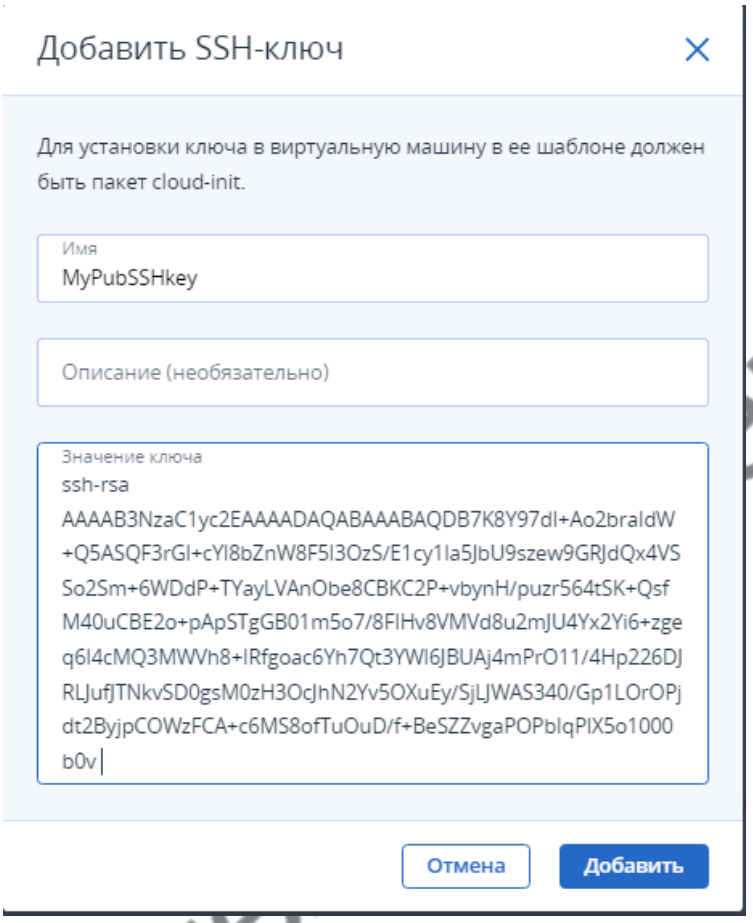


Выключим ВМ и освободим ресурсы:

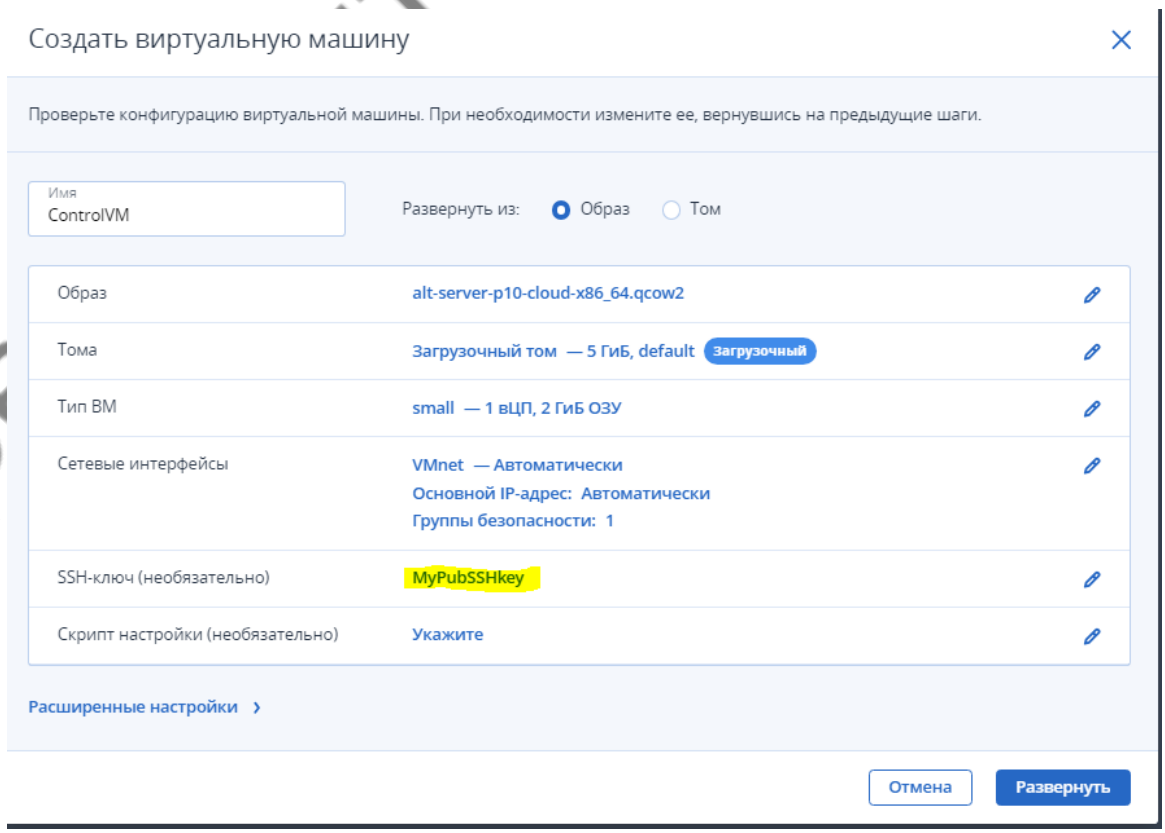


Однако, доступ к этой ВМ есть только через виртуальную консоль. Создадим другую ВМ, из образа Альт Сервер 10 и сконфигурируем доступ к ней по SSH с нашего компьютера. Для этого, нам необходимо проделать две дополнительные операции - добавить наш публичный ключ SSH в виртуальную машину, и подключить к ней плавающий IP.

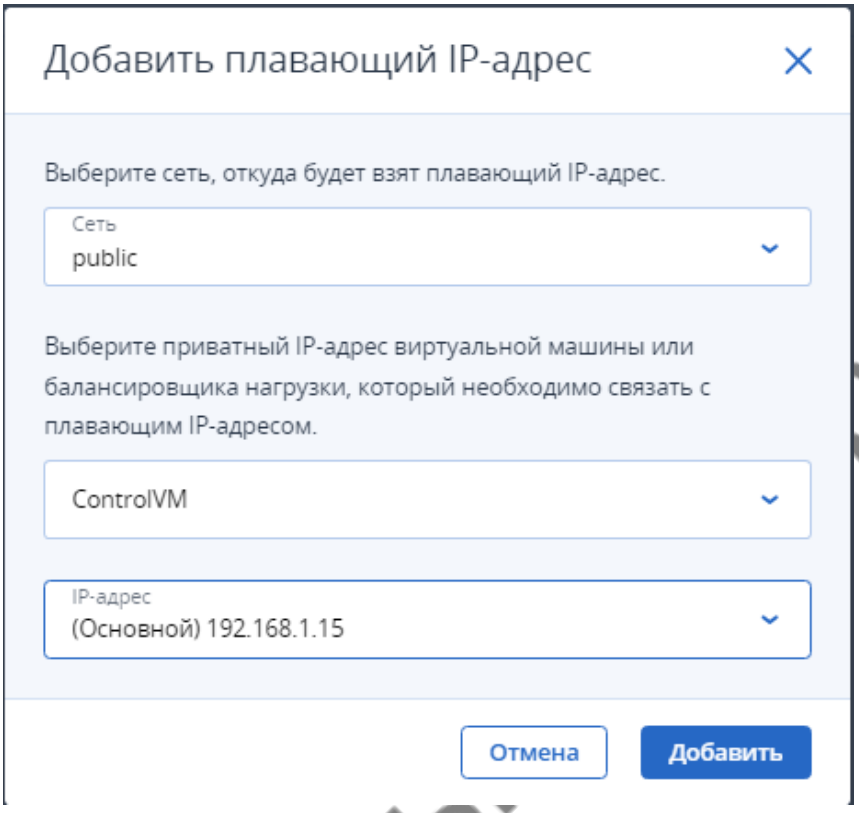
5. Переходим в пункт меню SSH ключи - Добавить SSH ключ, и добавляем заранее созданный публичный ключ (например, командой ssh-keygen -t rsa или любым online генератором):



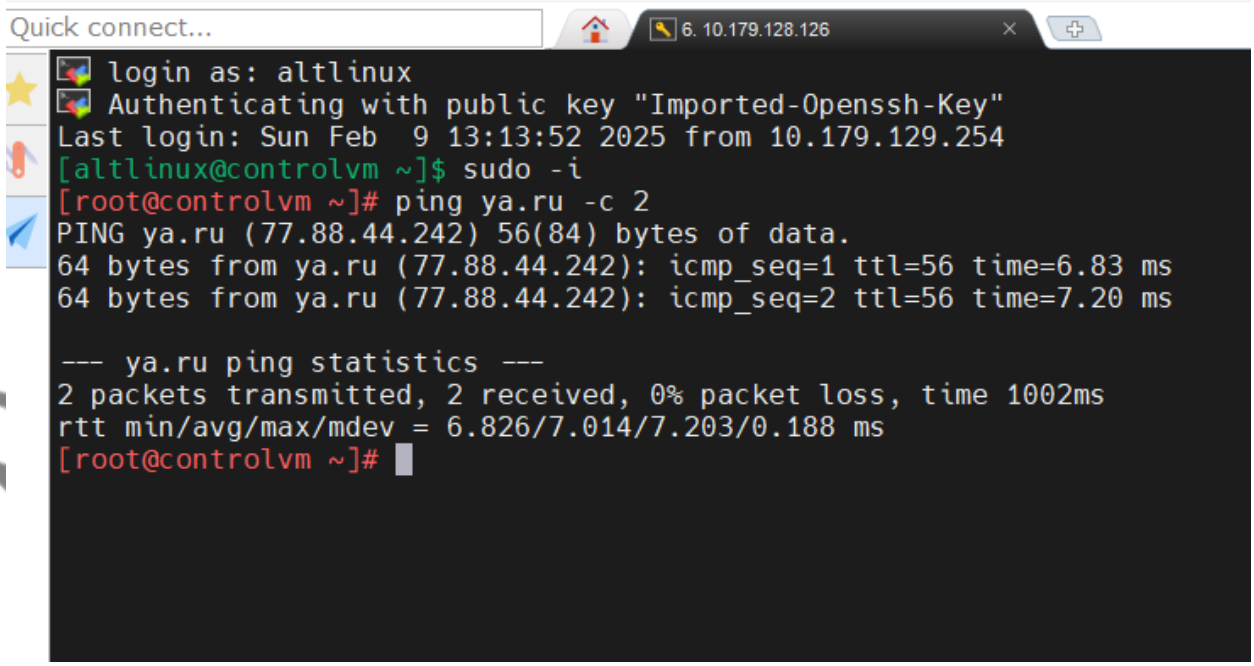
6. Создаем ВМ из образа Альт Сервер 10. В конце добавляем наш публичный ключ:



7. После запуска машины, добавляем к ней плавающий IP. Напоминаем, что плавающий IP-адрес предназначен для доступа к ВМ из внешних сетей:



Теперь у нас есть "белый" IP, по которому мы можем получить доступ к ВМ ControlVM. Обратите внимание, для подключения по SSH необходимо использовать приватный ключ из пары, созданной ранее. Мы будем использовать утилиту MobaXterm. В облачной версии Альт Сервер 10 используется учетная запись "altlinux" Введя sudo -i мы получаем права суперпользователя:



Таким образом, мы имеем доступ к ВМ со своего рабочего места, виртуальная машина имеет доступ в интернет, и может быть в дальнейшем использована для автоматизации развертывания инфраструктуры.

Автоматизация

Автоматизация (IaC)

Создавать ВМ в графическом режиме легко и просто. Алгоритм создания прост - Образ/том + тип ВМ (flavor) + сеть. При необходимости floating IP.

Если есть необходимость создавать штучные экземпляры (инстансы) ВМ, такой подход оптимален. Однако, как только появляется необходимость быстрой реакции на какие-то внешние события - увеличение/уменьшение нагрузки, изменение количества пользователей, быстрое развертывание/изменение/удаление инстансов - такой подход дает сбой.

Тут возникает потребность в автоматизации двух типичных видов облачных сервисов:

- Paas (Platform as a Service) - готовая платформа, как правило единичная.

- Iaas (Infrastructure as a Service) серверы, хранилище данных, сети, операционные системы.

Оба типа сервисов используют одну идеологию автоматизации - Infrastructure as Code (IaC)

Оба сервиса хорошо поддаются автоматизации различными инструментами.

В основном используют три вида таких инструментов:

- CLI - скрипты самой облачной инфраструктуры, характерной для каждого решения - например, а Yandex облаке это «yc», в Azure «Azure CLI». Однако многие решения гиперконвергентной инфраструктуры строится на открытом решении «OpenStack», имеющего свой «OpenStack command-line client». Это же решение используется в Кибер Инфраструктуре. Оно широко документировано, и имеет множество достоинств. «OpenStack CLI» используется для работы внутри проекта, для создания и настройки инстансов уже готовой Кибер Инфраструктуры. Однако, для создания, развертывания и настройки Кибер Инфраструктуры используется отдельный интерфейс командной строки «vinfra».
- Какая-либо система управления конфигурациями (SCM) которая позволяет автоматизировать настройку ПО. Наиболее популярное решение - «Ansible» имеет в своем составе целую коллекцию «Openstack.Cloud» и как пример, специализированный модуль «openstack.cloud.server» для создание и удаления инстансов.
- Специализированное решение развертывания и управления инфраструктурой «Terraform» для реализации концепции Infrastructure as Code (IaC). Используется специальные модули (провайдеры) подключения к облачным инфраструктурам. В нашем случае – «terraform-provider-openstack»

Два последних инструмента, особенно Ansible, используются в парадигме «декларативного программирования», когда мы используем множество инстансов, десятки и сотни, быстро меняющиеся ситуации и т.п. Инструменты используют свои форматы файлов, логику работы и обязательно требуют предварительного обучения.

Наша задача - научится основам автоматизации, и поэтому будем использовать OpenStack CLI

Установка и подключение OpenStack CLI

Для работы с openstack cli нам необходимы следующие пакеты (Названия актуальны для ОС Аль Сервер 10):

- python3-module-openstackclient — непосредственно сам клиент

- python3-module-octaviaclient — API балансировщика нагрузки

- python3-module-neutronclient — управление виртуальной сетевой инфраструктурой.

Для работы также могут быть использованы пакеты:

- sahara — среда обработки данных.

- cinder — блочное хранилище данных.

- glance — управление образами виртуальных машин.

- heat — оркестратор, позволяющий разворачивать из шаблонов инфраструктуру по принципу IaC.

- nova — контроль ресурсов — создание, запуск, перезапуск, остановка виртуальных машин и так далее.

- manila — предоставляет хранилища для совместно используемых или распределенных файловых систем.

Установим необходимое ПО, предварительно обновив список пакетов:

```
apt-get update && apt-get install python3-module-openstackclient python3-module-octaviaclient python3-module-neutronclient -y
```

Для подключения клиента openstack нужно экспортировать следующие переменные:

- OS_IDENTITY_API_VERSION — версия API.

- OS_PROJECT_NAME — имя проекта.

- OS_USER_DOMAIN_NAME — логический путь, где находится пользователь в openstack.

- OS_USERNAME — логин пользователя для входа в личный кабинет.

- OS_PASSWORD — пароль пользователя для входа в личный кабинет.

- OS_AUTH_URL — адрес подключения к API openstack.

-Кроме этого, поскольку мы не установили безопасный канал между машиной управления и инфраструктурой, то необходимо указать, что используем небезопасные методы:

OS_INSECURE=true

Создадим скрипт аутентификации, который позже сможем включать к скрипты автоматического создания ресурсов

`vim user-openrc.sh`

со следующим содержимым:

```
export OS_IDENTITY_API_VERSION=3
export OS_PROJECT_NAME=project1
export OS_USER_DOMAIN_NAME=Domain0
export OS_USERNAME=User1
export OS_PASSWORD=1
export OS_AUTH_URL=https://10.179.128.130/:5000/v3
```

```
export OS_INSECURE=true
```

Экспортируем переменные:

```
source user-openrc.sh
```

Проверим возможность подключения, например получив список инстансов нашего проекта

```
openstack --insecure server list
```

ключ "--insecure" нужен поскольку мы не произвели обмен ключевой информацией.

В случае успеха получаем список инстансов:

```
[altlinux@controlvm ~]$ openstack --insecure server list
+--------------------------------------+-----------+--------+----------------------------------+--------------------------+--------+
| ID                                   | Name      | Status | Networks                         | Image                    | Flavor |
+--------------------------------------+-----------+--------+----------------------------------+--------------------------+--------+
| 58c5d2b9-498d-424d-8f32-bc3e75d8fea4 | ControlVM | ACTIVE | VMnet=10.179.128.127, 192.168.1.15 | N/A (booted from volume) | small  |
+--------------------------------------+-----------+--------+----------------------------------+--------------------------+--------+
[altlinux@controlvm ~]$
```

Создание профиля Putty

Большинство создаваемых ВМ на основе ядра Linux не используют графический интерфейс. Основным протоколом, по которому мы подключаемся к инстансам является SSH

Для подключения к ВМ в инфраструктуре можно использовать различные эмуляторы, однако наиболее популярным является «PuTTY»

Рассмотрим методику подключения на основе элемента задания чемпионата "Профессионалы" по компетенции "Сетевое и системное администрирование".

с) Настройка внешнего подключения к ControlVM:

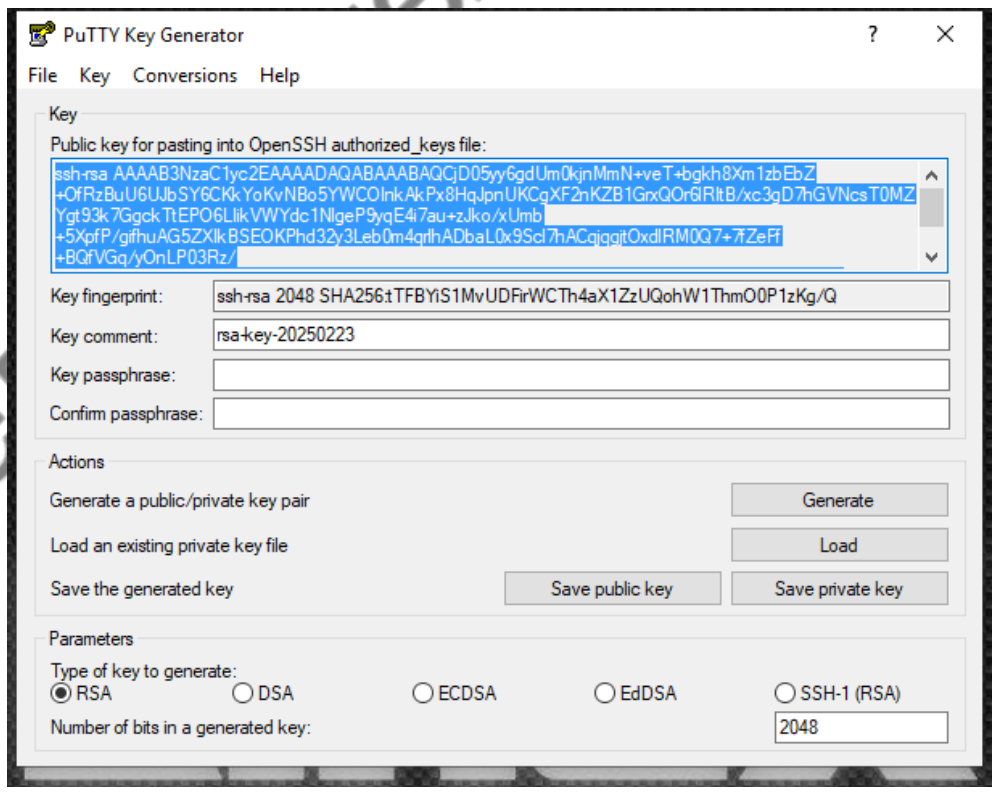
1. Установите на локальный ПК клиент SSH **PuTTY**.
2. Создайте в PuTTY профиль с именем **cloud**.
3. Убедитесь в возможности установления соединения с инстансом ControlVM с локального ПК через PuTTY, без необходимости ввода дополнительных параметров.
4. Для подключения используйте имя пользователя **altlinux** и ранее сохранённую ключевую пару.

Последовательное выполнение шагов:

1) Установка приложения из официального сайта (https://www.putty.org/)

2) Посредством приложения PuTTYgen в графическом режиме (Windows) или в командной строке (Linux) создаем ключевую пару:

1) Windows:

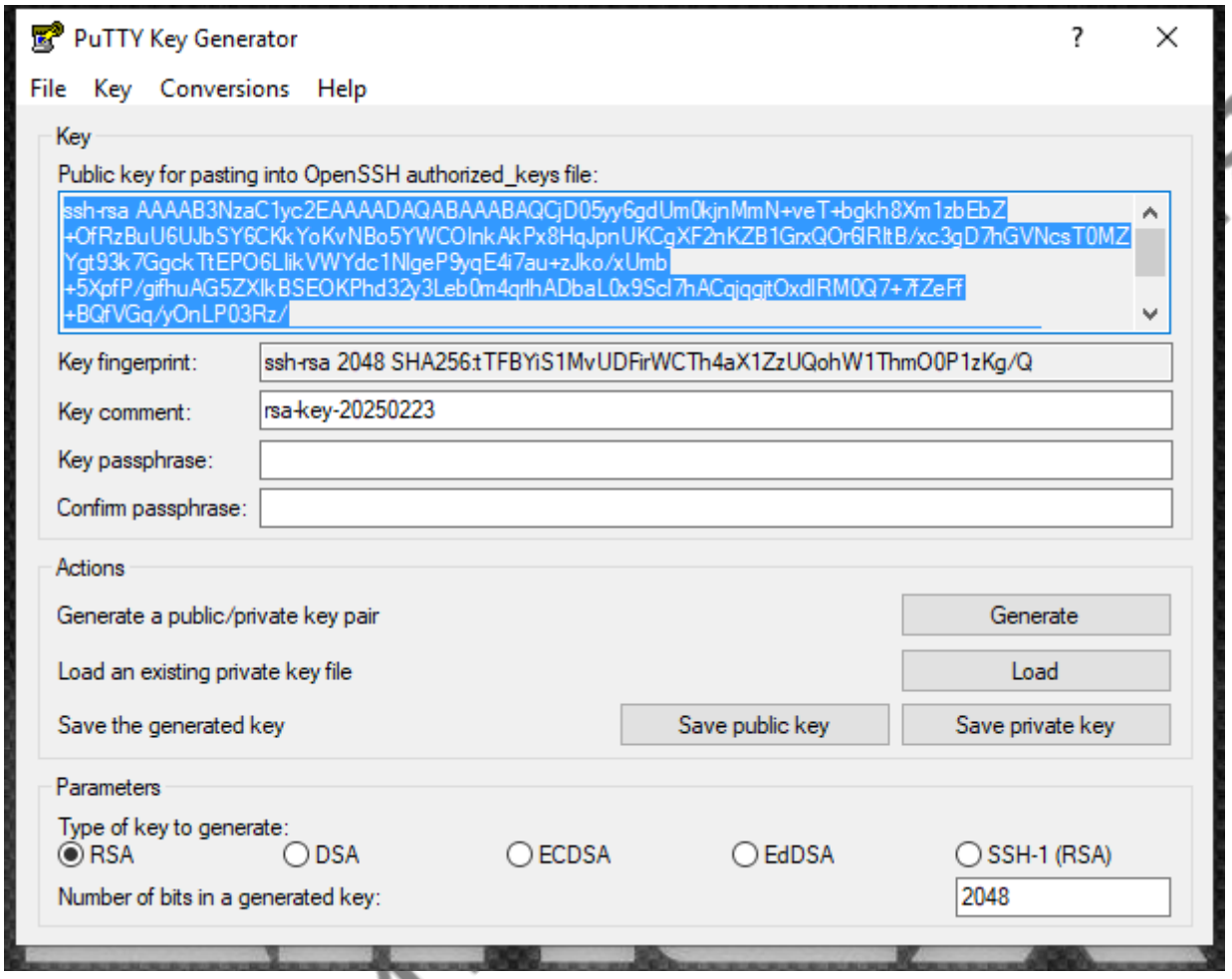


Копируем публичный ключ через Ctrl+C

Важно! После ssh-rsa и ключом ПРОБЕЛ. Публичный ключ в одну строку!

Сохраняем приватный ключ.

Загружаем ключ в проект



Подробнее – «5. Создание виртуальной машины»

2. Linux.

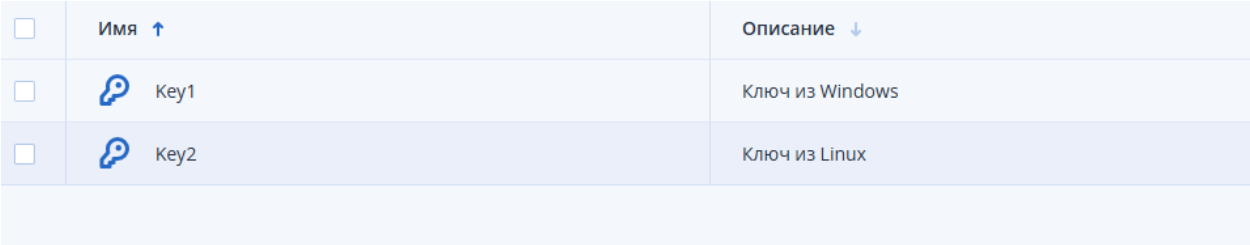
Генерируем ключевую пару с помощью конструкции:

```
puttygen -t rsa -o Lin_key.ppk && puttygen -L Lin_key.ppk > pub
```

```
[admn@host-1 keys]$ puttygen -t rsa -o Lin_key.ppk && puttygen -L Lin_key.ppk > pub
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Enter passphrase to save key:
Re-enter passphrase to verify:
[admn@host-1 keys]$ ls -l
итого 8
-rw------- 1 admn admn 1458 фев 23 17:35 Lin_key.ppk
-rw-r--r-- 1 admn admn  398 фев 23 17:35 pub
[admn@host-1 keys]$
```

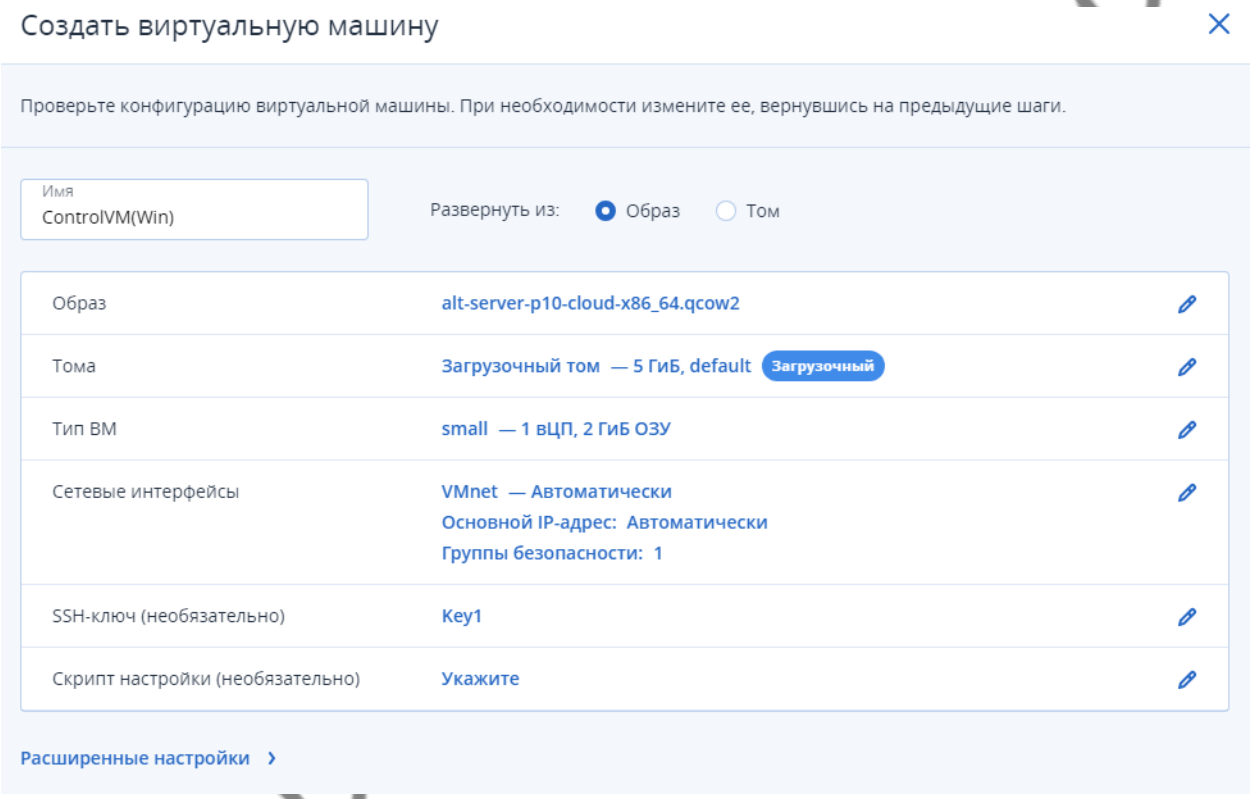
где первая половина команды генерирует приватный ключ Lin_key.ppk, а вторая копирует его открытую часть в файл pub.

Далее, копируем содержимое pub и создаем SSH ключ в инфраструктуре

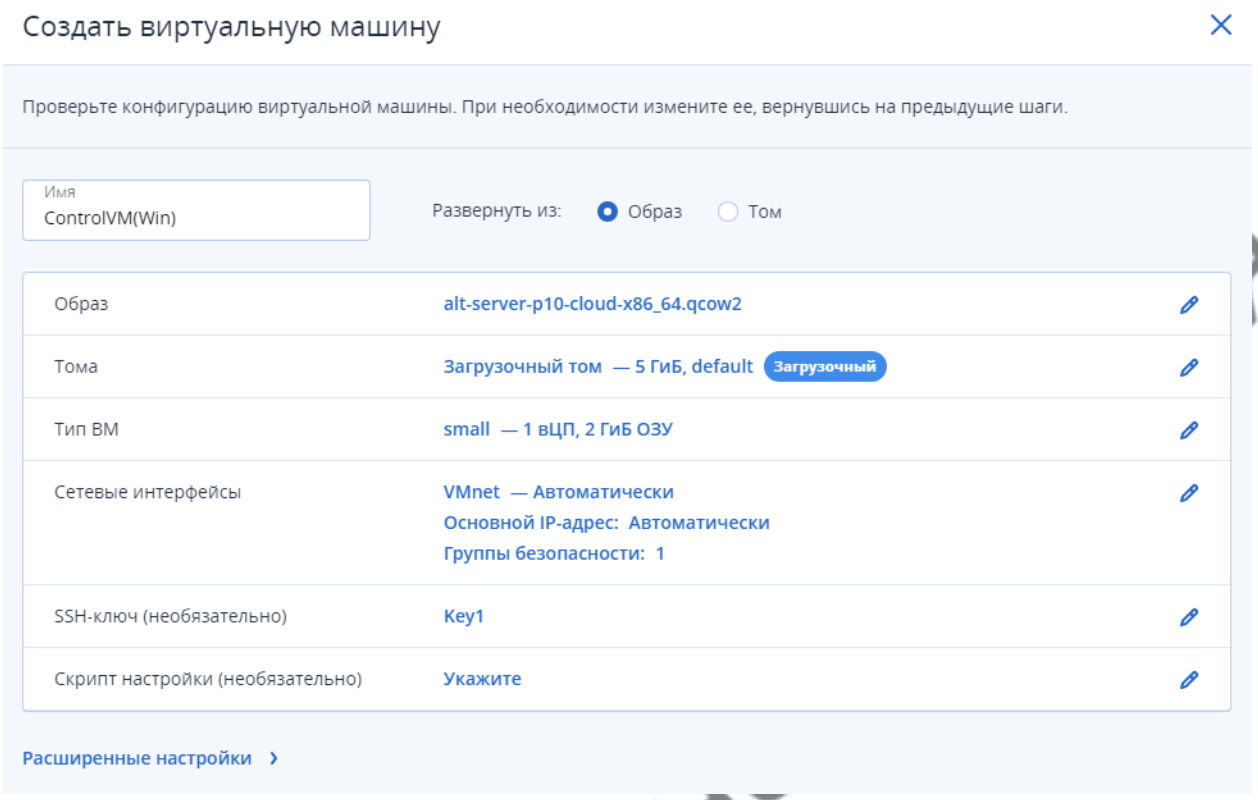


После этого, создаем ВМ, способом описанным в «Создание виртуальной машины», подключая ключ в конфигурацию ВМ

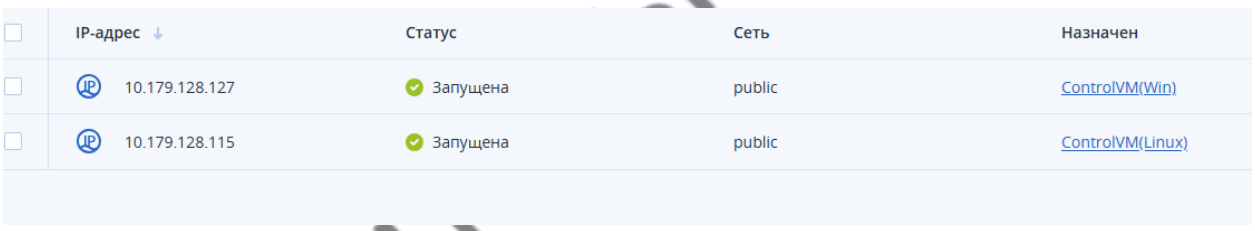
3. Первый ключ, созданный в Windows



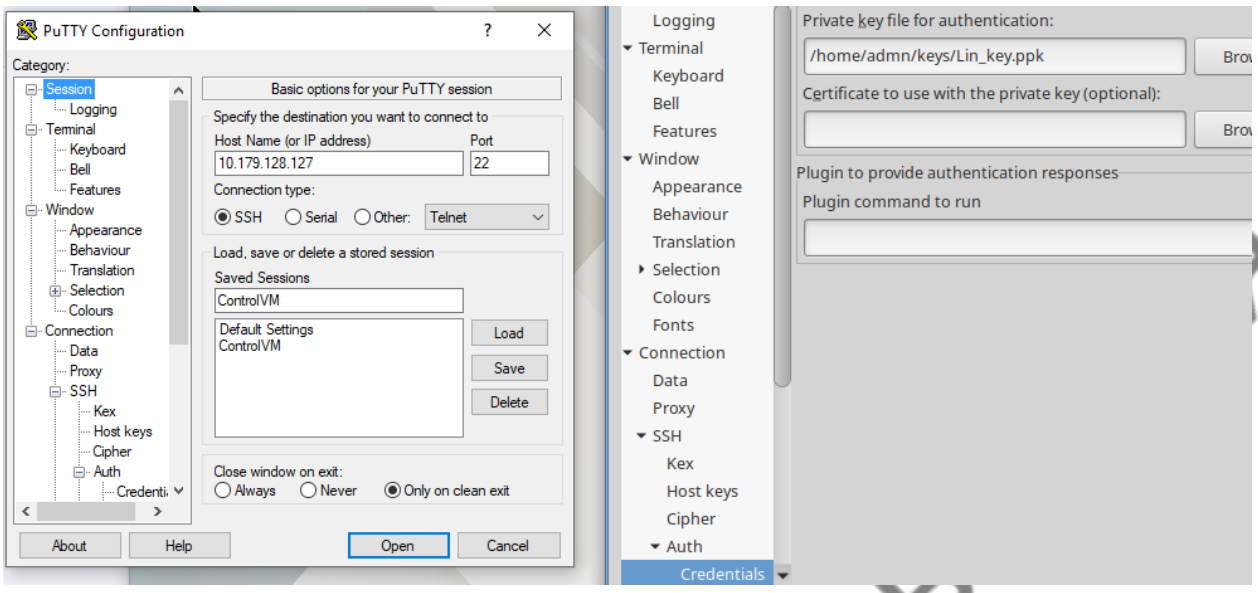
4. Второй ключ, созданный в Linux:



3. Назначаем инстансам плавающие адреса:



1. Настраиваем PuTTY
    1. Создаем профиль
    2. Прописываем соответствующие IP адреса
    3. Подключаем приватный ключ SSH - Auth - Credentials

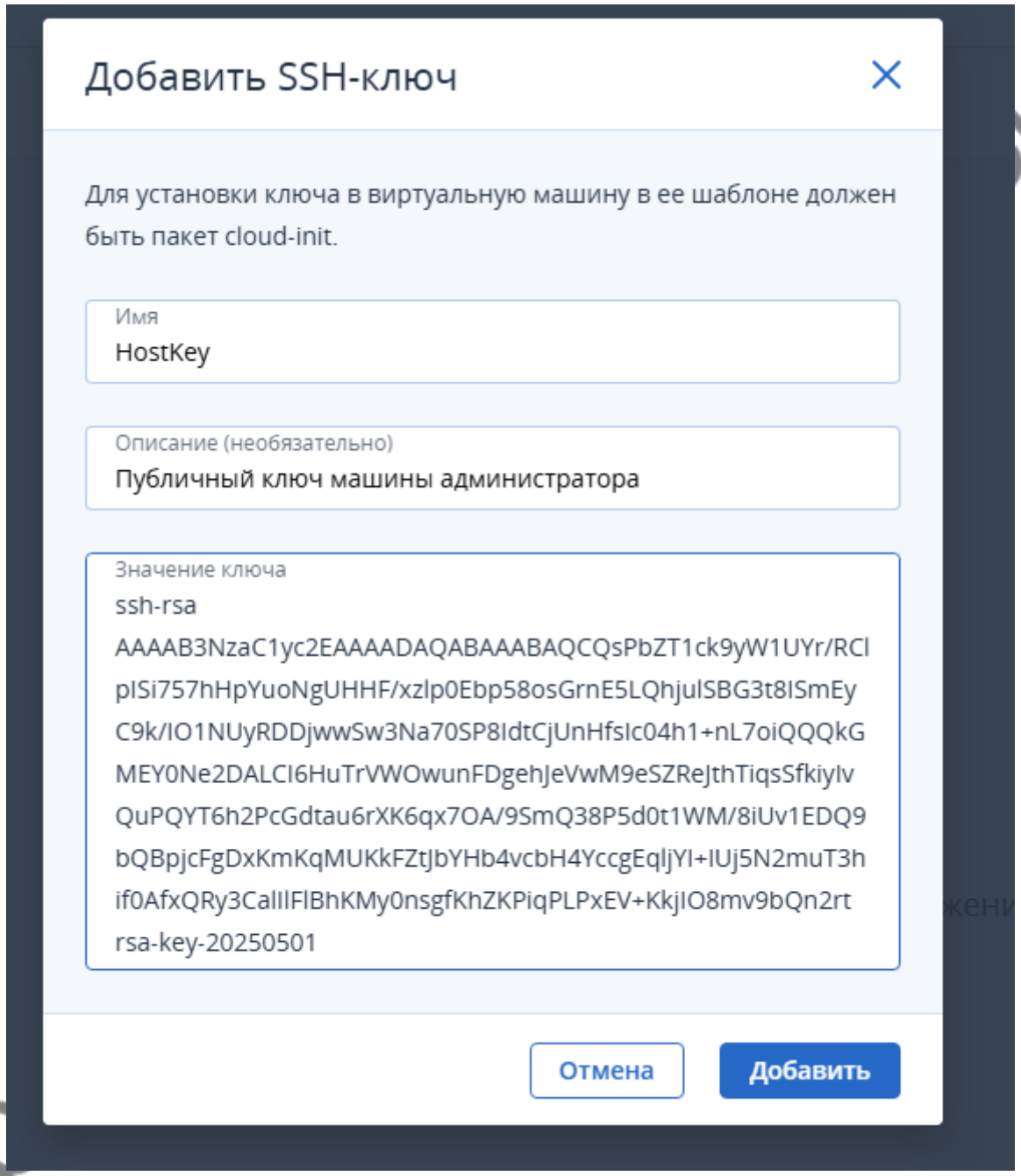


4. Connection - Data - Auto-login username - пишем altlinux

Работа в CLI

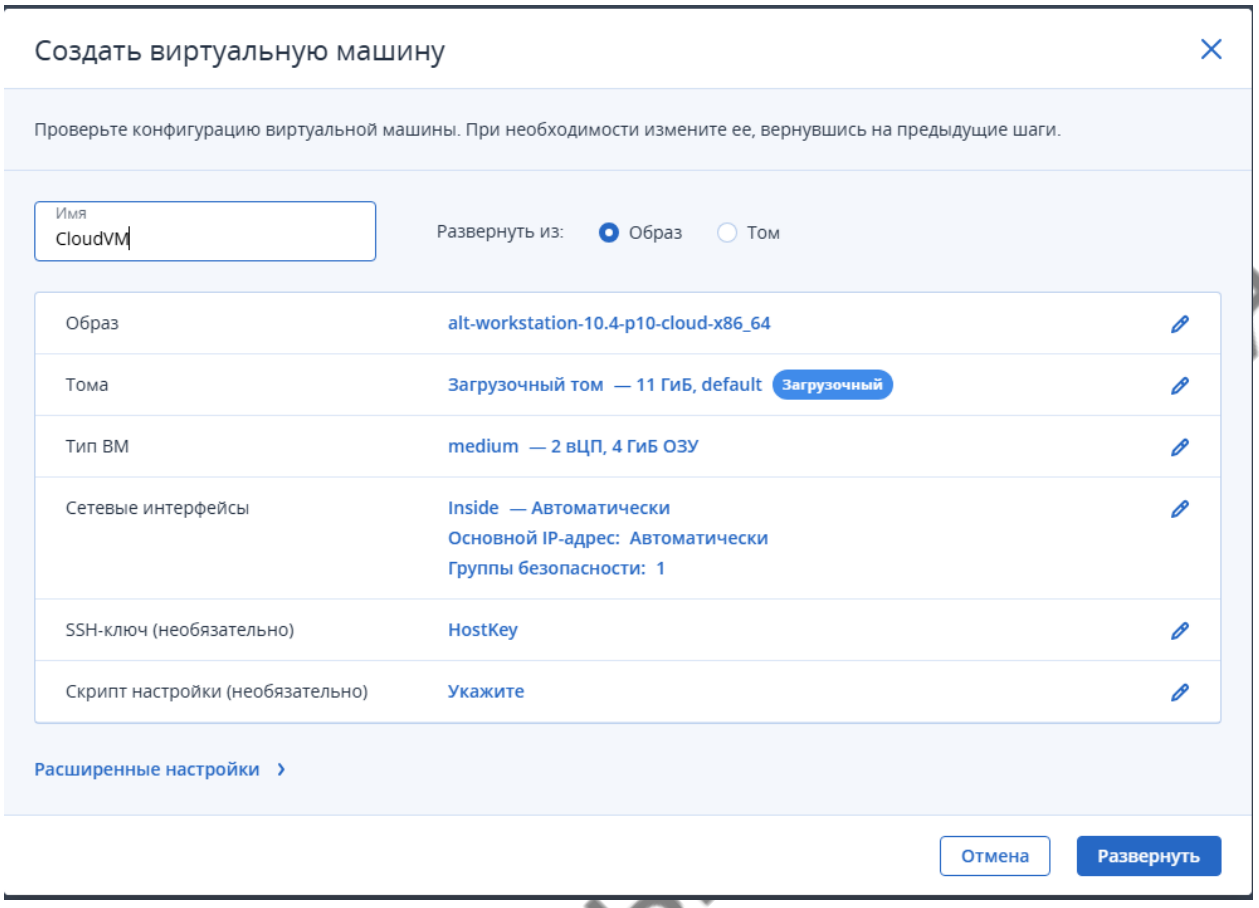
Начало работы

Для начала создадим (либо используем уже созданный) публичный SSH ключ хоста администратора, с которого мы будем подключатся к внутреннему инстансу, через который будем работать.



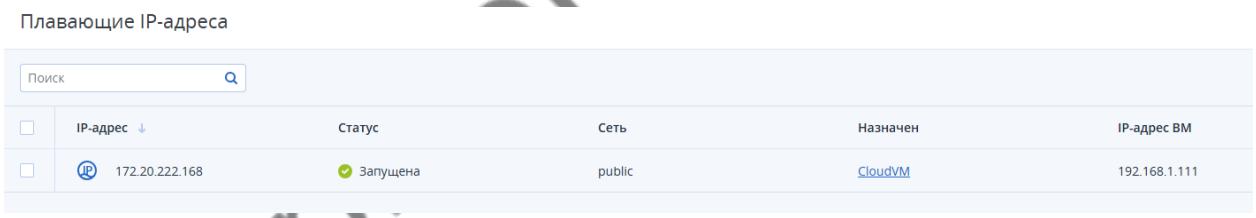
Создание ключа рассмотрено в разделе «3. Создание профиля PuTTY»

Далее нам необходимо создать инстанс (ВМ). В экспериментальных целях создадим ее с графическим интерфейсом, а так же подключим уделенный доступ по протоколу RDP

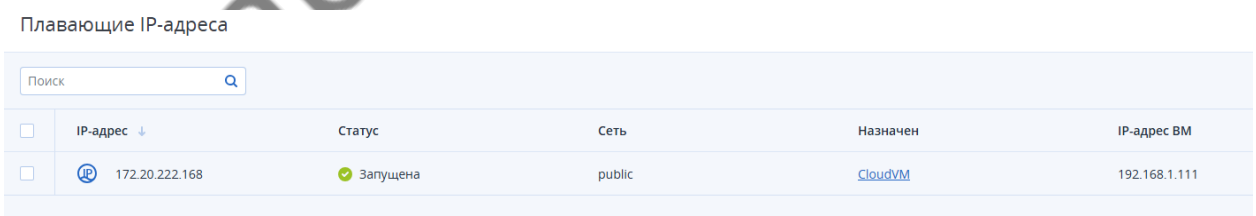


Параметры ВМ

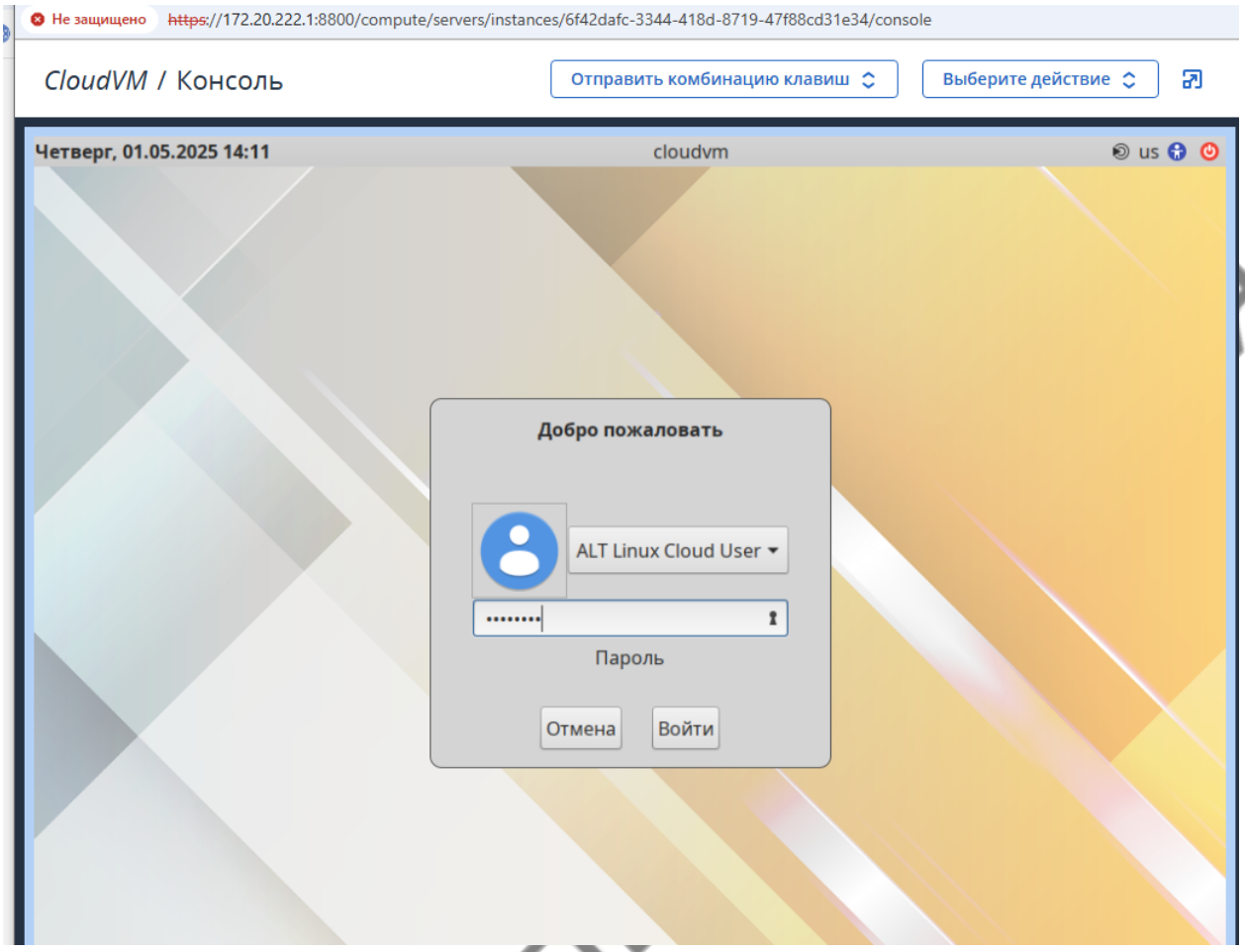
Подключим к ней плавающий IP



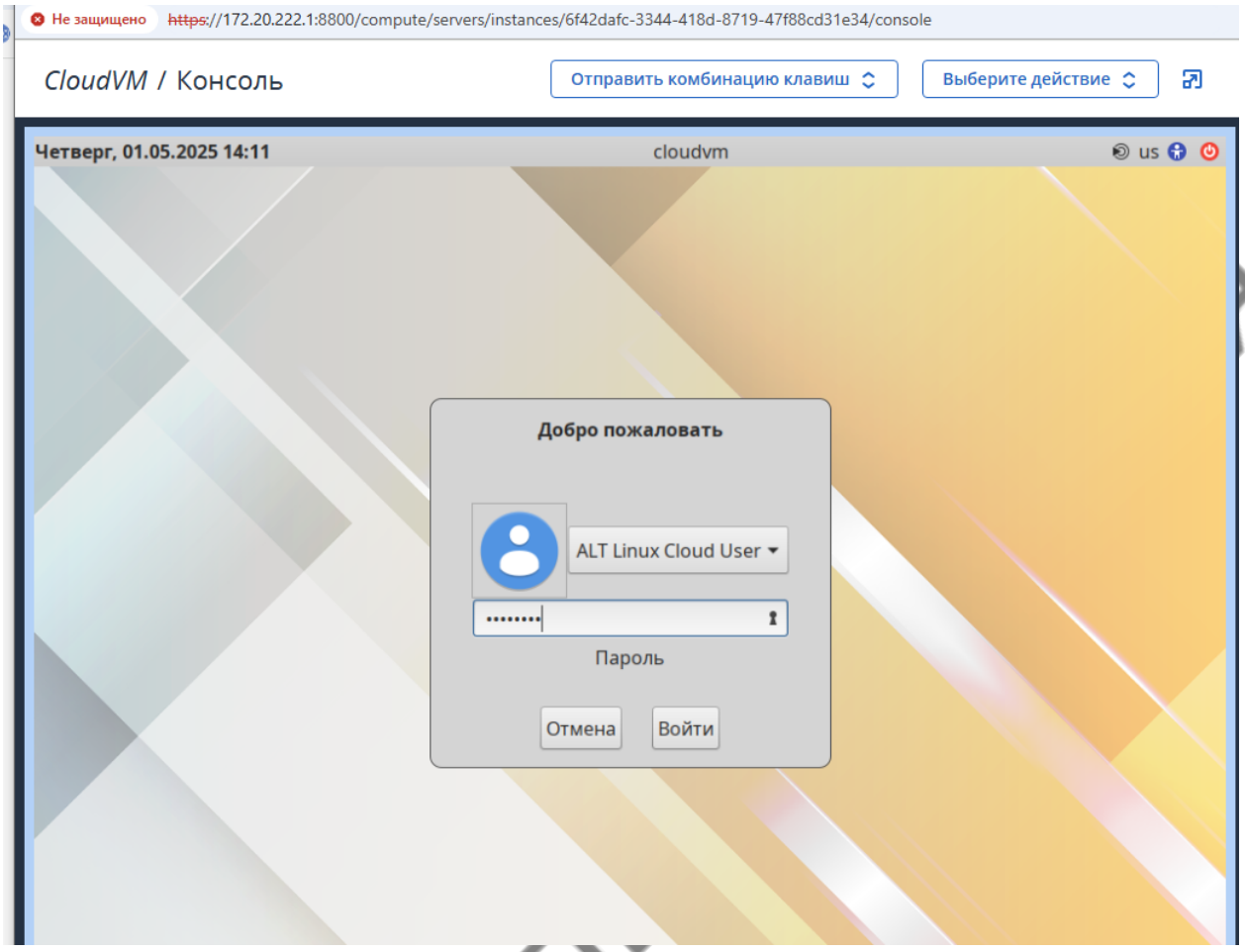
Теперь подключимся к ней по SSH, например через PuTTY



Создадим пароль для пользователя altlinux (не рассматриваем) и после создания пароля войдем на CloudVM через консоль



Для работы по протоколу RDP необходимо установить серверную часть пакета xrdp (не забудьте обновить список пакетов)



Далее, настраиваем автозапуск сервера и помещаем текущего пользователя в группу tsusers

```
# systemctl enable --now xrdp xrdp-sesman


# usermod -aG tsusers altlinux
```

Настройки сервера хранятся в файле /etc/xrdp/sesman.ini. Некоторые настройки сервера, установленные по умолчанию:

- AllowRootLogin=true — авторизация Root;

- MaxLoginRetry=4 — максимальное количество попыток подключения;

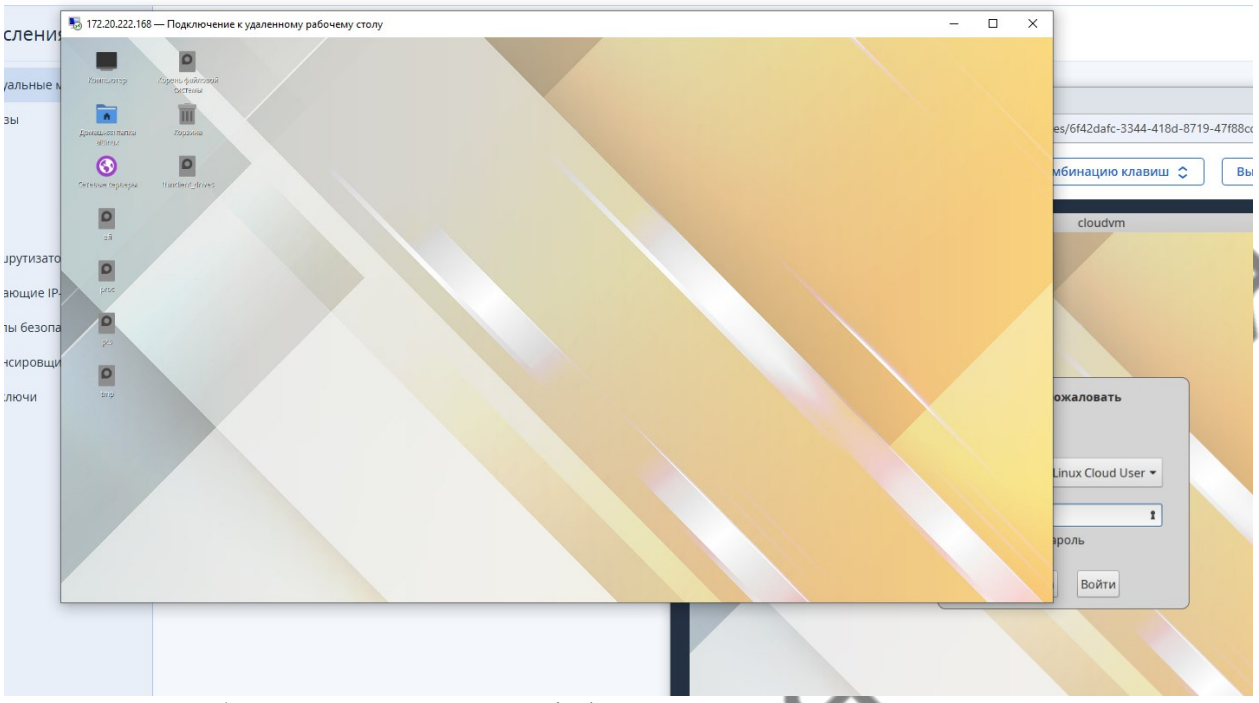
- TerminalServerUsers=tsusers — группа, в которую необходимо добавить пользователей для организации доступа к серверу;

- MaxSessions=50 — максимальное количество подключений к серверу;

- KillDisconnected=false — разрыв сеанса при отключении пользователя;

- FuseMountName=Mount_FOLDER — название монтируемой папки.

По умолчанию для подключения по RDP используется порт 3389. Номер порта можно изменить в файле /etc/xrdp/xrdp.ini.



Удаленный рабочий стол с хоста Windows с использованием стандартного слиента подключения по RDP. На машинах с Linux можно использовать различные утилиты, например «FreeRDP» или «Remmina»

Далее перейдем к работе с утилитой командной строки openstack cli

Openstack CLI

Подключение и проверка работы

Механизм подключения подробно расписан в разделе «2. Установка и подключение OpenStack CLI» поэтому просто создадим переменные и проверим доступность функционала

В дистрибутивах Alt Linux есть особенность - в переменной PATH, в которой определяется набор каталогов, в которых находятся исполняемые файлы программ по умолчанию добавляется каталог bin в домашнем каталоге пользователя. Поэтому, для удобства, будем создавать и хранить скрипты в этом каталоге.

Данного каталога по умолчанию нет, создадим его и создадим скрипт, в котором будут описаны параметры подключения.

Экспортируем переменные

```
source user-openrc.sh
```

Проверяем подключение командой

```
openstack --insecure server list
```

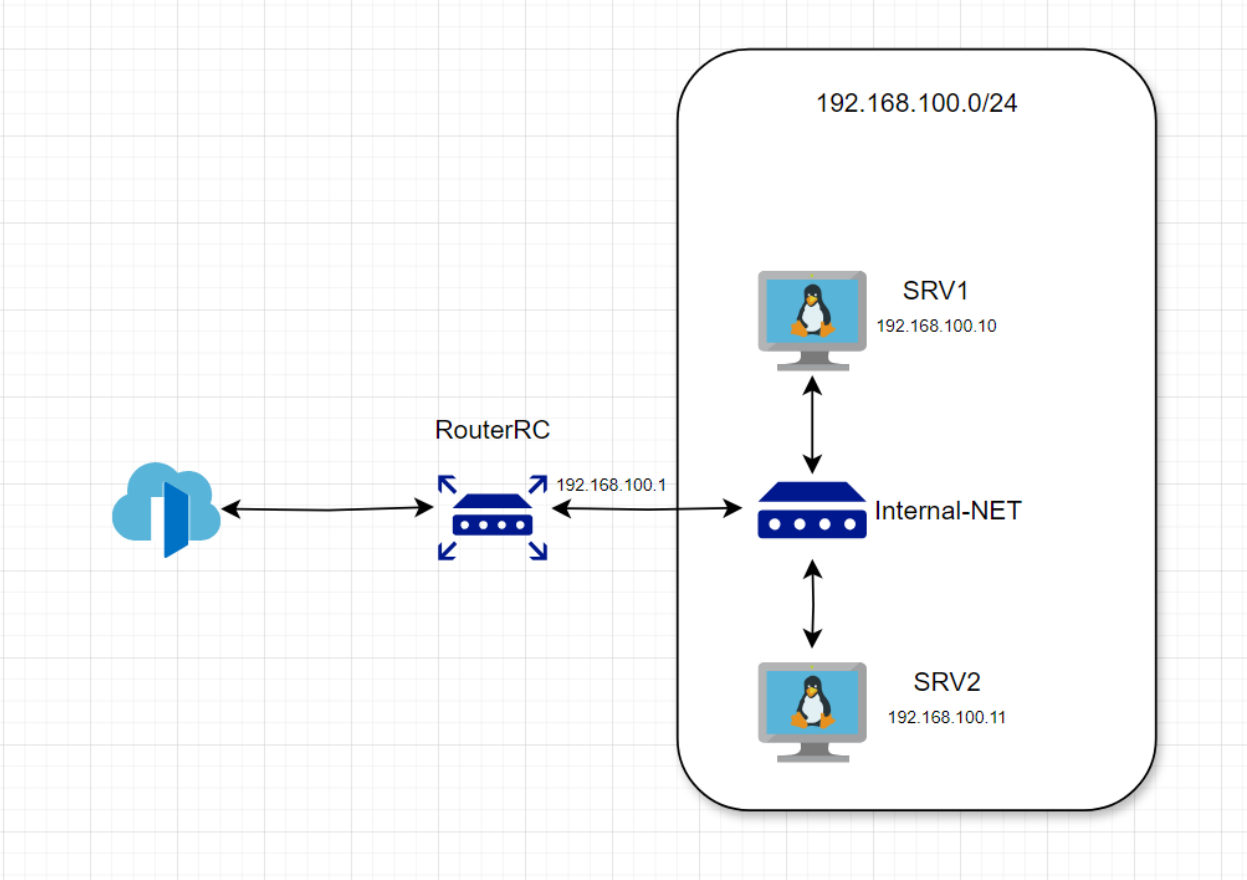
```
[altlinux@cloudvm ~]$ openstack --insecure server list
+--------------------------------------+---------+--------+-------------------------------------+--------------------------+--------+
| ID                                   | Name    | Status | Networks                            | Image                    | Flavor |
+--------------------------------------+---------+--------+-------------------------------------+--------------------------+--------+
| 6f42dafc-3344-418d-8719-47f88cd31e34 | CloudVM | ACTIVE | Inside=172.20.222.168, 192.168.1.111 | N/A (booted from volume) | medium |
+--------------------------------------+---------+--------+-------------------------------------+--------------------------+--------+
[altlinux@cloudvm ~]$
```

команда выводит список инстансов, подключение выполнено

переходим к настройке

Создание сетей

Мы будем работать со следующей простой схемой



1. Создадим сеть Internal-NET с IP подсетью 192.168.100.0/24.

2. В этой сети создадим маршрутизатор, RouterRC через который виртуальные машины будут получать доступ в интернет

3. Создадим два инстанса, SRV1 и SRV2, и дадим им статические адреса.

В самом начале работы, для того чтобы у нас был доступ к нашим инстансам, нам необходимо прописать ключевую пару SSH с именем CloudVM. В дальнейшем мы будем распространять публичный ключ для беспарольного доступа на инстансы ВМ. создаем ключевую пару SSH командой ssh-keygen и выполняем команду

```
openstack keypair create --public-key /home/altlinux/.ssh/id_rsa.pub CloudVM --insecure
```

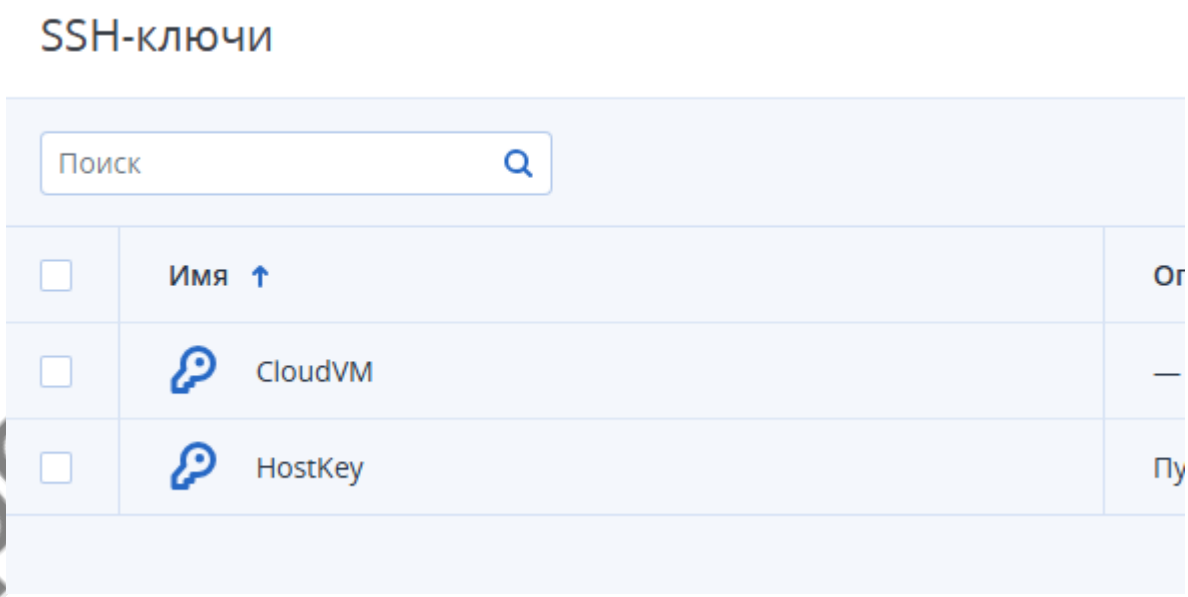
Где:

- --public-key <файл> - имя файла для открытого ключа для добавления.

- CloudVM - имя ключа

```
[altlinux@cloudvm ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/altlinux/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/altlinux/.ssh/id_rsa.
Your public key has been saved in /home/altlinux/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:M3cczMQJz537REVbRDNSd4I+SpeaD6G8AcLjsParxQM altlinux@cloudvm
The key's randomart image is:
+---[RSA 2048]----+
|          .o.+oBO|
|           *+..oO|
|    .       .*.o..|
|  . + .   o•=. o |
|  E+ o oSo.*o.. .|
|  oo.   ++=.   o |
| . .+    o o    .|
|   ...   .   .   |
|  ....           |
+----[SHA256]-----+
[altlinux@cloudvm ~]$ openstack keypair create --public-key /home/altlinux/.ssh/id_rsa.pub CloudVM --insecure
+-------------+-------------------------------------------------+
| Field       | Value                                           |
+-------------+-------------------------------------------------+
| created_at  | 2025-05-02T09:36:40.543535                      |
| fingerprint | 65:6d:67:2f:cb:6f:c8:47:f4:ce:c1:4a:79:16:8b:4a |
| id          | CloudVM                                         |
| is_deleted  | None                                            |
| name        | CloudVM                                         |
| type        | ssh                                             |
| user_id     | 1355f61efce148fd8fefd2cbab4d9850                |
+-------------+-------------------------------------------------+
[altlinux@cloudvm ~]$
[altlinux@cloudvm ~]$
[altlinux@cloudvm ~]$
[altlinux@cloudvm ~]$
[altlinux@cloudvm ~]$ openstack keypair list --insecure
+---------+-------------------------------------------------+------+
| Name    | Fingerprint                                     | Type |
+---------+-------------------------------------------------+------+
| CloudVM | 65:6d:67:2f:cb:6f:c8:47:f4:ce:c1:4a:79:16:8b:4a | ssh  |
| HostKey | 42:b8:d1:f7:49:46:99:26:42:11:6e:5c:32:9e:3f:d9 | ssh  |
+---------+-------------------------------------------------+------+
```

Команда `openstack keypair list --insecure` вывела список ключей



Наш ключ отображается в списке, в графической форме

Сеть — это изолированный сетевой сегмент уровня 2. Существует два типа сетей: проектные и провайдерские. Проектные сети полностью изолированы и не используются совместно с другими проектами. Сети провайдеров сопоставляются с существующими физическими сетями в центре обработки данных и обеспечивают внешний сетевой доступ для серверов и других ресурсов. Только администратор OpenStack может создавать провайдерские сети. Сети могут быть подключены через маршрутизаторы.

Итак, начнем создавать сеть. Предварительно выведем список сетей командой «openstack network list --insecure»

```
openstack network create Internal-NET --insecure
```

Фактически, создание сети, это создание изолированного виртуального коммутатора в системе. Для нормальной работы необходимо привязать к сети IP и создать правила маршрутизации из и в сеть.

Создаем IP подсеть

```
openstack subnet create --subnet-range 192.168.100.0/24 --gateway 192.168.100.1 --dns-
nameserver 77.88.8.8 --network Internal-NET  insubnet --insecure
```

Где:

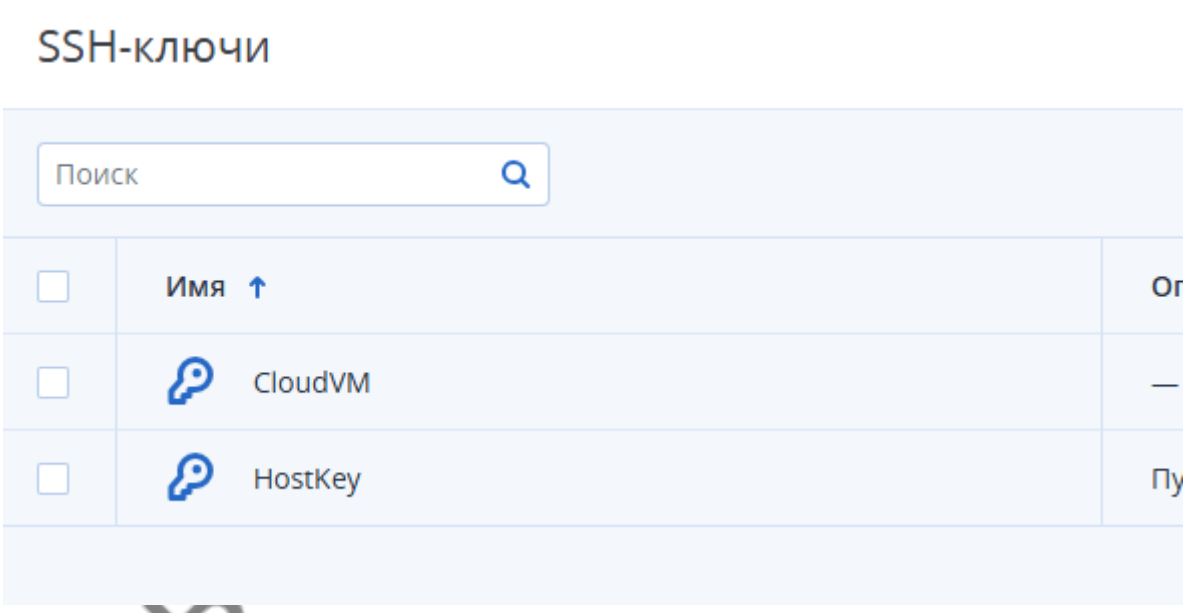
- --subnet-range - диапазон IP адресов/ IP сеть

- --gateway - IP адрес маршрутизатора/шлюза

- --dns-nameserver - DNS сервер

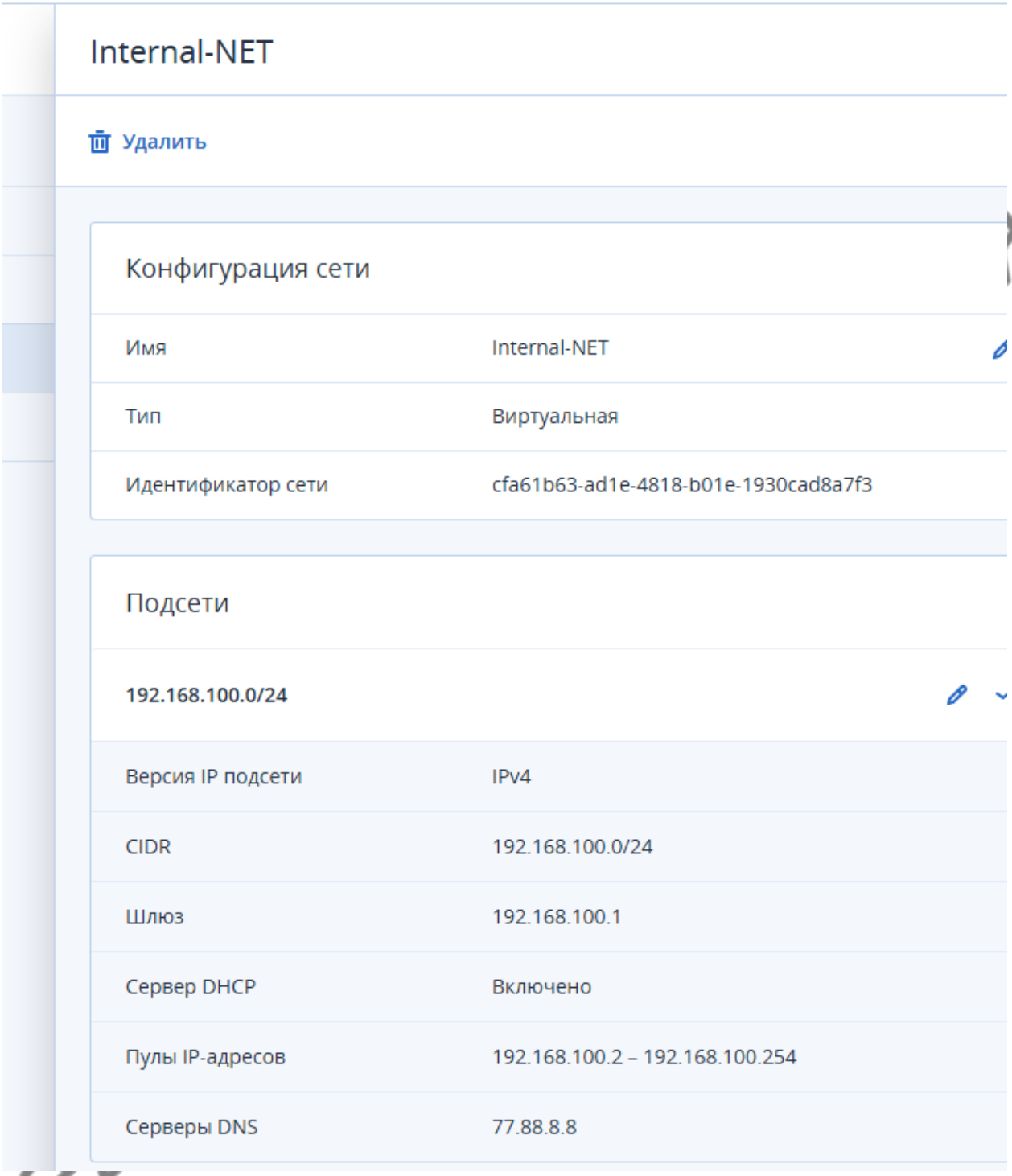
- --network - имя или идентификатор сети, к которой привязана подсеть

- insubnet - имя подсети



Проверяем создание подсети командой «openstack subnet list --insecure»

И в графике



Теперь необходимо создать маршрутизатор для внутренней сети Internal-NET

Создаем маршрутизатор командой

```
openstack router create RouterRC --enable-snat --external-gateway public --insecure
```

Где:

- RouterRC - имя маршрутизатора

- --enable-snat - включение sourceNAT

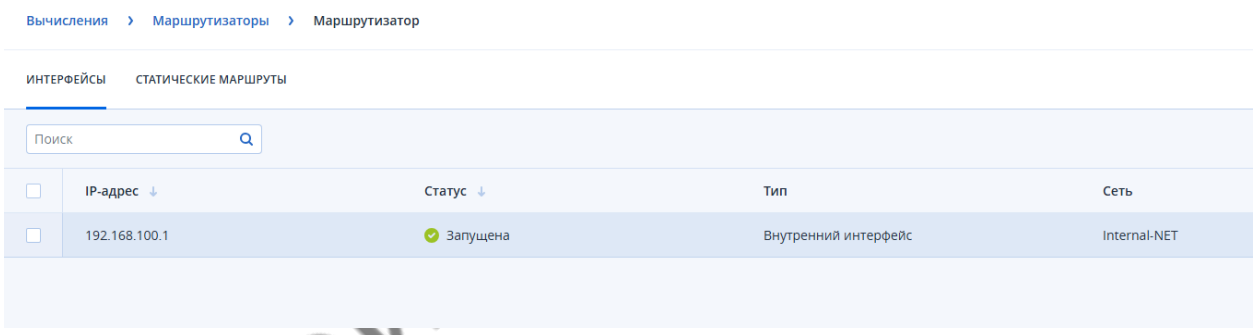
- --external-gateway -имя/ID внешней сети

Далее связываем подсеть «insubnet» с роутером

```
openstack router add subnet RouterRC insubnet  --insecure
```

```
[altlinux@cloudvm ~]$ openstack router create RouterRC --insecure
+-------------------------+--------------------------------------+
| Field                   | Value                                |
+-------------------------+--------------------------------------+
| admin_state_up          | UP                                   |
| availability_zone_hints |                                      |
| availability_zones      |                                      |
| created_at              | 2025-05-02T10:55:42Z                 |
| description             |                                      |
| enable_ndp_proxy        | None                                 |
| external_gateway_info   | null                                 |
| flavor_id               | None                                 |
| id                      | 1f533e53-d157-4ac1-bf33-e155d64101c1 |
| name                    | RouterRC                             |
| project_id              | 26351ce30e8647cfa6b02f524d36a1ca     |
| revision_number         | 2                                    |
| routes                  |                                      |
| status                  | ACTIVE                               |
| tags                    |                                      |
| tenant_id               | 26351ce30e8647cfa6b02f524d36a1ca     |
| updated_at              | 2025-05-02T10:55:42Z                 |
+-------------------------+--------------------------------------+
[altlinux@cloudvm ~]$ openstack router add subnet RouterRC insubnet  --insecure
[altlinux@cloudvm ~]$
```

В графике



Для доступа к нашим инстансам необходимо создать порты, которые в дальнейшем мы привяжем к нашим ВМ

Порт связывает MAC адрес, подсеть/IP адрес и инстанс. В нашем случае, IP адреса мы дадим статически Выполняем команды

```
openstack port create --network Internal-NET --fixed-ip ip-address=192.168.100.10 srv1port --insecure

openstack port create --network Internal-NET --fixed-ip ip-address=192.168.100.11 srv2port --insecure
```

Где

--network - сеть, к которой будет привязан порт

--fixed-ip - будет использован статический IP

ip-address=<IP>

srv1port - имя порта

Выполнив команду «openstack port list --insecure» видим оба созданных порта

Создание хостов

Сетевая подсистема у нас готова, можно приступить к созданию инстансов

Вы полним команду

```
openstack server create --flavor small  --port srv1port --image alt-p10-cloud-x86_64
--boot-from-volume 10 --key-name CloudVM srv1 --insecure
```

Где

- --flavor - тип ВМ (шаблон ресурсов)

- --port - сетевой порт, созданный на предыдущем шаге, подключенный к ВМ

- --image - образ, из которого будет создана ВМ

- --boot-from-volume - создание блочного загрузочного устройства с заданным размером, в Gb

- --key-name - публичный ключ из ключевой пары

- srv1 - имя инстанса

Список инстансов, полученный командой «openstack server list --insecure»

```
altlinux@cloudvm ~]$ openstack server list --insecure
+--------------------------------------+---------+--------+--------------------------------------+
| ID                                   | Name    | Status | Networks                             |
+--------------------------------------+---------+--------+--------------------------------------+
| 54c6f8eb-ff48-4e4e-8a28-0aa9319fd38d | srv2    | ACTIVE | Internal-NET=192.168.100.11          |
| 1edf54b3-d201-491c-b9c3-f5ff312f3173 | srv1    | ACTIVE | Internal-NET=192.168.100.10          |
| 6f42dafc-3344-418d-8719-47f88cd31e34 | CloudVM | ACTIVE | Inside=172.20.222.168, 192.168.1.111 |
+--------------------------------------+---------+--------+--------------------------------------+
altlinux@cloudvm ~]$
```

Однако доступа в srv1 и srv2 мы мы имеем, поскольку они находятся в другой сети. Решений этой проблемы есть несколько, мы выберем самую, на мой взгляд простую - создадим еще один порт в сети Internal-NET и подключим к хосту CloudVM. Данному порту мы не будем задавать фиксированный IP адрес, хост получит его по DHCP.

Создаем порт командой

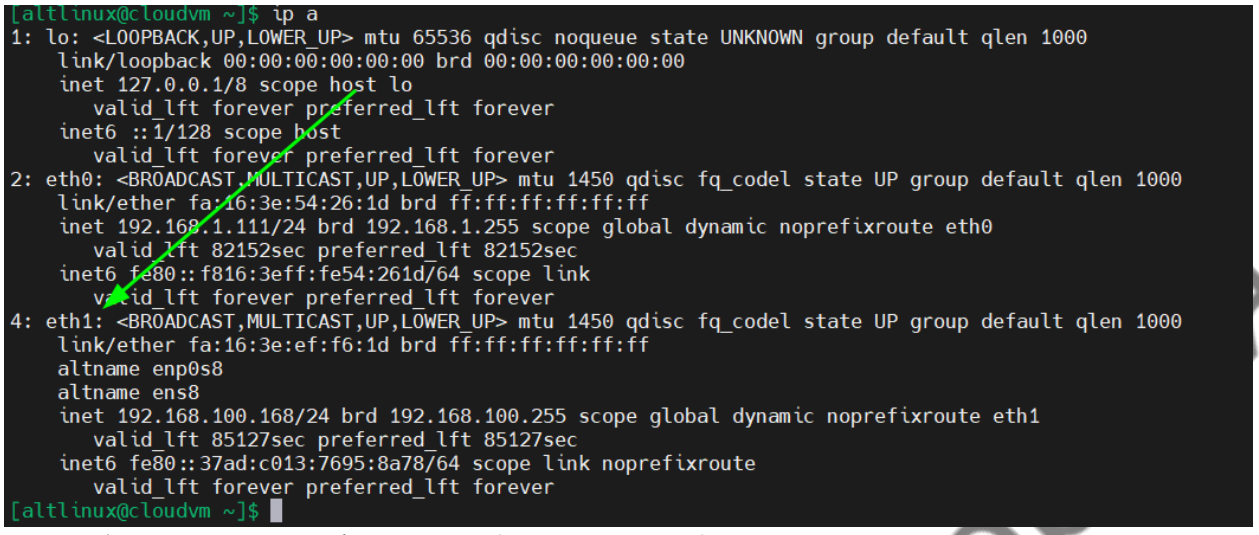
```
openstack port create --network Internal-NET  cloudVMport  --insecure
```

Далее, добавляем этот порт к существующему инстансу CloudVM

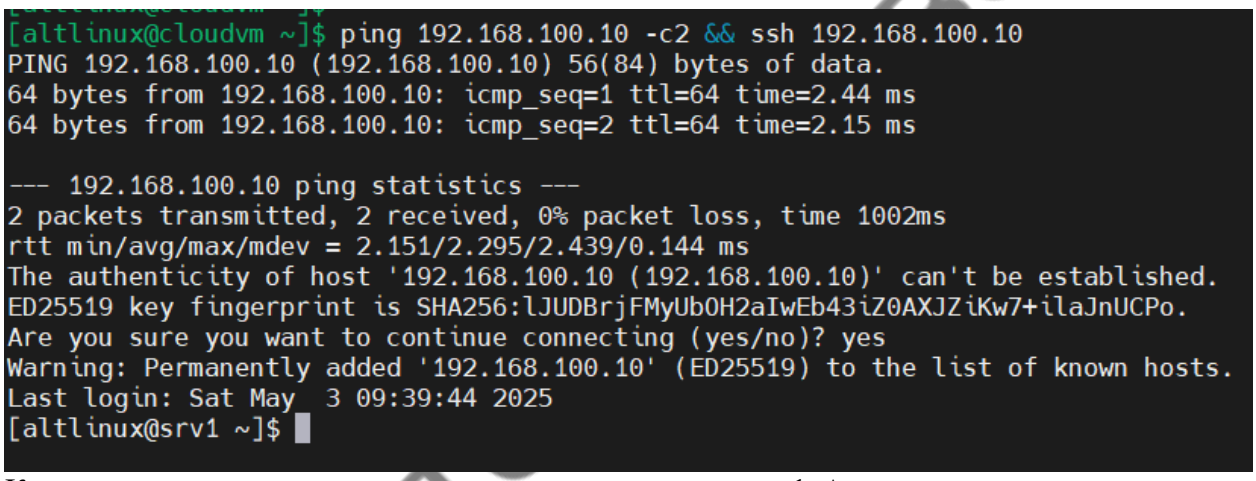
```
openstack server add port --tag eth1 CloudVM cloudVMport --insecure
```

Обратите внимание, нам необходимо указать тег интерфейса (eth1)

Теперь, выполнив ip a, мы видим, что у нас на CloudVM появился интерфейс eth1 с IP адресом из подсети insubnet



Попробуем выполнить ping на srv1 (192.168.100.10) и в случае успеха, подключится к нему по SSH



Как видно из скриншота, мы успешно подключились к srv1. Аналогичную операцию можно проделать и с srv2

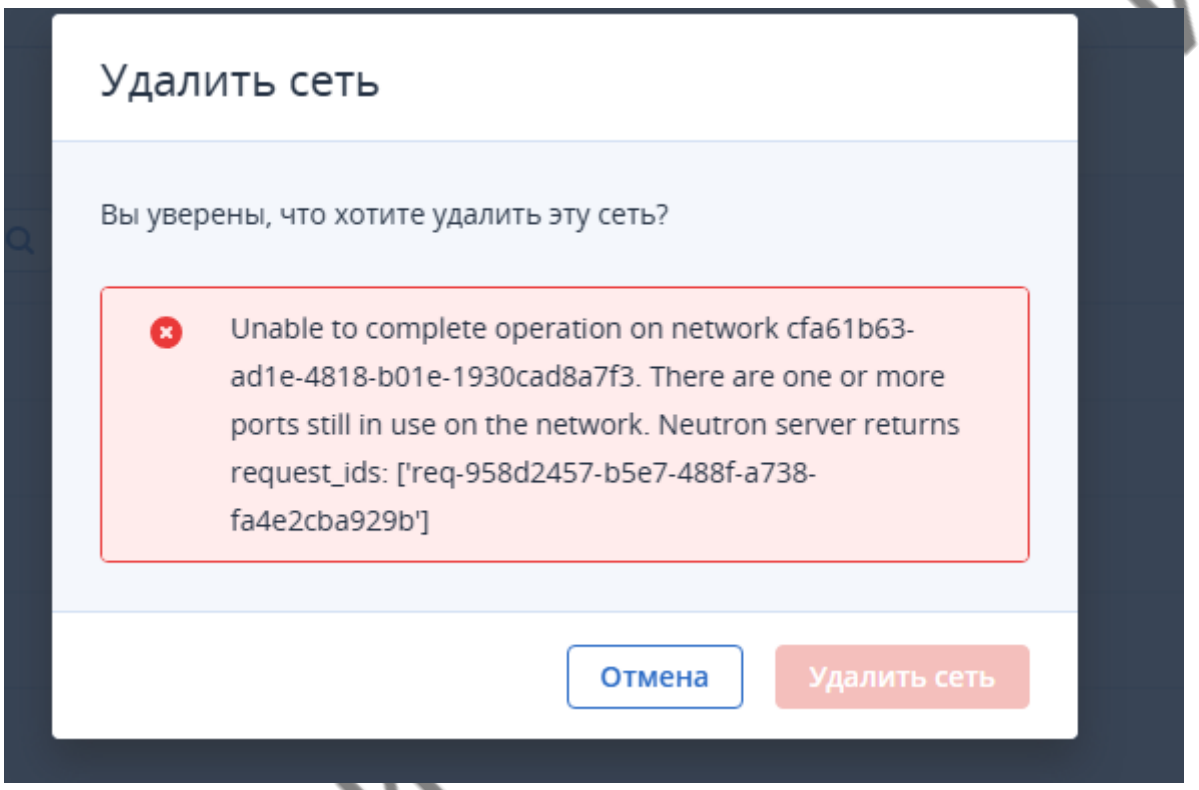
Удаление ресурсов

Конечной целью нашей работы является скрипт, который автоматизирует развёртывание данной инфраструктуры.

Для работы скрипта нам необходимо удалить созданные ресурсы, которые мы создадим вновь, но уже единым скриптом.

Но тут есть определенные нюансы, которые необходимо учитывать

Например, если мы попытаемся удалить сеть Internal-NET в графическом режиме, то получим сообщение о невозможности этой операции.



Дело в том, что в системе заложена проверка на целостность и непротиворечивость, и невозможно удалить сеть, если к ней подключены порты.

Таким образом, удаление ресурсов необходимо производить в обратном порядке их создания: Инстансы - порты - маршрутизаторы - подсети - сети

Как правило, удаление в OpenStack CLI - команда delete в соответствующем модуле.

Итак, удаляем инстансы

```
openstack server delete --force srv1 srv2 --insecure
```

```
[altlinux@cloudvm ~]$ openstack server list --insecure
+--------------------------------------+---------+--------+-----------------------------------------------------------------------
| ID                                   | Name    | Status | Networks
+--------------------------------------+---------+--------+-----------------------------------------------------------------------
| 6f42dafc-3344-418d-8719-47f88cd31e34 | CloudVM | ACTIVE | Inside=172.20.222.168, 192.168.1.111; Internal-NET=192.168
+--------------------------------------+---------+--------+-----------------------------------------------------------------------
[altlinux@cloudvm ~]$
```

ВМ srv1 и srv2 удалены

Удаляем порты

```
openstack port delete cloudVMport srv1port srv2port --insecure
```

```
[altlinux@cloudvm ~]$ openstack port list --insecure
+--------------------------------------+------+-------------------+--------------------------------
| ID                                   | Name | MAC Address       | Fixed IP Addresses
+--------------------------------------+------+-------------------+--------------------------------
| 38ea7b92-1f8d-4720-a161-25d47425e6ae |      | fa:16:3e:19:3d:7c | ip_address='172.20.222.75', subnet
| 4cc79aec-5706-4f9f-be3b-e2c04321ef39 |      | fa:16:3e:5f:96:dc | ip_address='192.168.1.100', subnet
| 4eea8a07-7735-43e8-97d8-abf424999cb6 |      | fa:16:3e:19:0e:ed | ip_address='172.20.222.168', subne
| 596b471c-d153-490c-bab0-3a4a6cf4f79f |      | fa:16:3e:79:1f:b6 | ip_address='192.168.100.75', subne
| 5bcd6ca8-b20b-489b-b7b2-873bf38b7ccf |      | fa:16:3e:26:11:5a | ip_address='192.168.1.146', subnet
| 79682482-626d-4d8a-81c3-1190bbdf39c2 |      | fa:16:3e:c5:c6:69 | ip_address='192.168.1.1', subnet_i
| 84955233-6c12-4370-a686-caea1cdcad4d |      | fa:16:3e:b0:06:99 | ip_address='192.168.100.2', subnet
| 8d8ed4e8-a95e-4191-a82c-30b3f0bdfa73 |      | fa:16:3e:54:26:1d | ip_address='192.168.1.111', subnet
| eb4afd0e-abab-4589-9ff9-c845cd9488df |      | fa:16:3e:b9:8b:10 | ip_address='192.168.100.1', subnet
+--------------------------------------+------+-------------------+--------------------------------
[altlinux@cloudvm ~]$
```

Порты удалены

Удаляем маршрутизатор

Сначала отключим подсеть от роутера

```
openstack router remove subnet RouterRC insubnet --insecure
```

Далее можно удалять сам маршрутизатор

```
openstack router delete RouterRC --insecure
```

Проверяем

```
[altlinux@cloudvm ~]$ openstack router list --insecure
+--------------------------------------+---------+--------+-------+----------------------------------+
| ID                                   | Name    | Status | State | Project                          |
+--------------------------------------+---------+--------+-------+----------------------------------+
| 599f173e-d0ae-4c00-a911-590bc3a99af2 | Router0 | ACTIVE | UP    | 26351ce30e8647cfa6b02f524d36a1ca |
+--------------------------------------+---------+--------+-------+----------------------------------+
[altlinux@cloudvm ~]$
```

Роутер удален

Удаляем подсеть

```
openstack subnet delete insubnet --insecure
```

Проверим

```
[altlinux@cloudvm ~]$ openstack subnet delete insubnet --insecure
[altlinux@cloudvm ~]$
[altlinux@cloudvm ~]$ openstack subnet list --insecure
+--------------------------------------+------+--------------------------------------+----------------+
| ID                                   | Name | Network                              | Subnet         |
+--------------------------------------+------+--------------------------------------+----------------+
| 4694d338-ec0a-4143-a431-59caa9f583c6 |      | 95dee5d9-ce0d-4315-ab77-c785c26b8c55 | 192.168.1.0/24 |
+--------------------------------------+------+--------------------------------------+----------------+
[altlinux@cloudvm ~]$
```

Подсеть удалена

И наконец, удаляем сеть

```
openstack network delete Internal-NET --insecure
```

Проверим

```
[altlinux@cloudvm ~]$ openstack network delete Internal-NET --insecure
[altlinux@cloudvm ~]$ openstack network list --insecure
+--------------------------------------+--------+--------------------------------------------------------------------------------------+
| ID                                   | Name   | Subnets                                                                              |
+--------------------------------------+--------+--------------------------------------------------------------------------------------+
| 95dee5d9-ce0d-4315-ab77-c785c26b8c55 | Inside | 4694d338-ec0a-4143-a431-59caa9f583c6                                                 |
| 9974afa8-3de9-425a-8a10-2981f0e455f2 | public | 84ca7cf4-6f06-430f-88e6-7ffce571b763, e8e019a8-58cc-4300-9812-7ff8bbf15ceb           |
+--------------------------------------+--------+--------------------------------------------------------------------------------------+
[altlinux@cloudvm ~]$
```

Таким образом, стенд очищен и готов к исполнению скрипта

Разворачивание инфраструктуры единым скриптом

Используя ранее изученные команды напишем bash скрипт, вновь разворачивающую нашу несложную инфраструктуру

Обратите внимание, в предыдущем модуле мы не удалили ключевую пару SSH с именем CloudVM, поэтому можем использовать ее вновь.

Скрипт:

```
#!/bin/sh


# import vars
source user-openrc.sh


# # # # # Create infrastructure


# # # # network
openstack network create Internal-NET --insecure
# # subnet
openstack subnet create --subnet-range 192.168.100.0/24 --gateway 192.168.100.1 --dns-nameserver 77.88.8.8 --network Internal-NET  insubnet --insecure
# # router
openstack router create RouterRC --enable-snat --external-gateway public --insecure
# # subnet
openstack router add  subnet RouterRC insubnet  --insecure
# # ports
openstack port create --network Internal-NET --fixed-ip ip-address=192.168.100.10 srv1port --insecure
openstack port create --network Internal-NET --fixed-ip ip-address=192.168.100.11 srv2port --insecure
openstack port create --network Internal-NET  cloudVMport  --insecure


# # # # # instance
openstack server create --flavor small  --port srv1port --image alt-p10-cloud-x86_64 --boot-from-volume 10 --key-name CloudVM srv1 --insecure
openstack server create --flavor small  --port srv2port --image alt-p10-cloud-x86_64 --boot-from-volume 10 --key-name CloudVM srv2 --insecure


# # add port to instance CloudVM
openstack server add port --tag eth1 CloudVM cloudVMport --insecure
```

Скрипт во время работы достаточно большой объём информации, в которой трудно разобраться новичку, поэтому в конец скрипта можно добавить следующий код, который выведет кратно созданные ресурсы

```
openstack network list --insecure | grep "Internal-NET"
openstack subnet  list --insecure | grep insubnet
```

```
openstack router  list --insecure | grep RouterRC
openstack port    list --insecure | grep -E "srv1port|srv2port|cloudVMport"
openstack server  list  --insecure | grep -E "srv1|srv2"
```

Кроме этого, если планируется в дальнейшем автоматизировать конфигурирование созданных инстансов, например с помощью Ansible, есть смысл отключить MITM защиту SSH, создав предварительно файл ~/.ssh/config и поместив туда параметр

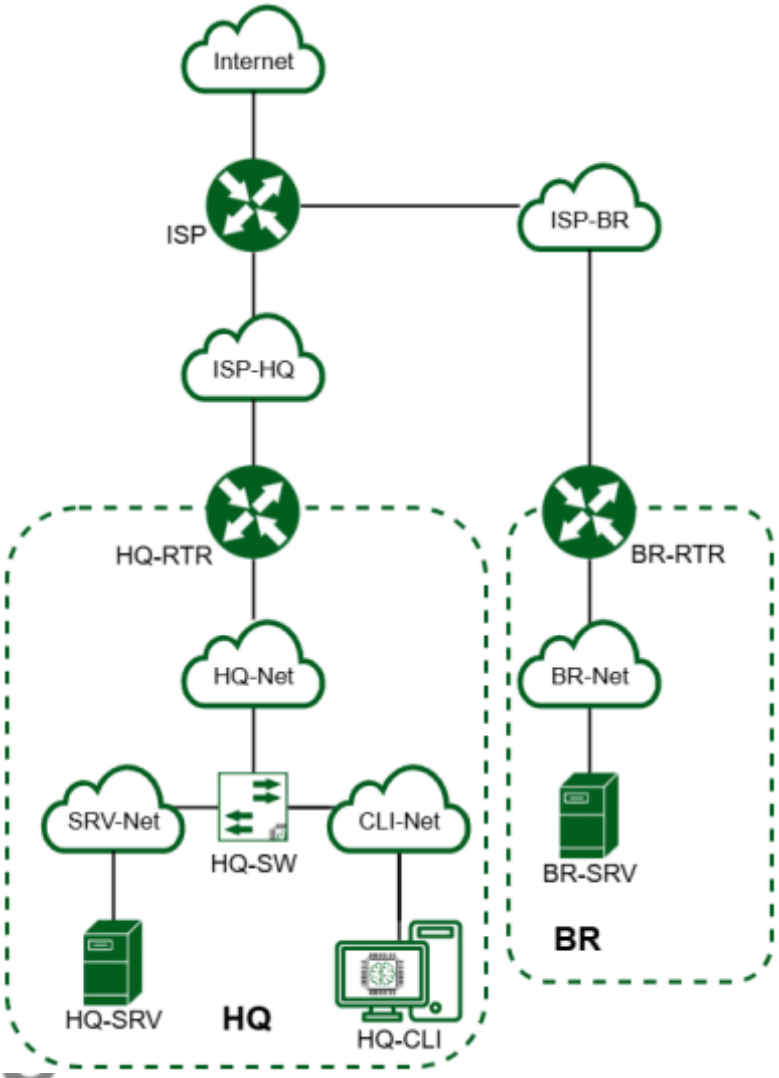
```
Host *
    StrictHostKeyChecking no
```

Таким образом не будет выводится сообщение при добавлении публичного SSH в файл known_hosts.

ПРИЛОЖЕНИЯ

Приложение 1

Инструкция по застройке стенда для демонстрационного экзамена по КОД 09.02.06-1-2025 сетевое и системное администрирование 2025



Застройка стендов участников

Рекомендуемые действия и лист проверки технического эксперта площадки сетевое и системное администрирование в проверочном листе 1.

Аппаратное обеспечение в соответствии с таблицей 10, разделом 3 пунктом 1

На одно рабочее место участника: 8 ядер ЦП, 10 ГБ ОП, крайне рекомендуется твердотельный накопитель, обеспечивающий линейное чтение от 450МБ/с, скорость сетевого адаптера от 1Гб/с. При кластерном подходе к застройке площадки ядра ЦП и объём ОП нод складываются. Рекомендуется учесть 20% запас мощностей.

Рекомендуется использование источников бесперебойного питания с исправной батареей на случай кратковременных сбоев электропитания.

Рекомендуемые решения:

- Альт Сервер Виртуализация или аналог;
- РедОС Виртуализация или аналог;

- Средство виртуализации «Брест», Астра или аналог;
- Другие решения на базе qemu/kvm или других технологий, рекомендуемые и протестированные на предмет работоспособности, стабильности и выполнимости задания ответственными лицами от застройщика площадки.

Рекомендации:

- Необходимо обеспечить полную логическую изоляцию стендов участников друг от друга;
- Крайне рекомендуется настроить квотирование ресурсов (нагрузка на стенд одного участника не должны повлиять на стенды других участников, особенно в части ЦП, ОП, хранилища и сети);
- Рекомендуется заблаговременное нагрузочное тестирование площадки с 20% запасом (в случае застройки 10 рабочих мест тестировать на 12 рабочих мест с одновременным выполнением задания);
- Рекомендуется генерация паролей учётных записей, последующая проверка на корректность и функциональность;
- Блокировка внешних подключений к решению виртуализации на время выполнения участниками задания и проведение экспертной оценки;
- Блокировка учётных записей участников после проведения экспертной оценки.

При проведении ДЭ ПА, участники выполняют задание модуля 1, стенд при этом застраивается в соответствии с топологией модуля 1.

При проведении ДЭ БУ. ДЭ ПУи, ДЭ ПУв, после выполнения участниками модуля 1 участникам необходимо остановить виртуальные машины, относящиеся к модулю 1, и запустить виртуальные машины модулей 2 и 3. Виртуальную машину BR-DC для модуля 3, для оптимизации ресурсов, участник включает в тот момент, когда она ему понадобится. Рекомендуется настроить две учётные записи участникам, одну для модуля 1, одну для модуля 2 и 3.

Стенд при этом застраивается следующим образом:

В начале ДЭ для выполнения модуля 1, в качестве преднастройки используются виртуальные машины, с установленной операционной системой, но без настроенных параметров.

После выполнения модуля 1, участник выключает виртуальные машины, относящиеся к модулю 1, и запускает виртуальные машины, относящиеся к модулю 2, которые кроме установленных операционных систем имеют ещё дополнительно настроенную адресацию, сетевую трансляцию, действующий туннель, действующую динамическую маршрутизацию, созданных пользователей, настроенные службы dns и dhcp в соответствии с заданием модуля 2.

Настройка производится и проверяется техническим экспертом площадки. Проверка производится в соответствии с проверочным листом 2.

Застройка рабочих мест участников

Рекомендации для обеспечения комфортного режима работы: 4-8 ядерный ЦП, 8Гб ОП с частотой от 2,6ГГц, твердотельный накопитель.

Рекомендуемые действия и лист проверки технического эксперта площадки сетевое и системное администрирование в проверочном листе 3.

Проверочный лист 1 День Д-2

- Установлена и настроена аппаратная часть в соответствии с планом застройки и инфраструктурным листом;

- Установлена и настроена программная часть;
- Установлен и настроен мониторинг аппаратной и программной части (по возможности);
- Установлено и настроено видеонаблюдение на площадке, проброшены порты, разрешен трафик;
- Видеопотоки доступны из сети Интернет;
- Созданы учетные записи участников модулей 1, 2 и 3. Разные учётные записи имеют разные пароли;
- Ресурсы разных учетных записей, изолированные друг от друга, участники не видят и не могут взаимодействовать с виртуальными машинами и сетями других участников, и не могут повлиять на их работоспособность;
- Не задействованные в ДЭ лица не имеют доступа к виртуальным машинам участников;
- Виртуальные машины работоспособны;
- Виртуальные сети работоспособны, при корректной настройке связность возможна и работоспособна;
- При корректной настройке динамической маршрутизации стенды участников не мешают друг-другу и не выводят из строя основную сеть площадки, в том числе доступ к сети Интернет;
- При некорректной настройке затрагиваются исключительно виртуальные машины конкретного участника, и не затрагиваются виртуальные машины, сети других участников;
- Преднастройка стендов для модуля 2 и 3.

Проверочный лист 2 День Д1

- Пароли учётных записей изменены;
- Виртуальные машины модуля 1 включены, модуля 2 и 3 выключены;
- Выполнение модуля 1;
- Технический перерыв, дезактивация учётных записей модуля 1, активация учётных записей модуля 2, отключение виртуальных машин модуля 1;
- Виртуальные машины модуля 1 выключены, ресурсы для модулей 2 и 3 освобождены;
- Включение виртуальных машин модуля 2;
- Проверка участниками корректности преднастройки;
- Доклад о готовности выполнения модуля 2 и 3;
- Выполнения модулей 2 и 3.

Проверочный лист 3 День Д-2

- Рабочие места участников установлены и настроены в соответствии с планом застройки и инфраструктурным листом;
- Каждое рабочее место проверено, отсутствуют лишние предметы, файлы. Присутствуют нужные программы и настройки;
- Рабочие места участников пронумерованы

Оборудование, приборы, ПО и материалы

В качестве системы виртуализации рекомендуется использование гипервизоров первого типа: proxmox, opennebula, другие решения. В качестве ОС рекомендуется использование отечественных дистрибутивов Linux: Alt Linux, Redos, Astra Linux, Rosa Linux. В качестве маршрутизаторов рекомендуется использовать ecorouter

Текстовый редактор Vim — мощный инструмент для работы с кодом и конфигурациями. Несмотря на его сложность для новичков, освоение базовых функций окупается гибкостью и эффективностью.

Для комфортного освоения Vim встроен интерактивный vim-tutor — введите эту команду в терминале, чтобы изучить основные приёмы за 20–30 минут.

Схема оценки

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии. Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше, чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств. Подробное описание методики проверки должно быть разработано экспертами, принимающими участие в оценке экзаменационного задания, и вынесено в отдельный документ.

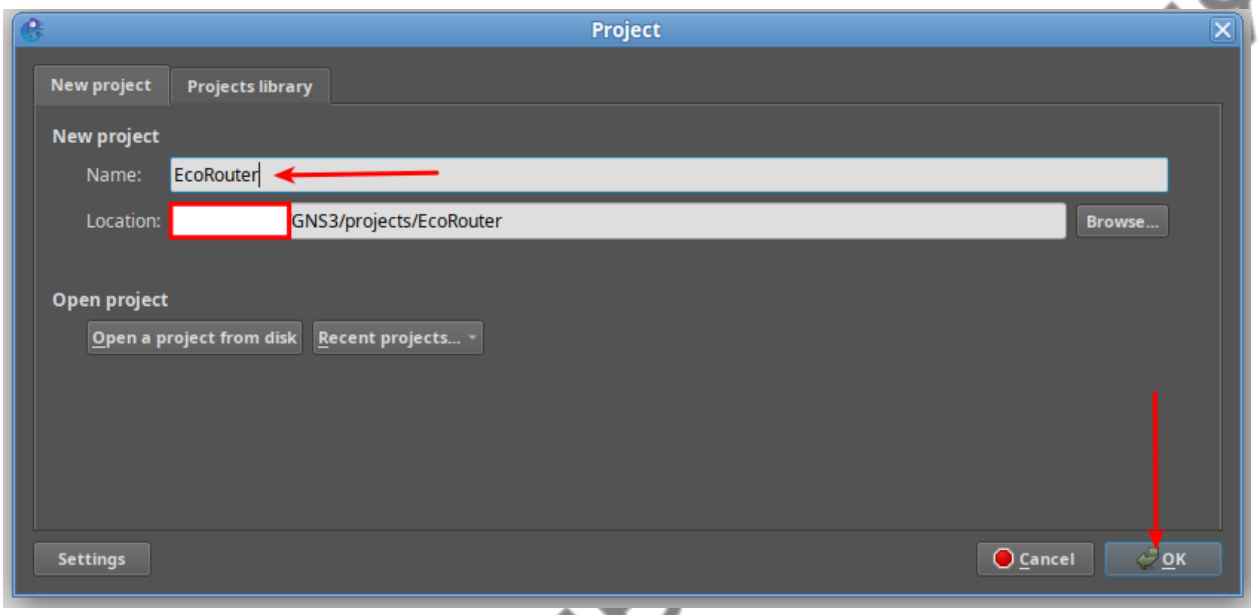
Приложение 2

Установка EcoRouter в GNS3

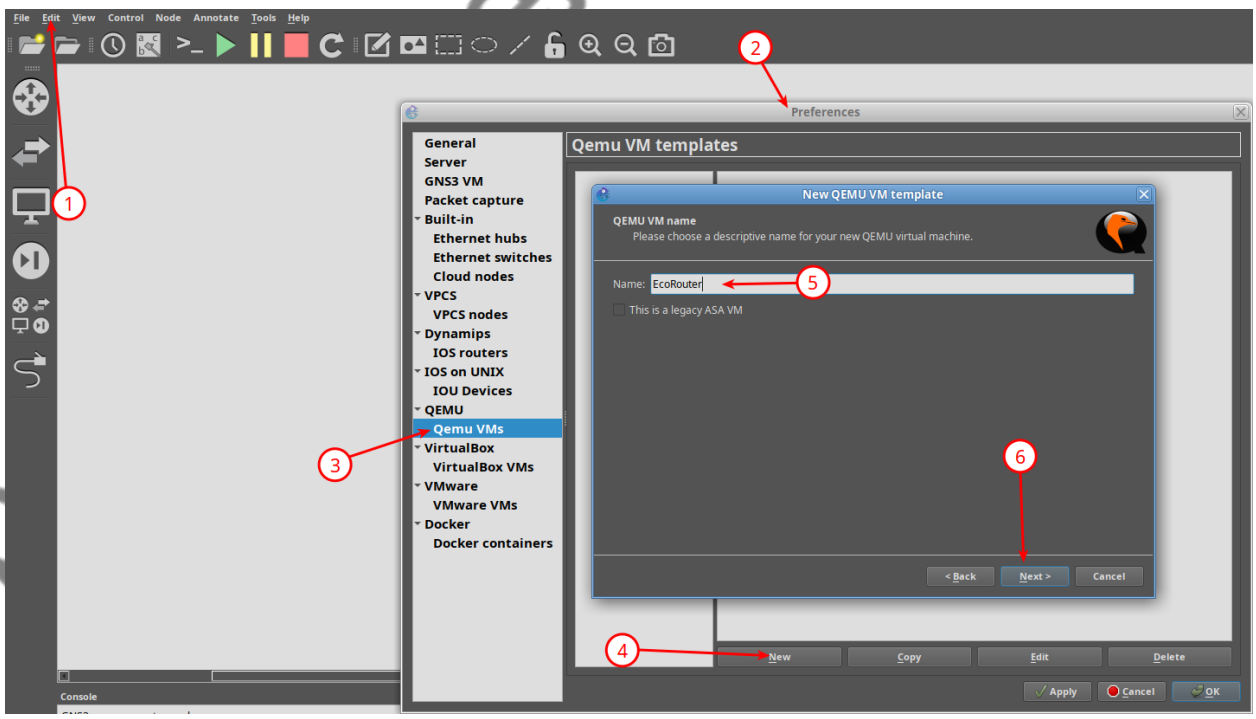
Для установки в операционной системе Windows 10/11 требует наличие GNS3VM под управлением VMWare Player 16+ версии.

В операционных средах Linux/MAC работает под управлением GNS3.

После открытия GNS3 необходимо создать проект:



Далее нажимать Edit, затем выбирать Preferences и переходим на вкладку Qemu VMs. После чего, нажимать New, задать Name для нового шаблона и нажимать Next:

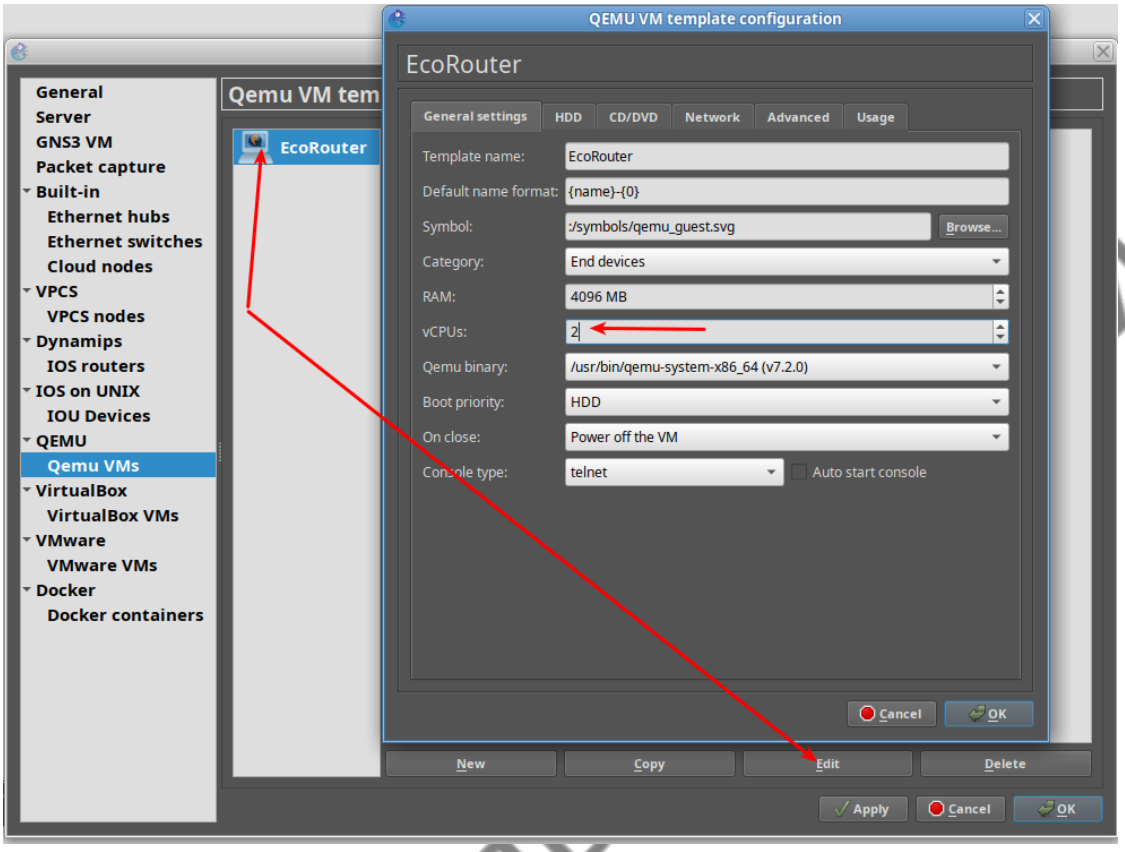


Задать необходимый объем ОЗУ (минимальное значение 4096) и нажимать Next.

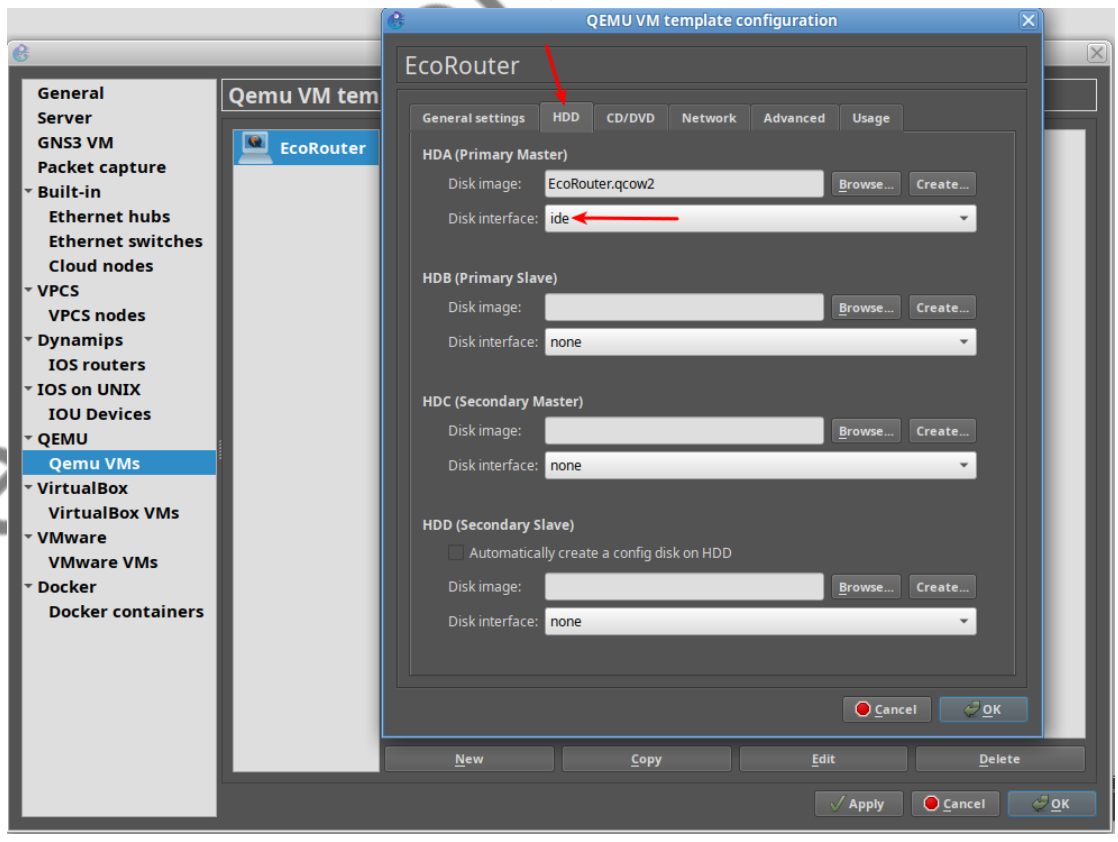
Выбрать необходимый тип консоли (telnet) и нажимать Next.

Выбрать Existing image (существующий образ – ранее был помещён в директорию GNS3/images/QEMU) и нажать Finish.

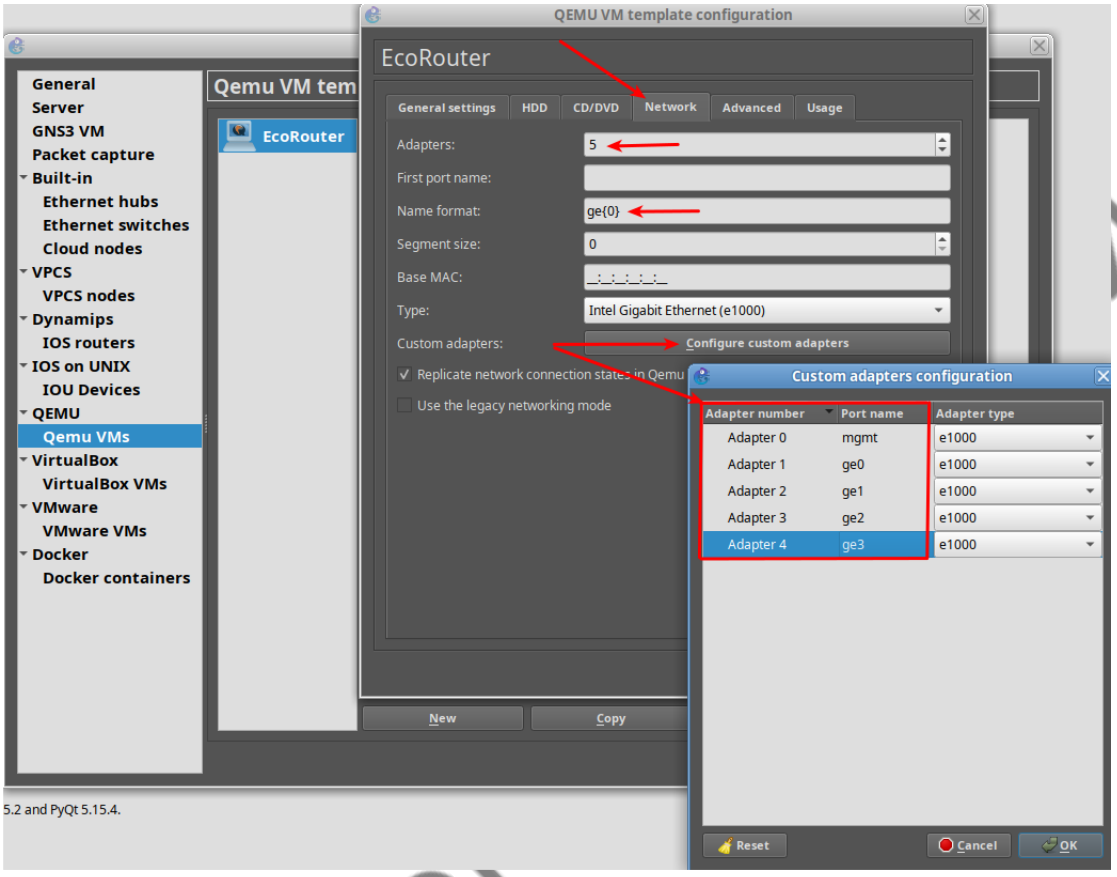
Выбрать только что созданный шаблон и нажать Edit. Далее на вкладке General settings задать необходимое кол-во vCPUs (минимально необходимое 2):



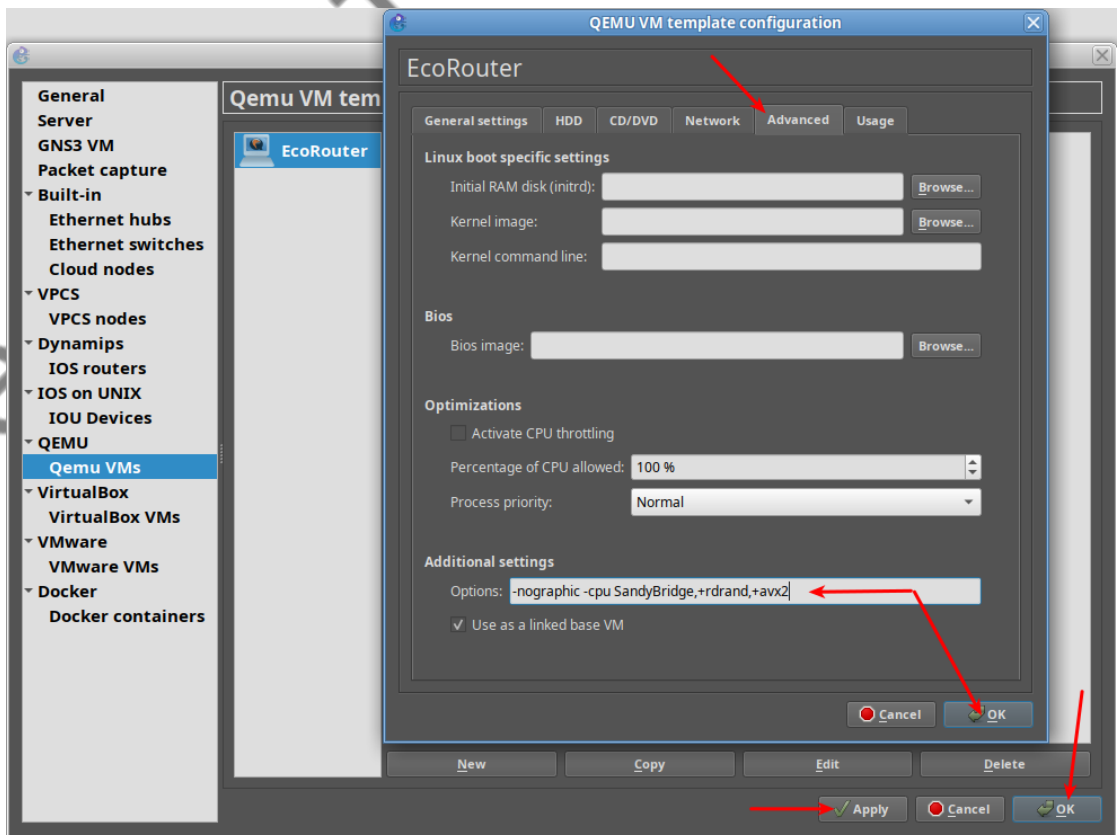
На вкладке HDD выбирать в качестве Disk interface – ide:



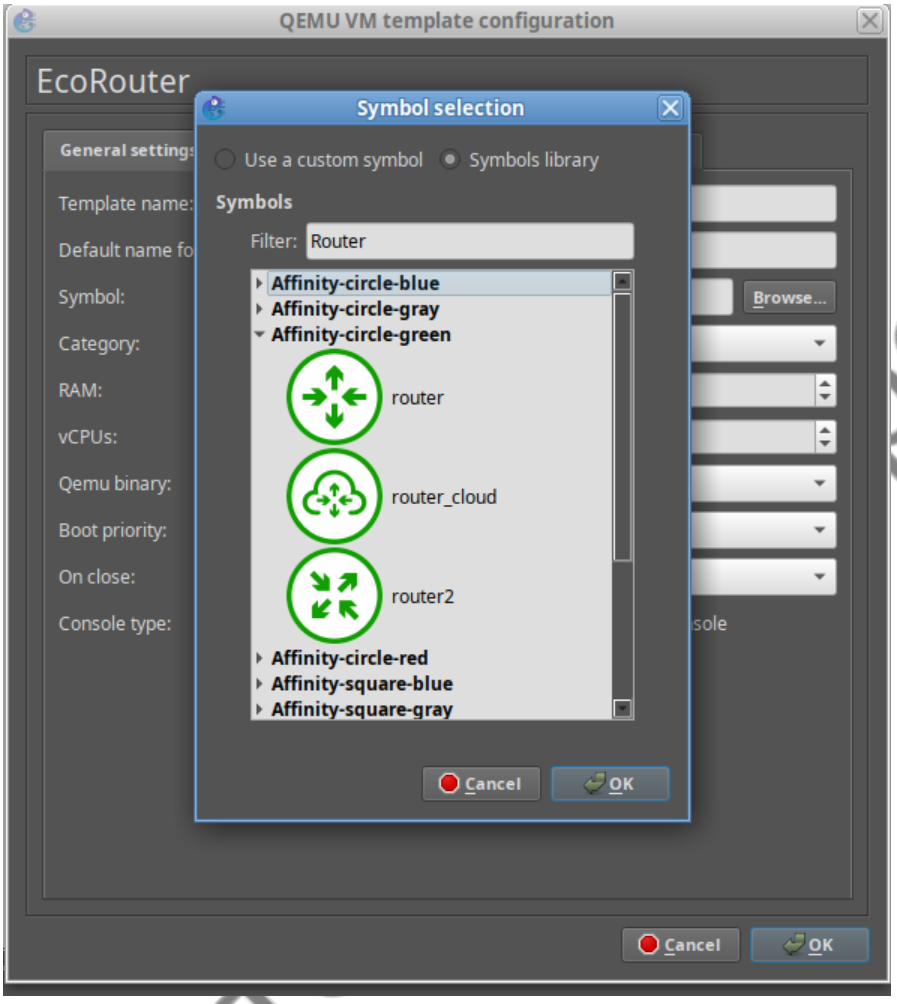
На вкладке Network произвести настройки для корректного отображения интерфейсов как на топологии в GNS3, так и внутри EcoRouter (mgmt - интерфейс необходим для корректной работы EcoRouter):



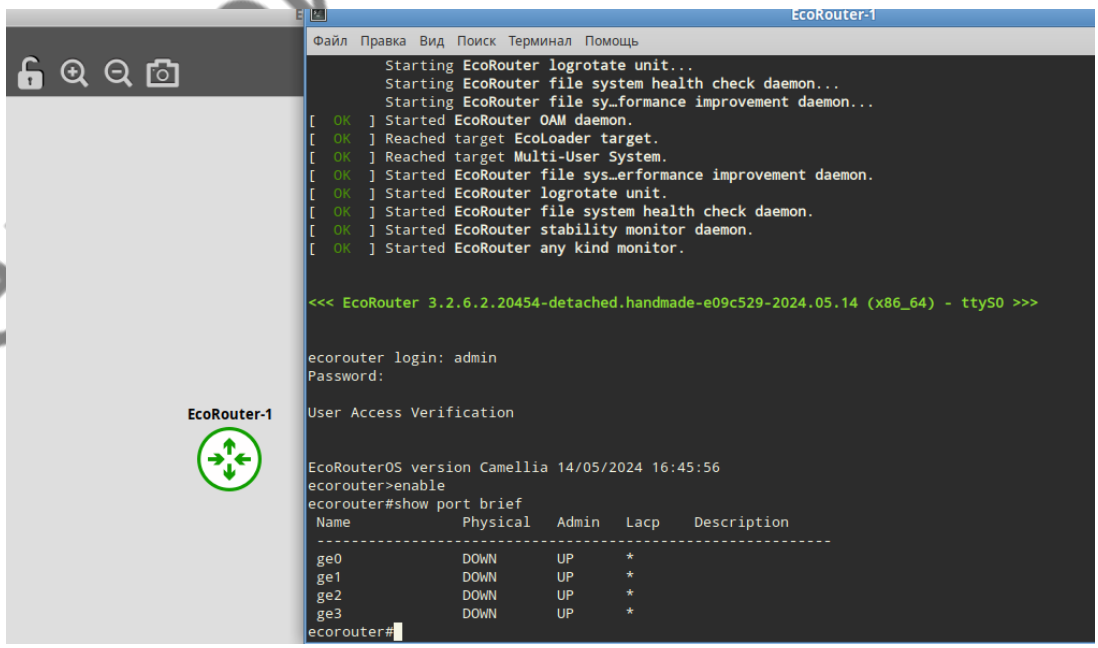
На вкладке Advanced в секции Additional settings передать правильные Options (-nographic -cpu SandyBridge,+rdrand,+avx2) затем нажать OK и Apply, OK:



При необходимости на вкладке General settings можно задать иконку для отображения маршрутизатора:



Добавить EcoRouter в топологию и проверить работоспособность (логин: пароль по умолчанию - admin:admin):

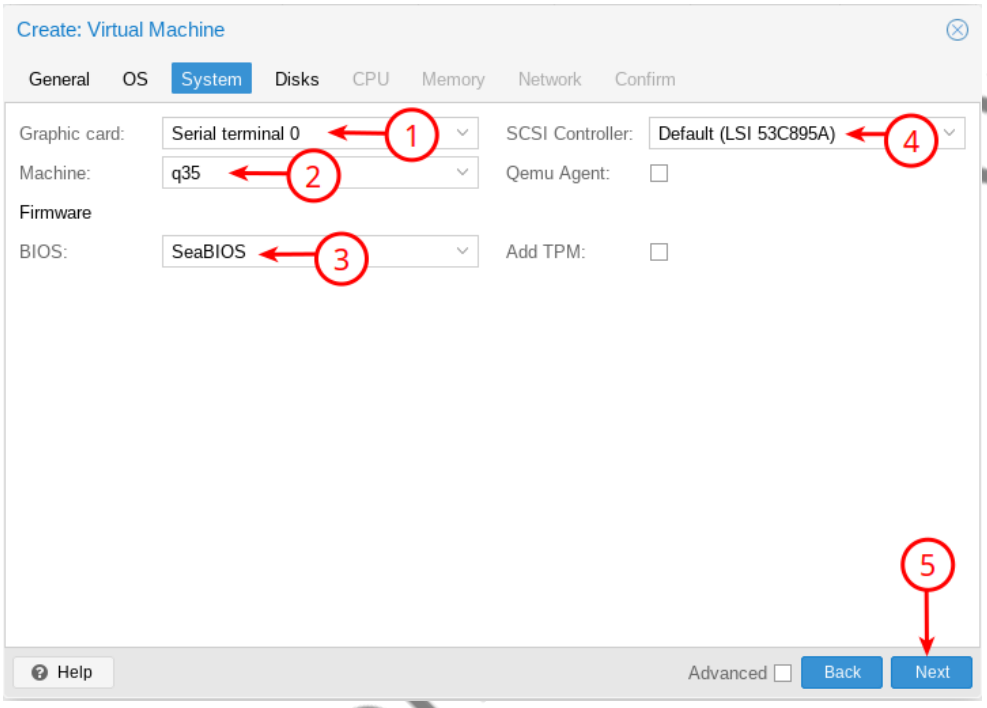


Установка EcoRouter в Альт Виртуализация PVE

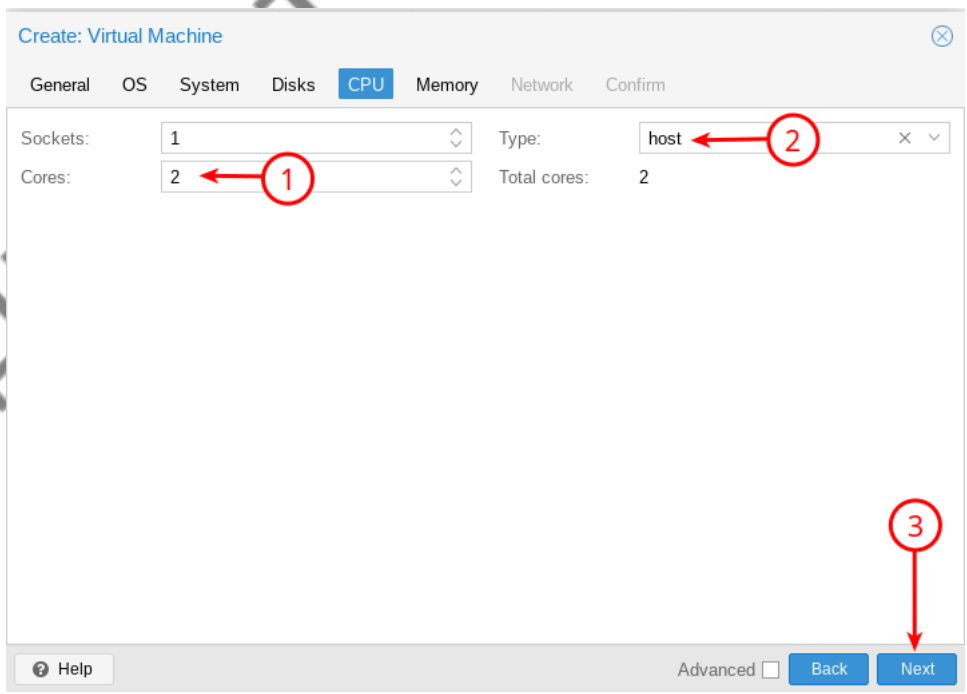
В веб-интерфейсе Альт Виртуализации для создания виртуальной машины нажимаем Create VM, задаём необходимое имя (Name) и нажимаем Next.

На следующем этапе (OS) выбираем Do not use any media (не использовать никаких носителей) и нажимаем Next.

На этапе System задаём необходимые для корректной работы настройки и нажимаем Next:

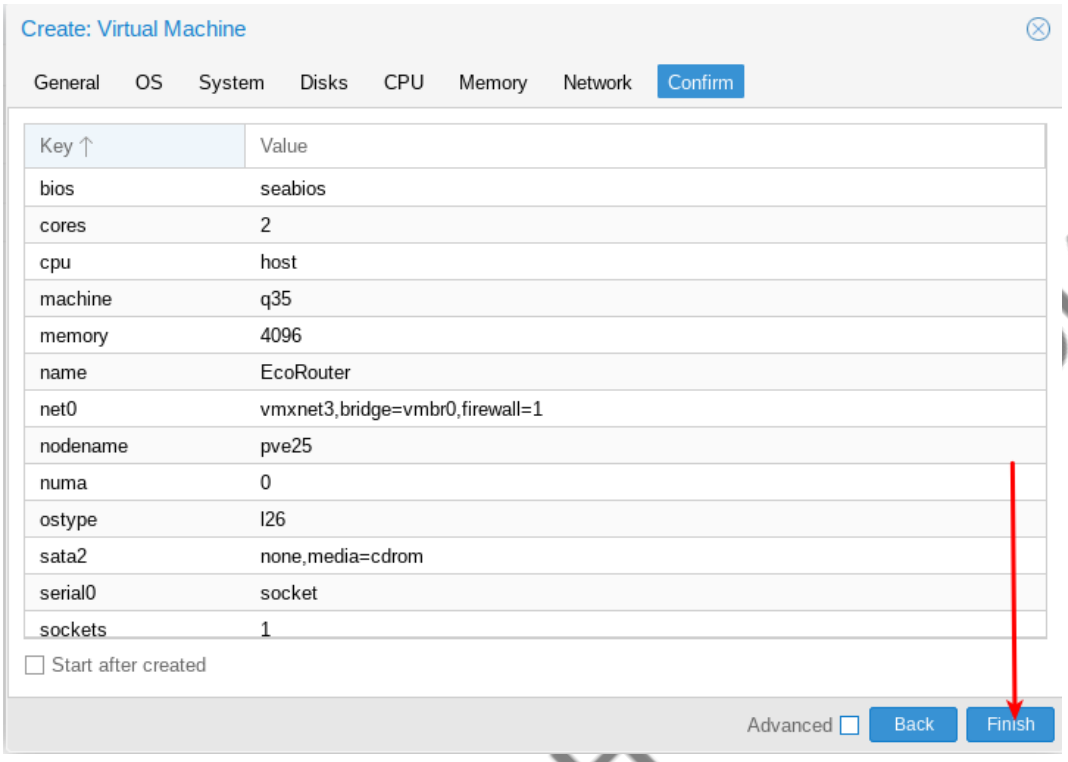


На этапе Disk удаляем scsi0 и нажимаем Next. На этапе CPU задаём необходимое кол-во (минимально необходимое для работы 2) в качестве Type выбираем host и нажимаем Next:



На этапе Memory задаём необходимый объем (минимально необходимое для работы 4 ГБ) и нажимаем Next.

Проверяем заданные ранее параметры для создаваемой виртуальной машины и нажимаем Finish:



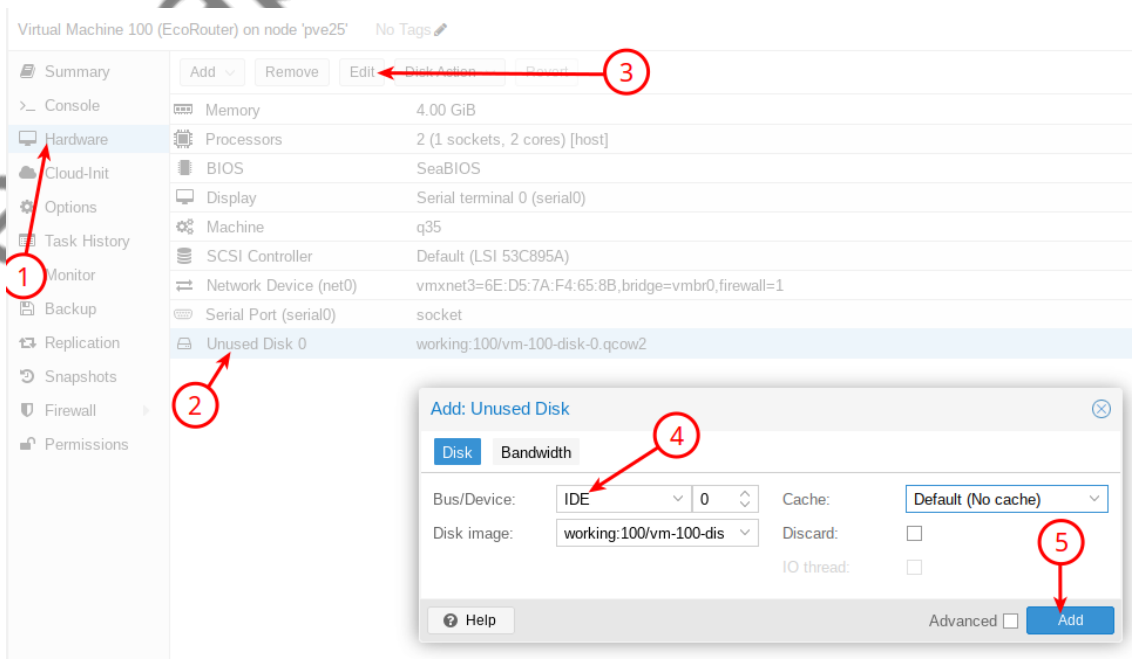
Далее переходим в консоль PVE и выполняем подключение существующего образа диска EcoRouter к только что созданной ВМ с помощью команды:

```
qm disk import 100 /home/admin/Загрузки/EcoRouter.qcow2 working --format qcow2
```

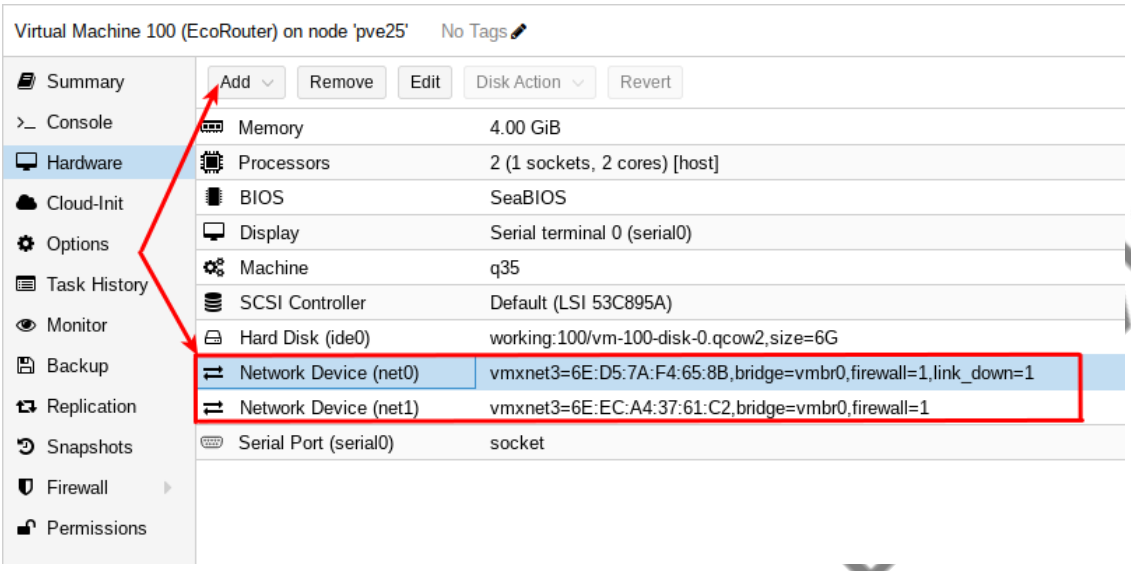
например, где:

- `100` – VM ID;
- `/home/admin/Загрузки/EcoRouter.qcow2` – путь до образа;
- `working` – имя хранилища в PVE.

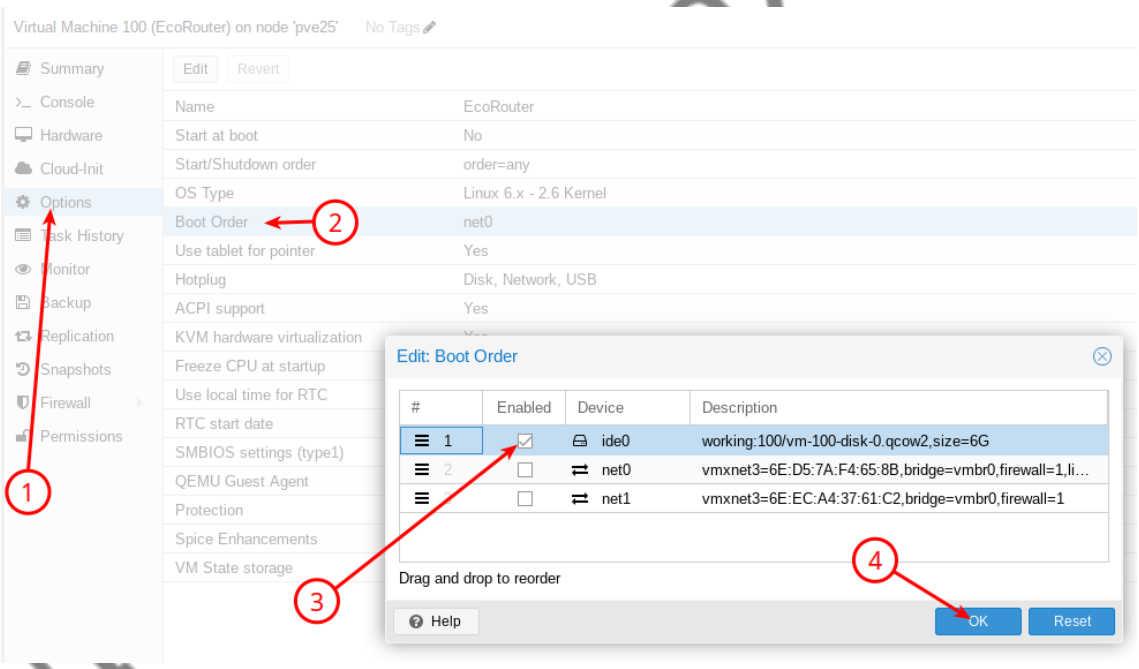
Переходим в настройки созданной ВМ на кладке Hardware выбираем только что импортированный диск и нажимаем Edit, затем выбираем IDE и нажимаем Add:



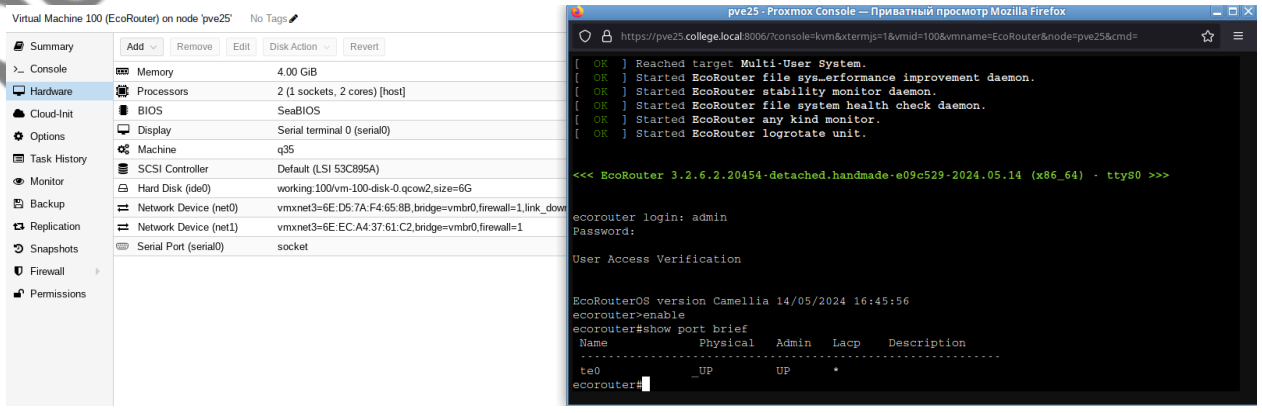
Далее для корректной работы необходимо добавить ещё один интерфейс (который можно выключить), который будет использоваться в EcoRouter в качестве mgmt:



Также на вкладке Options меняем приоритет загрузки на загрузку с диска, а не по сети как стоит по умолчанию:

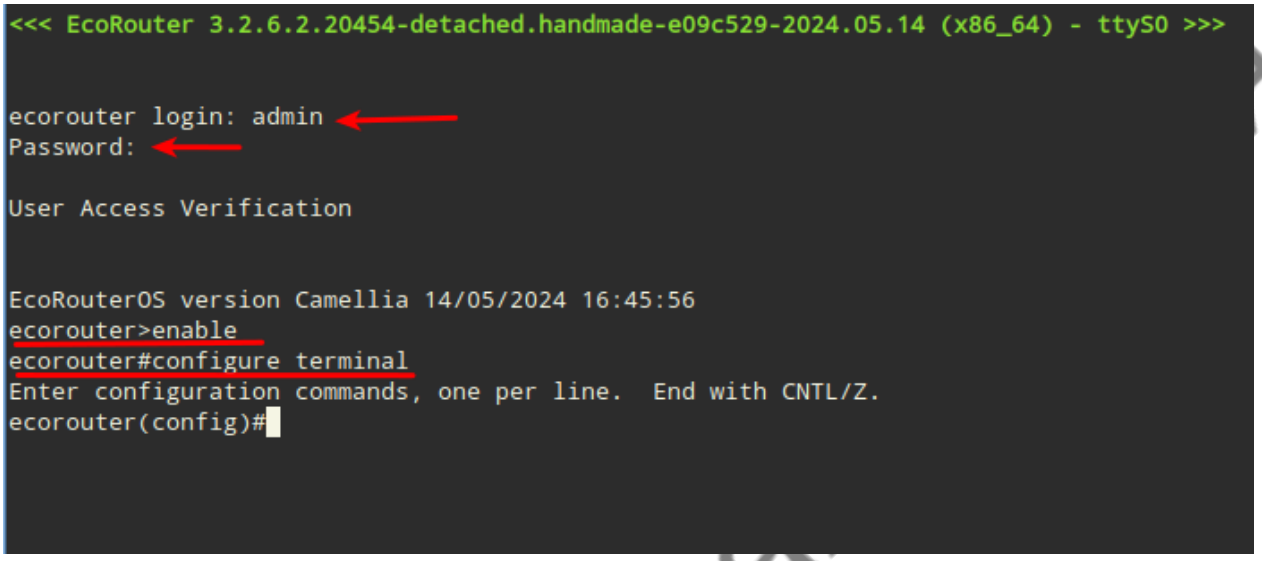


Запускаем ВМ и проверяем работоспособность (логин: пароль по умолчанию - admin:admin):



Базовая настройка EcoRouter

Вход на устройство выполняется из-под пользователя по умолчанию с логином **admin** и паролем **admin**, для перехода в привилегированный режим используется команда **enable**, для перехода из привилегированного режима в режим администрирования используется команда **configure terminal**:



Задать имя устройству можно из режима администрирования при помощи команды:

```
hostname <ИМЯ_УСТРОЙСТВА>
```

Например:

```
ecorouter(config)#hostname Eco-R1
```

Сменить пароль для пользователя по умолчанию можно из режима конфигурирования пользователя, например:

```
Eco-R1(config)#username admin
Eco-R1(config-user)#password P@ssw0rd
Eco-R1(config-user)#exit
```

В режиме конфигурирования консоли можно сменить время ожидания, чтобы не было "User is logged out by timeout":

- При значении 0 маршрутизатор не будет отключать пользователей от соответствующей линии никогда.
- Значение по умолчанию – 10 минут

Например:

```
Eco-R1(config)#line console 0
Eco-R1(config-line)#exec-timeout 0
Eco-R1(config-line)#exit
```

Аналогично и для VTY:

```
Eco-R1(config)#line vty 0 871
Eco-R1(config-line)#exec-timeout 0
Eco-R1(config-line)#exit
```

Для того чтобы задать пароль для входа в привилегированный режим (`enable`) можно воспользоваться командой из режима администрирования, например:

```
Eco-R1(config)#enable secret P@ssw0rd
```

Для того чтобы включить автоматическое шифрование паролей, можно воспользоваться командой из режима администрирования, например:

```
Eco-R1(config)#service password-encryption
```

Для того чтобы задать баннерное сообщение, можно воспользоваться командой из режима администрирования, например:

```
Eco-R1(config)#banner motd This is a secure system. Authorized Access Only!
```

Для того чтобы создать дополнительного пользователя с паролем и ролью, например позволяющей выполнять действия по администрированию устройства, можно воспользоваться командами из режима администрирования, например:

```
Eco-R1(config)#username netadmin
Eco-R1(config-user)#password P@ssw0rd
Eco-R1(config-user)#role admin
Eco-R1(config-user)#exit
```

Для того чтобы сохранить конфигурацию устройства, можно воспользоваться командой из режима администрирования, например:

```
Eco-R1(config)#write memory
```

Команды для просмотра из привилегированного режима:

Для просмотра текущей конфигурации:

```
Eco-R1#show running-config
```

Для просмотра баннера:

```
Eco-R1#show show banner motd
```

Для просмотра учетных записей пользователей, имеющихся в базе данных EcoRouter:

```
Eco-R1#show users localdb
```

Также разберёмся с основными понятиями касающимися EcoRouter:

Порт (port) – это устройство в составе EcoRouter, которое работает на уровне коммутации (L2);

Интерфейс (interface) – это логический интерфейс для адресации, работает на сетевом уровне (L3);

Service instance (Сабинтерфейс, SI, Сервисный интерфейс) является логическим сабинтерфейсом, работающим между L2 и L3 уровнями:

- Данный вид интерфейса необходим для соединения физического порта с интерфейсами L3, интерфейсами bridge, портами;
- Используется для гибкого управления трафиком на основании наличия меток VLANов в фреймах, или их отсутствия;
- Сквозь сервисный интерфейс проходит весь трафик, приходящий на порт.

Таким образом, для того чтобы назначить IPv4-адрес на EcoRouter необходимо придерживаться следующего алгоритма в общем виде:

- Создать интерфейс с произвольным именем и назначить на него IPv4;
- В режиме конфигурирования порта - создать service-instance с произвольным именем:

- указать (инкапсулировать) что будет обрабатываться тегированный или не тегированный трафик;
- указать в какой интерфейс (ранее созданный) нужно отправить обработанные кадры.

Например:

```
Eco-R1(config)#interface int0
Eco-R1(config-if)#description "Connect_S1"
Eco-R1(config-if)#ip address 192.168.0.1/24
Eco-R1(config-if)#exit
Eco-R1(config)#port ge0
Eco-R1(config-port)#service-instance ge0/int0
Eco-R1(config-service-instance)#encapsulation untagged
Eco-R1(config-service-instance)#connect ip interface int0
Eco-R1(config-service-instance)#exit
Eco-R1(config-port)#exit

Eco-R1(config)#interface int1
Eco-R1(config-if)#description "Connect_PC-B"
Eco-R1(config-if)#ip address 192.168.1.1/24
Eco-R1(config-if)#exit
Eco-R1(config)#port ge1
Eco-R1(config-port)#service-instance ge1/int1
Eco-R1(config-service-instance)#encapsulation untagged
Eco-R1(config-service-instance)#connect ip interface int1
Eco-R1(config-service-instance)#end
Eco-R1#write
Building configuration...

Eco-R1#
```

Команды проверки из привилегированного режима:

Состояние и конфигурация порта:

```
show port
```

```
show port brief
```

Конфигурация интерфейса:

```
show interface
```

Показывать информацию о сервисных экземплярах:

```
show service-instance brief
```

Показать информацию о назначенных IP-адресах:

```
show ip interface brief
```

Настройка удалённого доступа SSH

Для фильтрации принимаемого EcoRouter трафика используются так называемые профили безопасности.

Профиль безопасности представляет собой набор правил, определяющих, пакеты каких протоколов будут пропускаться маршрутизатором (и виртуальными маршрутизаторами в его составе).

Если трафик не подпадает ни под одно из правил, то он пропускается (permit).

В EcoRouter существует жестко заданный профиль по умолчанию. Изменить его нельзя.

Состав профиля по умолчанию:

```
Eco-R1#show ip vrf
 VRF default, VRF ID 0
  Interfaces:
    int0
    int1
 Security profile default
  0: deny tcp any any eq 22
  1: deny tcp any any eq 23
  2: deny tcp any any eq 161
  3: deny udp any any eq 22
  4: deny udp any any eq 23
  5: deny udp any any eq 161
  permit any any any

 VRF management, VRF ID 1
 Security profile none
  permit any any any

Eco-R1#
```

Все созданные интерфейсы относятся к профилю безопасности default по умолчанию (если не задано иное);

Таким образом, видно, что самое первое правило (0) в профиле безопасности default - запрещает любые подключения по порту 22 (ssh).

Для удаления всех правил для VRF или менеджмент порта можно назначить пустой профиль безопасности с названием security none.

```
Eco-R1#show security-profile
 Security profile none
  permit any any any

 Security profile default
  0: deny tcp any any eq 22
  1: deny tcp any any eq 23
  2: deny tcp any any eq 161
  3: deny udp any any eq 22
  4: deny udp any any eq 23
  5: deny udp any any eq 161
  permit any any any
```

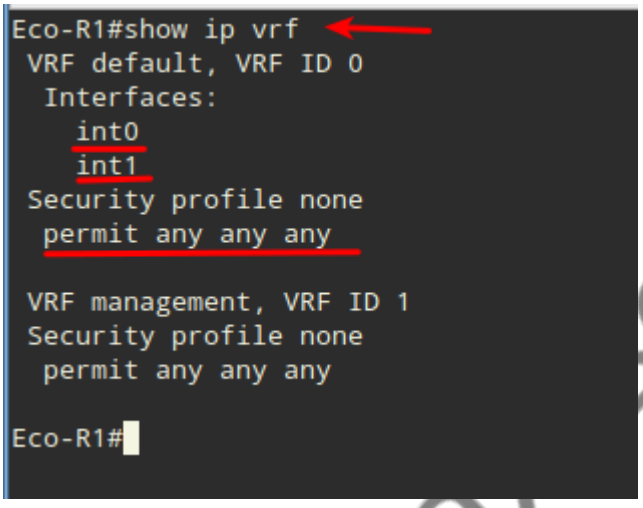
В отличие от профиля безопасности default - профиль безопасности none - не содержит каких-либо запрещающих правил.

Переключить профиль безопасности с default на none, можно из режима администрирования при помощи команды:

```
security none
```

Проверить можно используя команду привилегированного режима:

```
show ip vrf
```



Приложение 3

Знакомство с Ideco NGFW

Межсетевой экран Ideco NGFW – современное отечественное (российское) программное решение для защиты сетевого периметра, обеспечивающее полный контроль доступа в интернет, делающее доступ управляемым, безопасным и надежным. Данное решение входит в реестр российского программного обеспечения Минцифры Российской Федерации и имеет запись в Едином реестре российских программ для электронных вычислительных машин и баз данных № 329 от 08.04.2016.

Для начала работы с межсетевым экраном Ideco NGFW необходимо ознакомиться с минимальными системными требованиями, которые представлены в таблице ниже (согласно официальной документации). Минимальные системные требования предлагаются из расчёта обслуживания небольшого количества авторизованных субъектов безопасности (до 50).

Комплектующие	**Системные требования**
Процессор	Intel Core i3/i5/i7/i9/Xeon с поддержкой SSE 4.2
Объем оперативной памяти	16 ГБ (16-64 ГБ в зависимости от количества пользователей)
Дисковая подсистема	SSD, объемом 150 Гб или больше, с интерфейсом SATA, mSATA, SAS, NVMe. Дополнительный SSD при использовании почтового сервера
Сеть	Две сетевые карты (или два сетевых порта) 100/1000 Mbps. Рекомендуется использовать карты на чипах Intel. Поддерживаются Realtek, D-Link и другие
Гипервизоры	VMware, Microsoft Hyper-V (виртуальные машины 2-го поколения), VirtualBox, KVM, Citrix XenServer, Proxmox VE
Дополнительно	Монитор и клавиатура
Замечания	Обязательна поддержка UEFI. Не поддерживаются программные RAID-контроллеры (интегрированные в чипсет). Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти. Отключить опцию Secure Boot в UEFI.

Помимо минимальных системных требований, важно также соблюдать ряд обязательных условия для работы с Ideco NGFW:

1. Обязательная поддержка UEFI;
2. Для виртуальных машин необходимо использовать фиксированный, а не динамический размер хранилища и оперативной памяти (исключением является – использование в лабораторных и тестовых целях);
3. Должен быть отключён режим Legacy загрузки, он может называться CSM (Compatibility Support Module);
4. Должна быть отключена опция Secure Boot в UEFI.

Для оптимального выбора аппаратной платформы стоит обратить внимание на рекомендации по подбору оборудования для Ideco NGFW.

Примеры типовых конфигураций, которые зависят от количества пользователей, представлены ниже в таблице и относятся ко всем функциональным возможностям продукта Ideco NGFW.

Количество пользователей	**Модель процессора**	**Объем оперативной памяти**	**Дисковая подсистема**	**Сетевые адаптеры**
до 100	Intel Core i3 или совместимый	16 ГБ	150 ГБ	2 шт.
до 350	Intel Core i5 или совместимый	16 ГБ	240 ГБ	2 шт.
до 1000	Intel Core i7, Xeon-E, Xeon Scalable от 8 ядер или совместимый	32 ГБ	480 ГБ	2 шт.
от 1000 до 3000	Intel Xeon Silver 4214R или совместимый	64 ГБ	480 ГБ	2 шт.
от 3000	Xeon Gold 6238R 28 Cores или совместимый	64 ГБ	480 ГБ	2 шт.

Согласно официальной документации - Ideco NGFW получает обновления из следующих источников:

- Отсылка уведомлений в личный кабинет/телеграм-бот: alerts.v18.ideco.dev;
- Обновление баз Контент-фильтра: content-filter.v18.ideco.dev;
- Отсылка анонимной статистики: gatherstat.v18.ideco.dev;
- Обновления баз GeoIP: ip-list.v18.ideco.dev;
- Обмен информации о лицензии: license.v18.ideco.dev;
- Отправка отчетов по почте: send-reports.v18.ideco.dev;
- Обновления suricata: suricata.v18.ideco.dev;
- Обновления системы: sysupdate.v18.ideco.dev;
- Синхронизация времени: ntp.ideco.ru;
- Антивирус Касперского для обновления баз использует список серверов, указанный на официальном сайте "Лаборатории Касперского"

Часть запросов к указанным выше серверам может быть перенаправлена на mcs-vm.ideco.ru, update.ideco.ru, storage.yandexcloud.net.

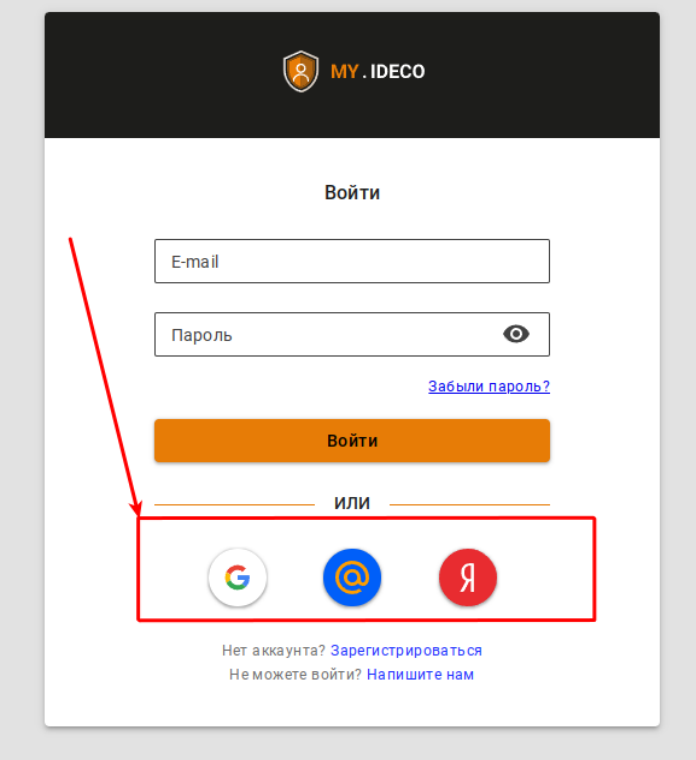
Таким образом, для корректной работы всех модулей фильтрации Ideco NGFW необходимо, чтобы доступ к вышеуказанным ресурсам был разрешен настройками фильтрации.

Чтобы начать работать с Ideco NGFW необходимо получить и загрузить установочный образ. Получить загрузочный образ нужно из личного кабинета MY.IDECO доступного по https://my.ideco.ru.

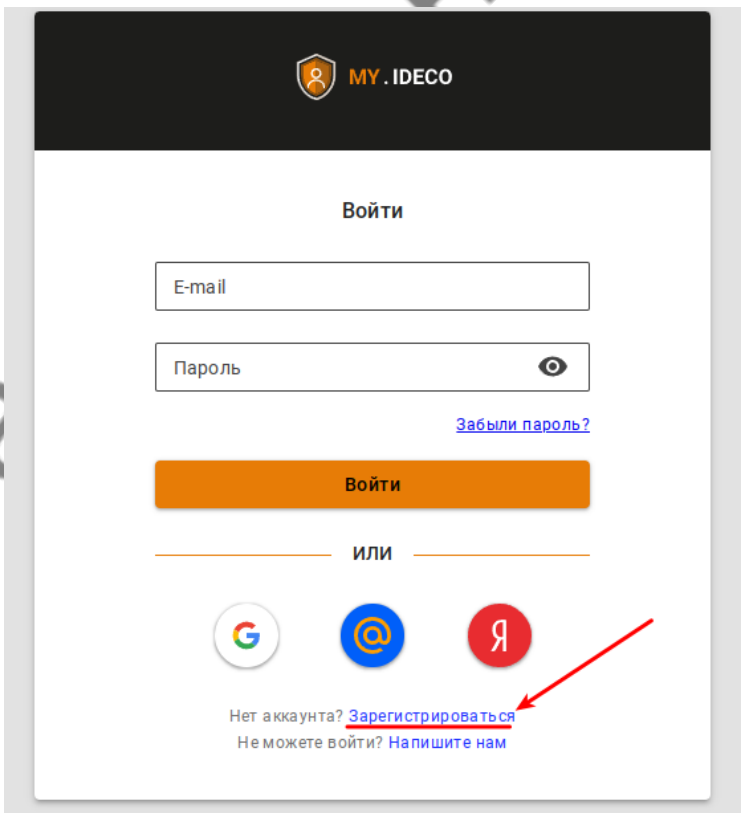
Зарегистрировавшись на my.ideco.ru вы сможете управлять лицензиями, скачивать загрузочные образы всех продуктов, разрабатываемых компанией Ideco.

Выполнить вход (регистрацию) в личный кабинет MY.IDECO можно двумя способами:

1) Выполнить вход через авторизованные социальные сети из предложенного списка:



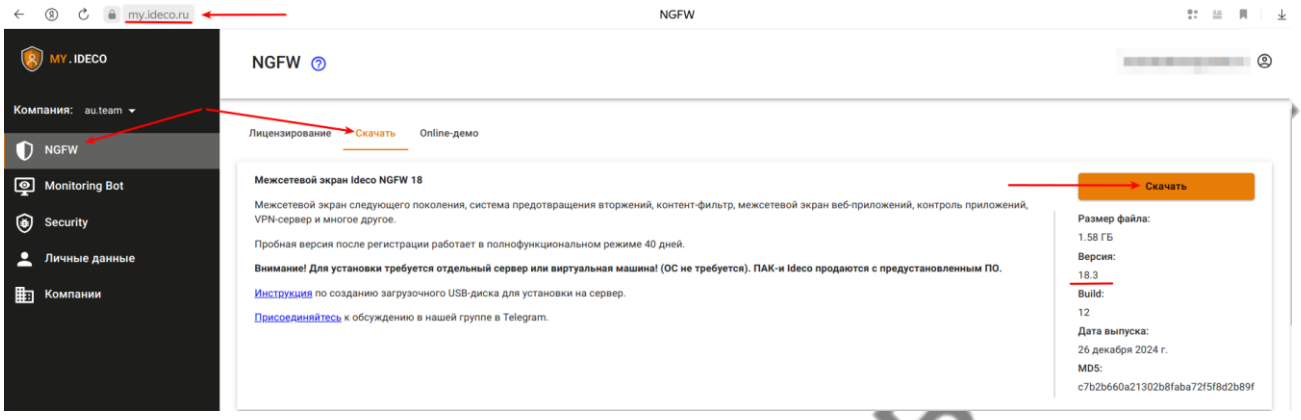
2) Выполнить процедуру полноценной регистрации нажав на ссылку «Зарегистрироваться»:



После выбранного вами способа входа (Регистрация или Авторизация через социальные сети) доступ в личный кабинет будет выглядеть следующим образом:

В данном случае вход выполнен с помощью «Авторизация через социальные сети» на примере Яндекс почты.

После успешной авторизации в личном кабинете MY.IDECO можно перейти в левом боковом меню на вкладку NGFW, после чего нажать на раздел Скачать, выбрать необходимую версию межсетевого экрана Ideco NGFW или иного продукта Ideco и нажать на кнопку Скачать, после чего будет выполнено скачивание установочного образа (в данном случае образ ideco-ngfw-18.3-release):



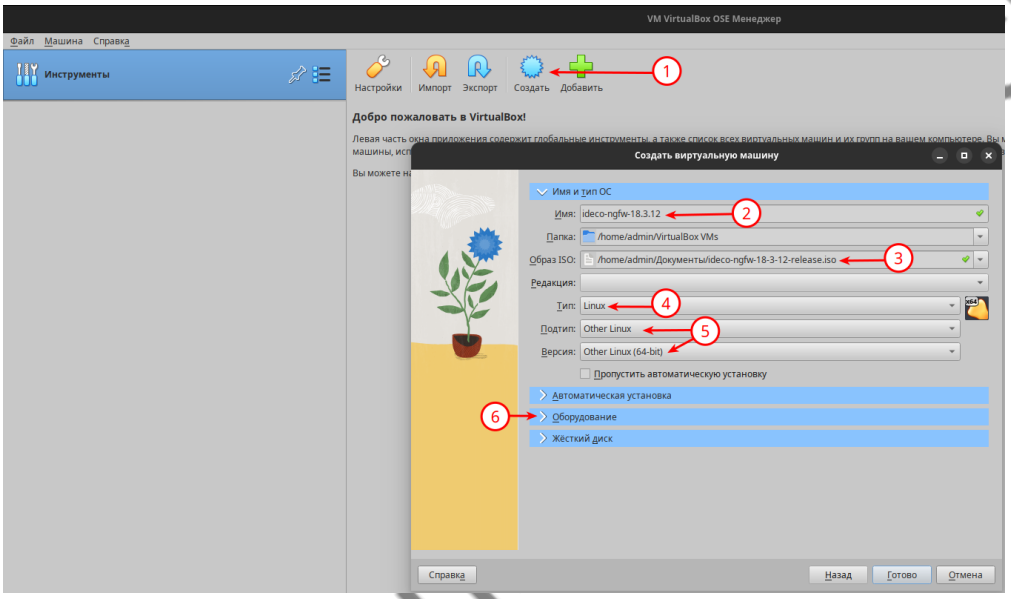
Помимо возможности загрузки актуальных версий различных продуктов Ideco, личный кабинет MY.IDECO позволяет пользователю получить информацию:

- об имеющихся лицензиях (раздел Лицензирование)
- о сроке окончания подписки на обновления модулей и технической поддержки

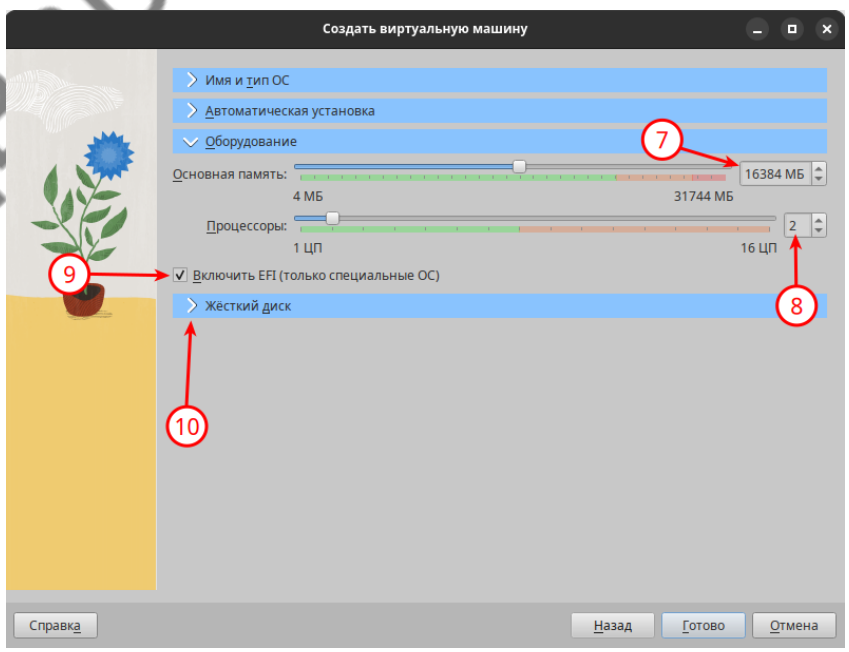
Установка Ideco NGFW в VirtualBox

Создание виртуальной машины в VirtualBox для установки Ideco NGFW:

1. В VirtualBox в главном окне Инструменты нажимаем «Создать»;
2. Задаём имя для создаваемой виртуальной машины, например: ideco-ngfw-18.3.12;
3. Указываем путь до установочного образа с Ideco NGFW в формате iso;
4. В качестве Тип: выбираем Linux;
5. В качестве Версия: выбираем Other Linux (64-bit);

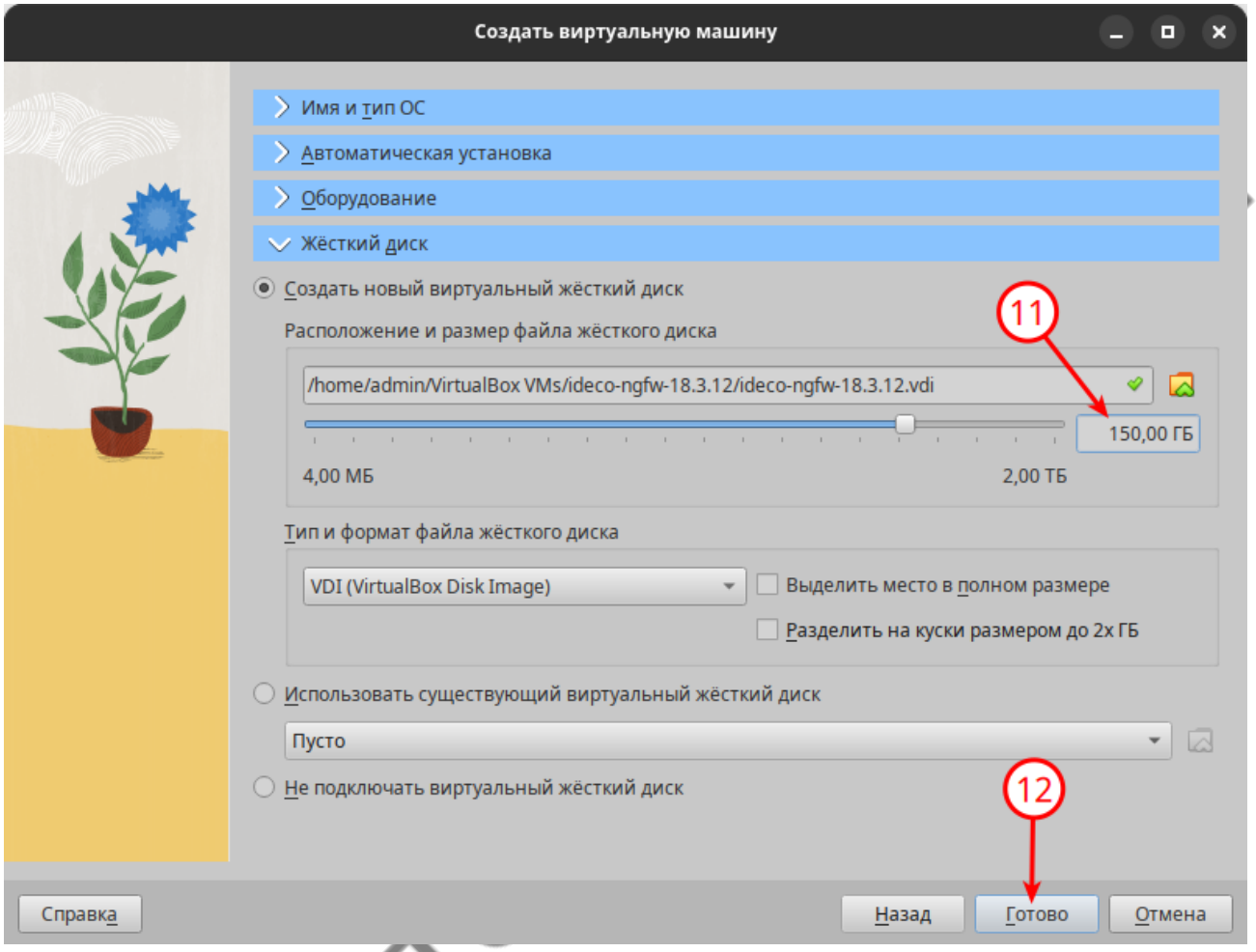


6. Нажимаем Оборудование;
7. Указываем минимально необходимый объем «Основной памяти» (ОЗУ/RAM) 16 ГБ;
8. Задаём произвольное количество vCPU, например 2;
9. Выставляем чек-бокс «Включить EFI»;
10. Нажимаем Жёсткий диск;

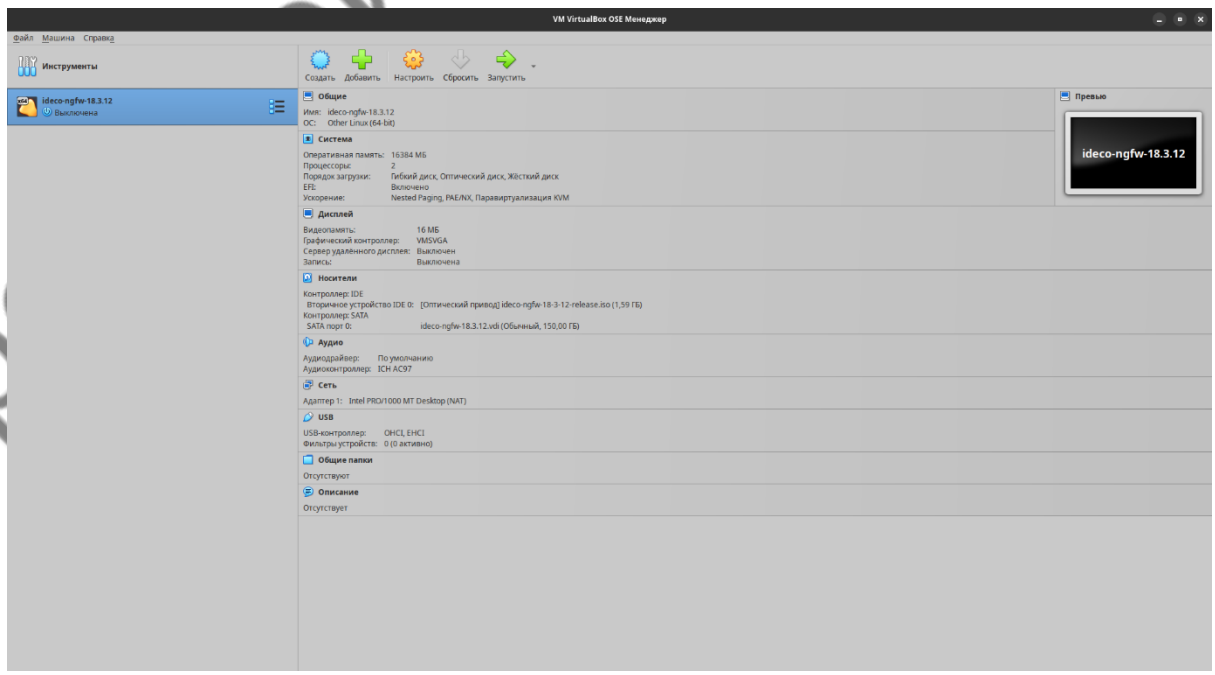


11. Задаём минимально необходимый размер дискового пространства 150 ГБ;

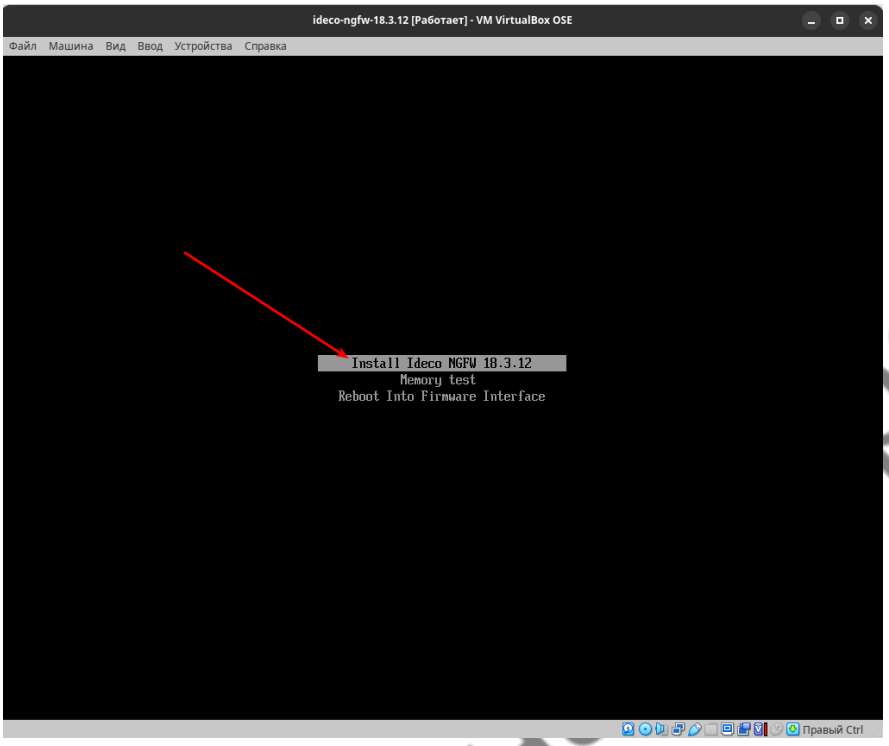
12. Нажимаем Готово.



В результате получаем созданную виртуальную машину с именем ideco-ngfw-18.3.12 со следующими параметрами (в правой части экрана):

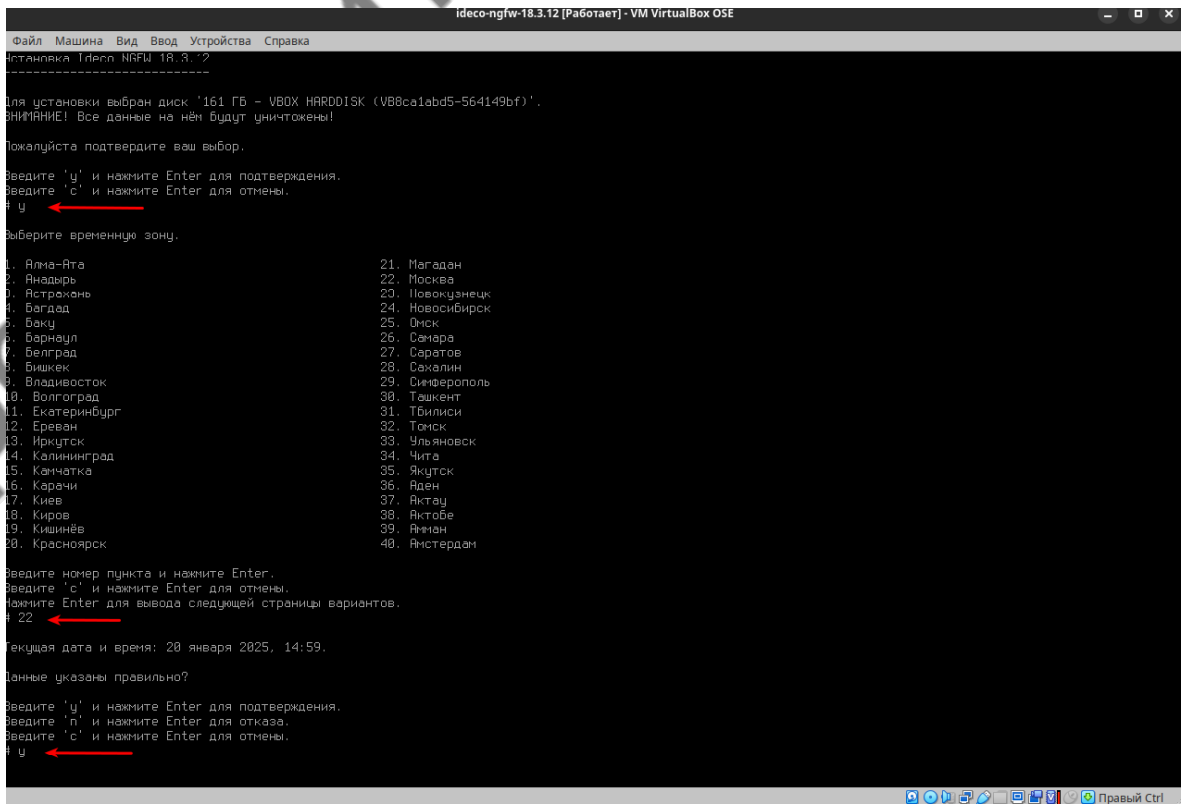


Запускаем виртуальную машину. Выбираем стрелками на клавиатуре пункт меню Install Ideco NGFW и нажимаем Enter (важно, чтобы была отключена опция Secure Boot в UEFI):

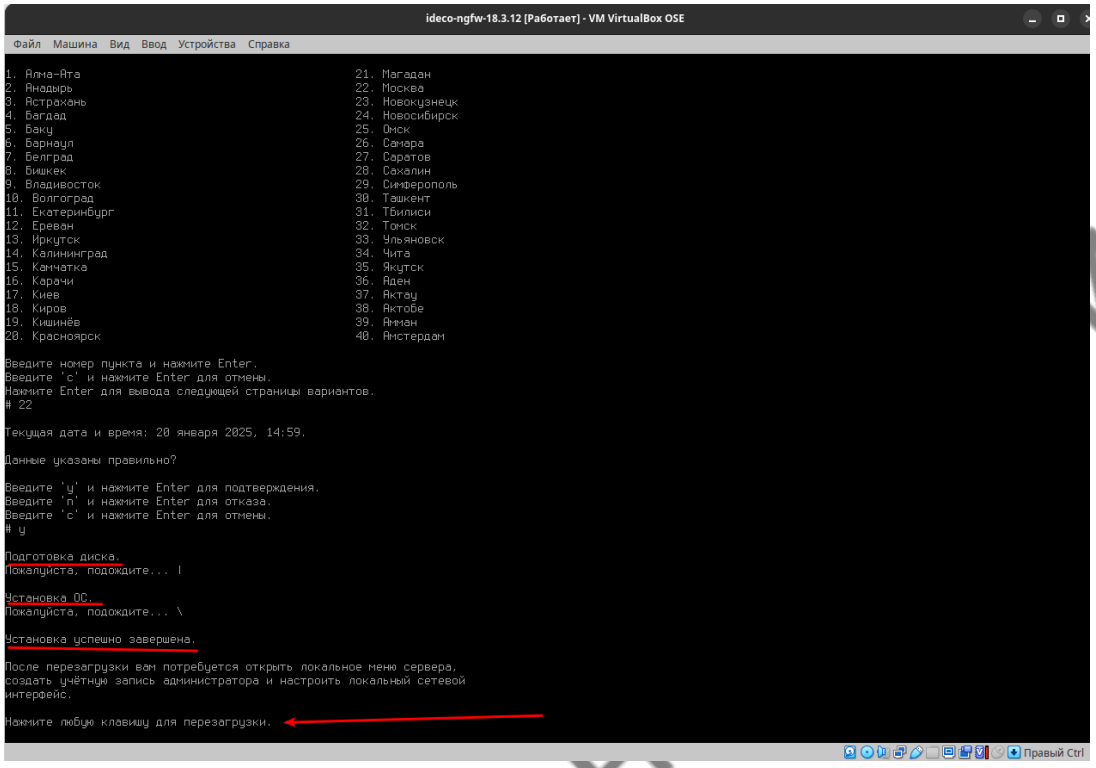


После чего начнётся процесс установки Ideco NGFW на виртуальную машину.

На первый вопрос в качестве подтверждения того, что данные на диске будут уничтожены отвечаем утвердительно вводим для этого с клавиатуры «y» и нажимаем Enter. Выбираем необходимую временную зону: так, для выбора зоны «Москва» вводим «22» (на выбор доступны 40 зон, с которыми можно ознакомиться на скриншоте) и нажимаем Enter. Проверяем корректность текущей даты и времени, после чего для подтверждения вводим с клавиатуры «y» и нажимаем Enter.



Далее начнётся сам процесс установки операционной системы на виртуальную машину. После завершения установки нажимаем любую клавишу на клавиатуре для перезагрузки:



После перезагрузки появится приглашение входа в терминал не пытайтесь выполнять вход из-под какого-либо пользователя.

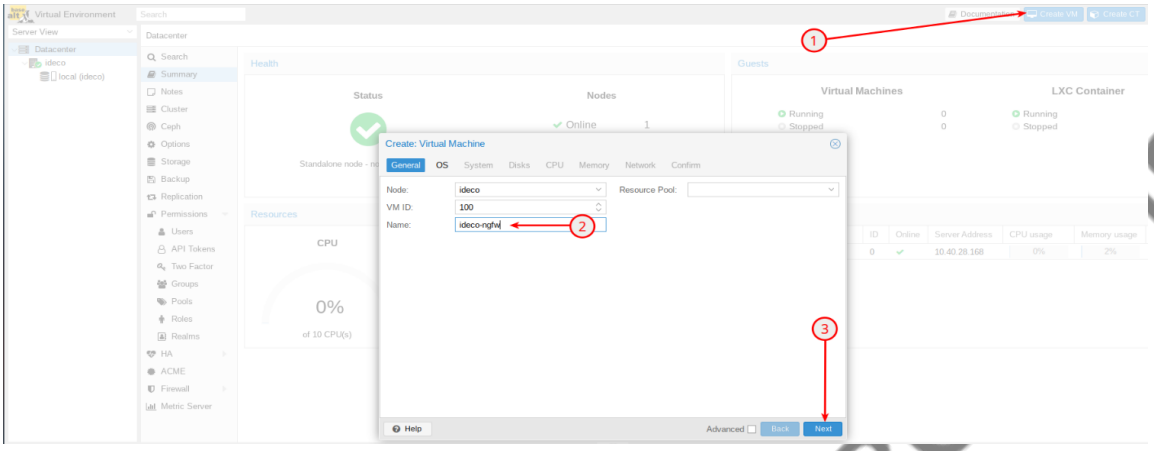
Ожидайте несколько минут (время может варьироваться и зависит от вычислительных мощностей), после чего вам станет доступна локальная консоль Ideco.

Примечание:

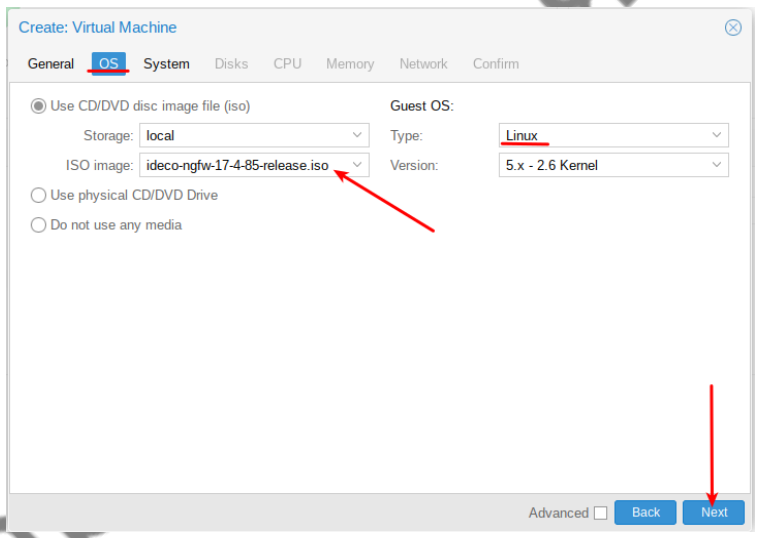
На данном этапе при необходимости можно выполнить создание шаблона виртуальной машины с установленным Ideco NGFW, для этого необходимо выключить виртуальную машину. Текущее состояние виртуальной машины наилучшим образом подходит для создания шаблона.

Установка Ideco NGFW в Альт Виртуализация PVE

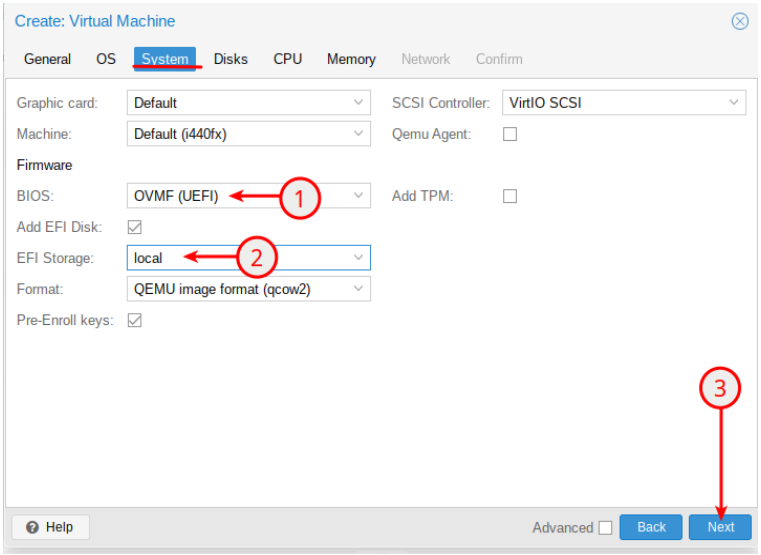
В веб-интерфейсе Альт PVE нажимаем Create VM, после чего задаём имя виртуальной машины (в данном случае имя ideco-ngfw) и нажимаем Next:



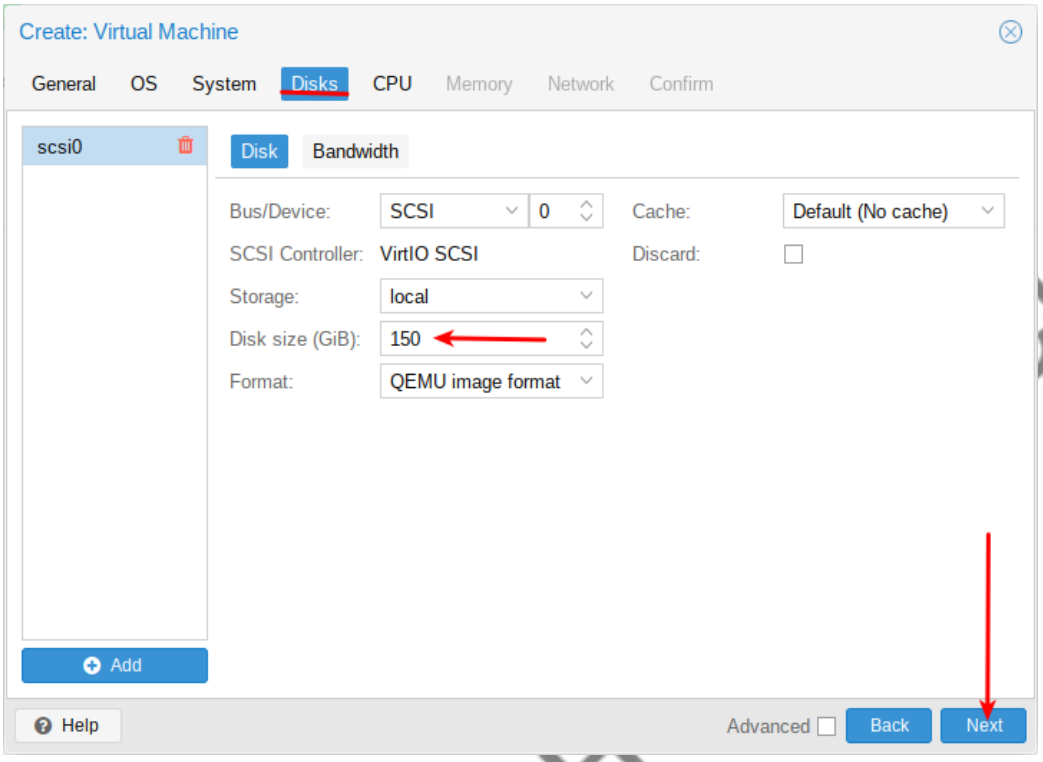
На вкладке OS – оставляем в качестве типа гостевой ОС (Guest OS) Linux, а в качестве установочного образа (ISO image) выбираем ранее скачанный и загруженный в хранилище Альт PVE ISO образ Ideco NGFW:



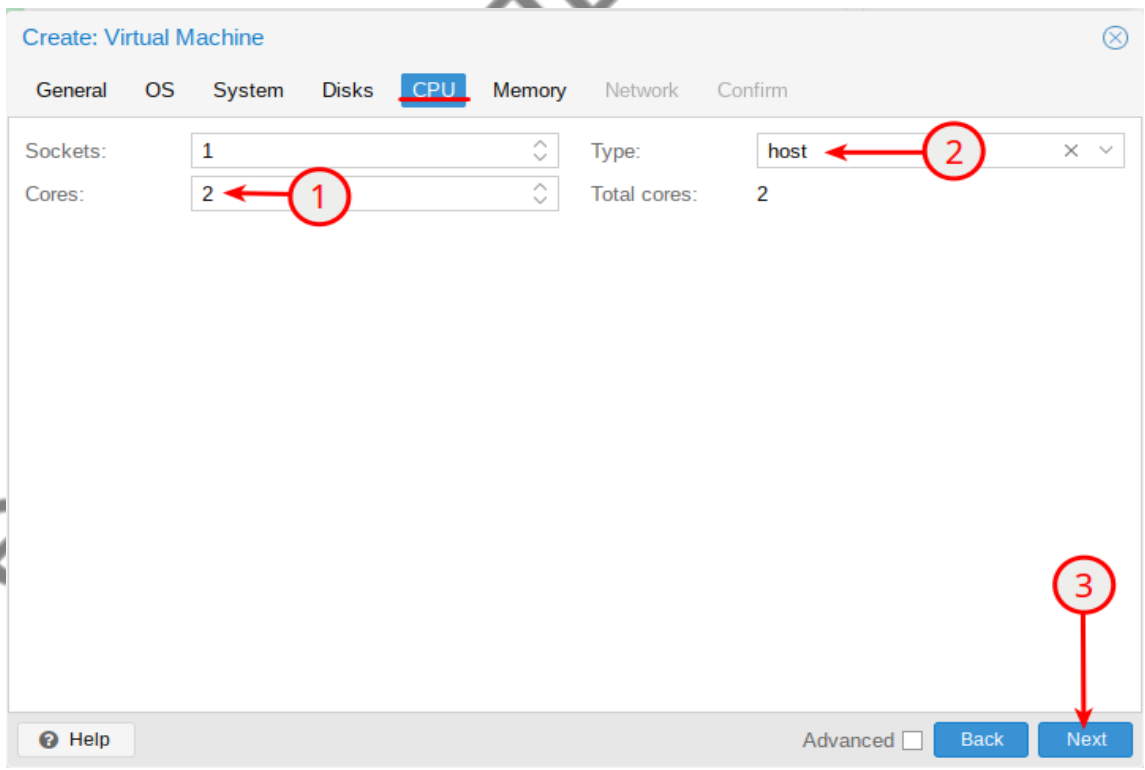
На этапе System выбираем в секции BIOS поддержку UEFI, указываем локальное хранилище Альт PVE с именем local для хранения диска EFI и нажимаем Next:



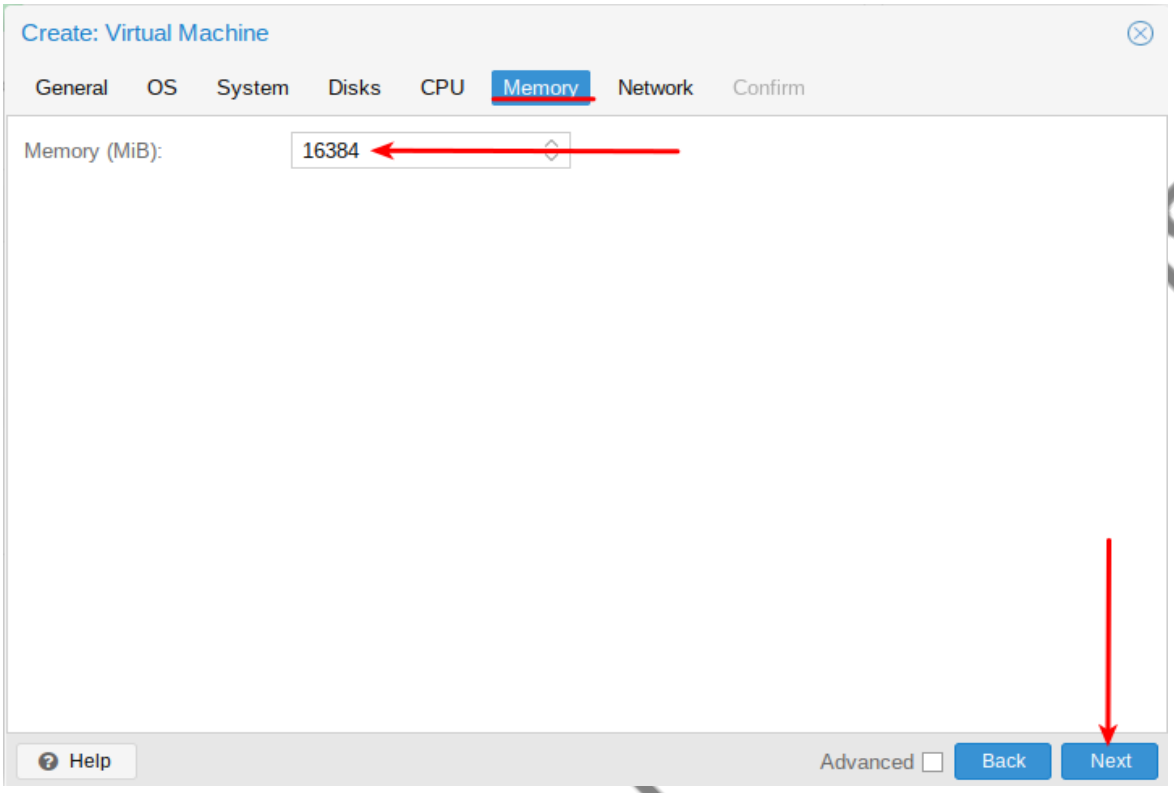
На этапе Disks задаём размер виртуального жёсткого диска согласно минимально необходимому объёму для установки Ideco NGFW в 150 ГБ и нажимаем Next:



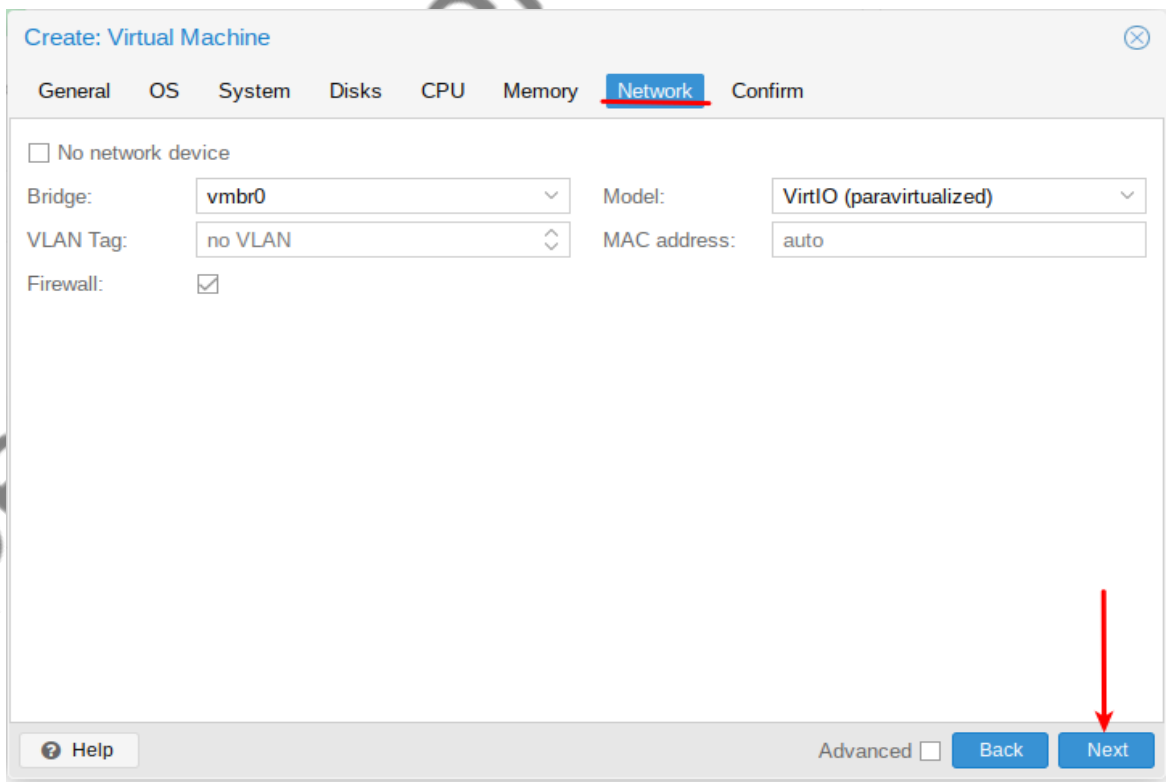
На этапе CPU задаём параметр количества ядер (Cores): 2, а в качестве типа выбираем host (т. к. необходима поддержка SSE 4.2), и нажимаем Next:



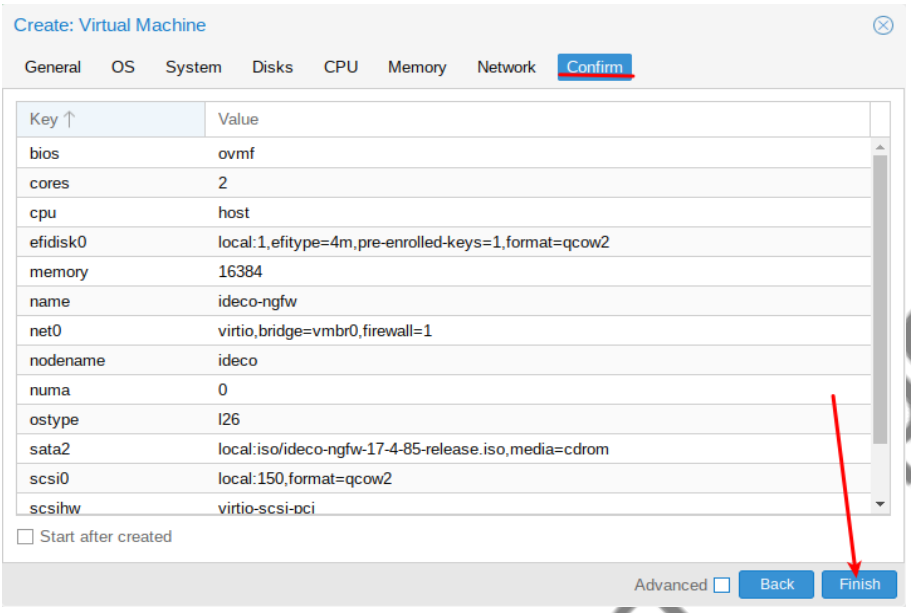
На этапе Memory задаём размер ОЗУ согласно минимально необходимому объёму для установки Ideco NGFW в 16 ГБ и нажимаем Next:



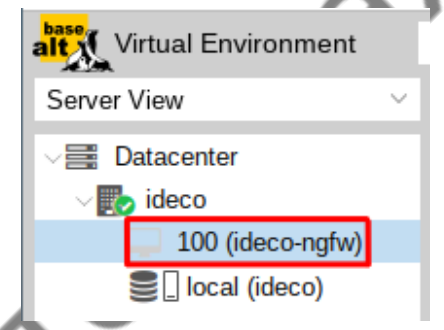
На этапе Network оставляем Bridge vmbr0 по умолчанию и нажимаем Next. Далее сетевой интерфейс с именем vmbr0 будет использоваться для доступа в сеть Интернет. Для локальной сети в дальнейшем необходимо дополнительно добавить Bridge с именем vmbr1.



На этапе Confirm проверяем ранее заданную конфигурацию виртуальной машины и нажимаем Finish:



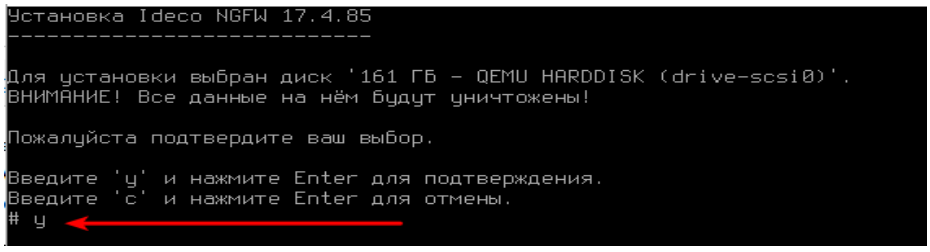
В результате будет создана виртуальная машина с именем ideco-ngfw:



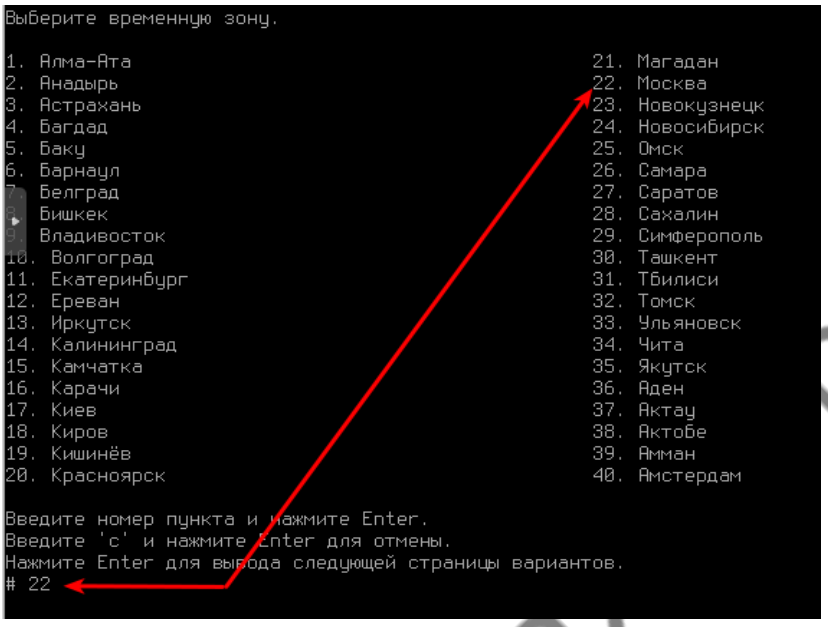
После запуска созданной виртуальной машины выбираем стрелками на клавиатуре пункт меню Install Ideco NGFW 17.4.85 и нажимаем Enter (важно, чтобы была отключена опция Secure Boot в UEFI)

После этого начнётся процесс установки Ideco NGFW на виртуальную машину.

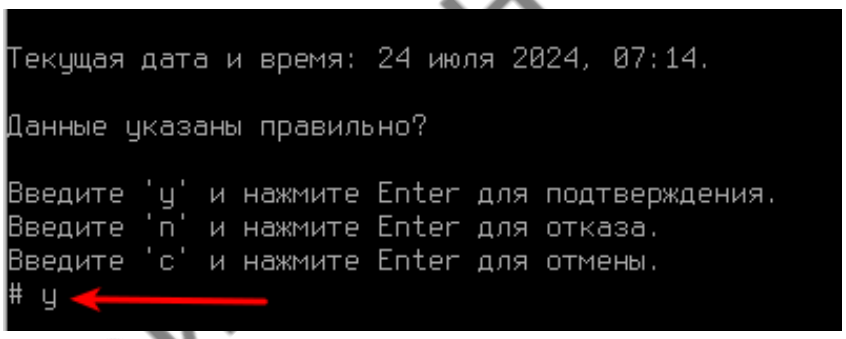
На первый вопрос в качестве подтверждения того, что данные на диске будут уничтожены отвечаем утвердительно и вводим для этого с клавиатуры «y» и нажимаем Enter:



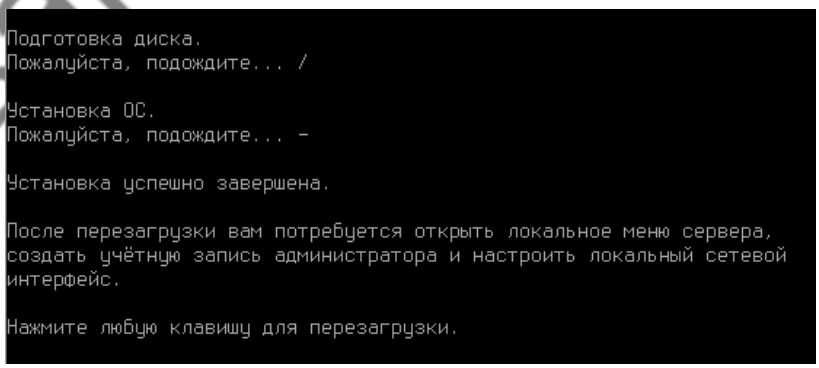
На следующем шаге выбираем необходимую временную зону: так, для выбора зоны «Москва» вводим «22» (на выбор доступны 40 зон, с которыми можно ознакомиться на скриншоте) и нажимаем Enter:



Проверяем корректность указания текущей даты и времени, после чего для подтверждения вводим с клавиатуры «y» и нажимаем Enter:



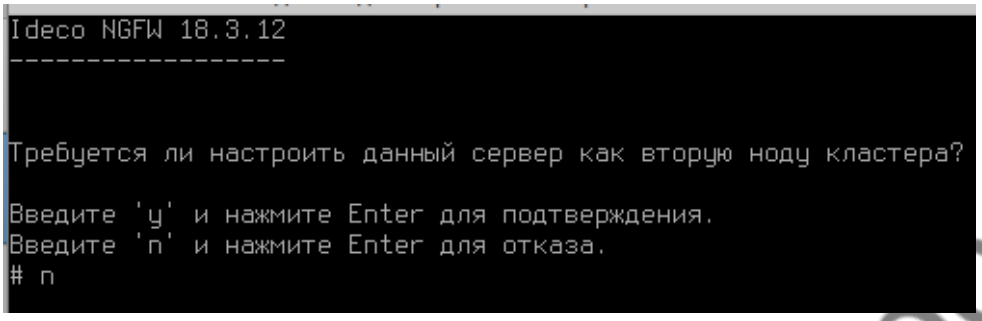
Далее начнётся сам процесс установки операционной системы на виртуальную машину. После завершения установки нажимаем любую клавишу на клавиатуре для перезагрузки:



После перезагрузки появится приглашение входа в терминал не пытайтесь выполнять вход из-под какого-либо пользователя. Ожидайте несколько минут (время может варьироваться и зависит от вычислительных мощностей), после чего вам станет доступна локальная консоль Ideco.

Базовая настройка Ideco NGFW

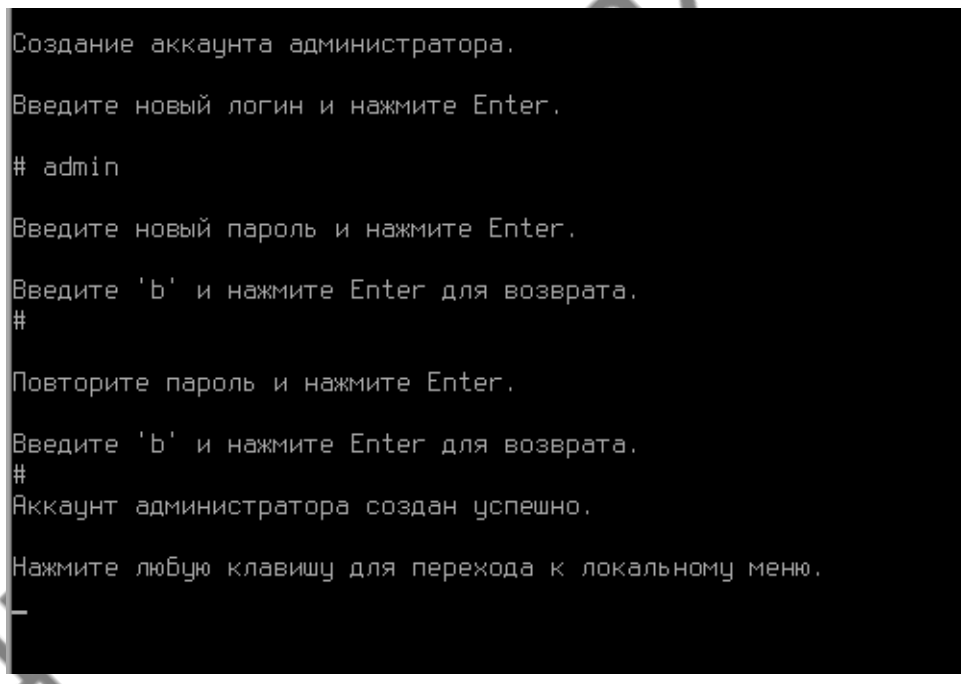
Поскольку в настоящий момент не рассматривается работа в кластерном режиме, то на первый вопрос вводим с клавиатуры «n» для отказа и нажимаем Enter:



На следующем этапе происходит создание аккаунта администратора:

Минимальные требования к паролю:

- Минимальная длина пароля – 12 символов;
- Содержит только строчные и заглавные латинские буквы;
- Содержит цифры;
- Содержит специальные символы (! # $ % & ' * + и другие).



Если пароль не соответствует требованиям политики безопасности, то появится надпись с информацией, что пароль ненадежен. Потребуется ввести новый пароль с учетом требований к нему (описанных выше).

Важно!

Не используйте Numpad при введении пароля, поскольку в будущем это может привести к проблемам при авторизации администратора.

После создания локального администратора необходимо выполнить настройку локального интерфейса, для дальнейшего доступа через веб-интерфейс.

Нажимаем любую клавишу на клавиатуре для перехода к локальному меню, после чего выполняем вход из-под только что созданного пользователя admin с паролем, который вы установили для данного пользователя (например: idecoP@ssw0rd):

```
Нажмите любую клавишу для перехода к локальному меню.
Вход в локальное меню.

Введите логин и нажмите Enter.

# admin

Введите пароль и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
#

Внимание! Не найдено ни одного настроенного локального
сетевого интерфейса. Его необходимо настроить для доступа
к веб-интерфейсу управления сервером.
```

При использовании сетевых карт одного производителя могут возникнуть трудности с их идентификацией при настройке сетевого интерфейса. Для правильной идентификации рекомендуется использовать MAC-адрес сетевой карты.

После того как выбран соответствующий локальный интерфейс необходимо настроить на нём статический адрес. Для отказа в настройке локальной сети автоматически через DHCP вводим с клавиатуры «n» и нажимаем Enter. Назначаем статический адрес на локальный интерфейс в формате IP/префикс. В данном случае назначаем первый адрес из сети 10.0.10.0/24:

```
Внимание! Не найдено ни одного настроенного локального
сетевого интерфейса. Его необходимо настроить для доступа
к веб-интерфейсу управления сервером.


Выберите сетевую карту.

1. 08:00:27:4b:d9:46 Intel Corporation 82540EM Gigabit Ethernet Controller Link N/A
2. 08:00:27:66:22:db Intel Corporation 82540EM Gigabit Ethernet Controller Link N/A

Введите номер пункта и нажмите Enter.
Введите 'c' и нажмите Enter для отмены.
# 2

Настроить локальную сеть автоматически через DHCP?

Введите 'y' и нажмите Enter для подтверждения.
Введите 'n' и нажмите Enter для отказа.
# n

Введите IP/префикс и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# 10.0.10.1/24

Введите адрес шлюза (или оставьте пустым) и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
#

Введите VLAN тэг (или оставьте пустым) и нажмите Enter.

Введите 'b' и нажмите Enter для возврата.
Введите 'c' и нажмите Enter для отмены.
# _
```

После успешной настройки локального интерфейса станет доступно основное меню в консоли Ideco NGFW:

```
Локальный интерфейс успешно настроен.

Управление сервером

1. Консоль
2. Отключить все интерфейсы и настроить новый
3. Включить доступ к веб-интерфейсу из внешней сети
4. Включить доступ к серверу по SSH из Интернет
5. Включить доступ к серверу по SSH из локальных сетей
6. Включить режим `Разрешить Интернет всем`
7. Сбросить блокировки по IP
8. Отключить пользовательский файрвол
9. Отключение VCE-интерфейсов
10. Создать новый бэкап
11. Восстановить из бэкапа
12. Мгновенно восстановить из бэкапа
13. Включить доступ Удаленного Помощника
14. Контакты технической поддержки
15. Управление кластером
16. Восстановиться на предыдущую версию
17. Перезагрузка сервера
18. Отключить сервер
19. Выход

Введите номер пункта и нажмите Enter.
# _
```

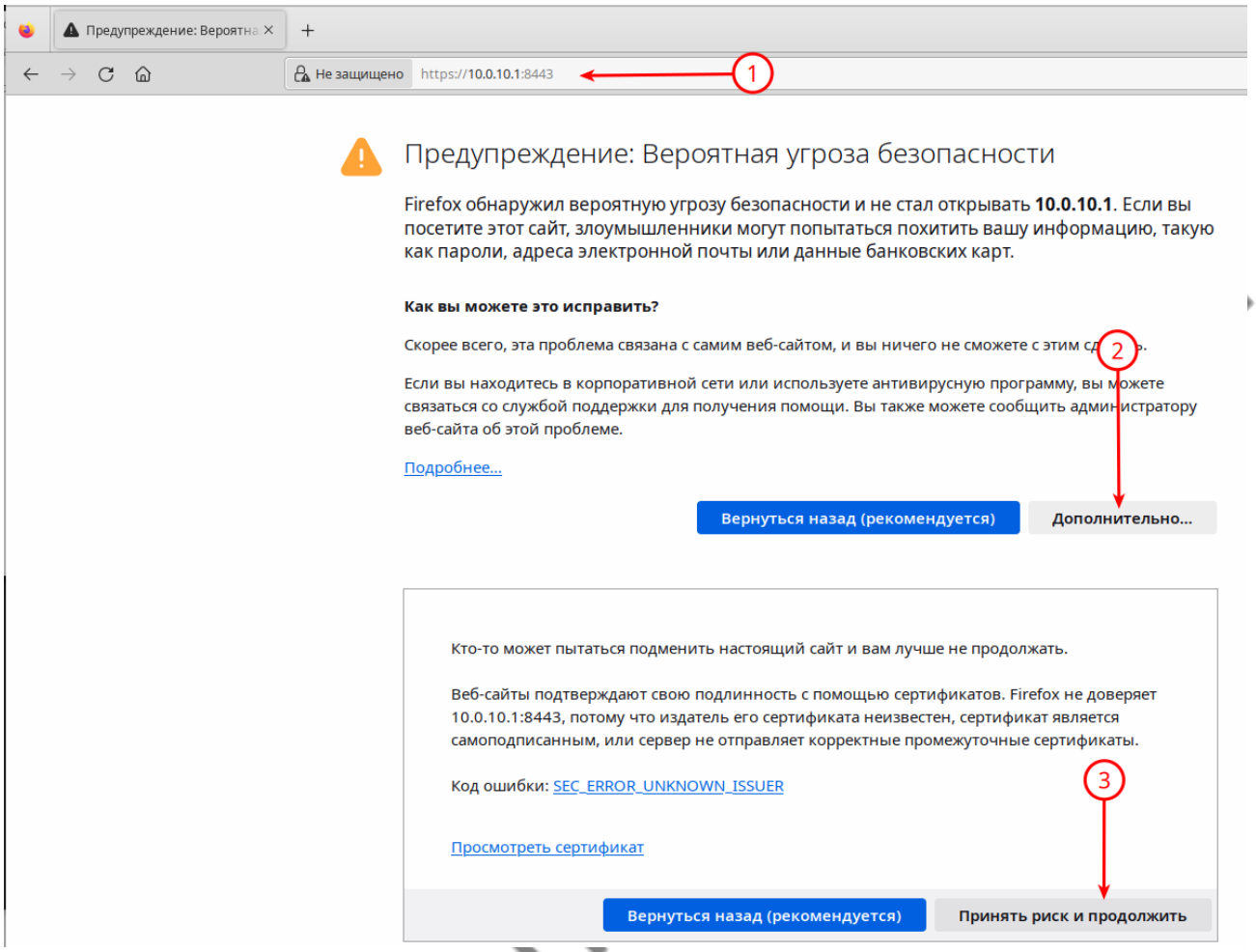
Для выхода введите с клавиатуры номер пункта «Выход»» и нажмите Enter.

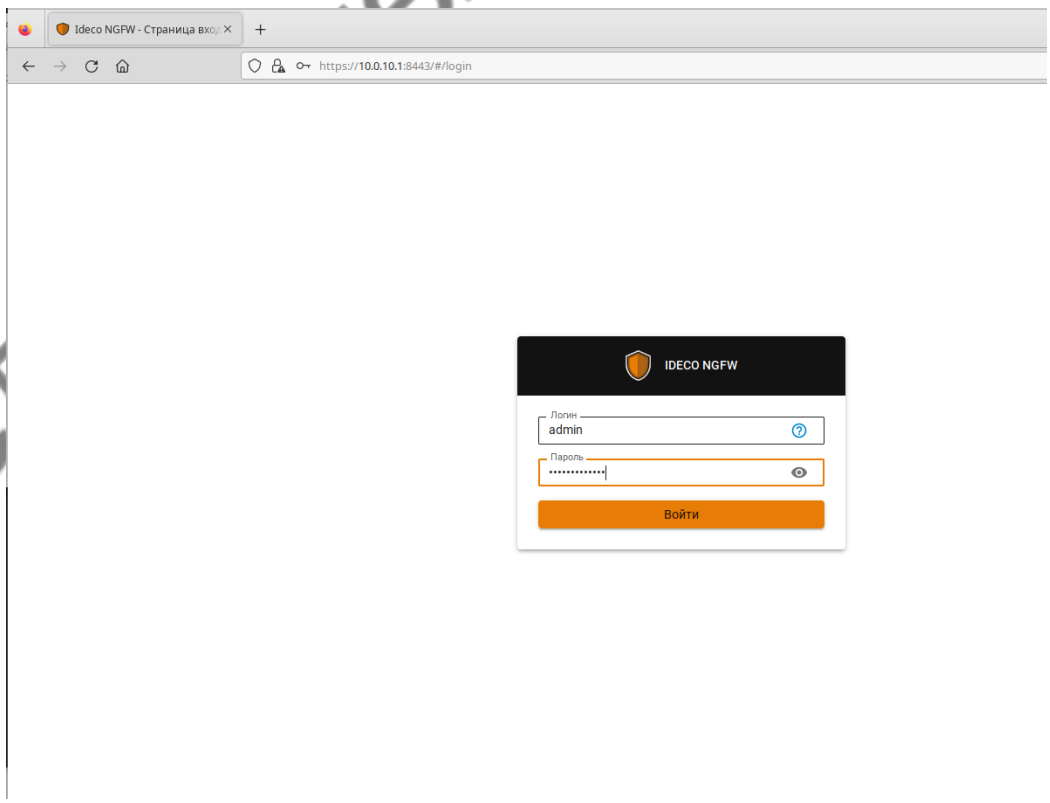
Доступ к веб-интерфейсу Ideco NGFW осуществляется по протоколу https на порт 8443:

```
Добро пожаловать в панель мониторинга сервера Ideco NGFW 18.3.12!

Название сервера:                          Без названия a7672d69-f1ad-624a-8dcd-33eec24113b7
Состояние локальных интерфейсов:           Настроены
Доступ Удаленного Помощника:               Отключено
Режим `Разрешить Интернет всем`:           Отключено
Доступ в веб-интерфейс:                    Доступен
Доступ к веб-интерфейсу из внешней сети:   Отключено

Адреса веб-интерфейса:
    https://10.0.10.1:8443

В случае возникновения ошибок на сервере, пожалуйста,
обратитесь в техподдержку:

Группа в Телеграм: @idecoutm
Email: help@ideco.ru
Портал тех. поддержки: help.ideco.ru
Время работы тех. поддержки: ideco.ru/support


Нажмите любую клавишу для перехода к локальному меню.
Press Ctrl+R if you don't see the symbols above.
```

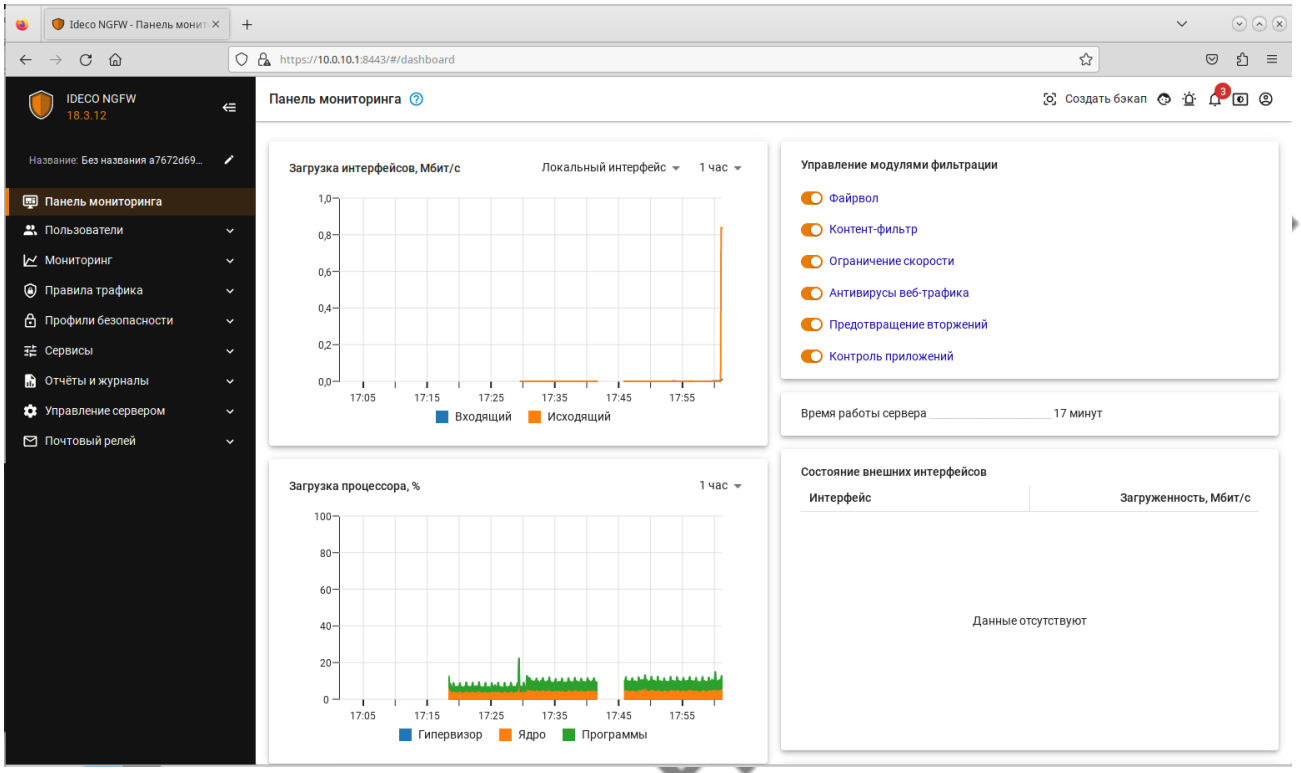
Поддерживаются версии Firefox, Chrome и браузеров, актуальные на текущий момент.

После чего можно выполнять аутентификацию веб-интерфейсе Ideco NGFW из-под ранее созданного пользователя. Поскольку сертификат на ideco-ngfw является самоподписанным, необходимо добавить исключение: нажимаем «Дополнительно» и потом «Принять риск» и продолжить:


Предупреждение: Вероятна
Не защищено
https://10.0.10.1:8443
1
Предупреждение: Вероятная угроза безопасности
Firefox обнаружил вероятную угрозу безопасности и не стал открывать 10.0.10.1. Если вы посетите этот сайт, злоумышленники могут попытаться похитить вашу информацию, такую как пароли, адреса электронной почты или данные банковских карт.
Как вы можете это исправить?
Скорее всего, эта проблема связана с самим веб-сайтом, и вы ничего не сможете с этим сделать.
Если вы находитесь в корпоративной сети или используете антивирусную программу, вы можете связаться со службой поддержки для получения помощи. Вы также можете сообщить администратору веб-сайта об этой проблеме.
Подробнее...
2
Вернуться назад (рекомендуется)
Дополнительно...
Кто-то может пытаться подменить настоящий сайт и вам лучше не продолжать.
Веб-сайты подтверждают свою подлинность с помощью сертификатов. Firefox не доверяет 10.0.10.1:8443, потому что издатель его сертификата неизвестен, сертификат является самоподписанным, или сервер не отправляет корректные промежуточные сертификаты.
Код ошибки: SEC_ERROR_UNKNOWN_ISSUER
3
Просмотреть сертификат
Вернуться назад (рекомендуется)
Принять риск и продолжить


Ideco NGFW - Страница вхо
https://10.0.10.1:8443/#/login
IDECO NGFW
Логин
admin
Пароль
Войти

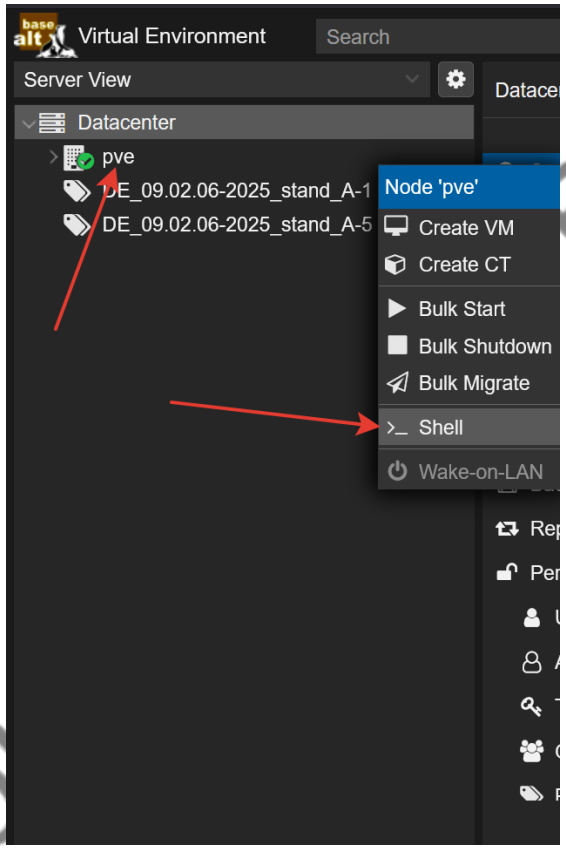
Результат успешной аутентификации в веб-интерфейсе Ideco NGFW с учетными данными пользователя, созданного в локальной консоли Ideco:



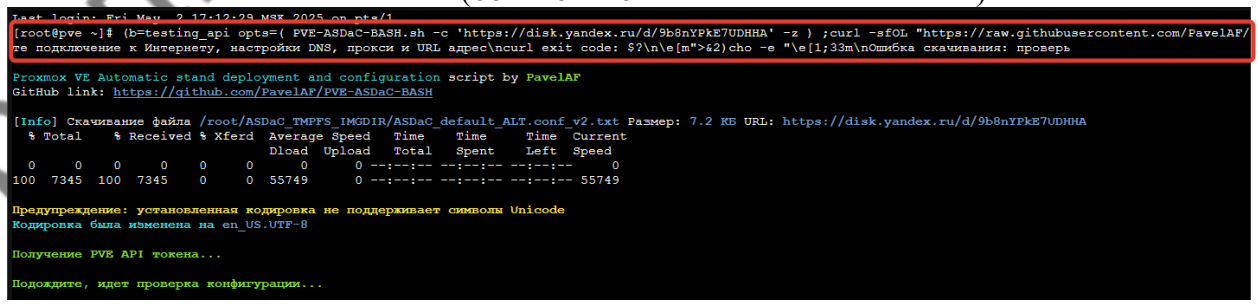
Приложение 4

Развёртывание инфраструктуры при помощи автоматизированного скрипта

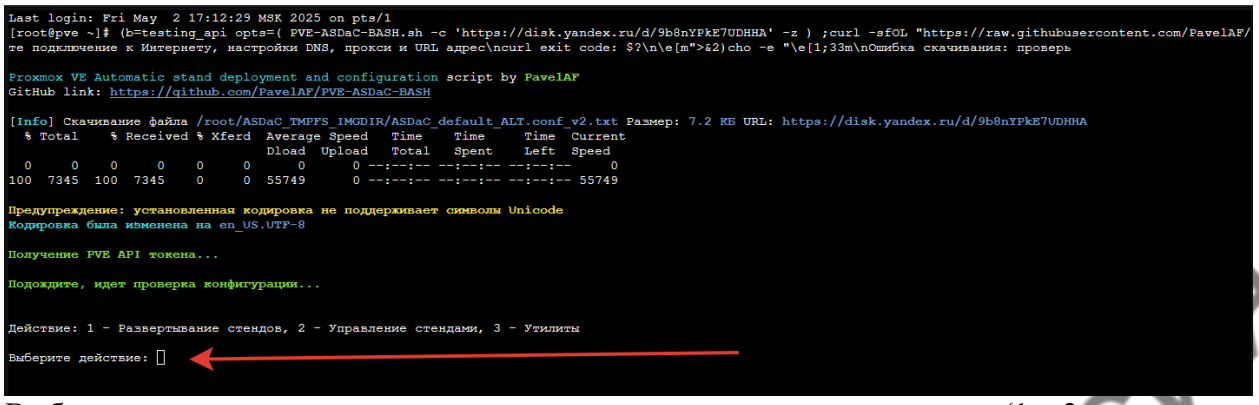
PVE-ASDaC-BASH - скрипт простого авторазвертывания конфигураций ИТ-инфраструктуры на базе платформ виртуализаций Proxmox VE и Альт Виртуализация (PVE).
Поддерживаемые версии: Proxmox VE 7.0 - 8.2 (8.3+ - в ветке testing_api), Альт Виртуализация 10.0 - 10.2
Откройте сервер виртуализации и перейдите в командную оболочку подготовленной вами ноды.



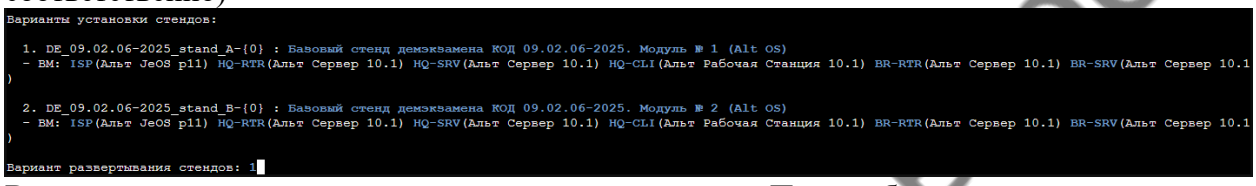
Для того, чтобы развернуть готовую конфигурацию с github по ссылке: https://github.com/PavelAF/PVE-ASDaC-BASH?tab=readme-ov-file, скопируйте строку для скачивания и вставьте в консоль (`Ctrl+Shift+V` или ПКМ -> Вставить).



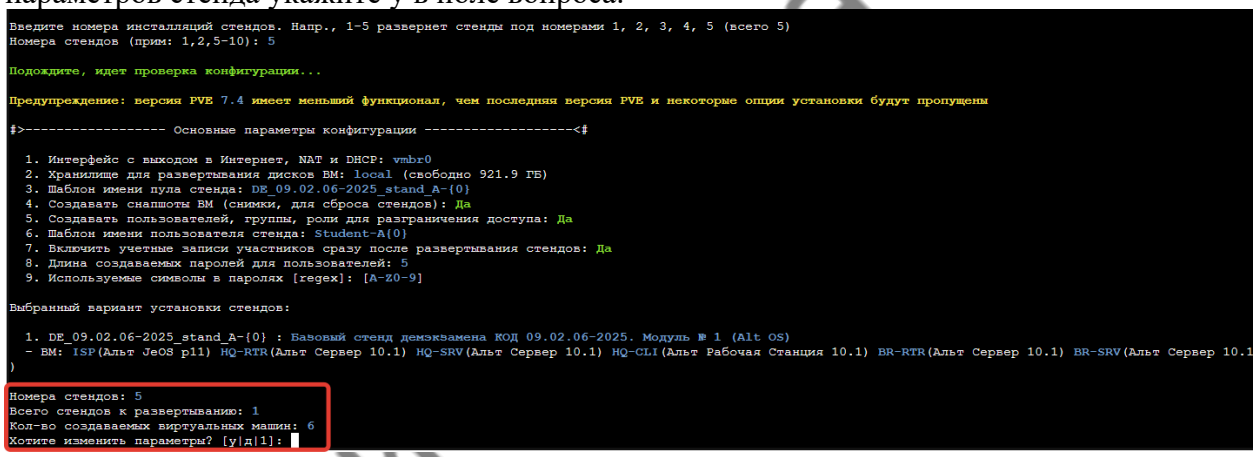
Для развёртывания выберете пункт 1.



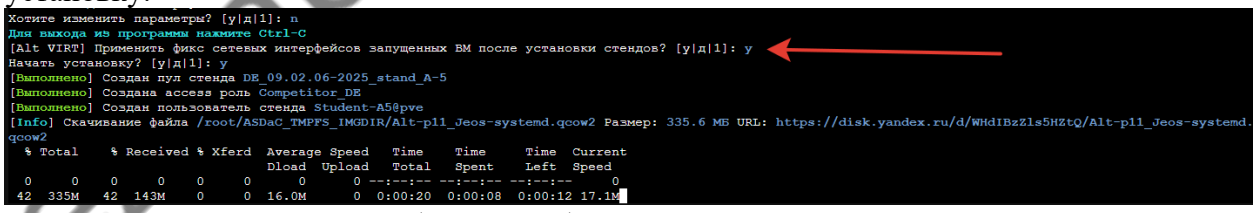
Выберите пункт для установки стендов для первого или второго модуля (1 и 2 соответственно)



В следующем пункте укажите номер стенда установки. При необходимости изменения параметров стенда укажите y в поле вопроса.



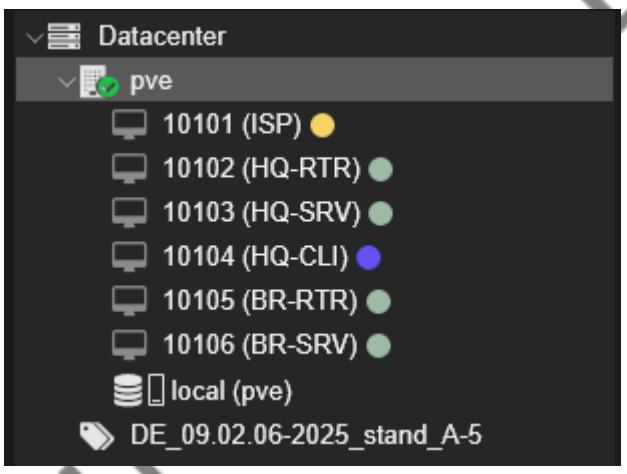
При использовании среды виртуального сервера ALT VIRT установите скрипт починку интерфейсов и начните установку. При использовании Proxmox VE сразу начинайте установку.



По завершении установки выберите удобный вам вид представления учётных данных пользователей стендов и получите их.

```
Выберите вид отображения учетных данных (логин/паролей) для доступа к стендам:
  1. Обычный   {username} | {passwd}
  2. HTML-вариант для вставки в Excel
  3. HTML-вариант для вставки в Excel (с заголовками к каждой записи)
  4. CSV: универсальный табличный вариант
  5. CSV: универсальный табличный вариант (с заголовками к каждой записи)

Вариант отображения:

#>========== Учетные данные пользователей ==========<#

Student-A5 | NWQSA

#>====================== Конец ======================<#


Установка завершена. Выход

Удалить временный раздел со скачанными образами ВМ (/root/ASDaC_TMPFS_IMGDIR)? [у|д|1]:
```

При успешной установке стенды развернутся на вашем виртуальном сервере.



БЛАГОДАРНОСТИ

Коллективу компании "Базальт СПО" за предоставление возможности преподавателям и студентам изучать системное администрирование GNU/Linux-систем на примере ОС семейства «Альт», помощь и содействие в решении технических вопросов и выборе технологий при написании пособия и отдельно Губиной Татьяне Николаевне, к.п.н., руководителю направления по работе с образовательными организациями "Базальт СПО" за помощь в экспертной оценке материалов.

ООО "РДП Инновации" (бренд EcoRouter) за возможность изучать сетевые технологии на примере высокотехнологичного российского оборудования, которое формирует облик современной сетевой инфраструктуры и решает вопросы импортозамещения. Благодаря образовательным инициативам ООО "РДП Инновации" (бренд EcoRouter) у системы образования появляются сетевые инженеры, востребованные в промышленности, телеком секторе, банках и государственных организациях по всей стране.

Отдельно хотелось бы отметить вклад EcoRouter и Базальт СПО в поддержку чемпионатного движения по компетенции «Сетевое и системное администрирование», участники которого демонстрируют высокий уровень профессионального мастерства, наглядно демонстрирующий развитие российской отрасли ИТ.

ООО «Киберпротект» за активную поддержку компетенции Сетевое и системное администрирование в области резервного копирования и систем виртуализации.

ООО «Айдеко» за активную поддержку компетенции Сетевое и системное администрирование в области сетевой безопасности.

Барышниковой Алене Дмитриевне, за вклад в оформление и вычитку текста.

УЧЕБНОЕ ПОСОБИЕ

ДЕГТЯРЕВ СЕРГЕЙ СЕРГЕЕВИЧ
ЕФИМЕНКО ТАТЬЯНА ИВАНОВНА
ЗОЛОТАРЁВ АНДРЕЙ ПЕТРОВИЧ
МОРОЗОВ ИЛЬЯ МИХАЙЛОВИЧ
НОСЕНКО ДМИТРИЙ ИГОРЕВИЧ
УЙМИН АНТОН ГРИГОРЬЕВИЧ
ШАЛЬНЕВ ВЛАДИМИР ВАЛЕНТИНОВИЧ

ПРАКТИКУМ. ПОДГОТОВКА К ДЕМОНСТРАЦИОННОМУ ЭКЗАМЕНУ ПО 09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

В авторской редакции

ISBN: 978-5-91961-583-5

Сведения о программном обеспечении, которое использовано для создания электронного издания:
LibreOffice - набор, вёрстка текста, генерация PDF
https://ru.libreoffice.org/

Техническая обработка и подготовка материалов выполнены авторами

Комплектация издания: 1 CD-ROM;
119991, Город Москва, проспект Ленинский, дом 65, корпус 1, РГУ нефти и газа (НИУ) имени И.М. Губкина, управление наукометрических исследований и поддержки публикационной активности (040)