Сетевое и системное администрирование

Подготовка к Демонстрационному экзамену КОД 09.02.06-1-2026

ПРАКТИКУМ

Команда управления компетенции
«Сетевое и системное администрирование»

СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ. ПОДГОТОВКА К ДЕМОНСТРАЦИОННОМУ ЭКЗАМЕНУ КОД 09.02.06-1-2026

ПРАКТИКУМ

Рекомендовано Федеральным учебно-методическим объединением в системе среднего профессионального образования по укрупненной группе профессий и специальностей 09.00.00 «Информатика и вычислительная техника» в качестве учебно-методического пособия для преподавателей при подготовке обучающихся к демонстрационному экзамену по специальности 09.02.06 «Сетевое и системное администрирование»

Саратов
Профобразование
2026

УДК 004.7(075.8)
ББК 32.81я73
С33

Рецензенты:
Евсютин О.О. — канд. техн. наук, доц.,
руководитель департамента кибербезопасности МИЭМ НИУ ВШЭ;
Щербаков С.М. — д-р экон. наук, доц.,
заведующий кафедрой информационных систем
и прикладной информатики РГЭУ (РИНХ)

С33 **Сетевое и системное администрирование. Подготовка к Демонстрационному экзамену КОД 09.02.06-1-2026** : практикум / Д.И. Носенко, А.П. Золотарёв, А.Г. Уймин [и др.] ; Базальт СПО. — Саратов : Профобразование, 2026. — 216 с.
ISBN 978-5-4488-2908-6

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

Книга является дополненным и переработанным переизданием книги «Подготовка к Демонстрационному экзамену по 09.02.06 2026 “Сетевое и системное администрирование”», вышедшей в 2025 г. Материалы, составляющие данную книгу, распространяются на условиях лицензии GNU FDL.

ISBN 978-5-4488-2908-6

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»

Практикум предназначен для подготовки студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования (далее — СПО) укрупненных групп профессий и специальностей «Информатика и вычислительная техника», «Информационная безопасность» и «Электроника, радиотехника и системы связи» 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 (ДЭ), который проводится независимыми экспертами по итогам обучения либо при промежуточной аттестации. Данный практикум включает рекомендации по выполнению заданий Демонстрационного экзамена (ДЭ), организуемого в рамках государственной итоговой аттестации по завершении освоения образовательной программы СПО по специальности «Сетевое и системное администрирование».

Содержание практикума соответствует:

• требованиям Федерального государственного образовательного стандарта среднего профессионального образования (Федеральный государственный образовательный стандарт (ФГОС) по специальности 09.02.06 «Сетевое и системное администрирование», утвержден приказом Министерства образования и науки РФ от 09.12.2016 № 1548 (ред. от 17.12.2020);

• требованиям Федерального государственного образовательного стандарта (ФГОС) по специальности 09.02.06 «Сетевое и системное администрирование», утвержден приказом Министерства просвещения РФ от 10.07.2023 № 519);

• профессиональным квалификационным требованиям, описанным в профстандарте 06.026 «Системный администратор информационно-коммуникационных систем», утвержденном приказом Министерства труда и социальной защиты Российской Федерации от 29.09.2020 № 680н.

Издание также поддержано специалистами ФГБОУ ДПО «Институт развития профессионального образования».

Практикум составлен с учетом следующих нормативных документов, регламентирующих процедуру проведения Демонстрационного экзамена (ДЭ):

• приказ Министерства просвещения Российской Федерации от 08.11.2021 № 800 «Об утверждении порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» (в ред. приказов Минпросвещения РФ от 05.05.2022 № 311, от 19.01.2023 № 37, от 24.04.2024 № 272, от 22.11.2024 № 812);

• приказ ФГБОУ ДПО ИРПО от 25.04.2024 № 01-09-139/2024 «Об утверждении Методических указаний по разработке оценочных материалов для проведения демонстрационного экзамена»;

• приказ ФГБОУ ДПО ИРПО от 22.06.2023 № 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, Ростовский государственный экономический университет, старший преподаватель кафедры ИСиПИ, 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 обл., Кировский политехнический техникум, преподаватель, ведущий эксперт компетенции «Сетевое и системное администрирование»
Морозов Илья Михайлович	г. Москва, Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, мастер производственного обучения, ведущий эксперт компетенции «Сетевое и системное администрирование», эксперт НОВОТЕХ, менеджер компетенции «Облачные технологии»
Носенко Дмитрий Игоревич	г. Боровичи, Новгородская обл., Боровичский педагогический колледж, преподаватель, ведущий эксперт компетенции «Сетевое и системное администрирование», тренер чемпиона России 2024 года по сетевому и системному администрированию
Уймин Антон Григорьевич	г. Москва, Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М. Губкина, заведующий лабораторией, эксперт НОВОТЕХ, менеджер компетенции «Сетевое и системное администрирование», руководитель команды #au_team
Шальнев Владимир Валентинович	г. Ногинск, Московская обл., Ногинский колледж, преподаватель высшей квалификационной категории по специальности 09.02.06 «Сетевое и системное администрирование», 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», за помощь и содействие в решении технических вопросов и выборе технологий при написании практикума, и отдельно Губиной Татьяне Николаевне, канд. пед. наук, 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.

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

Коллективу компании ООО «Киберпротект» за активную поддержку компетенции «Сетевое и системное администрирование» в области резервного копирования, систем виртуализации и облачных технологий, за активное участие представителей ООО «Киберпротект» в профильных вебинарах с участием преподавателей, экспертов компетенции и студентов по технологиям компании, а также за интенсивы для экспертов компетенции, которые позволили глубже изучить применяемые технологии. Отдельная благодарность в адрес руководства ООО «Киберпротект» за постоянную поддержку этапов проведения компетенции облачными ресурсами.

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

Благодаря образовательным инициативам российских компаний ООО «РДП Инновации» (бренд EcoRouter), ООО «Базальт СПО», ООО «Айдеко» и ООО «Киберпротект» у системы образования появляются сетевые и системные инженеры, востребованные в промышленности, телеком-секторе, банках и государственных организациях по всей стране.

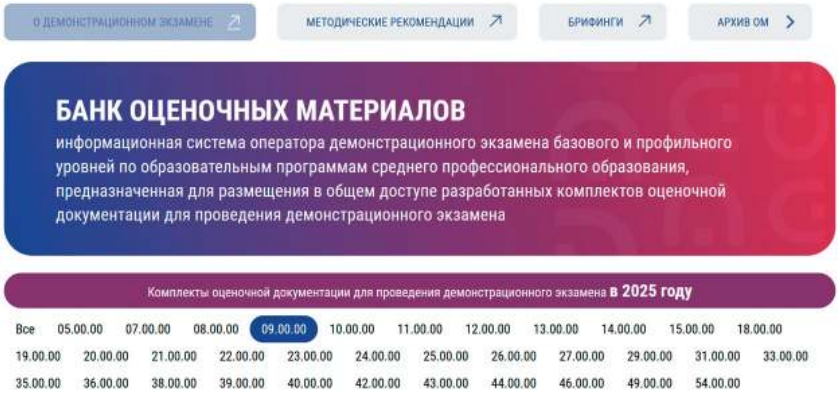
Команда #au_team

ВВЕДЕНИЕ

Проведение ГИА в 2026 году в форме Демонстрационного экзамена (ДЭ) 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 (ДЭ) разработаны прошедшими конкурсный отбор экспертами и открыто размещены на следующих информационных ресурсах:

2026 г. — https://bom.firpo.ru/;

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



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

ФГОС 09.02.06 Сетевое и системное администрирование (приказ № 1548 от 09.12.2016) (https://spolab.firpo.ru/storage/NPD//0JLPhkk6Wi1rTWUlJWUDhifmY1EX5JLxyZAczvbA.docx)	
09.02.06-1-2026: Сетевой и системный администратор (https://bom.firpo.ru/Public/5502)	

09.02.06-5-2026: Специалист по администрированию сети (https://bom.firpo.ru/Public/5505)	
ФГОС 09.02.06 Сетевое и системное администрирование (приказ № 519 от 10.07.2023) (https://spolab.firpo.ru/npdv2/category-doc/get/3774)	
09.02.06-2-2026: Системный администратор (Эксплуатация облачных сервисов) (https://bom.firpo.ru/Public/5503)	
09.02.06-3-2026: Системный администратор (Эксплуатация объектов сетевой инфраструктуры) (https://bom.firpo.ru/Public/5504)	
09.02.06-4-2026: Системный администратор (Эксплуатация операционных систем) (https://bom.firpo.ru/Public/5431)	

Видеообзор комплекта оценочной документации за 2026 год:

https://vkvideo.ru/video-219561594_456240041?list=ln-BkXecsRABZcEtgRpxa&t=0s&ref_domain=bom.firpo.ru

Чат компетенции, структурированный по темам (https://t.me/+Sz-uToWW2zc5OWMy)	
ДЭ 2026 (https://vkvideo.ru/playlist/-228030577_10)	
ДЭ 2025 (https://vkvideo.ru/playlist/-228030577_7)	
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 09.02.06-1-2026
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. рис. 1.1).

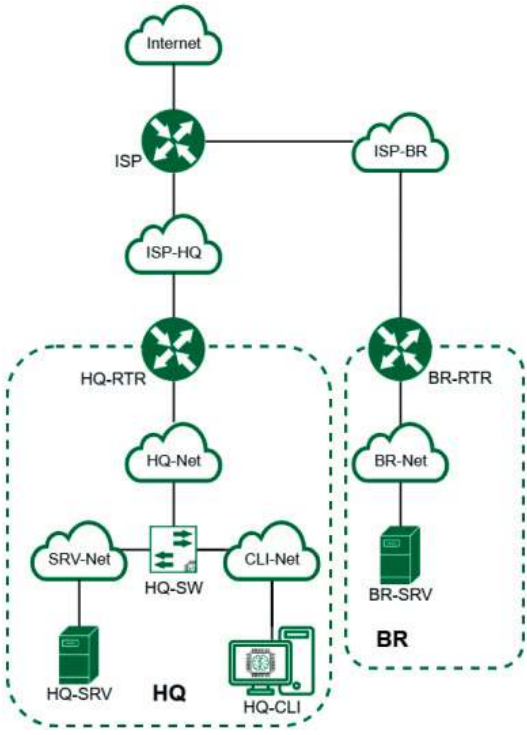


Рис. 1.1. Топология сети

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. По каждому пункту задания, требующего отчет, составить текстовый документ, название которого должно содержать индекс пункта и краткое описание. Текстовый документ должен содержать текстовую информацию и может включать снимки экрана, кадрированные таким образом, чтобы относящаяся к выполнению задания информация на снимках была читаемой.

Итоговый отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла — ФамилияУчастникаМодуль1, без учета расширения.

Таблица 1.1

Имя виртуальной машины	**Оперативная память**	**Центральный процессор, ядер**	**Накопитель**	**Операционная система**
ISP	1 ГБ	1 ядро	5 ГБ	Дистрибутив ОС JeOS/Linux или аналог
HQ-RTR	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	10 ГБ	ОС «EcoRouterOS», в случае невозможности использования EcoRouter — дистрибутив ОС JeOS/Linux или аналог
BR-RTR	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	10 ГБ	ОС «EcoRouterOS», в случае невозможности использования — EcoRouter дистрибутив ОС JeOS/Linux или аналог
HQ-SRV	2 ГБ	1 ядро	10 ГБ	ОС «Альт Сервер» или аналог
BR-SRV	2 ГБ	1 ядро	10 ГБ	ОС «Альт Сервер» или аналог

Окончание табл. 1.1

Имя виртуальной машины	Оперативная память	Центральный процессор, ядер	Накопитель	Операционная система
HQ-CLI	2 ГБ	2 ядра	20 ГБ	ОС «Альт Рабочая станция» или аналог
Итого	15 (9 в случае использования ОС «Альт» или аналога)	13 (7 в случае использования ОС «Альт» или аналога)	60 ГБ	–

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 (VLAN 100) должна вмещать не более 32 адресов;

◦ локальная сеть в сторону HQ-CLI (VLAN 200) должна вмещать не менее 16 адресов;

◦ локальная сеть для управления (VLAN 999) должна вмещать не более 8 адресов;

◦ локальная сеть в сторону BR-SRV должна вмещать не более 16 адресов;

• сведения об адресах занесите в табл. 1.2, в качестве примера используйте Приложение Б.

2. Настройте доступ к сети Интернет, на маршрутизаторе ISP:

• настройте адресацию на интерфейсах:

◦ интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP;

◦ настройте маршрут по умолчанию, если это необходимо;

◦ настройте интерфейс в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28;

◦ настройте интерфейс в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28;

◦ на ISP настройте динамическую сетевую трансляцию портов для доступа к сети Интернет HQ-RTR и BR-RTR.

3. Создайте локальные учетные записи на серверах HQ-SRV и BR-SRV:

• создайте пользователя sshuser:

◦ пароль пользователя sshuser — P@ssw0rd;

◦ идентификатор пользователя — 2026;

◦ пользователь sshuser должен иметь возможность запускать sudo без ввода пароля;

• создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR:

◦ пароль пользователя net_admin — P@ssw0rd;

◦ при настройке ОС на базе Linux нужно запускать sudo без ввода пароля;

◦ при настройке ОС, отличных от Linux, пользователь должен обладать максимальными привилегиями.

4. Настройте коммутацию в сегменте HQ следующим образом:

• трафик HQ-SRV должен принадлежать VLAN 100;

• трафик HQ-CLI должен принадлежать VLAN 200;

• предусмотреть возможность передачи трафика управления в VLAN 999;

• реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта;

• сведения о настройке коммутации внесите в отчет.

5. Настройте безопасный удаленный доступ на серверах HQ-SRV и BR-SRV:

• для подключения используйте порт 2026;

• разрешите подключения исключительно пользователю sshuser;

• ограничьте количество попыток входа до двух;

• настройте баннер «Authorized access only».

6. Между офисами HQ и BR, на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать IP-туннель:

• на выбор технологии GRE или IP in IP;

• сведения о туннеле занесите в отчет.

7. Обеспечьте динамическую маршрутизацию на маршрутизаторах HQ-RTR и BR-RTR: сети одного офиса должны быть доступны из другого офиса и наоборот. Для обеспечения динамической маршрутизации используйте link state протокол на усмотрение участника:

• разрешите выбранный протокол только на интерфейсах IP-туннеля;

• маршрутизаторы должны делиться маршрутами только друг с другом;

• обеспечьте защиту выбранного протокола посредством парольной защиты;

• сведения о настройке и защите протокола занесите в отчет.

8. Настройка динамической трансляции адресов на маршрутизаторах HQ-RTR и BR-RTR:

• настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет.

9. Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI:

• настройте нужную подсеть;

• 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 — au-team.irpo;
• сведения о настройке протокола занесите в отчет.

10. Настройте инфраструктуру разрешения доменных имен для офисов HQ и BR:
• основной DNS-сервер реализован на HQ-SRV;
• сервер должен обеспечивать разрешение имен в сетевые адреса устройств и обратно в соответствии с табл. 1.3;
• в качестве DNS-сервера пересылки используйте любой общедоступный DNS-сервер (77.88.8.7, 77.88.8.3 или другие).

11. Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора в случае его использования) согласно месту проведения экзамена.

Таблица 1.2

Имя устройства	IP-адрес	Шлюз по умолчанию
HQ-RTR		
BR-RTR		
HQ-SRV		
HQ-CLI		
BR-SRV		

Таблица 1.3

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
ISP (интерфейс, направленный в сторону HQ-RTR)	docker.au-team.irpo	A
ISP (интерфейс, направленный в сторону BR-RTR)	web.au-team.irpo	A

Выполнение задания:

Базовая настройка устройств

Задание 1.

Настройте имена устройств согласно топологии (см. рис. 1.2). Используйте полное доменное имя.

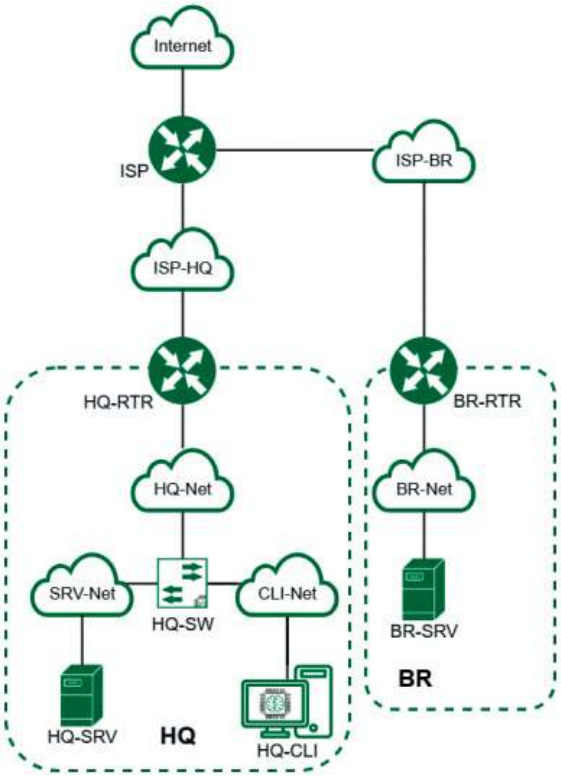


Рис. 1.2. Публичная схема экзаменационного задания

Как делать?

Переименование устройств с ОС «Альт».

Изначально имя машины стандартное — localhost:

```
Welcome to ALT Server 11.0 (Mendelevium)!

Hostname: localhost
IP: 127.0.0.1
localhost login: root
Password:
Last login: Tue Oct 21 17:41:39 MSK 2025 on tty1
[root@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
```

```
[root@localhost ~]# hostnamectl set-hostname hq-srv.au-team.irpo; exec bash
[root@hq-srv ~]# _
```

Описание применяемых команд:

`hostnamectl` — программа для управления именем машины;

`set-hostname` — аргумент, позволяющий выполнить изменение имени устройства;

`<hostname>` — целевое имя машины;

`<domain-name>` — имя домена;

`exec bash` — перезапуск оболочки bash для отображения нового имени устройства.

Как проверить?

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

```
ISP login: root
Password:
Last login: Fri Oct 17 18:27:27 MSK 2025 on tty1
[root@ISP ~]# _
```

Команда `hostname` выведет текущее название машины, используйте ключ `-f` для отображения полного доменного имени (Fully Qualified Domain Name).

```
[root@hq-srv ~]# hostname -f
hq-srv.au-team.irpo
[root@hq-srv ~]#
```

Где выполнять?

На машинах с ОС «Альт».

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).

Как делать?

Для переименования устройств с ОС «EcoRouterOS».

Используйте следующие команды:

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

```
EcoRouterOS version Edelweiss 16/07/2025 14:11:48
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 используйте команду:

```
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#
```

Где выполнять?

На машинах с ОС «EcoRouterOS».

Краткая справка:

– Документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

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 удаленно, имя устройства дает ему понимание, на каком устройстве 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:

• IP-адрес должен быть из приватного диапазона в случае, если сеть локальная, согласно RFC1918;

• локальная сеть в сторону HQ-SRV (VLAN 100) должна вмещать не более 32 адресов;

• локальная сеть в сторону HQ-CLI (VLAN 200) должна вмещать не менее 16 адресов;

• локальная сеть для управления (VLAN 999) должна вмещать не более 8 адресов;

• локальная сеть в сторону BR-SRV должна вмещать не более 16 адресов.

Как делать?

Для устройств с ОС «Альт».

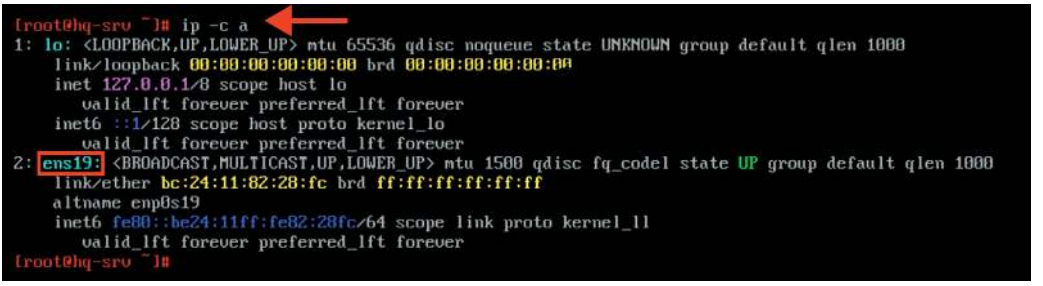
Базовая настройка сетевых параметров на ОС «Альт» будет осуществляться с использованием текстового редактора vim, а также с использованием сетевой подсистемы `etcnet`. Для открытия файла для редактирования необходимо прописать vim и нужный путь (например: vim /etc/net/sysctl.conf) до файла, после чего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

Внимание! Для применения настроек необходимо перезагрузить службу network командой:

```
systemctl restart network
```

Просмотр существующих интерфейсов выполняется командой:

```
ip -c a
```



Голубым 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, параметр `BOOTPROTO=static` означает, что настройка статического IP-адреса и маршрутов будет взята из файлов `ipv4address` и `ipv4route`.

```
[root@hq-srv ~]# ls /etc/net/ifaces/
default  ens19  lo  unknown
[root@hq-srv ~]#
```

```
[root@hq-srv ~]# cat /etc/net/ifaces/ens19/options
SYSTEMD_CONTROLLED=no
DISABLED=no
TYPE=eth
CONFIG_WIRELESS=no
BOOTPROTO=static
SYSTEMD_BOOTPROTO=static
CONFIG_IPV4=yes
NM_CONTROLLED=no
[root@hq-srv ~]#
```

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 значения параметров `DISABLED`, `NM_CONTROLLED`, `SYSTEMD_CONTROLLED` были установлены в `no` или же указание данных параметров в файле `options` не является обязательным условием.

Режим из Alterator	Параметры в options
NetworkManager (native)	DISABLED=yes NM_CONTROLLED=yes BOOTPROTO=static
NetworkManager (etcnet)	DISABLED=no NM_CONTROLLED=yes
Etcnet	DISABLED=no NM_CONTROLLED=no

Далее опишем обязательное к указанию содержимое конфигурационных файлов: `ipv4address`, `ipv4route`, `resolv.conf`, 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@br-srv ~]# echo "192.168.0.2/28" > /etc/net/ifaces/ens19/ipv4address
[root@br-srv ~]# echo "default via 192.168.0.1" > /etc/net/ifaces/ens19/ipv4route
[root@br-srv ~]# echo "nameserver 77.88.8.8" > /etc/net/ifaces/ens19/resolv.conf
[root@br-srv ~]# systemctl restart network
[root@br-srv ~]# _
```

Для применения настроек необходимо перезагрузить службу network командой:

```
systemctl restart network
```

Как проверить?
Проверка IP-адреса осуществляется командой:

```
ip –c a
```

```
[root@br-srv ~]# ip -c 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 proto kernel_lo
       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 bc:24:11:6e:b5:f5 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.0.2/28 brd 192.168.0.15 scope global ens19
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe6e:b5f5/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@br-srv ~]#
```

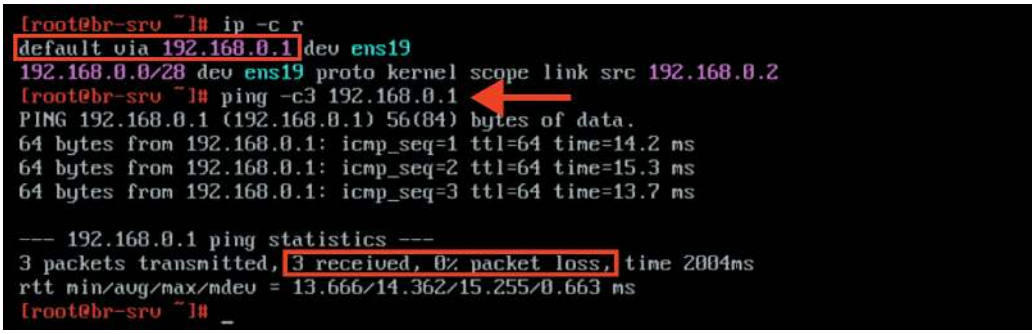
Проверка IP-адреса шлюза по умолчанию осуществляется командой:

```
ip -c r
```

Проверка доступности шлюза по умолчанию осуществляется утилитой:

```
ping
```

Проверка с hq-srv возможна только после настройки коммутации и маршрутизации между VLAN.



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

Где выполнять?

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

Краткая справка:

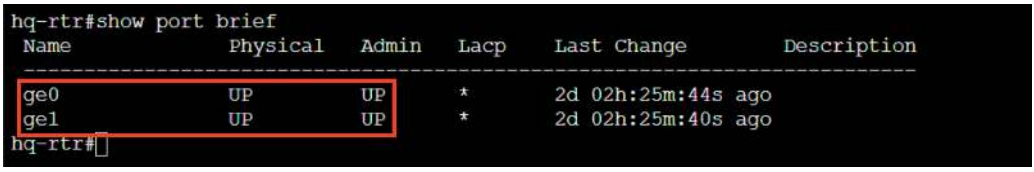
– подсказки пользователю /etc/net (https://www.altlinux.org/Etcnet);

– на серверах вместо Network Manager удобнее использовать сетевой менеджер Etcnet (https://www.altlinux.org/Etcnet_start).

Как делать?

Для устройств 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 физическом уровне (L1) модели OSI;

• интерфейс (interface) — это логический интерфейс для адресации, работает на сетевом уровне (L3);

• service instance (Сабинтерфейс, SI, Сервисный интерфейс) является логическим сабинтерфейсом, работающим на канальном уровне (L2), связывает L1, L2 и L3:

◦ 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 администрирования (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 обрабатывать тегированный или нетегированный трафик, указать в какой интерфейс (ранее созданный) нужно отправить обработанные кадры.

Для нетегированного трафика:

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

Для тегированного трафика:

```
port <ИМЯ_ПОРТА>
service-instance <ИМЯ>
encapsulation dot1q <TAG>
connect ip interface <ИМЯ_ИНТЕРФЕЙСА>
exit
```

Также стоит отметить, что интерфейс переходит в состояние «up» только после использования команды connect. Кроме того, команду connect можно использовать и на интерфейсе, так как интерфейс можно связать с портом с помощью команды connect port <ИМЯ_ПОРТА> service-instance <ИМЯ>.

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

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

Пример описания настроек на виртуальных машинах экзаменационного стенда

Создание интерфейсов с последующим назначением IP-адресов, создание сервис-инстансов на порту с указанием тегированного трафика и конкретного интерфейса:

```
hq-rtr(config)#interface vl100
hq-rtr(config-if)#description “VLAN 100”
hq-rtr(config-if)#ip address 192.168.100.1/27
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl200
hq-rtr(config-if)#description “VLAN 200”
hq-rtr(config-if)#ip address 192.168.200.1/24
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl999
hq-rtr(config-if)#description “VLAN 999”
hq-rtr(config-if)#ip address 192.168.99.1/29
hq-rtr(config-if)#exit
hq-rtr(config)#port ge1
hq-rtr(config-port)#service-instance ge1/vl100
hq-rtr(config-service-instance)#encapsulation dot1q 100 exact
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl100
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#service-instance ge1/vl200
hq-rtr(config-service-instance)#encapsulation dot1q 200 exact
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl200
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#service-instance ge1/vl999
hq-rtr(config-service-instance)#encapsulation dot1q 999 exact
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl999
hq-rtr(config-service-instance)#exit
```

```
hq-rtr(config-port)#exit
hq-rtr(config)#write memory
```

Как проверить?

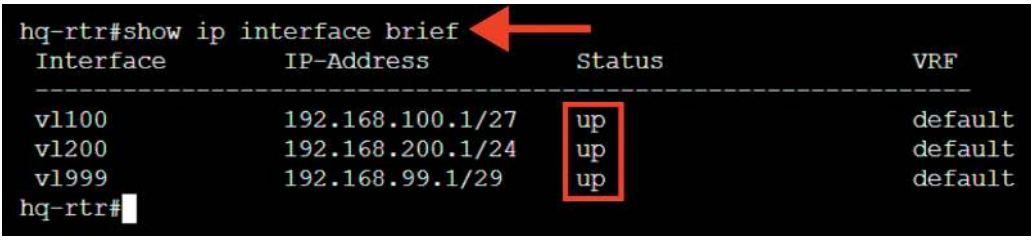
Проверка осуществляется командами привилегированного режима.

Краткий вывод настройки service-instance:

```
show service-instance brief
```

Краткий вывод статусов всех интерфейсов:

```
show ip interface brief
```



Пример описания настроек на виртуальных машинах экзаменационного стенда

Создание сервис-инстанса на порту с указанием нетегированного трафика, с последующим созданием интерфейса и назначением IP-адреса, а также подключения порта на созданный интерфейс:

```
br-rtr(config)#port ge1
br-rtr(config-port)#service-instance ge1/int1
br-rtr(config-service-instance)#encapsulation untagged
br-rtr(config-service-instance)#exit
br-rtr(config-port)#exit
br-rtr(config)#interface int1
br-rtr(config-if)#description “BR-Net”
br-rtr(config-if)#ip address 192.168.0.1/28
br-rtr(config-if)#connect port te1 service-instance ge1/int1
br-rtr(config-if)#exit
br-rtr(config)#write memory
```

Как проверить?

Проверка осуществляется командами привилегированного режима.

Краткий вывод настройки service-instance:

```
show service-instance brief
```

Краткий вывод статусов всех интерфейсов:

```
show ip interface brief
```

Где выполнять?

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

Краткая справка:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

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 построения и функционирования компьютерных сетей;

– Программное обеспечение компьютерных сетей;

– Организация администрирования компьютерных систем и далее.

Задание 3. Сведения об адресах занесите в табл. 1.2, в качестве примера используйте Приложение Б.

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.

Пример заполненной таблицы:

Имя устройства	IP-адрес	Шлюз по умолчанию
HQ-RTR	172.16.1.2/28	172.16.1.1
	192.168.100.1/27	
	192.168.200.1/24	
	192.168.99.1/29	
BR-RTR	172.16.2.2/28	172.16.2.1
	192.168.0.1/28	
HQ-SRV	192.168.100.2/27	192.168.100.1
HQ-CLI	192.168.200.2/24	192.168.200.1
BR-SRV	192.168.0.2/28	192.168.0.1

Краткая справка:

– распределение адресов для частных IP-сетей (https://www.ietf.org/rfc/rfc1918.txt).

Дополнительно:

Создание таблиц адресов устройств в сети с указанием имен, 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;

• повышения эффективности работы сети и облегчения администрирования.

Где изучается?

– на учебной и производственной практике.

2 курс:

– Компьютерные сети.

3 курс:

– Эксплуатация объектов сетевой инфраструктуры.

Настройка доступа к сети Интернет

Задание 1. Настройте адресацию на интерфейсах.

Подробное описание пункта задания

Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP. Настройте маршрут по умолчанию, если это необходимо.

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 proto kernel_lo
       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 bc:24:11:3d:7d:bf brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 10.20.0.68/16 brd 10.20.255.255 scope global dynamic noprefixroute ens19
       valid_lft 3595sec preferred_lft 3145sec
    inet6 fe80::be24:11ff:fe3d:7dbf/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
3: ens20: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:4e:ef:c2 brd ff:ff:ff:ff:ff:ff
    altname enp0s20
    inet6 fe80::be24:11ff:fe4e:efc2/64 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 bc:24:11:0c:78:d8 brd ff:ff:ff:ff:ff:ff
    altname enp0s21
    inet6 fe80::be24:11ff:fe0c:78d8/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
[root@ISP ~]# _
```

На рисунке красным цветом выделено название интерфейса, в формате «ensXX», и его MAC-адрес, в формате «XX:XX:XX:XX:XX:XX» (в примере они могут 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`:

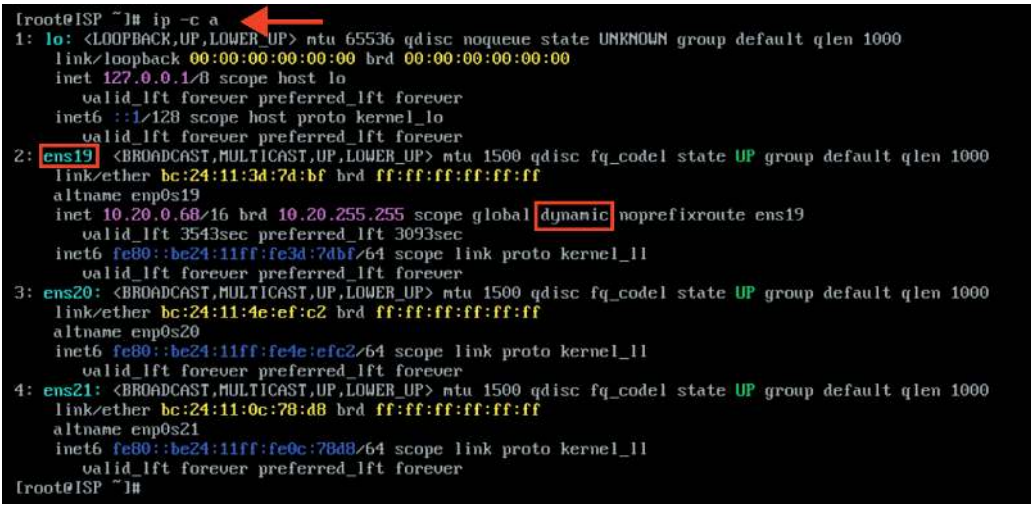
```
[root@ISP ~]# ls /etc/net/ifaces/
default  ens19  ens20  ens21  lo  unknown
[root@ISP ~]# cat /etc/net/ifaces/ens19/options
BOOTPROTO=dhcp
TYPE=eth
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
DISABLED=no
NM_CONTROLLED=no
SYSTEMD_CONTROLLED=no
[root@ISP ~]#
```

Для применения настроек необходимо перезагрузить службу `network` командой:

```
systemctl restart network
```

Как проверить?
Проверка IP-адреса осуществляется командой:

```
ip –c a
```

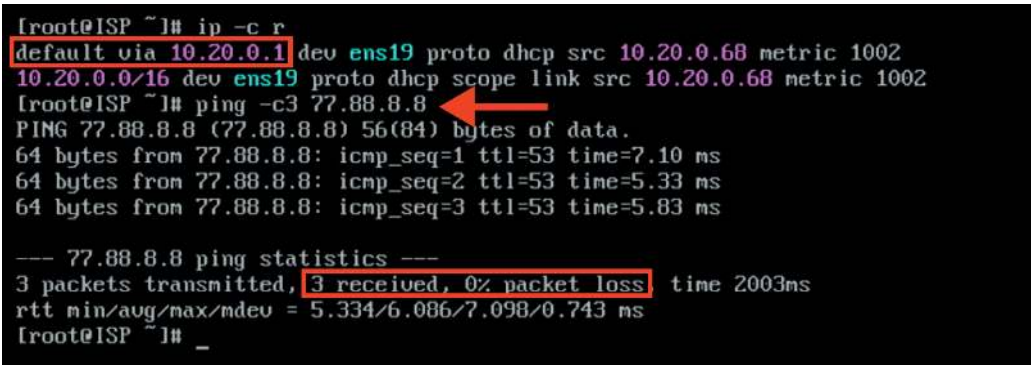


Проверка IP-адреса шлюза по умолчанию осуществляется командой:

```
ip -c r
```

Проверка доступа к сети Интернет осуществляется утилитой:

```
ping
```



Где выполнять?
На машинах: 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 интерфейс в сторону HQ-RTR и BR-RTR.

Подробное описание пункта задания:

• настройте интерфейс в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28;

• настройте интерфейс в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28.

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, параметр `BOOTPROTO=static` означает настройку 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>
```

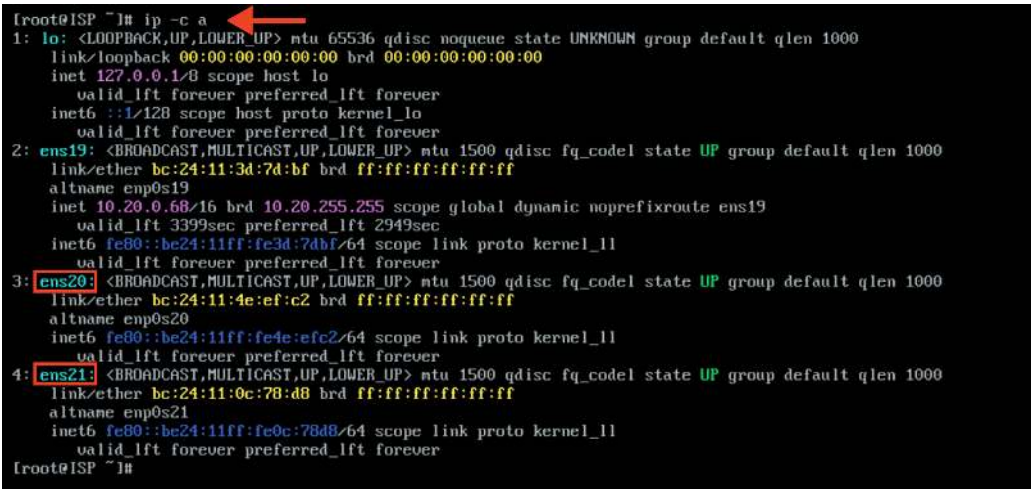
Для применения настроек необходимо перезагрузить службу `network` командой:

```
systemctl restart network
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

Просмотр существующих интерфейсов выполняется командой:

```
ip –c a
```



Создание директории для конкретного интерфейса выполняется утилитой `mkdir`:

```
mkdir /etc/net/ifaces/ens20
mkdir /etc/net/ifaces/ens21
```

Создание файла `options` для конкретного интерфейса выполняется с использованием текстового редактора `vim` и указания необходимых параметров:

```
vim /etc/net/ifaces/ens20/options
vim /etc/net/ifaces/ens21/options
```

Создание файла `ipv4address` для конкретного интерфейса выполняется утилитой `echo` с указанием соответствующих IPv4-адресов:

```
echo «172.16.1.1/28» > /etc/net/ifaces/ens20/ipv4address
echo «172.16.2.1/28» > /etc/net/ifaces/ens20/ipv4address
```

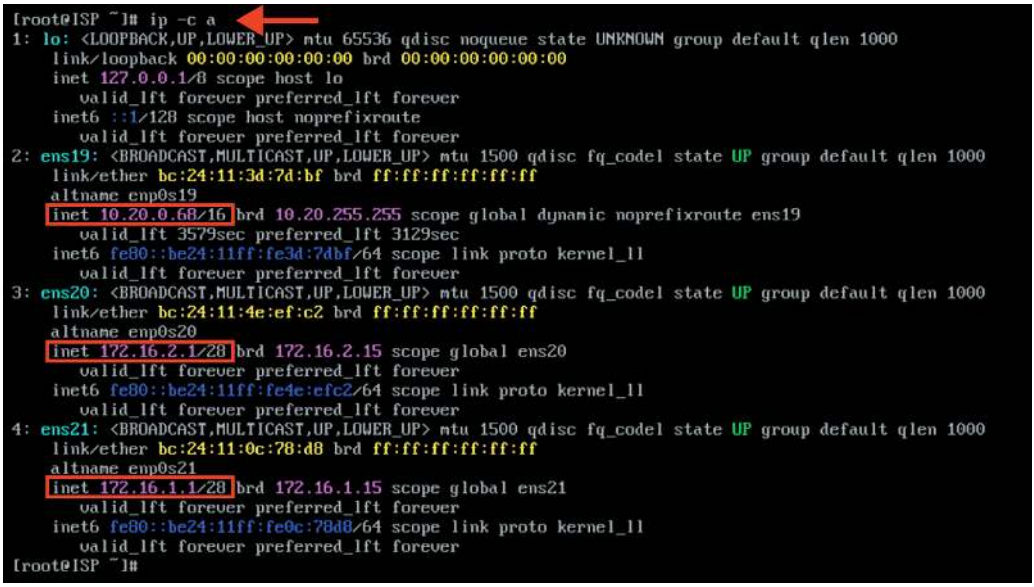
Для применения настроек необходимо перезагрузить службу `network` командой:

```
systemctl restart network
```

Как проверить?

Проверка IP-адреса осуществляется командой:

```
ip –c a
```



Где выполнять?

На машинах: 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 3. На ISP настройте динамическую сетевую трансляцию портов.

Подробное описание пункта задания

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

Как делать?

Для того чтобы устройство ISP могло пересылать пакеты с интерфейса на интерфейс, необходимо включить пересылку пакетов (forwarding/передача транзитных пакетов между сетевыми интерфейсами). 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
```

```
# 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 «JeOS» необходимо установить пакет `iptables`. Выполнить установку можно с помощью команды:

```
apt-get install iptables
```

предварительно обновив список пакетов с помощью команды:

```
apt-get update
```

```
[root@ISP ~]# systemctl status iptables
● iptables.service - IPv4 firewall with iptables
     Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; preset: disabled)
     Active: active (exited) since Fri 2025-10-24 19:29:23 MSK; 1min 47s ago
    Process: 624 ExecStart=/etc/init.d/iptables start (code=exited, status=0/SUCCESS)
   Main PID: 624 (code=exited, status=0/SUCCESS)
        CPU: 63ms

Oct 24 19:29:23 ISP systemd[1]: Starting iptables.service - IPv4 firewall with iptables...
Oct 24 19:29:23 ISP iptables[636]: egrep: warning: egrep is obsolescent; using grep -E
Oct 24 19:29:23 ISP iptables[660]: Applying iptables firewall rules: succeeded
Oct 24 19:29:23 ISP iptables[624]: Applying iptables firewall rules: [ DONE ]
Oct 24 19:29:23 ISP systemd[1]: Finished iptables.service - IPv4 firewall with iptables.
[root@ISP ~]#
```

Реализацию 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 в 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;

— --out-interface (от англ. наружу, вне, за пределами) — исходящий интерфейс;

j — --jump (от англ. прыжок) — прописывается действие, которое будет выполняться этим правилом.

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

Включить функцию пересылки пакетов между интерфейсами:

```
sed –i “s/net.ipv4.ip_forward = 0/net.ipv4.ip_forward = 1/g” /etc/
net/sysctl.conf
```

Для применения настроек необходимо перезагрузить службу network командой:

```
systemctl restart network
```

Обновить список пакетов и установить пакет iptables:

```
apt-get update
apt-get install –y iptables
```

Создать правила трансляции адресов для доступа к сети Интернет HQ-RTR и BR-RTR:

```
iptables –t nat –A POSTROUTING –s 172.16.1.0/28 –o ens19 –j MASQUERADE
iptables –t nat –A POSTROUTING –s 172.16.2.0/28 –o ens19 –j MASQUERADE
```

Сохранить созданные правила и запустить службу iptables с добавлением в автозагрузку:

```
iptables-save >> /etc/sysconfig/iptables
systemctl enable --now iptables
```

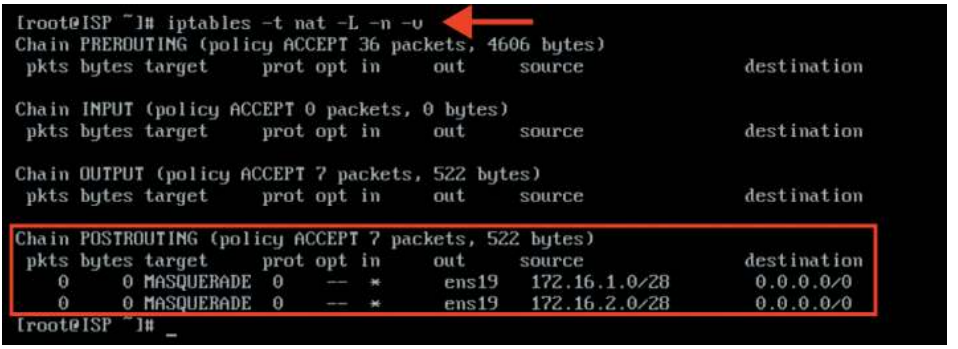
Как проверить?

Проверить включение функции пересылки пакетов:

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

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

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



Где выполнять?

На машинах: 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.

Задание 4. Настройте адресацию на интерфейсах.

Подробное описание пункта задания

Настройте адресацию на интерфейсах:

• настройте интерфейс на HQ-RTR в сторону ISP, интерфейс подключен к сети 172.16.1.0/28;

• настройте интерфейс на BR-RTR в сторону ISP, интерфейс подключен к сети 172.16.2.0/28.

Пример описания настроек на виртуальных машинах экзаменационного стенда

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

```
hq-rtr(config)#interface isp
hq-rtr(config-if)#description “ISP”
hq-rtr(config-if)#ip address 172.16.1.2/28
hq-rtr(config-if)#exit
hq-rtr(config)#ip route 0.0.0.0/0 172.16.1.1
hq-rtr(config)#port ge0
hq-rtr(config-port)#service-instance ge0/isp
hq-rtr(config-service-instance)#encapsulation untagged
hq-rtr(config-service-instance)#connect ip interface isp
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#exit
```

```
hq-rtr(config)#write memory
```

Как проверить?

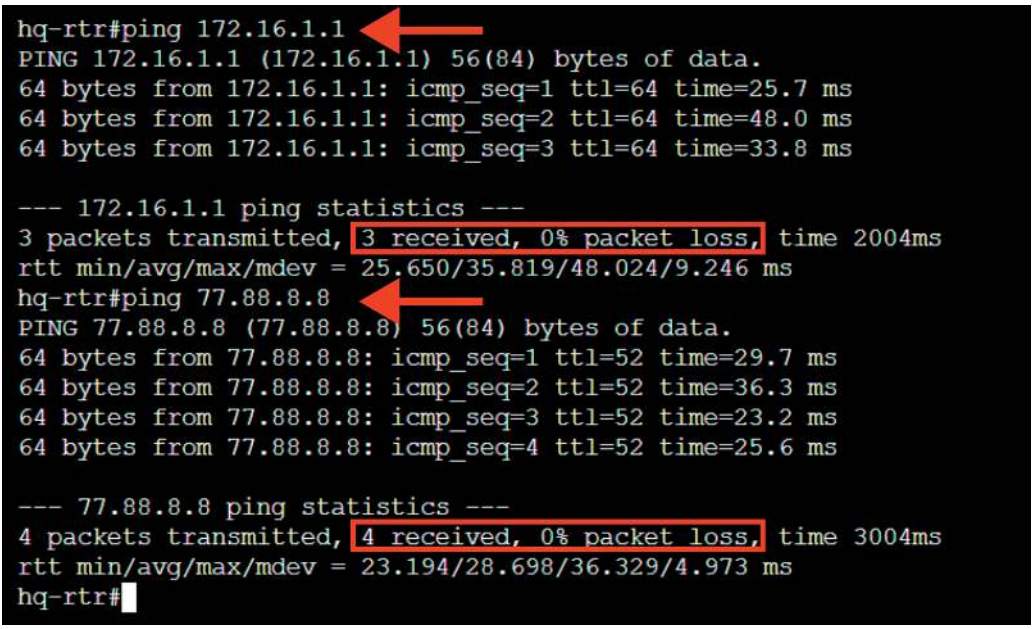
Проверка осуществляется командой привилегированного режима:

```
show ip interface brief
```

```
show ip route
```

```
hq-rtr#show ip interface brief
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 vl100            192.168.100.1/27    up                    default
 vl200            192.168.200.1/24    up                    default
 vl999            192.168.99.1/29     up                    default
 isp              172.16.1.2/28       up                    default
hq-rtr#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.16.1.1, isp
C       172.16.1.0/28 is directly connected, isp
C       192.168.99.0/29 is directly connected, vl999
C       192.168.100.0/27 is directly connected, vl100
C       192.168.200.0/24 is directly connected, vl200
hq-rtr#
```

Проверка доступности шлюза по умолчанию и доступа в сеть Интернет:



Где выполнять?

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

Краткая справка:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

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.

Создание локальных учетных записей

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

Подробное описание пункта задания

Создайте пользователя sshuser на серверах HQ-SRV и BR-SRV:

• пароль пользователя sshuser — P@ssw0rd;

• идентификатор пользователя — 2026;

• пользователь sshuser должен иметь возможность запускать sudo без ввода пароля.

Как делать?

Во время создания учетных записей на ОС «Альт» создается пользователь `sshuser` с идентификатором `2026`, после чего задается пароль `P@ssw0rd`. Затем запускается файл редактирования `sudo`, где необходимо раскомментировать 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 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 или добавить 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

Создать пользователя `sshuser` с явным указанием UID со значением `2026` можно с помощью команды:

```
useradd sshuser –u 2026
```

Задать пароль для пользователя `sshuser` можно с помощью утилиты `passwd`:

```
[root@hq-srv ~]# passwd sshuser
passwd: updating all authentication tokens for user sshuser.

You can now choose the new password or passphrase.

A valid password should be a mix of upper and lower case letters, digits, and
other characters.  You can use a password containing at least 7 characters
from all of these classes, or a password containing at least 8 characters
from just 3 of these 4 classes.
An upper case letter that begins the password and a digit that ends it do not
count towards the number of character classes used.

A passphrase should be of at least 3 words, 11 to 72 characters long, and
contain enough different characters.

Alternatively, if no one else can see your terminal now, you can pick this as
your password: "paddy-Barn4Knew".

Enter new password:
Weak password: based on a dictionary word and not a passphrase.
Re-type new password:
passwd: all authentication tokens updated successfully
[root@hq-srv ~]# _
```

Добавить пользователя `sshuser` в группу `wheel` можно с помощью команды:

```
usermod -aG wheel sshuser
```

Добавить строку в конфигурационный файл `/etc/sudoers`, позволяющую пользователям, входящим в группу wheel, выполнять через `sudo` любую команду:

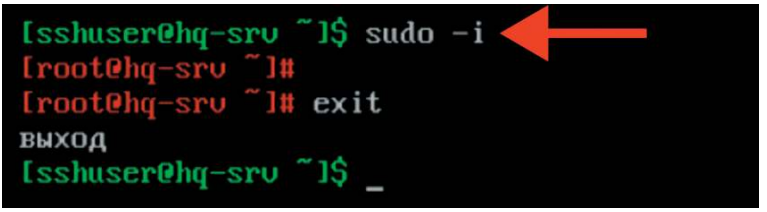
```
echo «sshuser ALL=(ALL:ALL) NOPASSWD: ALL» >> /etc/sudoers
```

Как проверить?

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

```
Welcome to ALT Server 11.0 (Mendelevium)!

Hostname: hq-srv.au-team.irpo
IP: 192.168.0.2
Hint: Num Lock on

hq-srv login: sshuser
Password:
Last login: Fri Oct 24 19:56:25 MSK 2025 on tty1
[sshuser@hq-srv ~]$ id
uid=2026(sshuser) gid=2026(sshuser) группы=2026(sshuser),10(wheel)
[sshuser@hq-srv ~]$ _
```

Попытаться перейти в режим суперпользователя, используя sudo без ввода пароля.



Где выполнять?

На машинах: HQ-SRV и BR-SRV.

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, удалять 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 net_admin на маршрутизаторах HQ-RTR и BR-RTR.

Подробное описание пункта задания

Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR:

• пользователь net_admin с паролем P@ssw0rd;

• при настройке ОС на базе Linux нужно запускать sudo без ввода пароля;

• при настройке ОС отличных от Linux пользователь должен обладать максимальными привилегиями.

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;

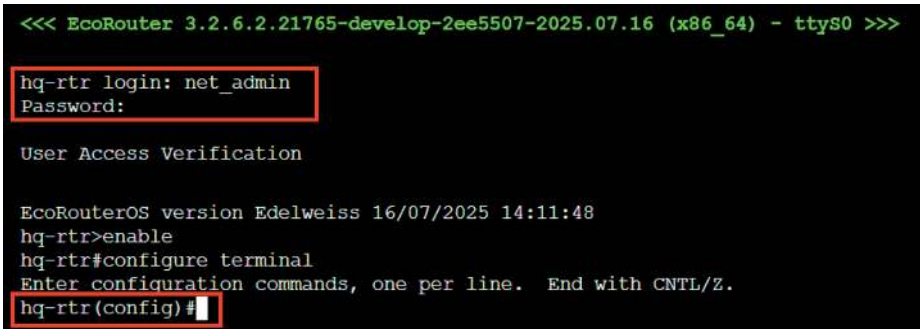
`noc` — привилегии оператора.

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr(config)#username net_admin
hq-rtr(config-user)#password P@ssw0rd
hq-rtr(config-user)#role admin
hq-rtr(config-user)#exit
```

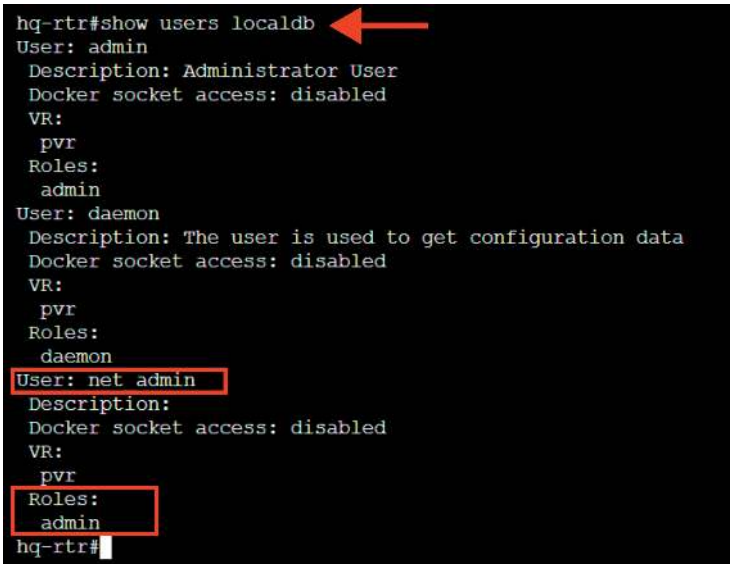
```
hq-rtr(config)#write memory
```

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
```



Где выполнять?
На машинах: HQ-RTR и BR-RTR.
Краткая справка:
– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).
Где изучается?
2 курс:
– Операционные системы и среды;
– Компьютерные сети.

Настройка коммутации, если HQ-SW — виртуальная машина

Подробное описание пункта задания

Настройте коммутацию в сегменте HQ следующим образом:

• трафик HQ-SRV должен принадлежать VLAN 100;

• трафик HQ-CLI должен принадлежать VLAN 200;

• предусмотрите возможность передачи трафика управления в VLAN 999;

• реализуйте на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта;

• сведения о настройке коммутации внесите в отчет.

Как делать?

Убедитесь, что службы `ovs-vswitchd` и `ovsdb-server` запущены, интерфейсы ovs включены и переведены в режим `manual`. Для этого необходимо установить openvswitch командой `apt-get install openvswitch`, после чего добавить в автозагрузку:

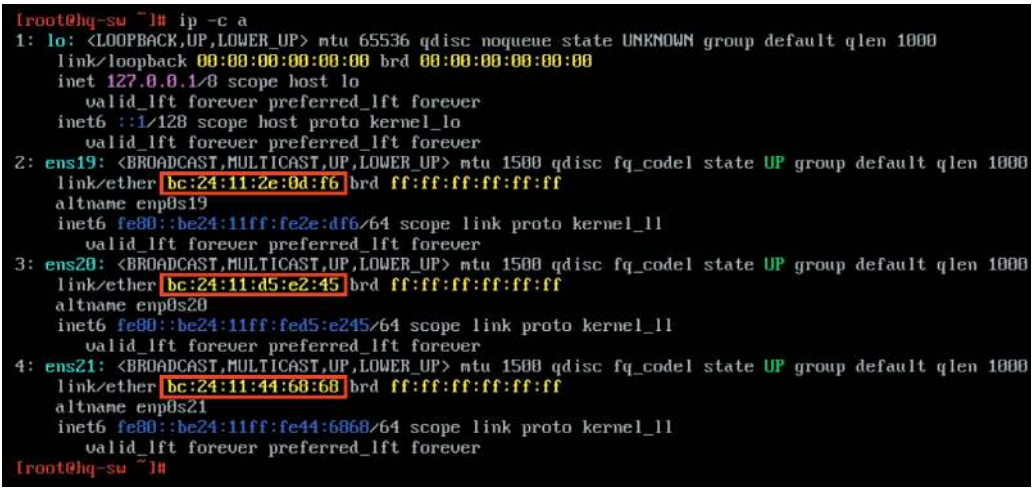
```
systemctl enable –-now openvswitch
```

Для всех интерфейсов должны быть созданы свои директории в `/etc/net/ifaces/` и файл `/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/options`, в котором прописано `TYPE = eth`.

После этого перезагрузите `network` командой:

```
systemctl restart network
```

Сверку соответствия сетям рекомендуется проводить по MAC-адресам.



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.

Создать мост:

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

Добавить в мост транковый интерфейс:

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

Добавить в мост интерфейс доступа, трафик которого будет тегироваться:

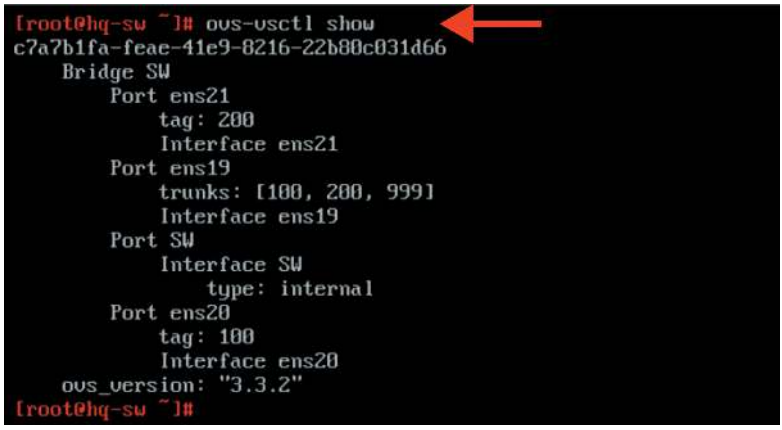
```
ovs-vsctl add-port SW ens4 tag=100
```

Добавить в мост интерфейс доступа, трафик которого будет тегироваться:

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

Как проверить?

```
ovs-vsctl show
```



Где выполнять?

На HQ-SW.

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.

Настройка коммутации, если HQ-SW не является виртуальной машиной

Подробное описание пункта задания

Настройте коммутацию в сегменте HQ следующим образом:

• трафик HQ-SRV должен принадлежать VLAN 100;

• трафик HQ-CLI должен принадлежать VLAN 200;

• предусмотреть возможность передачи трафика управления в VLAN 999;

• реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта;

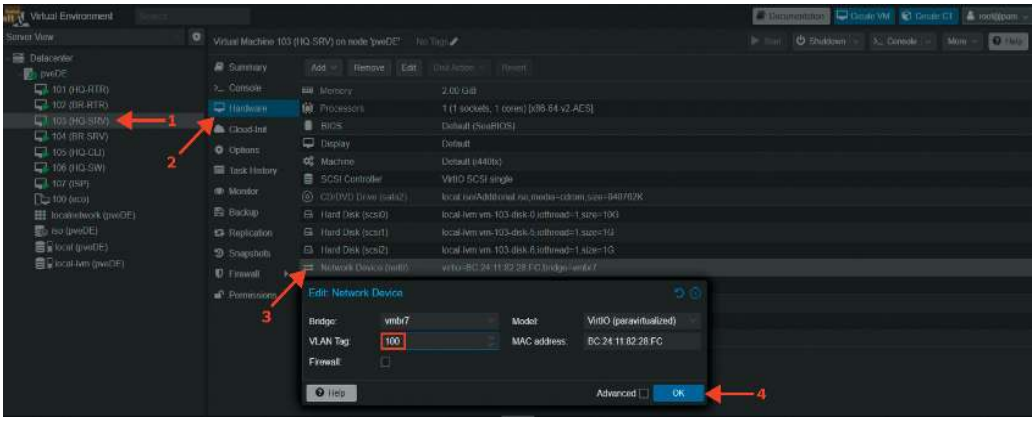
• сведения о настройке коммутации внесите в отчет.

Как делать?

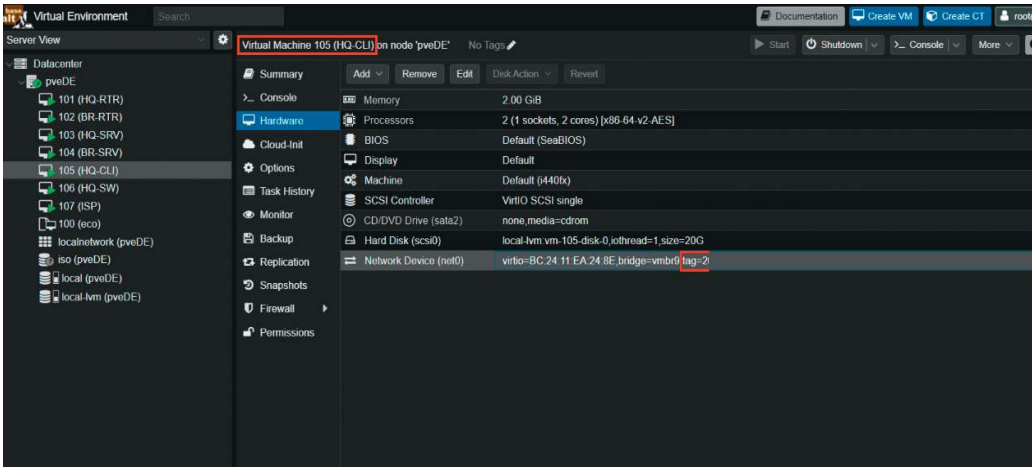
Поскольку данный вариант не подразумевает использование в качестве HQ-SW выделенной виртуальной машины, необходимо на конечных устройствах настроить порты доступа на уровне гипервизора, например, «Альт Виртуализация» (редакция PVE).

Пример описания настроек на виртуальных машинах экзаменационного стенда

Настройка порта доступа для виртуальной машины HQ-SRV с указанием VID — `100`:

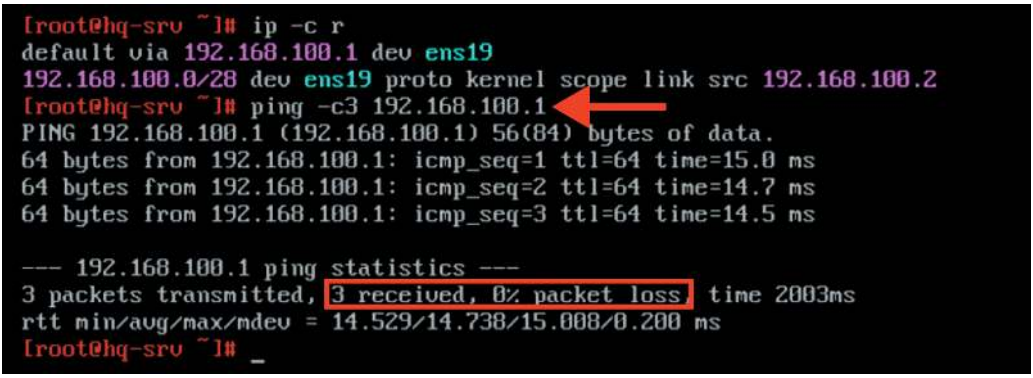


Настройка порта доступа для виртуальной машины HQ-CLI с указанием VID — `200`:



Как проверить?

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



Где выполнять?

На машинах: гипервизор (порты доступа).

Краткая справка:

– PVE поддерживает настройку VLAN для гостевых систем «из коробки» (https://docs.altlinux.org/ru-RU/alt-server-v/11.0/html/alt-server-v/ch28s06.html).

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

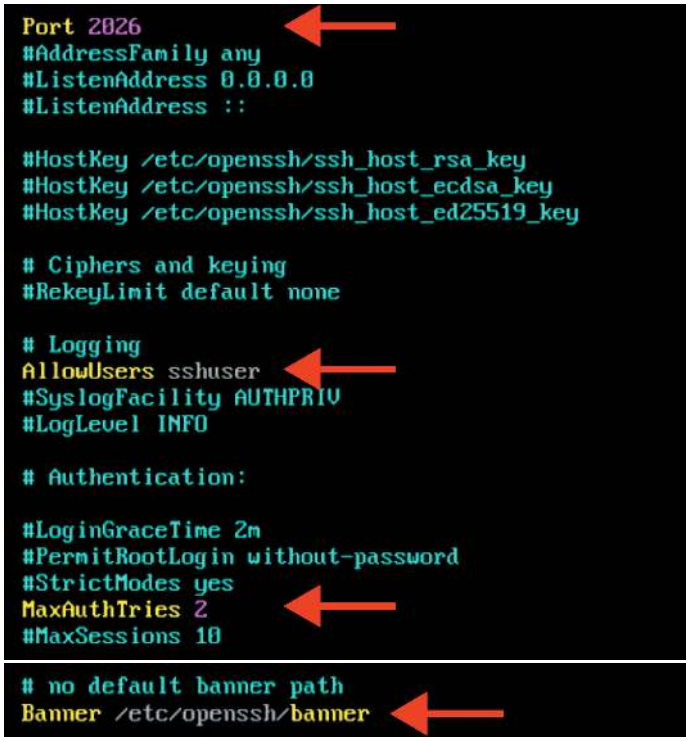
Подробное описание пункта задания

Настройте безопасный удаленный доступ на серверах HQ-SRV и BR-SRV:

- для подключения используйте порт 2026;
- разрешите подключения исключительно пользователю sshuser;
- ограничьте количество попыток входа до двух;
- настройте баннер «Authorized access only».

Как делать?

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



Здесь:

• `Port 2026` — порт, на котором следует ожидать запросы на соединение. Значение по умолчанию — 22;

• `AllowUsers sshuser` — список имен пользователей через пробел. Если параметр определен, 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;

• `Banner /etc/openssh/banner` — содержимое указанного файла будет отправлено удаленному пользователю прежде, чем будет разрешена аутентификация.

Редактируем баннер, а именно файл по пути `/etc/openssh/banner` и добавляем в него следующее содержимое `Authorized access only:`

```
echo «Authorized access only» > /etc/openssh/banner
```

Для применения всех изменений необходимо перезапустить службу `sshd`, для этого можно использовать команду:

```
systemctl restart sshd
```

Как проверить?

Попытаться подключиться не из-под пользователя `sshuser`:

```
[root@hq-srv ~]# ssh -p 2026 user@localhost
Authorized access only
user@localhost's password:
ssh: Permission denied, please try again.
user@localhost's password:
ssh: Received disconnect from 127.0.0.1 port 2026:2: Too many authentication failures
Disconnected from 127.0.0.1 port 2026
[root@hq-srv ~]#
```

Попытаться подключиться под пользователем `sshuser`:

```
[root@hq-srv ~]# ssh -p 2026 sshuser@localhost
Authorized access only
sshuser@localhost's password:
Last login: Fri Oct 24 19:58:26 2025
[sshuser@hq-srv ~]$
```

Попытаться подключиться под пользователем `sshuser` на стандартный порт ssh:

```
[root@hq-srv ~]# ssh sshuser@localhost
ssh: connect to host localhost port 22: Connection refused
[root@hq-srv ~]# _
```

Попытаться подключиться под пользователем `sshuser` с указанием неверных паролей более чем 2 раза:

```
[root@hq-srv ~]# ssh -p 2026 sshuser@localhost
Authorized access only
sshuser@localhost's password:
ssh: Permission denied, please try again.
sshuser@localhost's password:
ssh: Received disconnect from 127.0.0.1 port 2026:2: Too many authentication failures
Disconnected from 127.0.0.1 port 2026
[root@hq-srv ~]#
```

Где выполнять?

На серверах: HQ-SRV и BR-SRV.

Дополнительно:

ssh (secure shell) — это сетевой протокол, который обеспечивает безопасный доступ к удаленным 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;

• удаленное 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 на маршрутизаторах IP-туннеля с использованием технологии GRE

Подробное описание пункта задания

Между офисами HQ и BR на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать IP-туннель:

• на выбор технологии GRE или IP in IP;

• сведения о туннеле занесите в отчет.

Как делать?

Для создания интерфейса GRE-туннеля на ОС «EcoRouterOS» создается 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 должен быть выбран как `gre`.

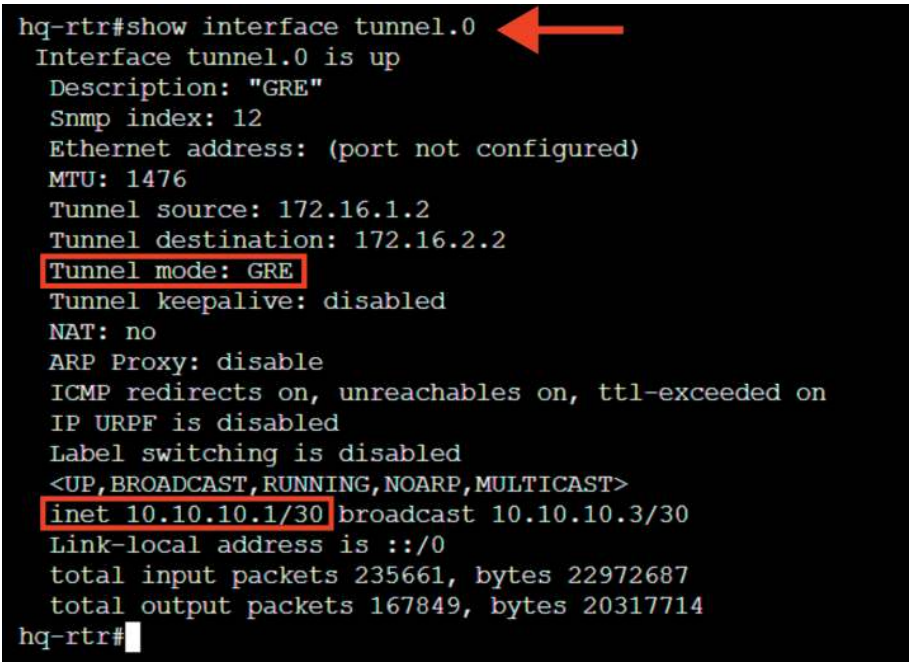
Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#description “GRE”
hq-rtr(config-if-tunnel)#ip address 10.10.10.1/30
hq-rtr(config-if-tunnel)#ip tunnel 172.16.1.2 172.16.2.2 mode gre
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
```

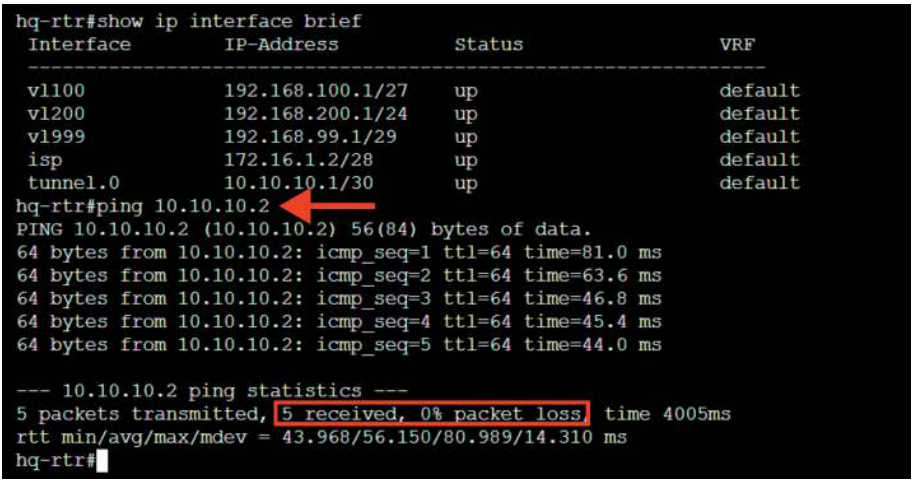
```
br-rtr(config)#interface tunnel.0
br-rtr(config-if-tunnel)#description “GRE”
br-rtr(config-if-tunnel)#ip address 10.10.10.2/30
br-rtr(config-if-tunnel)#ip tunnel 172.16.2.2 172.16.1.2 mode
gre
br-rtr(config-if-tunnel)#exit
br-rtr(config)#write memory
```

Как проверить?
Выполнить команду (из привилегированного режима):

```
show interface tunnel.<№>
```



Средствами утилиты ping проверить связность с противоположной стороной туннеля:



Где выполнять?

На машинах: HQ-RTR и BR-RTR.

Дополнительно:

Применение GRE:

• связывание удаленных 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 защищенных 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:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

Где изучается?

2 курс:

– Компьютерные сети и далее.

Настройка на маршрутизаторах IP-туннеля с использованием технологии IP in IP

Подробное описание пункта задания

Между офисами HQ и BR на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать IP-туннель:

• на выбор технологии GRE или IP in IP;

• сведения о туннеле занесите в отчет.

Как делать?

Для создания интерфейса IP-in-IP-туннеля на ОС «EcoRouterOS» создается 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>
```

Выставляется значение MTU, для этого используется команда (в режиме конфигурирования туннельного интерфейса):

```
ip mtu <значение_MTU>
```

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 должен быть выбран как `ipip`.

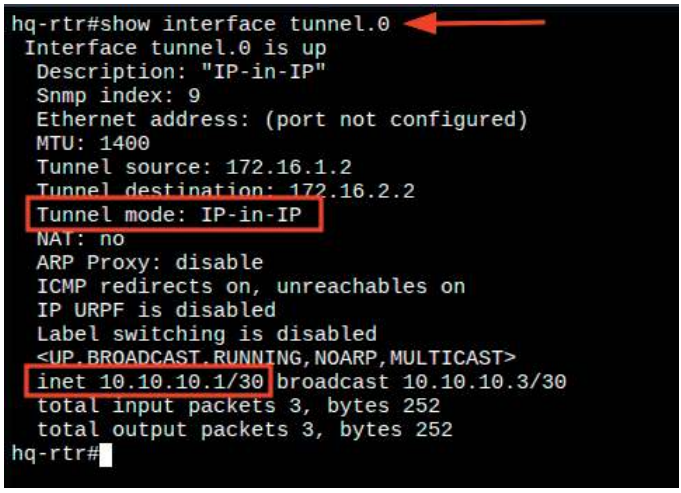
Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#description “IP-in-IP”
hq-rtr(config-if-tunnel)#ip address 10.10.10.1/30
hq-rtr(config-if-tunnel)#ip mtu 1400
hq-rtr(config-if-tunnel)#ip tunnel 172.16.1.2 172.16.2.2 mode ipip
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
```

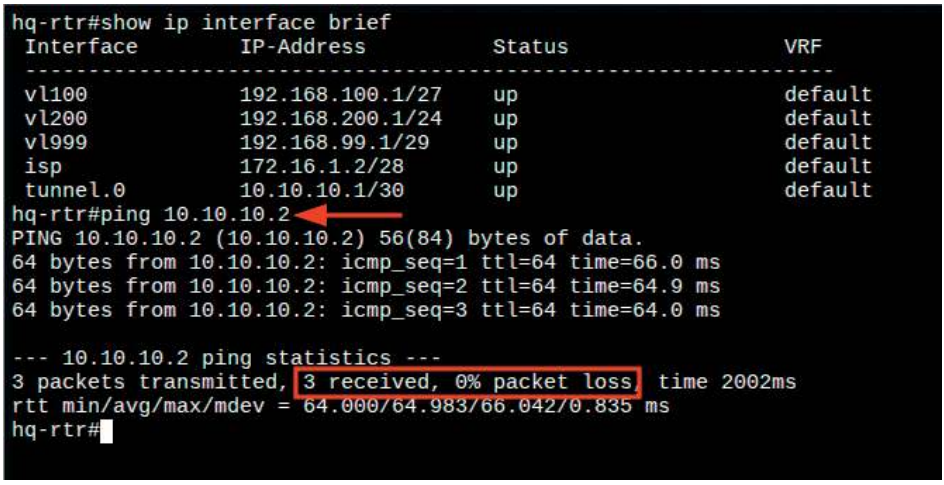
```
br-rtr(config)#interface tunnel.0
br-rtr(config-if-tunnel)#description “IP-in-IP”
br-rtr(config-if-tunnel)#ip address 10.10.10.2/30
br-rtr(config-if-tunnel)#ip mtu 1400
br-rtr(config-if-tunnel)#ip tunnel 172.16.2.2 172.16.1.2 mode ipip
br-rtr(config-if-tunnel)#exit
br-rtr(config)#write memory
```

Как проверить?

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



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



Где выполнять?

На машинах: HQ-RTR и BR-RTR.

Дополнительно:

IP in IP — механизм туннелирования, который помещает один IP-пакет в другой IP-пакет.

Процесс туннелирования заключается в добавлении еще одного IP-заголовка к стандартному IP-пакету. В верхнем заголовке будут содержаться

IP-адреса начала и окончания туннеля. После доставки на маршрутизатор, на котором находится окончание туннеля, верхний заголовок снимается, пакет передается с обычным, внутренним IP-заголовком дальше.

Типичная размерность MTU для L3 интерфейса 1500 байт. В связи с добавлением служебного заголовка появляются новые требования к допустимому значению MTU при передаче пакета. Заголовок IP in IP имеет размерность 20 байт, заголовок IP-пакета 20 байт, таким образом возникает необходимость задавать размер допустимого MTU на интерфейсах туннеля меньше стандартного значения для Ethernet.

Краткая справка:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

Где изучается?

2 курс:

– Компьютерные сети и далее.

Настройка динамической маршрутизации

Подробное описание пункта задания

Обеспечьте динамическую маршрутизацию на маршрутизаторах HQ-RTR и BR-RTR: сети одного офиса должны быть доступны из другого офиса и наоборот. Для обеспечения динамической маршрутизации используйте link state протокол (на усмотрение участника):

• разрешите выбранный протокол только на интерфейсах IP-туннеля;

• маршрутизаторы должны делиться маршрутами только друг с другом;

• обеспечьте защиту выбранного протокола посредством парольной защиты;

• сведения о настройке и защите протокола занесите в отчет.

Как делать?

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

```
router ospf <№>
```

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

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

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

```
passive-interface default
```

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

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

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

```
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(config)#router ospf 1
hq-rtr(config-router)#ospf router-id 10.10.10.1
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 192.168.100.0/27 area 0
hq-rtr(config-router)#network 192.168.200.0/24 area 0
hq-rtr(config-router)#network 192.168.99.0/29 area 0
hq-rtr(config-router)#exit
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#ip ospf authentication message-digest
hq-rtr(config-if-tunnel)#ip  ospf  message-digest-key  1  md5
P@ssw0rd
hq-rtr(config-if-tunnel)#exit
```

```
hq-rtr(config)#write memory
```

```
br-rtr(config)#router ospf 1
br-rtr(config-router)#ospf router-id 10.10.10.2
br-rtr(config-router)#passive-interface default
```

```
br-rtr(config-router)#no passive-interface tunnel.0
br-rtr(config-router)#network 192.168.0.0/28 area 0
br-rtr(config-router)#network 10.10.10.0/30 area 0
br-rtr(config-router)#exit
br-rtr(config)#interface tunnel.0
br-rtr(config-if-tunnel)#ip ospf authentication message-digest
br-rtr(config-if-tunnel)#ip ospf message-digest-key 1 md5 P@ssw0rd
br-rtr(config-if-tunnel)#exit
```

```
br-rtr(config)#write memory
```

Как проверить?

Для просмотра данных о состоянии и сконфигурированных настройках на интерфейсах, участвующих в OSPF процессе, воспользуйтесь командой:

```
show ip ospf interface brief
```

```
hq-rtr#show ip ospf interface brief
Interface    PID   Area            Intf ID    Cost  State           Neighbors  Status
vl100        1     0.0.0.0         5          1     DROther         0          Up

Interface    PID   Area            Intf ID    Cost  State           Neighbors  Status
vl200        1     0.0.0.0         6          1     DROther         0          Up

Interface    PID   Area            Intf ID    Cost  State           Neighbors  Status
vl999        1     0.0.0.0         7          1     DROther         0          Up

Interface    PID   Area            Intf ID    Cost  State           Neighbors  Status
tunnel.0     1     0.0.0.0         9          1     DR              1          Up

hq-rtr#
```

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           Instance ID
10.10.10.2        1   Full/Backup     00:00:38    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
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.16.1.1, isp
C       10.10.10.0/30 is directly connected, tunnel.0
C       172.16.1.0/28 is directly connected, isp
O       192.168.0.0/28 [110/11] via 10.10.10.2, tunnel.0, 00:01:10
C       192.168.99.0/29 is directly connected, vl999
C       192.168.100.0/27 is directly connected, vl100
C       192.168.200.0/24 is directly connected, vl200
hq-rtr#
```

```
br-rtr#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.2.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.16.2.1, isp
C       10.10.10.0/30 is directly connected, tunnel.0
C       172.16.2.0/28 is directly connected, isp
C       192.168.0.0/28 is directly connected, int1
O       192.168.99.0/29 [110/11] via 10.10.10.1, tunnel.0, 00:02:35
O       192.168.100.0/27 [110/11] via 10.10.10.1, tunnel.0, 00:02:35
O       192.168.200.0/24 [110/11] via 10.10.10.1, tunnel.0, 00:02:35
br-rtr#
```

Проверить защиту выбранного протокола посредством парольной защиты можно из привилегированного режима с помощью команды:

```
show ip ospf interface tunnel.0
```

```
hq-rtr#show ip ospf interface tunnel.0
tunnel.0 is up, line protocol is up
  Internet Address 10.10.10.1/30, Area 0.0.0.0, MTU 1476
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.10.10.1, Interface Address 10.10.10.1
  Backup Designated Router (ID) 10.10.10.2, Interface Address 10.10.10.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 599215
  Hello received 25 sent 44, DD received 3 sent 5
  LS-Req received 0 sent 1, LS-Upd received 3 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  Message-digest authentication, using key-id 1
hq-rtr#
```

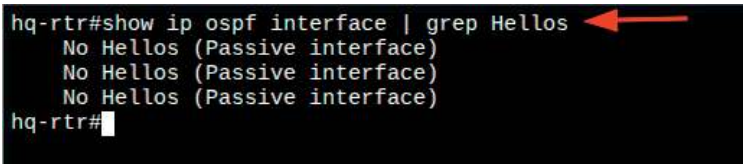
Проверить, что маршрутизаторы должны делиться маршрутами только друг с другом, можно из привилегированного режима с помощью команды:

```
show ip ospf interface
```

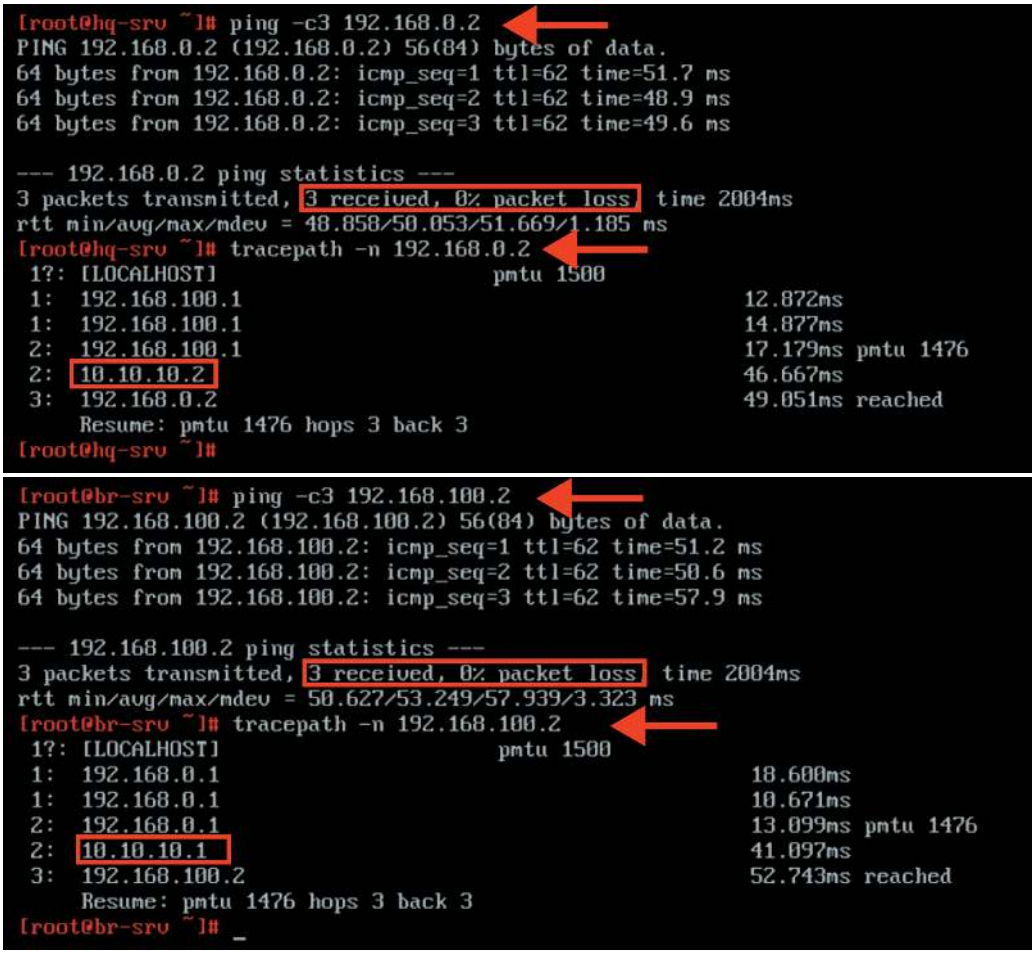
```
hq-rtr#show ip ospf interface
vl100 is up, line protocol is up
  Internet Address 192.168.100.1/27, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 10
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
vl200 is up, line protocol is up
  Internet Address 192.168.200.1/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 10
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
vl999 is up, line protocol is up
  Internet Address 192.168.99.1/29, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 10
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
tunnel.0 is up, line protocol is up
  Internet Address 10.10.10.1/30, Area 0.0.0.0, MTU 1476
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DR, Priority 1, TE Metric 1
  Designated Router (ID) 10.10.10.1, Interface Address 10.10.10.1
  Backup Designated Router (ID) 10.10.10.2, Interface Address 10.10.10.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 599236
  Hello received 46 sent 65, DD received 3 sent 5
  LS-Req received 0 sent 1, LS-Upd received 3 sent 3
  LS-Ack received 2 sent 3, Discarded 0
  Message-digest authentication, using key-id 1
hq-rtr#
```

Или с помощью команды:

```
show ip ospf interface | grep Hellos
```



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



Где выполнять?
На машинах: HQ-RTR, BR-RTR, BR-SRV и HQ-SRV.

Дополнительно:

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

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

Вот несколько ключевых преимуществ OSPF:

• быстрая сходимость: 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:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

Где изучается?

2 курс:

– Компьютерные сети и далее на других курсах.

Настройка динамической трансляции адресов

Подробное описание пункта задания

Настройка динамической трансляции адресов на маршрутизаторах HQ-RTR и BR-RTR:

• настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет.

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>
```

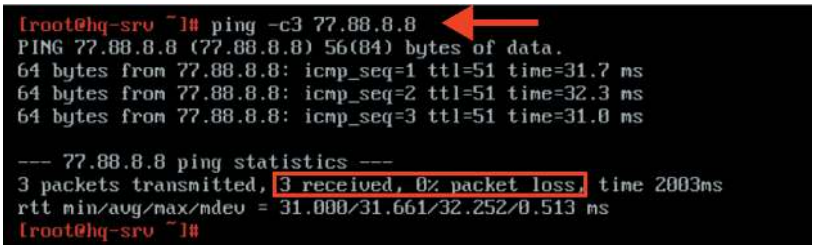
Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr(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 VLAN100 192.168.100.1-192.168.100.30
hq-rtr(config)#ip nat pool VLAN200 192.168.200.1-192.168.200.254
hq-rtr(config)#ip nat pool VLAN999 192.168.99.1-192.168.99.6
hq-rtr(config)#ip nat source dynamic inside-to-outside pool VLAN100 overload interface isp
hq-rtr(config)#ip nat source dynamic inside-to-outside pool VLAN200 overload interface isp
hq-rtr(config)#ip nat source dynamic inside-to-outside pool VLAN999 overload interface isp
hq-rtr(config)#write memory
```

```
br-rtr(config)#interface isp
br-rtr(config-if)#ip nat outside
br-rtr(config-if)#exit
br-rtr(config)#interface int1
br-rtr(config-if)#ip nat inside
br-rtr(config-if)#exit
br-rtr(config)#ip nat pool BR-Net 192.168.0.1-192.168.0.14
br-rtr(config)#ip nat source dynamic inside-to-outside pool BR-Net
overload interface isp
br-rtr(config)#exit
```

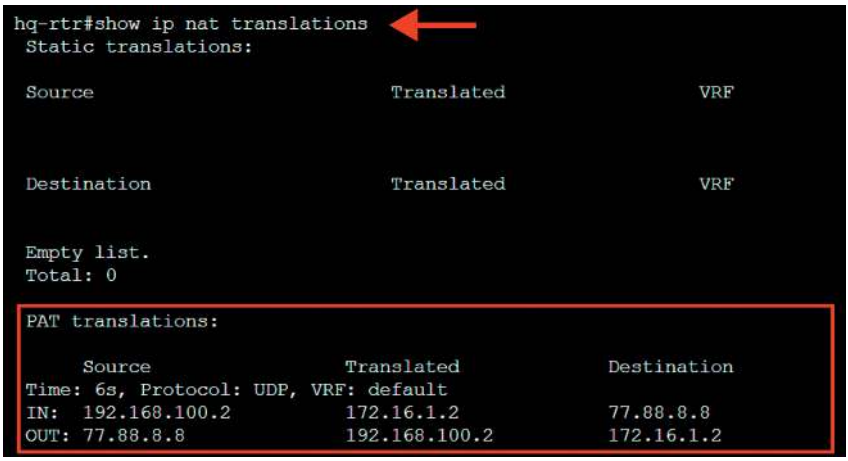
```
br-rtr#write memory
```

Как проверить?
Средствами утилиты `ping` с HQ-SRV попытаться проверить связность с ISP:



После чего на HQ-RTR из привилегированного режима просмотреть таблицу NAT при помощи команды:

```
show ip nat translations
```



Где выполнять?
На виртуальных машинах: HQ-RTR и BR-RTR.

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 ее менее уязвимой к внешним атакам. Внешние устройства не могут напрямую обращаться к внутренним адресам;

• гибкость и управляемость: позволяет 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:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

Где изучается?

2 курс:

– Операционные системы и среды;

– Компьютерные сети и далее.

Настройка протокола динамической конфигурации хостов

Подробное описание пункта задания

Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI:

• настройте нужную подсеть;

• 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 — au-team.irpo;

• сведения о настройке протокола занесите в отчет.

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 определенного интерфейса при помощи следующей команды:

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

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr(config)#ip pool VLAN200 192.168.200.2-192.168.200.254
hq-rtr(config)#dhcp-server 1
hq-rtr(config-dhcp-server)#pool VLAN200 1
hq-rtr(config-dhcp-server-pool)#mask 24
hq-rtr(config-dhcp-server-pool)#gateway 192.168.200.1
hq-rtr(config-dhcp-server-pool)#dns 192.168.100.2
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
```

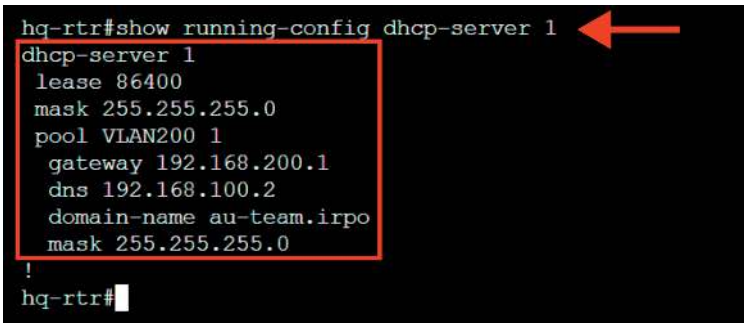
```
hq-rtr(config-if)#dhcp-server 1
hq-rtr(config-if)#exit
```

```
hq-rtr(config)#write memory
```

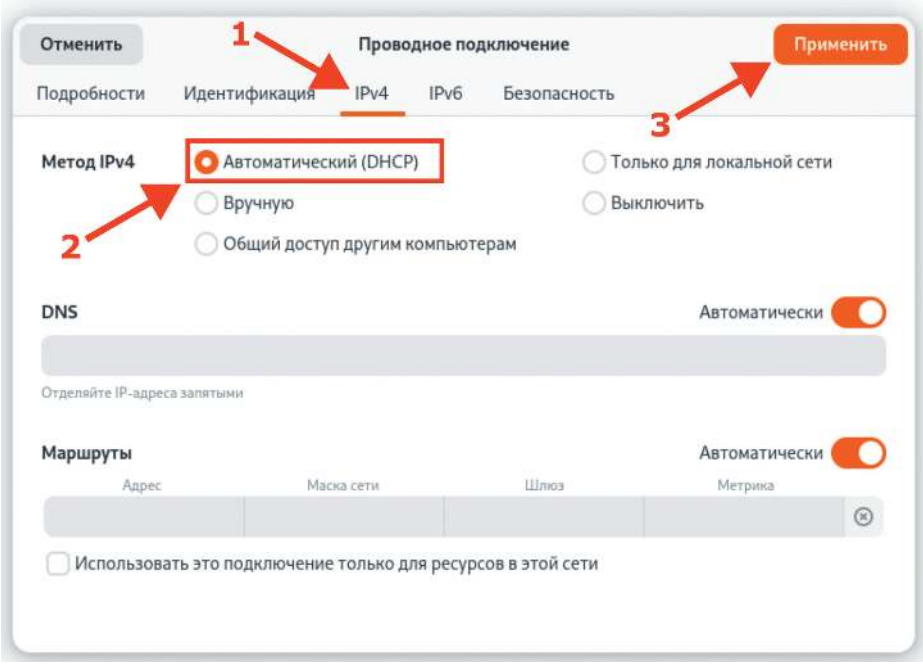
Как проверить?

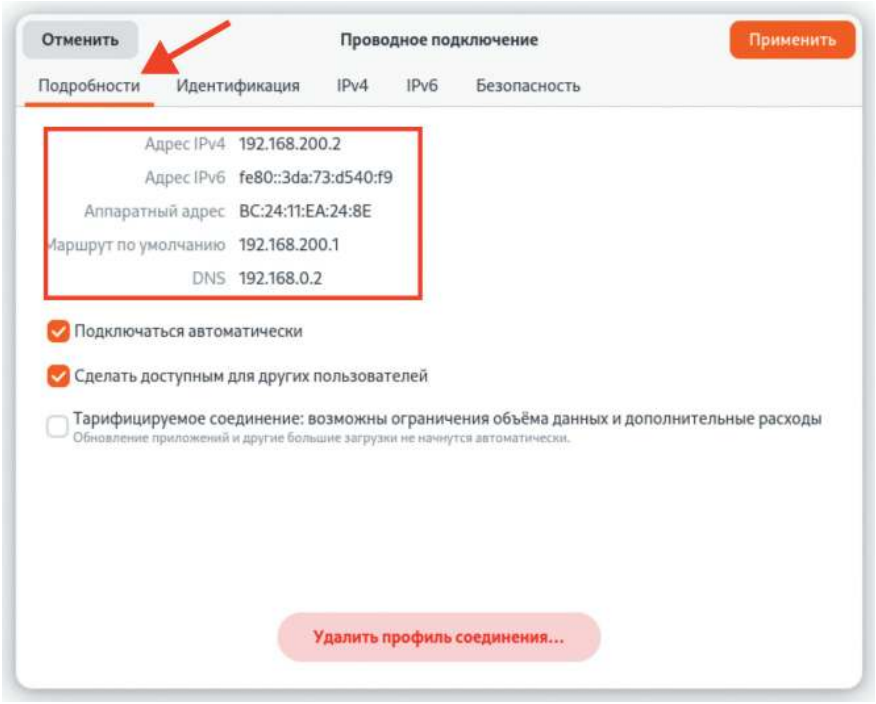
Из привилегированного режима можно проверить информацию о созданном DHCP-пуле, используя команду:

```
show running-config dhcp-server 1
```



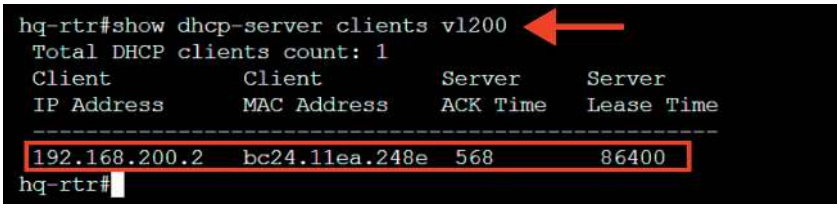
На виртуальной машине HQ-CLI должен быть получен IP-адрес и все необходимые сетевые параметры автоматически:





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

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



Где выполнять?

На виртуальной машине: 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 определенных 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:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

Где изучается?

2 курс:

– Операционные системы и среды;

– Компьютерные сети и далее.

Настройка инфраструктуры разрешения доменных имен

Подробное описание пункта задания

Настройте инфраструктуру разрешения доменных имен для офисов HQ и BR:

• основной DNS-сервер реализован на HQ-SRV;

• сервер должен обеспечивать разрешение имен в сетевые адреса устройств и обратно в соответствии с табл. 1.3;

• в качестве DNS-сервера пересылки используйте любой общедоступный DNS-сервер (77.88.8.7, 77.88.8.3 или другие).

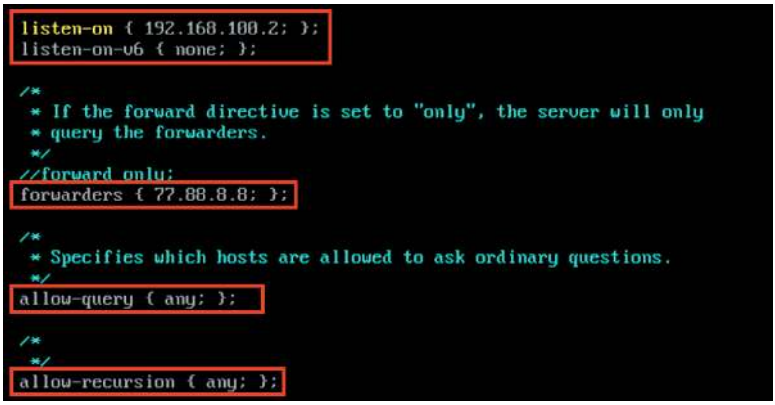
Устройство	Запись	Тип
HQ-RTR	hq-rtr.au-team.irpo	A,PTR
BR-RTR	br-rtr.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A,PTR
HQ-CLI	hq-cli.au-team.irpo	A,PTR
BR-SRV	br-srv.au-team.irpo	A
ISP (интерфейс, направленный в сторону HQ-RTR)	docker.au-team.irpo	A
ISP (интерфейс, направленный в сторону BR-RTR)	web.au-team.irpo	A

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 bind-utils -y
```

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



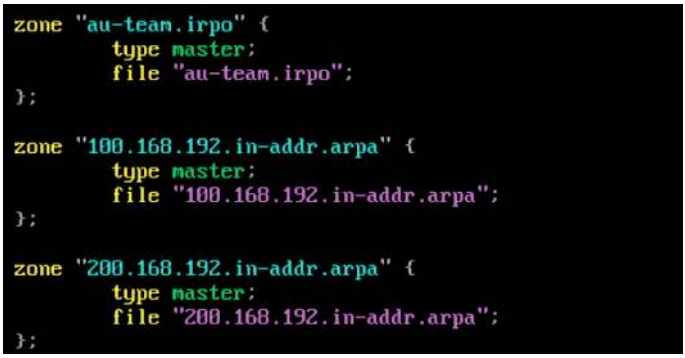
На фото выделены следующие элементы конфигурационного файла:

• listen-on — этот 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 конец файла (но не заменить) /var/lib/bind/etc/rfc1912.conf, используя текстовый редактор vim:



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

```
cp /var/lib/bind/etc/zone/empty /var/lib/bind/etc/zone/au-team.irpo
cp  /var/lib/bind/etc/zone/empty  /var/lib/bind/etc/zone/
100.168.192.in-addr.arpa
```

```
cp  /var/lib/bind/etc/zone/empty  /var/lib/bind/etc/zone/
200.168.192.in-addr.arpa
```

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

```
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025062300      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
        IN      A       192.168.100.2
hq-srv  IN      A       192.168.100.2
hq-cli  IN      A       192.168.200.2
hq-rtr  IN      A       192.168.100.1
hq-rtr  IN      A       192.168.200.1
hq-rtr  IN      A       192.168.99.1
docker  IN      A       172.16.1.1
web     IN      A       172.16.2.1
br-srv  IN      A       192.168.0.2
br-rtr  IN      A       192.168.0.1
```

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

```
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025062300      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
1       IN      PTR     hq-rtr.au-team.irpo.
2       IN      PTR     hq-srv.au-team.irpo.
```

Далее необходимо настроить обратную зону и привести файл `200.168.192.in-addr.arpa` к следующему виду:

```
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025062300      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
1       IN      PTR     hq-rtr.au-team.irpo.
2       IN      PTR     hq-cli.au-team.irpo.
```

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, 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' /etc/bind/rndc.key
```

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:

```
chown -R root:named /var/lib/bind/etc/zone/*
```

```
[root@hq-srv ~]# named-checkconf
[root@hq-srv ~]#
```

```
[root@hq-srv ~]# named-checkconf -z
zone localhost/IN: loaded serial 2025062300
zone localdomain/IN: loaded serial 2025062300
zone 127.in-addr.arpa/IN: loaded serial 2025062300
zone 0.in-addr.arpa/IN: loaded serial 2025062300
zone 255.in-addr.arpa/IN: loaded serial 2025062300
zone au-team.irpo/IN: loaded serial 2025062300
zone 100.168.192.in-addr.arpa/IN: loaded serial 2025062300
zone 200.168.192.in-addr.arpa/IN: loaded serial 2025062300
[root@hq-srv ~]#
```

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 ~]# systemctl enable --now bind.service
Synchronizing state of bind.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable bind
[root@hq-srv ~]# systemctl status bind.service
● bind.service - Berkeley Internet Name Domain (DNS)
     Loaded: loaded (/usr/lib/systemd/system/bind.service; enabled; preset: disabled)
     Active: active (running) since Tue 2025-10-28 17:24:38 MSK; 10s ago
    Process: 2380 ExecStartPre=/etc/init.d/bind rndc_keygen (code=exited, status=0/SUCCESS)
    Process: 2384 ExecStartPre=/usr/bin/named-checkconf $CHROOT -z /etc/named.conf (code=exited, status=0/SUCCESS)
    Process: 2386 ExecStart=/usr/sbin/named -u named $CHROOT $RETAIN_CAPS $EXTRAOPTIONS (code=exited, status=0/SUCCESS)
      Tasks: 4 (limit: 2343)
     Memory: 30.2M (peak: 30.6M)
        CPU: 149ms
     CGroup: /system.slice/bind.service
             └─2387 /usr/sbin/named -u named
```

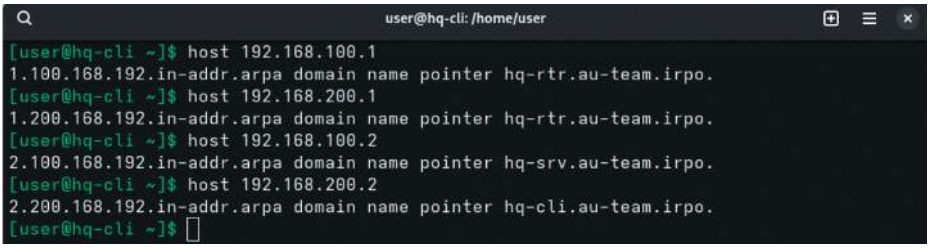
Как проверить?

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

```
[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 192.168.100.2
[root@hq-srv ~]#
[root@hq-srv ~]# 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=51 time=32.6 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=2 ttl=51 time=28.3 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=3 ttl=51 time=30.3 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 28.292/30.395/32.633/1.774 ms
[root@hq-srv ~]#
```

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

```
user@hq-cli: /home/user
[user@hq-cli ~]$ host hq-srv.au-team.irpo
hq-srv.au-team.irpo has address 192.168.100.2
[user@hq-cli ~]$ host hq-cli.au-team.irpo
hq-cli.au-team.irpo has address 192.168.200.2
[user@hq-cli ~]$ host hq-rtr.au-team.irpo
hq-rtr.au-team.irpo has address 192.168.99.1
hq-rtr.au-team.irpo has address 192.168.100.1
hq-rtr.au-team.irpo has address 192.168.200.1
[user@hq-cli ~]$ host docker.au-team.irpo
docker.au-team.irpo has address 172.16.1.1
[user@hq-cli ~]$ host web.au-team.irpo
web.au-team.irpo has address 172.16.2.1
[user@hq-cli ~]$ host br-rtr.au-team.irpo
br-rtr.au-team.irpo has address 192.168.0.1
[user@hq-cli ~]$ host br-srv.au-team.irpo
br-srv.au-team.irpo has address 192.168.0.2
[user@hq-cli ~]$
```



Где выполнять?

На виртуальной машине: HQ-SRV.

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 часового пояса

Подробное описание пункта задания
Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора в случае его использования) согласно месту проведения экзамена.

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

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

Например:

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

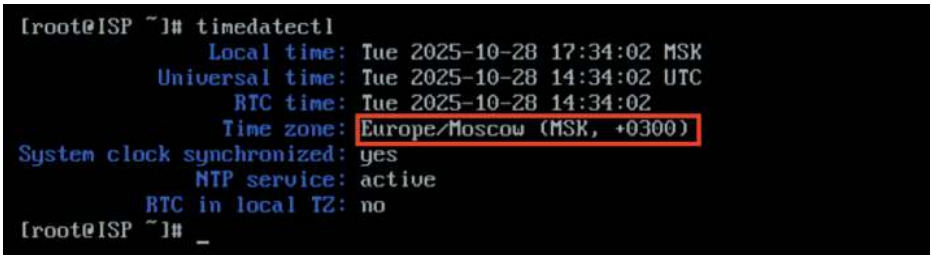
На устройствах с ОС «EcoRouterOS» необходимо выполнить следующую команду из режима администрирования (`conf t`):

```
ntp timezone utc+<ЦИФРА>
```

Например:

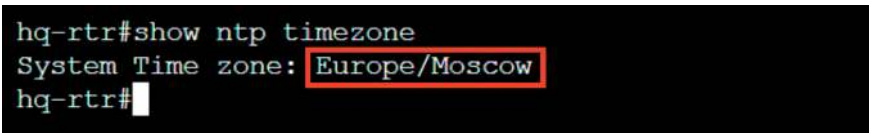
```
ntp timezone utc+3
```

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



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

```
show ntp timezone
```



Где выполнять?

На всех машинах.

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 задачах 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 и далее.

МОДУЛЬ 2. ОРГАНИЗАЦИЯ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ

Модуль 2
Организация сетевого администрирования
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. рис. 2.1).

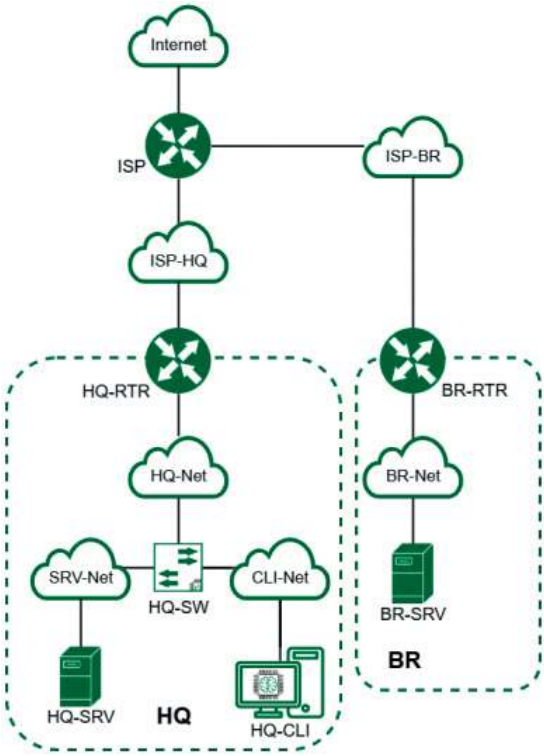


Рис. 2.1. Топология сети

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;

• порты ssh на серверах;
• DHCP-сервер;
• DNS-сервер;
• сервер HQ-SRV имеет два дополнительных накопителя размером 1 ГБ.

Задание Модуля 2 содержит развертывание доменной инфраструктуры, внедрение и настройку ansible как инфраструктуры на основе открытых ключей, установку и настройку отказоустойчивого дискового массива, установку и настройку файловых служб, службы сетевого времени, настройки веб-серверов, установку приложения.

В ходе проектирования и настройки сетевой инфраструктуры следует заносить записи в отчет о своих действиях, когда это требуется в задании. Отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла без учета расширения — ФамилияУчастникаМодуль2.

Таблица 2.1

Имя виртуальной машины	**Оперативная память**	**Центральный процессор, ядер**	**Накопитель**	**Операционная система**
ISP	1 ГБ	1 ядро	5 ГБ	Дистрибутив ОС JeOS/Linux или аналог
HQ-RTR	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter 1 ядро в случае использования дистрибутива Linux	10 ГБ	ОС «EcoRouterOS», в случае невозможности использования EcoRouter — дистрибутив ОС JeOS/Linux или аналог
BR-RTR	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter ядро ГБ в случае использования дистрибутива Linux	10 ГБ	ОС «EcoRouterOS», в случае невозможности использования EcoRouter — дистрибутив ОС JeOS/Linux или аналог
HQ-SRV	2 ГБ	1 ядро	10 ГБ	ОС «Альт Сервер» или аналог
BR-SRV	2 ГБ	1 ядро	10 ГБ	ОС «Альт Сервер» или аналог
HQ-CLI	2 ГБ	2 ядра	20 ГБ	ОС «Альт Рабочая станция» или аналог

Окончание табл. 2.1

Имя виртуальной машины	Оперативная память	Центральный процессор, ядер	Накопитель	Операционная система
Итого	15 (9 в случае использования ОС «Альт» или аналога)	13 (7 в случае использования ОС «Альт» или аналога)	60 ГБ	–

1. Настройте контроллер домена Samba DC на сервере BR-SRV:

• имя домена au-team.irpo;

• введите в созданный домен машину HQ-CLI;

• создайте 5 пользователей для офиса HQ: имена пользователей формата hquser№ (например: hquser1, hquser2 и т.д.);

• создайте группу hq, введите в группу созданных пользователей;

• убедитесь, что пользователи группы hq имеют право аутентифицироваться на HQ-CLI;

• пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы права не имеют.

2. Сконфигурируйте файловое хранилище на сервере HQ-SRV:

• при помощи двух подключенных к серверу дополнительных дисков размером 1 ГБ сконфигурируйте дисковый массив уровня 0;

• имя устройства — md0, при необходимости конфигурация массива размещается в файле /etc/mdadm.conf;

• создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4;

• обеспечьте автоматическое монтирование в папку /raid.

3. Настройте сервер сетевой файловой системы (nfs) на HQ-SRV:

• в качестве папки общего доступа выберите /raid/nfs, доступ для чтения и записи исключительно для сети в сторону HQ-CLI;

• на HQ-CLI настройте автомонтирование в папку /mnt/nfs;

• основные параметры сервера отметьте в отчете.

4. Настройте службу сетевого времени на базе сервиса chrony на маршрутизаторе ISP:

• вышестоящий сервер ntp на маршрутизаторе ISP — на выбор участника;

• стратум сервера — 5;

• в качестве клиентов ntp настройте: HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.

5. 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.

6. Разверните веб-приложение testapp с использованием средств контейнеризации на сервере BR-SRV:

• все необходимые компоненты разместите в директории docker образа Additional.iso;

• импортируйте все необходимые образы из директории ./docker;

• доступный набор переменных указан в файле readme.txt;

• веб-приложение должно быть:

◦ работоспособным после перезапуска узла или контейнеров;

◦ доступно с других узлов через порт 8080;

• подключение к СУБД:

◦ тип mariadb;

◦ порт 3306;

◦ учетная запись СУБД webapp;

◦ пароль P@ss2026-db;

◦ название БД appdb_maria.

7. Разверните веб-приложение на сервере HQ-SRV:

• используйте веб-сервер apache;

• в качестве системы управления базами данных используйте mariadb;

• файлы веб-приложения и дамп базы данных находятся в директории web-образа Additional.iso;

• выполните импорт схемы и данных из файла dump.sql в базу данных webdb;

• создайте пользователя web с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных;

• файлы index.php и директорию images скопируйте в каталог веб-сервера apache;

• в файле index.php укажите правильные учетные данные для подключения к БД;

• запустите веб-сервер и убедитесь в работоспособности приложения;

• основные параметры отметьте в отчете.

8. На маршрутизаторах сконфигурируйте статическую трансляцию портов:

• пробросьте порт 8080 в порт приложения testapp BR-SRV на маршрутизаторе BR-RTR для обеспечения работы приложения testapp извне;

• пробросьте порт 8080 в порт веб-приложения на HQ-SRV на маршрутизаторе HQ-RTR для обеспечения работы веб-приложения извне;

• пробросьте порт 2026 на маршрутизаторе HQ-RTR в порт 2026 сервера HQ-SRV для подключения к серверу по протоколу ssh из внешних сетей;

• пробросьте порт 2026 на маршрутизаторе BR-RTR в порт 2026 сервера BR-SRV для подключения к серверу по протоколу ssh из внешних сетей.

9. Настройте веб-сервер nginx как обратный прокси-сервер на ISP:

• при обращении по доменному имени web.au-team.irpo у клиента должно открываться веб-приложение на HQ-SRV;

• при обращении по доменному имени docker.au-team.irpo клиента должно открываться веб-приложение testapp.

10. На маршрутизаторе ISP настройте web-based аутентификацию:

• при обращении к сайту web.au-team.irpo клиенту должно быть предложено ввести аутентификационные данные:

◦ в качестве логина для аутентификации выберите WEB с паролем P@ssw0rd;

◦ выберите файл /etc/nginx/.htpasswd в качестве хранилища учетных записей;

◦ при успешной аутентификации клиент должен перейти на веб-сайт.

11. Удобным способом установите приложение Яндекс Браузер на HQ-CLI:

• установку браузера отметьте в отчете.

Выполнение задания:

Настройка контроллера домена Samba DC

Задание 1. Настройте контроллер домена Samba DC на сервере BR-SRV.

Подробное описание пункта задания

Настройте контроллер домена Samba DC на сервере BR-SRV:

• имя домена au-team.irpo.

Как делать?

Для Samba DC на базе Heimdal Kerberos необходимо установить пакет `task-samba-dc`:

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

Если настройка домена выполняется не сразу после установки ОС, перед установкой необходимо остановить конфликтующие службы `krb5kdc` и `slapd`, а также `bind`:

```
for service in smb nmb krb5kdc slapd bind; do \
systemctl disable $service; \
systemctl stop $service; \
done
```

Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удален):

```
rm -f /etc/samba/smb.conf
rm -rf /var/lib/samba
rm -rf /var/cache/samba
mkdir -p /var/lib/samba/sysvol
```

Для интерактивного развертывания запустите `samba-tool domain provision`, это запустит утилиту развертывания, которая будет задавать различные вопросы о требованиях к установке:

```
samba-tool domain provision
```

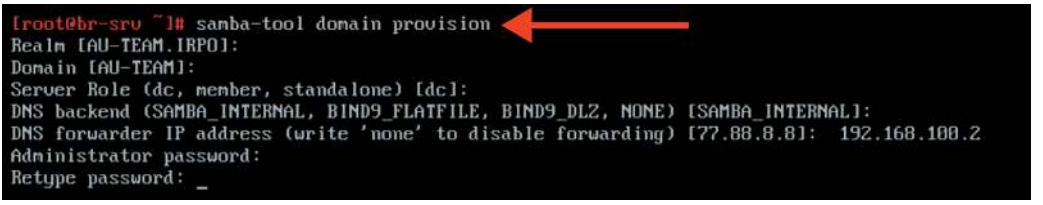
• у Samba свой собственный DNS-сервер. В DNS forwarder IP address нужно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена;

• при запросе ввода нажимайте Enter за исключением запроса пароля администратора («Administrator password:» и «Retype password:»);

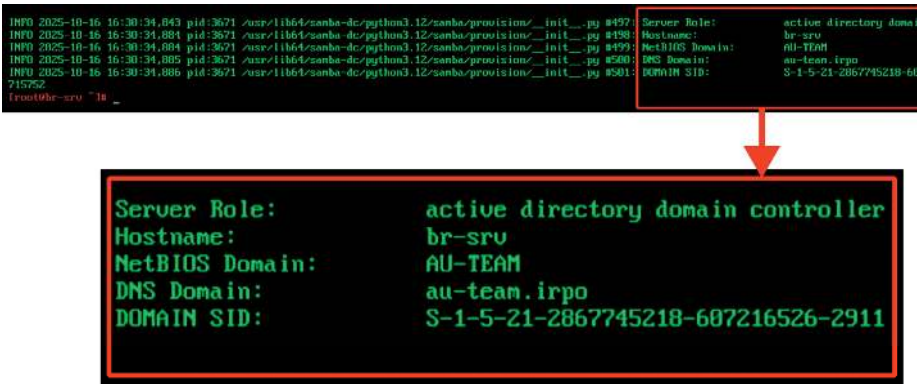
• пароль администратора должен быть не менее 7 символов и содержать символы как минимум трех групп из четырех возможных: латинских букв в верхнем и нижнем регистрах, чисел и других не буквенно-цифровых символов;

• пароль, не полностью соответствующий требованиям, является одной из причин завершения развертывания домена ошибкой;

• при правильной базовой настройке устройства все параметры подставятся автоматически.



Результат успешного интерактивного развертывания домена Samba DC:



После создания домена необходимо внести изменения в файл `/etc/krb5.conf`. В этом файле следует раскомментировать строку `default_realm` и содержимое разделов `realms` и `domain_realm`, указать название доме-

на (обратите внимание на регистр символов), в строке `dns_lookup_realm` должно быть установлено значение `false`. В момент создания домена Samba конфигурирует шаблон файла `krb5.conf` для домена в каталоге `/var/lib/samba/private/`. Можно просто заменить этим файлом файл, находящийся в каталоге `/etc/`:

```
cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

Включить и добавить в автозагрузку службу `samba`:

```
systemctl enable --now samba
```

Как проверить?

Просмотр общей информации о домене и предоставляемых службах:

```
[root@br-srv ~]# samba-tool domain info 127.0.0.1
Forest          : au-team.irpo
Domain          : au-team.irpo
Netbios domain  : AU-TEAM
DC name         : br-srv.au-team.irpo
DC netbios name : BR-SRV
Server site     : Default-First-Site-Name
Client site     : Default-First-Site-Name
[root@br-srv ~]# smbclient -L 127.0.0.1 -U administrator
Password for [AU-TEAM\administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        sysvol          Disk
        netlogon        Disk
        IPC$            IPC       IPC Service (Samba 4.21.7-alt4)
SMB1 disabled -- no workgroup available
[root@br-srv ~]#
```

Проверка Kerberos (имя домена должно быть в верхнем регистре) и просмотр полученного билета:

• убедиться в наличии `nameserver 127.0.0.1` в `/etc/resolv.conf` перед проверкой.

```
[root@br-srv ~]# cat /etc/net/ifaces/ens19/resolv.conf
nameserver 127.0.0.1
search au-team.irpo
[root@br-srv ~]# kinit Administrator@AU-TEAM.IRPO
Password for Administrator@AU-TEAM.IRPO:
Warning: Your password will expire in 41 days on Thu Nov 27 16:30:27 2025
[root@br-srv ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@AU-TEAM.IRPO

Valid starting     Expires            Service principal
10/16/25 16:34:46  10/17/25 02:34:46  krbtgt/AU-TEAM.IRPO@AU-TEAM.IRPO
        renew until 10/17/25 16:34:43
[root@br-srv ~]#
```

Проверка конфигурации DNS.
Утилита `host` находится в пакете `bind-utils`

```
[root@br-srv ~]# host au-team.irpo
au-team.irpo has address 192.168.0.2
[root@br-srv ~]# host -t SRV _kerberos._udp.au-team.irpo.
_kerberos._udp.au-team.irpo has SRV record 0 100 88 br-srv.au-team.irpo.
[root@br-srv ~]# host -t SRV _ldap._tcp.au-team.irpo.
_ldap._tcp.au-team.irpo has SRV record 0 100 389 br-srv.au-team.irpo.
[root@br-srv ~]# host br-srv.au-team.irpo.
br-srv.au-team.irpo has address 192.168.0.2
[root@br-srv ~]# _
```

Где выполнять?
На виртуальной машине: BR-SRV.
Дополнительно:
«Альт Домен» — служба каталогов (доменная служба), позволяющая централизованно управлять компьютерами и пользователями в корпоративной сети с операционными системами (ОС) на ядре Linux и Windows по единым правилам из единого центра. В системе реализовано хранение данных о пользователях, компьютерах (рабочих станциях) и других объектах корпоративной сети, а также управление профилями пользователей и компьютеров с помощью групповых политик в доменах MS Active Directory / Samba DC. Состав программного комплекса «Альт Домен»:
• контроллер(ы) домена (DC) на базе дистрибутива ОС «Альт Сервер»;
• модуль для ввода компьютера в домен;
• модуль удаленного управления базой данных конфигурации (ADMC) — графический инструмент для управления объектами домена и групповыми политиками;
• модуль редактирования настроек клиентской конфигурации (GPUI) — предназначен для изменения параметров групповых политик;
• шаблоны групповых политик;
• модуль применения конфигурации на целевой ОС Linux (gpupdate);
• аналитический инструмент, формирующий отчеты о применении групповых политик (GPResult);
• инструмент диагностики (ADT).
Краткая справка:
– «Альт Домен» (https://docs.altlinux.org/ru-RU/alt-server/11.1/html/alt-server/sambadc--chapter.html);
– «Альт Домен» 11.0 Руководство администратора (https://docs.altlinux.org/ru-RU/alt-domain/11.0/html/alt-domain/index.html).
Где изучается?
2 курс:
– Операционные системы и среды.

3 курс:
– Администрирование сетевых операционных систем;
– Программное обеспечение компьютерных сетей;
– Организация администрирования компьютерных систем и далее.

Задание 2. Настройте пользовательскую структуру домена Samba DC на сервере BR-SRV.

Подробное описание пункта задания

Настройте контроллер домена Samba DC на сервере BR-SRV:

• создайте 5 пользователей для офиса HQ: имена пользователей формата hquser№ (например: hquser1, hquser2 и т.д.);

• создайте группу hq, введите в группу созданных пользователей.

Как делать?

Для управления группами в «Альт Домен» можно использовать подкоманду `group` утилиты `samba-tool`:

• создать группу с именем `hq`:

```
samba-tool group add hq
```

Для управления пользователями в «Альт Домен» можно использовать подкоманду `user` утилиты `samba-tool`:

• создать пользователя `hquser1` с паролем `P@ssw0rd`:

```
samba-tool user add hquser1 P@ssw0rd
```

• установить срок действия для учетной записи пользователя в значение «`период действия неограничен`»:

```
samba-tool user setexpiry hquser1 --noexpiry
```

• добавить пользователя `hquser1` в группу `hq`:

```
samba-tool group addmembers «hq» hquser1
```

Для ускорения процесса создания пользователей и добавления их в соответствующую группу можно использовать цикл.

Как проверить?
Просмотр списка всех групп в рамках домена:

```
[root@br-srv ~]# samba-tool group list
RAS and IAS Servers
Read-only Domain Controllers
Administrators
Certificate Service DCOM Access
Performance Monitor Users
Denied RODC Password Replication Group
Cryptographic Operators
Account Operators
Domain Guests
Cert Publishers
Terminal Server License Servers
Domain Controllers
Group Policy Creator Owners
Server Operators
Pre-Windows 2000 Compatible Access
Domain Users
Allowed RODC Password Replication Group
Windows Authorization Access Group
Distributed COM Users
Incoming Forest Trust Builders
Print Operators
Schema Admins
Enterprise Admins
hq
Backup Operators
Domain Admins
Event Log Readers
Guests
Network Configuration Operators
Enterprise Read-only Domain Controllers
Remote Desktop Users
Domain Computers
Performance Log Users
IIS_IUSRS
Protected Users
DnsAdmins
DnsUpdateProxy
Users
Replicator
[root@br-srv ~]# _
```

Просмотр списка всех пользователей в рамках группы hq:

```
[root@br-srv ~]# samba-tool group listmembers hq
hquser1
hquser3
hquser5
hquser4
hquser2
[root@br-srv ~]# _
```

Где выполнять?

На виртуальной машине: BR-SRV.

Дополнительно:

Для управления пользователями и группами в «Альт Домен» можно использовать модуль удаленного управления базой данных конфигурации (ADMC). Компонент удаленного управления базой данных конфигурации (далее — ADMC) предназначен для управления:

• объектами в домене (пользователями, группами, компьютерами, подразделениями);

• групповыми политиками.

ADMC позволяет:

• создавать и администрировать учетные записи пользователей, компьютеров и групп;

• менять пароль пользователя;

• создавать организационные подразделения для структурирования и выстраивания иерархической системы распределения учетных записей в AD;

• просматривать и редактировать атрибуты объектов;

• создавать и просматривать объекты групповых политик;

• выполнять поиск объектов по разным критериям;

• сохранять поисковые запросы;

• переносить поисковые запросы между компьютерами (выполнять экспорт и импорт поисковых запросов).

Краткая справка:

– модуль удаленного управления базой данных конфигурации (ADMC) (https://docs.altlinux.org/ru-RU/alt-domain/11.0/html/alt-domain/admc.html);

– «Альт Домен» 11.0 Управление пользователями и группами (https://docs.altlinux.org/ru-RU/alt-domain/11.0/html/alt-domain/users-management.html).

Где изучается?

2 курс:

– Операционные системы и среды.

3 курс:

– Администрирование сетевых операционных систем;

– Программное обеспечение компьютерных сетей;

– Организация администрирования компьютерных систем и далее.

Задание 3. Введите в созданный домен машину HQ-CLI.

Подробное описание пункта задания

Настройте контроллер домена Samba DC на сервере BR-SRV:

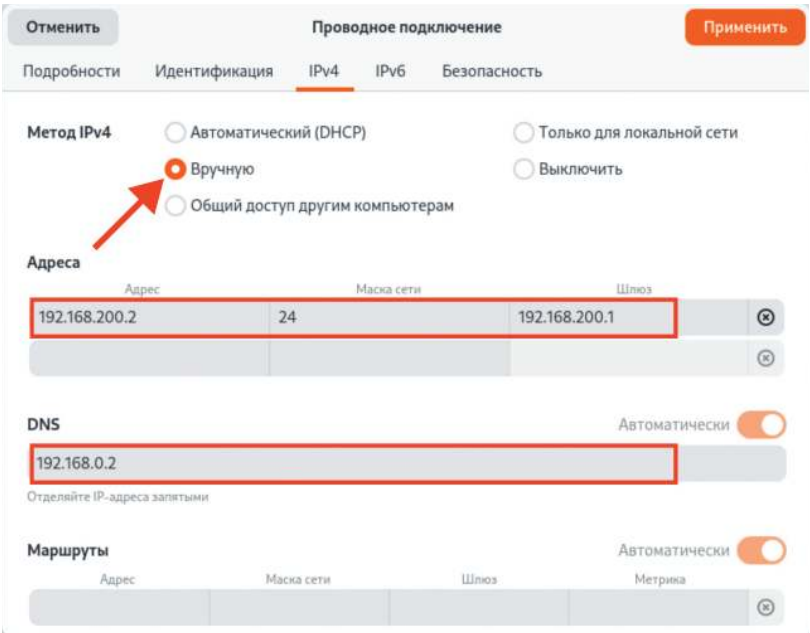
• введите в созданный домен машину HQ-CLI;

• убедитесь, что пользователи группы hq имеют право аутентифицироваться на HQ-CLI;

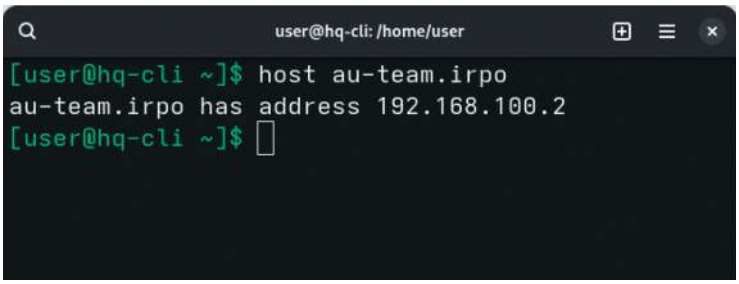
• пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы права не имеют.

Как делать?

На клиенте необходимо установить статические параметры для сетевого интерфейса, также важно в качестве адреса DNS-сервера указать IP-адрес виртуальной машины BR-SRV (контроллера домена):



Также необходимо проверить, что имя домена корректно преобразуется в IP-адрес:

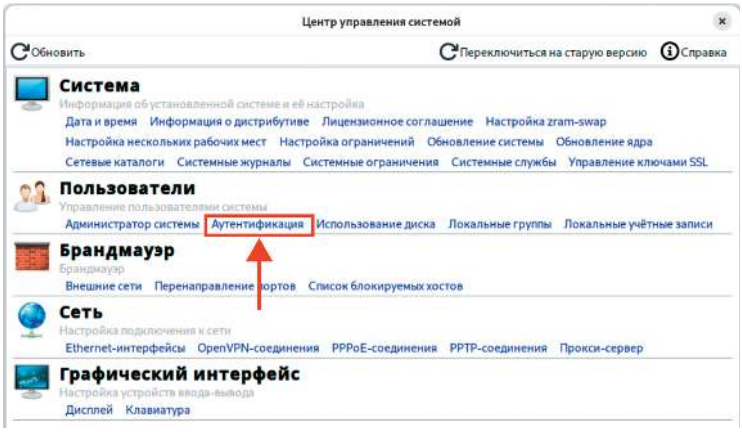


Подключение к домену с использованием SSSD:

• необходимо установить пакет `task-auth-ad-sssd`:

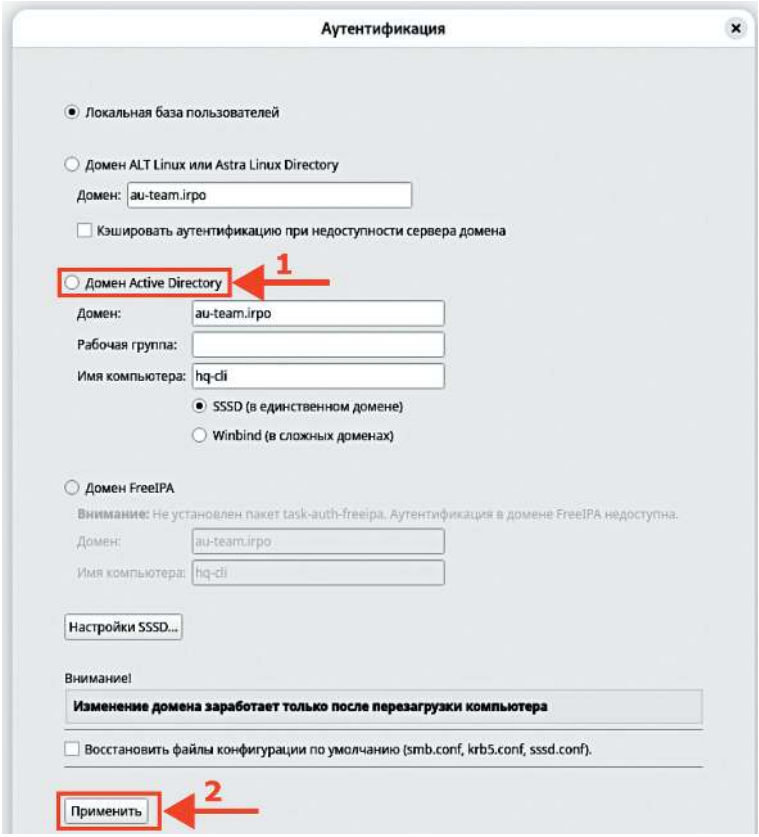
```
apt-get update && apt-get install -y task-auth-ad-sssd
```

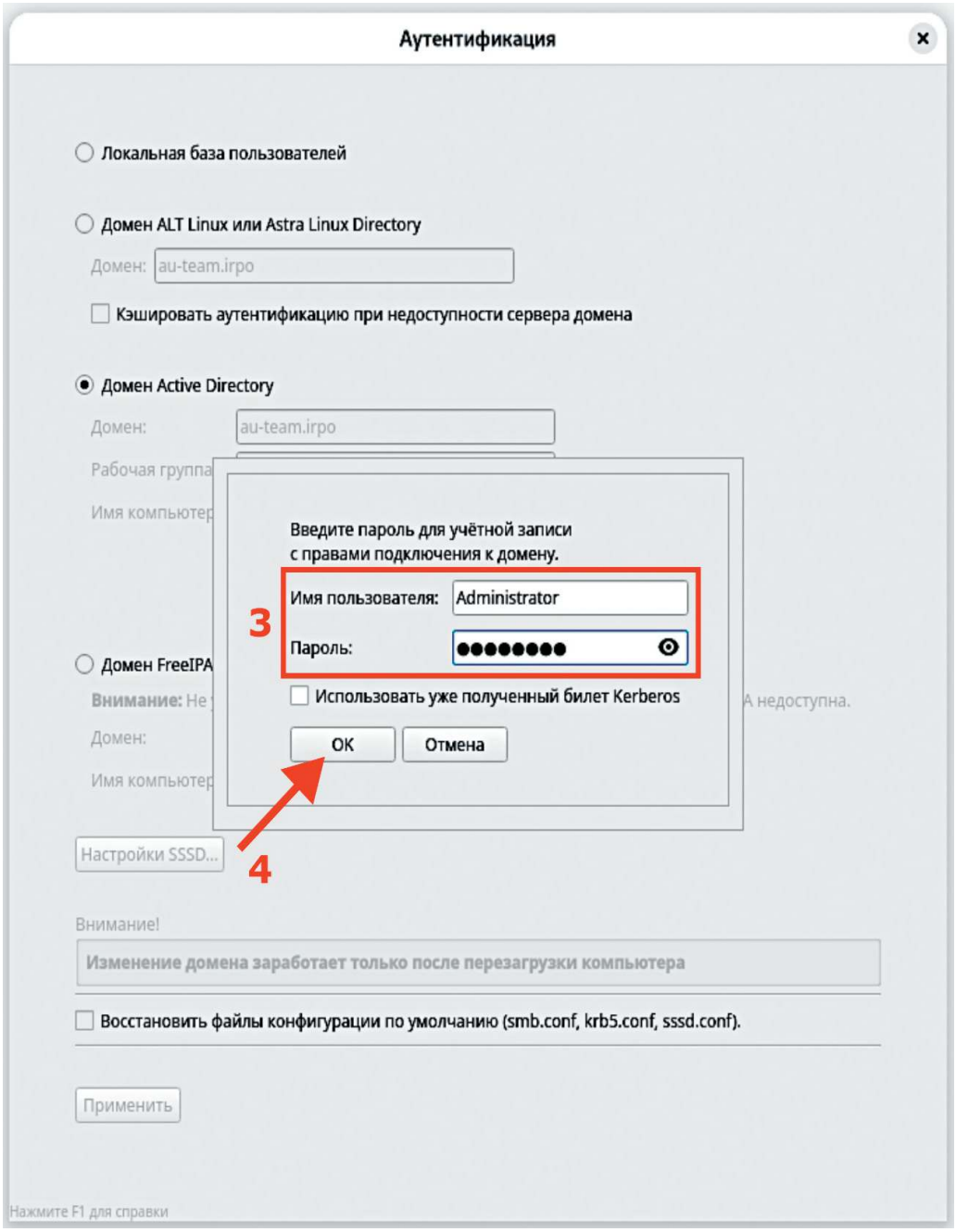
• для ввода компьютера в домен в ЦУС необходимо выбрать пункт Пользователи → Аутентификация:



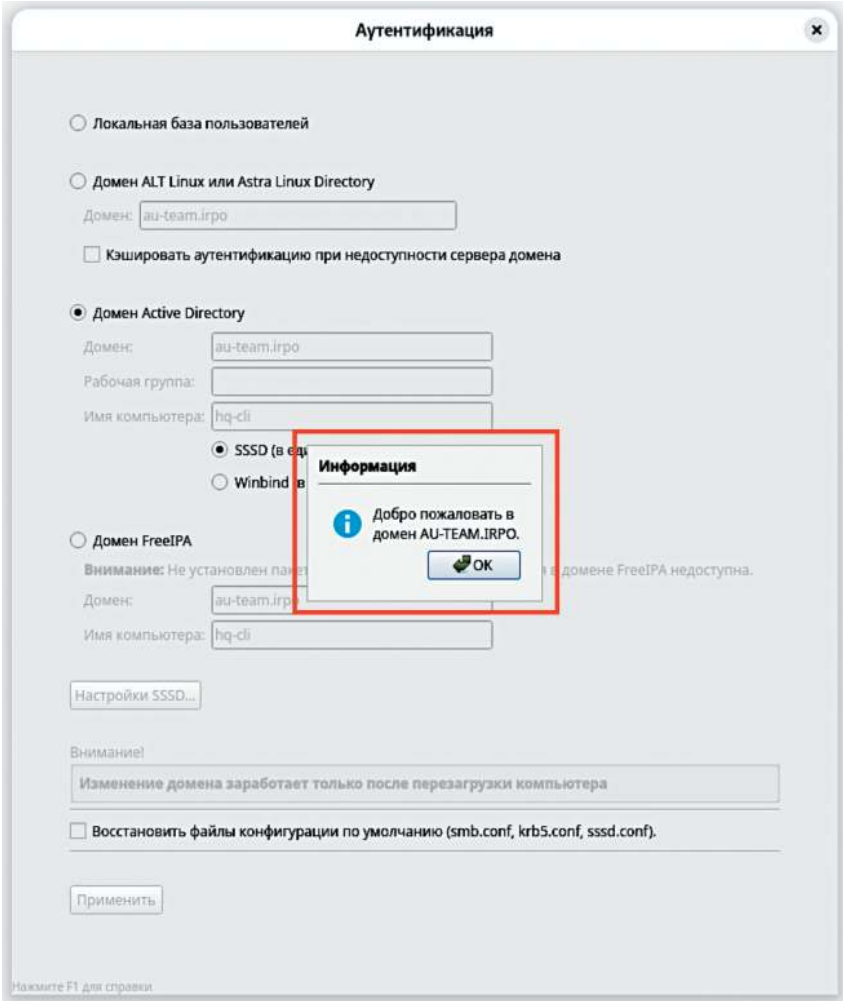
• в окне модуля Аутентификация следует выбрать пункт Домен Active Directory, заполнить поля (Домен, Рабочая группа, Имя компьютера), выбрать пункт SSSD (в единственном домене) и нажать кнопку Применить;

• в открывшемся окне необходимо ввести имя пользователя, имеющего право вводить машины в домен, его пароль и нажать кнопку OK.





При успешном подключении к домену отобразится соответствующая информация:



Перезагрузить рабочую станцию для применения всех настроек.

На HQ-CLI установить библиотеку `libnss-role` для NSS и набор инструментов для администрирования ролей и привилегий:

```
apt-get install -y libnss-role
```

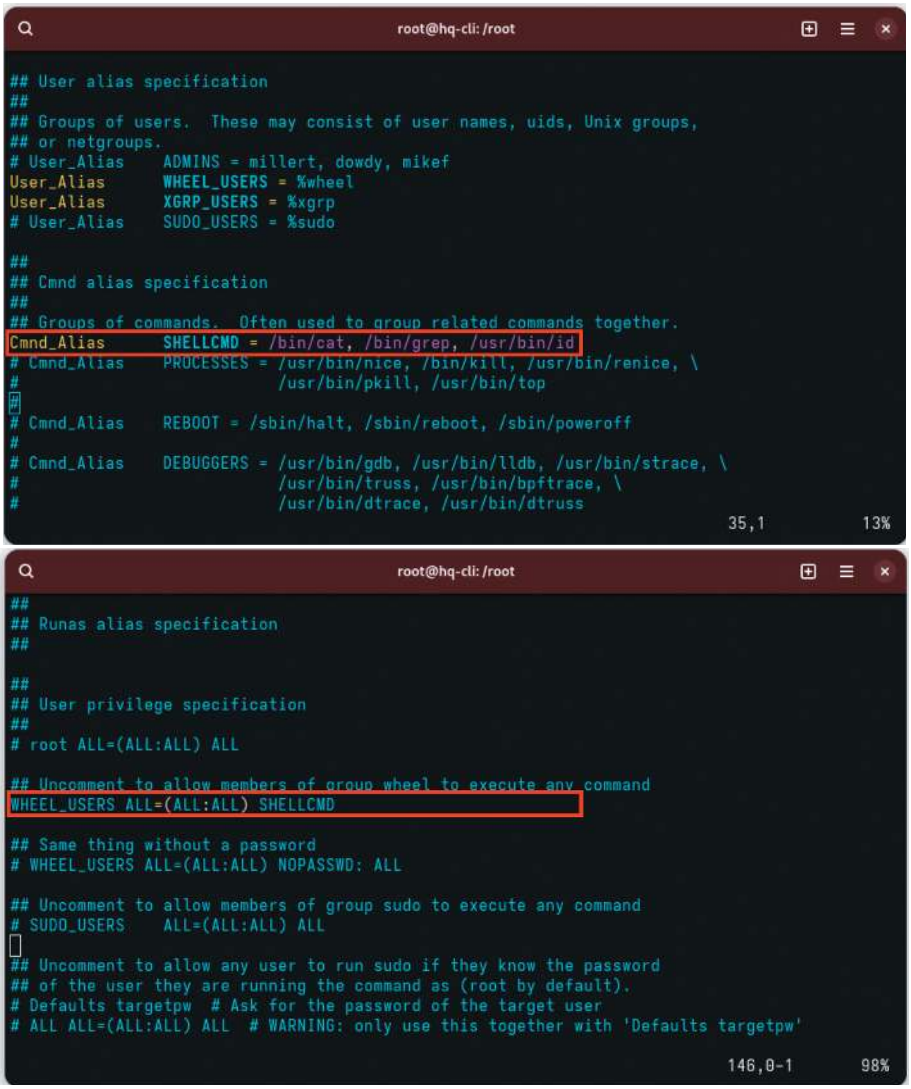
Данный модуль должен быть включен:

```
control libnss-role
```

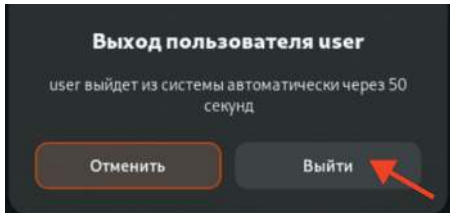
Связать доменную группу `hq` с локальной группой `wheel`:

```
roleadd hq wheel
```

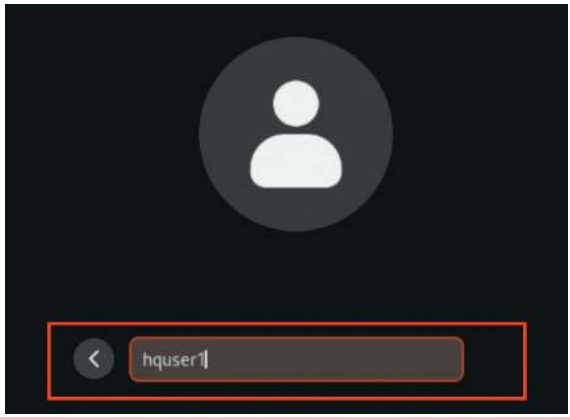
Отредактировать конфигурационный файл /etc/sudoers:



Как проверить?
Выйти из учетной записи локального пользователя:



Выполнить вход из-под учетной записи доменного пользователя из группы hq, проверить возможность запуска утилиты sudo для необходимых утилит:




```
hquser1@hq-cli: /home/AU-TEAM.IRPO/hquser1
[hquser1@hq-cli ~]$ sudo id
uid=0(root) gid=0(root) группы=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel
),19(proc)
[hquser1@hq-cli ~]$ sudo cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain localhost6
[hquser1@hq-cli ~]$ sudo grep '127.0.0.1' /etc/hosts
127.0.0.1       localhost.localdomain localhost
[hquser1@hq-cli ~]$
```

Проверить возможность запуска утилиты sudo для других команд:

```
hquser1@hq-cli: /home/AU-TEAM.IRPO/hquser1
[hquser1@hq-cli ~]$ sudo su -
Извините, пользователю hquser1 не разрешено выполнять «/bin/su -» как root на hq-cli.a
u-team.irpo.
[hquser1@hq-cli ~]$
```

Где выполнять?

На виртуальной машине: HQ-CLI.

Дополнительно:

SSSD используется для доступа к пользовательскому каталогу для аутентификации и авторизации через общую структуру с кешированием пользователей, чтобы разрешить автономный вход в систему.

SSSD легко настраивается; он обеспечивает интеграцию подключаемых модулей аутентификации (PAM) и службы переключения имен (NSS), базу данных для хранения локальных пользователей, а также расширенных пользовательских данных, полученных с центрального сервера.

Краткая справка:

– подключение к домену с использованием SSSD (https://docs.altlinux.org/ru-RU/alt-domain/11.0/html/alt-domain/client-sssd.html).

Где изучается?

2 курс:

– Операционные системы и среды.

3 курс:

– Администрирование сетевых операционных систем;

– Программное обеспечение компьютерных сетей;

– Организация администрирования компьютерных систем и далее.

Настройка файлового хранилища

Подробное описание пункта задания

Сконфигурируйте файловое хранилище на сервере HQ-SRV:

• при помощи двух подключенных к серверу дополнительных дисков размером 1 ГБ сконфигурируйте дисковый массив уровня 0;

• имя устройства — md0, при необходимости конфигурация массива размещается в файле /etc/mdadm.conf;

• создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4;

• обеспечьте автоматическое монтирование в папку /raid.

Как делать?

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

```
[root@hq-srv ~]# lsblk
NAME
    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda   8:0    0   10G  0 disk /
sdb   8:16   0    1G  0 disk
sdc   8:32   0    1G  0 disk
sr0  11:0    1 1024M  0 rom
[root@hq-srv ~]# _
```

Неразмеченные диски должны быть одного размера — 1 ГБ, 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 --verbose /dev/md0 –l 0 –n 2 /dev/sdb /dev/sdc
```

Описание применяемых команд:

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

`-l 0` — уровень RAID;

`-n 2` — количество дисков, из которых собирается массив;

`/dev/sdb /dev/sdc` — сборка выполняется из дисков sdb и sdc.

При необходимости конфигурация массива размещается в файле `/etc/mdadm.conf`:

```
mdadm --detail --scan --verbose | tee –a /etc/mdadm.conf
```

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

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

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

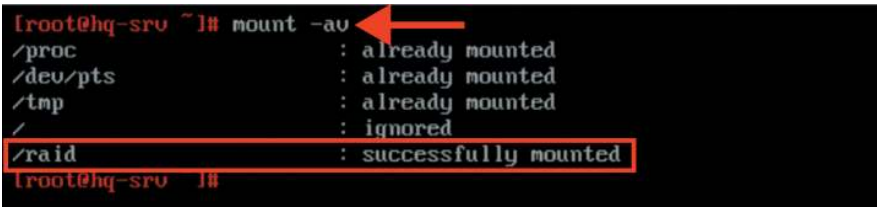
```
mkdir /raid
```

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

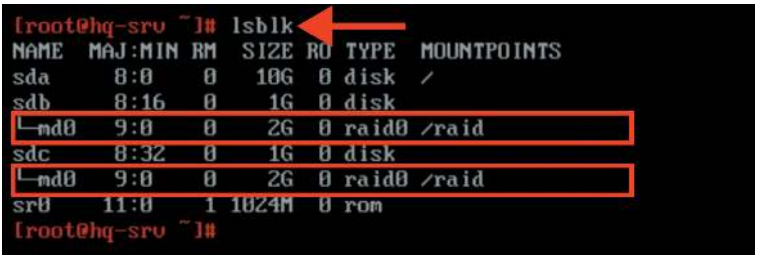
```
proc            /proc                   proc    nosuid,noexec,gid=proc                          0 0
devpts          /dev/pts                devpts  nosuid,noexec,gid=tty,mode=620,ptmxmode=0666    0 0
tmpfs           /tmp                    tmpfs   nosuid                                          0 0
UUID=024571e2-3eb5-4f4a-b353-bc910bef52cd       /       ext4    relatime        1       1
/dev/md0        /raid   ext4    defaults        0       0
```

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

```
mount -av
```

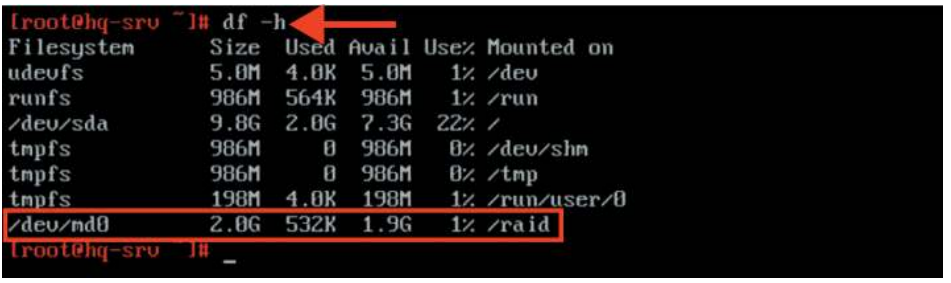


Как проверить?
Средствами утилиты `lsblk`:



Средствами утилиты `blkid`:

Средствами утилиты `df`:



Описание применяемых команд:
`-h` — «человекочитаемый формат» (human readable).
Где выполнять?
На виртуальной машине: HQ-SRV.

Дополнительно:

RAID — технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности. Типы RAID:

• RAID0 — технология, когда диски объединяются в один большой диск;

• RAID1 — технология, когда диски зеркалируются, дублируют друг друга;

• RAID4 — технология, когда данные разбиваются на блоки и распределяются по n−1 дискам;

• RAID5 — технология, когда создается массив дисков с поблочным чередованием с одной контрольной суммой;

• RAID6 — технология, когда создается массив дисков с поблочным чередованием с двумя контрольными суммами;

• RAID10 — зеркалированный массив, данные в котором записываются последовательно на несколько дисков, как в RAID0. Эта архитектура представляет собой массив типа RAID0, сегментами которого вместо отдельных дисков являются массивы RAID1.

Краткая справка:

– 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 и далее.

Настройка сервера сетевой файловой системы

Подробное описание пункта задания

Настройте сервер сетевой файловой системы (nfs) на HQ-SRV:

• в качестве папки общего доступа выберите /raid/nfs, доступ для чтения и записи исключительно для сети в сторону HQ-CLI;

• на HQ-CLI настройте автомонтирование в папку /mnt/nfs;

• основные параметры сервера отметьте в отчете.

Как делать?

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 /raid/nfs, данную директорию необходимо создать командой:

```
mkdir /raid/nfs
```

Также стоит выдать права для созданной директории:

```
chmod 777 /raid/nfs
```

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

```
/srv/public -ro,insecure,no_subtree_check,fsid=1 *
#/srv/share -rw,insecure,fsid=0,sec=krb5 *
/raid/nfs       192.168.200.0/24(rw,no_root_squash)
~
```

где: /raid/nfs — общий ресурс; 192.168.200.0/24 — клиентская сеть, которой разрешено монтирование общего ресурса;

rw — разрешение на чтение и запись;

no_root_squash — отключение ограничения прав root.

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 пакеты nfs-utils и nfs-clients. Сделать это можно, воспользовавшись командой:

```
apt-get install –y nfs-utils nfs-clients
```

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

```
mkdir /mnt/nfs
```

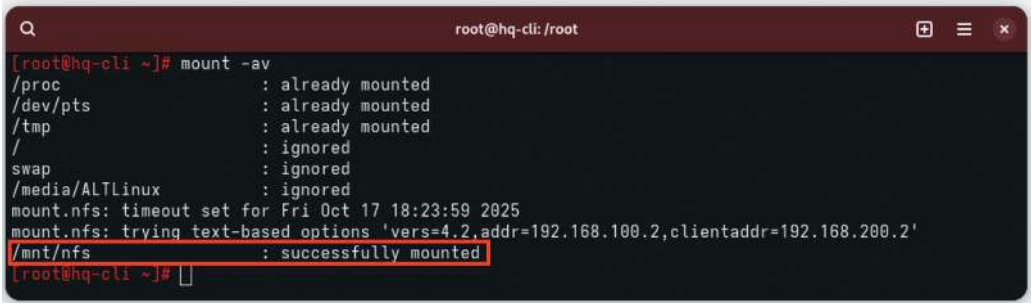
Выдать соответствующие права на созданную директорию:

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

В конец конфигурационного файла /etc/fstab удобным текстовым редактором vim дописываем следующую строку:

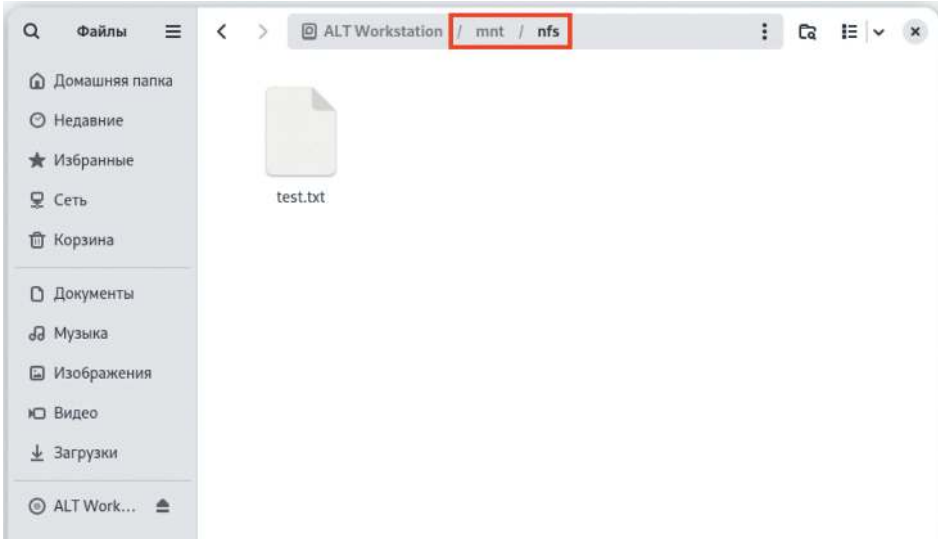
Для применения монтирования можно воспользоваться утилитой `mount`, выполнив команду:

```
mount -av
```



Как проверить?

Проверить возможность создания файлов на общем ресурсе:



Проверить наличие созданного файла на сервере:

Где выполнять?

На виртуальных машинах: HQ-SRV, 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 удаленными 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 удаленные 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).

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.

Настройка служб сетевого времени

Подробное описание пункта задания

Настройте службу сетевого времени на базе сервиса chrony на маршрутизаторе ISP:

• вышестоящий сервер ntp на маршрутизаторе ISP — на выбор участника;

• стратум сервера — 5;

• в качестве клиентов ntp настройте: HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.

Как делать?

На виртуальной машине ISP, которая будет выступать в роли сервера времени, необходимо привести конфигурационный файл /etc/chrony.conf в текстовом редакторе vim к следующему виду:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
#pool pool.ntp.org iburst
server ntp5.ntp-servers.net iburst prefer minstratum 4
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:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
#pool pool.ntp.org iburst
server 172.16.1.1 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:

```
(config)# ntp server <IP_АДРЕС_ШЛЮЗА>
(config)# write memory
```

Как проверить?

Источник синхронизации времени при помощи утилиты chronyc на ОС «Альт»:

```
[root@ISP ~]# chronyc sources
MS Name/IP address         Stratum Poll Reach LastRx Last sample
===============================================================================
^* sv1.ggsrv.de                  4   6   177    46   +136us[ +918us] +/-   29ms
[root@ISP ~]#
```

Источник синхронизации времени при помощи команды `show ntp status` на ОС «EcoRouterOS»:

```
br-rtr#show ntp status
Status  Description
*       best
+       sync
-       failed
?       unknown

-------------------------------------------------------------------------------------------------------
Status |     VR name     |     Server      | Stratum |   Delay   | Version |   Offset   | Last |  Source IP
-------------------------------------------------------------------------------------------------------
     *|         default |      172.16.2.1 |       5 |    0.0516 |       4 |     0.6810 |   21 |
br-rtr#
```

Где выполнять?

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

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 удаленными 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 и далее.

Настройка ansible

Подробное описание пункта задания

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;

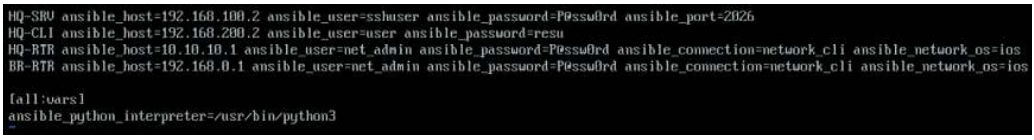
• все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV.

Как делать?

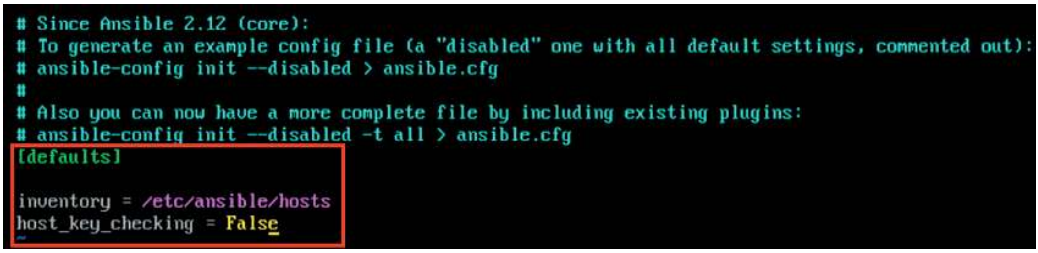
Необходимо установить пакеты `ansible` и `sshpass`. Выполнить установку можно следующей командой:

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

Привести файл инвентаря Ansible к виду, приведенному на скриншоте ниже, отредактировав конфигурационный файл по пути `/etc/ansible/hosts` любым удобным текстовым редактором, например `vim`:



Отредактировать файл `/etc/ansible/ansible.cfg`, приводя его к следующему виду:



Установить необходимые коллекции для подключения к ОС «EcoRouterOS»:

```
ansible-galaxy collection install ansible.netcommon
```

```
ansible-galaxy collection install cisco.ios
```

Установить пакет `python3-module-pip`, далее поставить библиотеку `ansible-pylibssh`:

```
apt-get install –y python3-module-pip
```

```
pip3 install ansible-pylibssh
```

На виртуальных машинах с ОС «EcoRouterOS» из режима администрирования (`conf t`) разрешить подключения к устройству по `ssh`:

```
(config)# security none
(config)# write memory
```

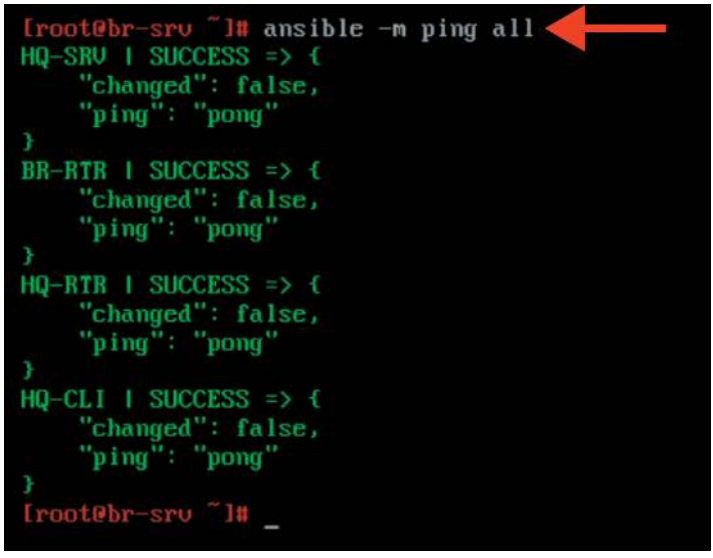
Важное замечание: данный способ не рекомендуется использовать в производственных средах, применимо исключительно только для экономии времени при выполнении задания Демонстрационного экзамена (ДЭ).

За рамками выполнения задания Демонстрационного экзамена (ДЭ) лучше сделать отдельный `security profille` для интерфейса управления типа In-Band Management с соответствующими правилами безопасности, а также добавить созданный профиль безопасности в отдельный VRF.

Как проверить?

Ответы от машин должны быть зеленого цвета и содержать поле pong:

```
ansible all -m ping
```



Где выполнять?

На виртуальных машинах: BR-SRV, HQ-RTR, BR-RTR.

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 и далее.

Настройка веб-приложения с использованием средств контейнеризации

Подробное описание пункта задания

Разверните веб-приложение в docker на сервере BR-SRV:

• средствами docker должен создаваться стек контейнеров с веб-приложением и базой данных;

• используйте образы site_latest и mariadb_latest, располагающиеся в директории docker в образе Additional.iso;

• основной контейнер testapp должен называться tespapp;

• контейнер с базой данных должен называться db. Импортируйте образы в docker, укажите в yaml-файле параметры подключения к СУБД, имя БД — mariadb, пользователь — maria, пароль — Passw0rd, порт приложения — 8080, при необходимости другие параметры;

• приложение должно быть доступно для внешних подключений через порт 8080.

Как делать?

Установить необходимые пакеты для работы с Docker и Docker Compose с помощью следующей команды:

```
apt-get install –y docker-engine docker-compose-v2
```

После установки необходимых пакетов стоит запустить службу `docker`:

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

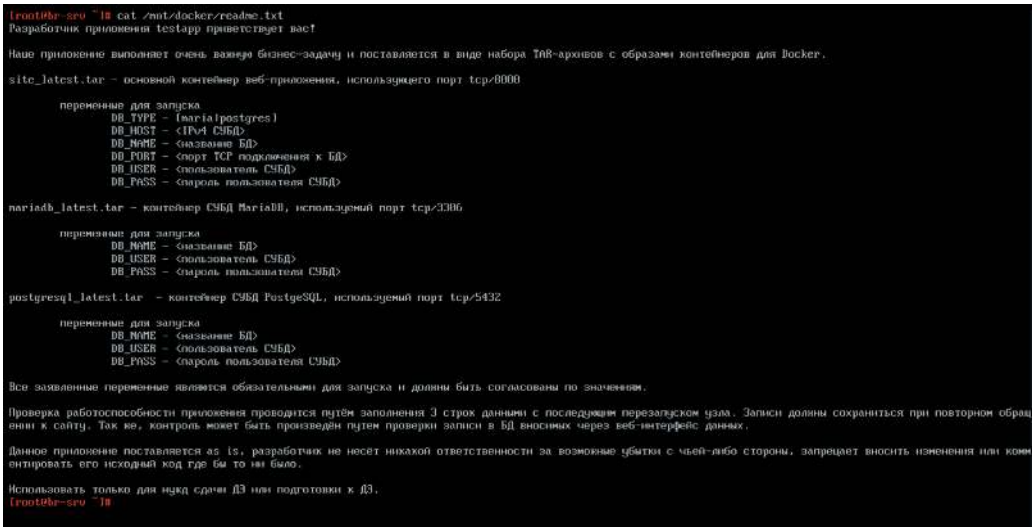
Выполнить монтирование `Additional.iso` в директорию `/mnt`:

```
mount /dev/sr0 /mnt/
```

Выполнить импорт образа `mariadb_latest` и `site_latest`:

```
docker load < /mnt/docker/site_latest.tar
docker load < /mnt/docker/mariadb_latest.tar
```

Также у данного веб-приложения есть инструкция в виде файла `readme.txt`:



Создать любым удобным текстовым редактором, например `vim`, файл `compose.yaml` и поместить в него следующее содержимое:

```yaml
services:
  database:
    container_name: db
    image: mariadb:latest
    restart: always
    ports:
      - "3306:3306"
    environment:
      DB_USER: maria
      DB_PASS: Passw0rd
      DB_NAME: mariadb
      MARIADB_ROOT_PASSWORD: P@ssw0rd

  app:
    container_name: testapp
    image: site:latest
    restart: always
    ports:
      - "8080:8000"
    environment:
      DB_HOST: "192.168.0.2"
      DB_PORT: "3306"
      DB_NAME: mariadb
      DB_USER: maria
      DB_PASS: Passw0rd
      DB_TYPE: maria
    depends_on:
      - database
```

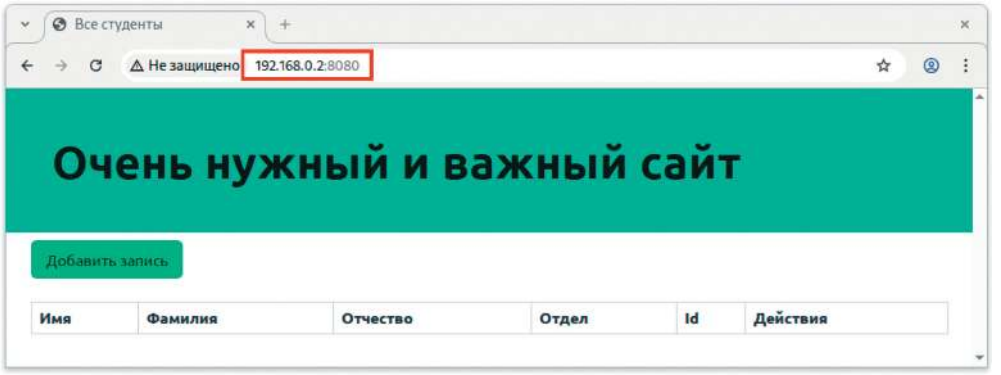
Запустить стек контейнеров с веб-приложением и базой данных:

```
docker compose up -d
```

Как проверить?
Проверяем стек контейнеров с веб-приложением и базой данных:

```
docker compose ps
```

Проверяем доступ до веб-приложения из браузера:



Где выполнять?
На виртуальных машинах: BR-SRV, HQ-CLI.
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 хосте;

• 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:

– начало работы с Docker (https://docs.docker.com/get-started/);

– установка Docker в ОС «Альт» (https://www.altlinux.org/Docker).

Где изучается?

3, 4 курс:

– Организация администрирования компьютерных систем и далее.

Настройка веб-приложения на сервере

Подробное описание пункта задания

Разверните веб-приложение на сервере HQ-SRV:

• используйте веб-сервер apache;

• в качестве системы управления базами данных используйте mariadb;

• файлы веб-приложения и дамп базы данных находятся в директории web-образа Additional.iso;

• выполните импорт схемы и данных из файла dump.sql в базу данных webdb;

• создайте пользователя web с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных;

• файлы index.php и директорию images скопируйте в каталог веб-сервера apache;

• в файле index.php укажите правильные учетные данные для подключения к БД;

• запустите веб-сервер и убедитесь в работоспособности приложения;
• основные параметры отметьте в отчете.

Как делать?

Установить пакет `lamp-server` для работы веб-сервера Apache с базой данных MariaDB и PHP:

```
apt-get install –y lamp-server
```

Выполнить монтирование `Additional.iso` в директорию `/mnt`:

```
mount /dev/sr0 /mnt/
```

Произвести копирование файлов веб-приложения в директорию `/var/www/html`:

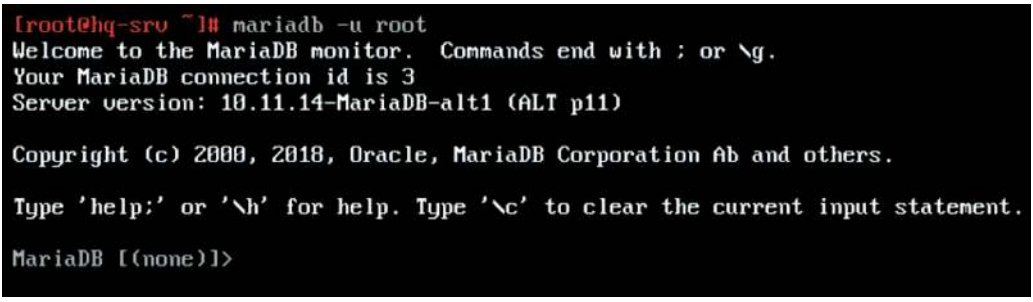
```
cp /mnt/web/index.php /var/www/html
cp /mnt/web/logo.png /var/www/html
```

Включить и добавить в автозагрузку службу `mariadb`:

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

Перейти в интерфейс управления MariaDB:

```
mariadb –u root
```



Создать базу данных с именем `webdb`:

```
CREATE DATABASE webdb;
```

Создать пользователя `webc` с паролем `P@ssw0rd`:

```
CREATE USER ‘webc’@’localhost’ IDENTIFIED BY ‘P@ssw0rd’;
```

Назначить пользователю `webc` полные права на базу данных `webdb`, после чего выйти из интерфейса управления MariaDB:

```
GRANT ALL PRIVILEGES ON webdb.* TO ‘webc’@’localhost’ WITH GRANT OPTION;
EXIT;
```

Из директории `/mnt/web/` скопировать файл `dump.sql` и выполнить импорт схемы и данных из файла `dump.sql` в базу данных `webdb`:

```
cp /mnt/web/dump.sql ./
mariadb –u webc –p –D webdb < dump.sql
```

Если `dump.sql` имеет кодировку UTF-16, то перед этим сделать:

```
Iconv -f UTF-16LE -t UTF-8 dump.sql -o dump_new.sql
```

И тогда в итоге для импорта схемы и данных необходимо будет использовать команду:

```
mariadb –u webc –p –D webdb < dump_new.sql
```

```
[root@hq-srv ~]# mariadb
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 5
Server version: 10.11.14-MariaDB-alt1 (ALT p11)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE webdb;
Database changed
MariaDB [webdb]> SHOW TABLES;
+-----------------+
| Tables_in_webdb |
+-----------------+
| employees       |
+-----------------+
1 row in set (0.002 sec)

MariaDB [webdb]> _
```

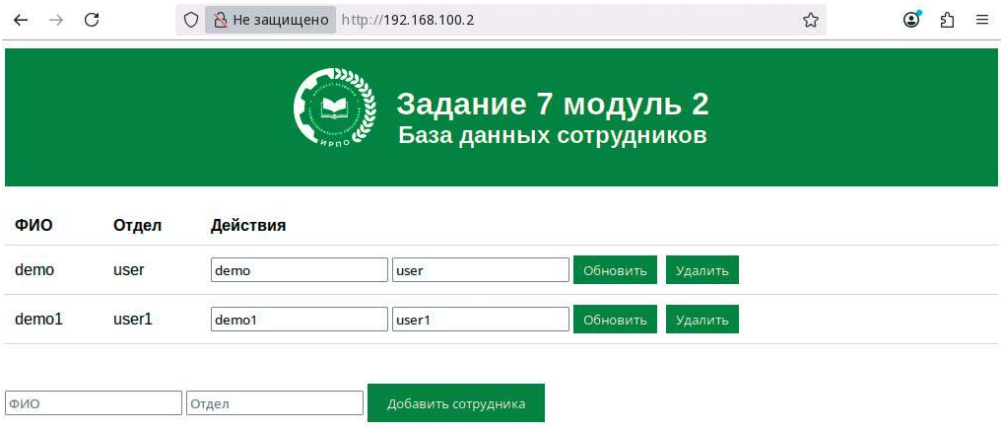
В файле `/var/www/html/index.php` указать правильные учетные данные для подключения к БД любым удобным текстовым редактором, например `vim`:

```
<?php
$servername = "localhost";
$username = "webc";
$password = "P@ssw0rd";
$dbname = "webdb";

$conn = new mysqli($servername, $username, $password, $dbname);
```

Включить и добавить в автозагрузку службу `httpd2`:

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

Как проверить?
Проверить доступ до веб-приложения из браузера:



Где выполнять?
На виртуальных машинах: HQ-SRV, HQ-CLI.
Дополнительно:
Apache2 *(Apache HTTP Server)* — веб-сервер, который представляет собой программное обеспечение с открытым исходным кодом. Он используется для размещения веб-сайтов и доступа к ним. Благодаря модульной структуре Apache обладает гибкостью и расширяемостью, а также надежностью и стабильностью работы. Apache поддерживается многими операционными системами, в том числе ОС «Альт».

MariaDB — ответвление от системы управления базами данных MySQL, разрабатываемое сообществом под лицензией GNU GPL. Разработку и под-

держку MariaDB осуществляет компания MariaDB Corporation Ab и фонд MariaDB Foundation. Толчком к созданию стала необходимость обеспечения свободного статуса СУБД, в противовес политике лицензирования MySQL компанией Oracle.

Краткая справка:

– apache2 (Apache HTTP Server) (https://www.altlinux.org/Apache2);

– MariaDB (https://www.altlinux.org/EnterpriseApps/MariaDB).

Где изучается?

2 курс:

– Операционные системы и среды;

– Компьютерные сети.

3,4 курс:

– Организация, принципы построения и функционирования компьютерных систем;

– Организация администрирования компьютерных систем и далее.

Настройка трансляции портов

Подробное описание пункта задания

На маршрутизаторах сконфигурируйте статическую трансляцию портов:

• пробросьте порт 8080 в порт приложения testapp BR-SRV на маршрутизаторе BR-RTR для обеспечения работы приложения testapp извне;

• пробросьте порт 8080 в порт веб-приложения на HQ-SRV на маршрутизаторе HQ-RTR для обеспечения работы веб приложения извне;

• пробросьте порт 2026 на маршрутизаторе HQ-RTR в порт 2026 сервера HQ-SRV, для подключения к серверу по протоколу ssh из внешних сетей;

• пробросьте порт 2026 на маршрутизаторе BR-RTR в порт 2026 сервера BR-SRV для подключения к серверу по протоколу ssh из внешних сетей.

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>
```

Пример описания настроек на виртуальных машинах экзаменационного стенда

```
hq-rtr(config)#ip nat source static tcp 192.168.100.2 80 172.16.1.2
8080
hq-rtr(config)#ip nat source static tcp 192.168.100.2 2026 172.16.1.2
2026
```

```
hq-rtr(config)#write memory
```

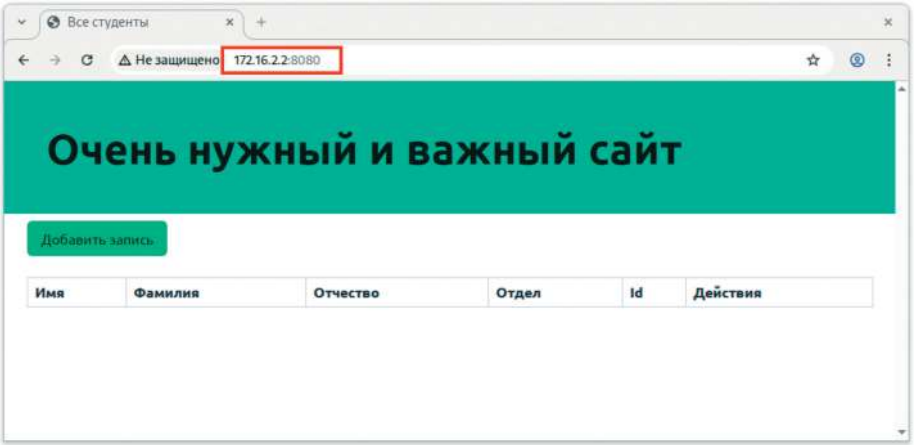
```
br-rtr(config)#ip nat source static tcp 192.168.0.2 8080 172.16.2.2 8080
br-rtr(config)#ip nat source static tcp 192.168.0.2 2026 172.16.2.2 2026
br-rtr(config)#write memory
```

Как проверить?

Проверить статическую трансляцию портов:

```
hq-rtr#show ip nat translations
 Static translations:

 Source                          Translated                      VRF
 TCP: 192.168.100.2 80           172.16.1.2 8080                 default
 TCP: 192.168.100.2 2026         172.16.1.22 2026                default
```

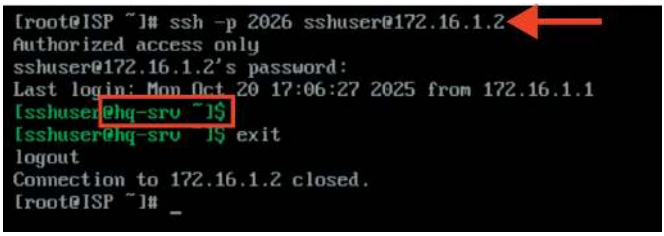
Проверить возможность доступа извне до веб-приложения, развернутого на базе стека контейнеров из браузера на клиенте:

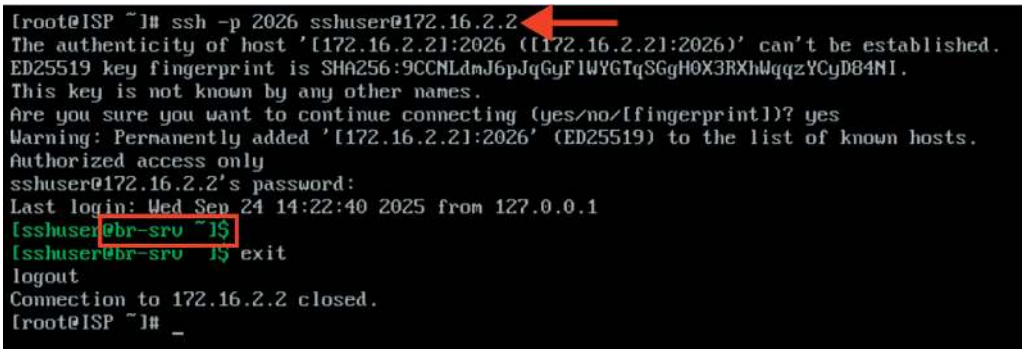


Проверяем возможность доступа извне до веб-приложения, развернутого на базе веб-сервера Apache с виртуальной машины ISP:

```
[root@ISP ~]# curl http://172.16.1.2:8080 | head
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  2694  100  2694    0     0  44218      0 --:--:-- --:--:-- --:--:-- 45661
<!DOCTYPE html>
<html>
<head>
    <title>■■■■■■■ 7 ■■■■■■ 2</title>
    <style>
        body { font-family: Arial, sans-serif; }
        .header {
            background-color: #017d0c;
            color: white;
            text-align: center;
[root@ISP ~]#
```

Проверяем возможность доступа извне по SSH с виртуальной машины ISP:





Где выполнять?

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

Дополнительно:

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

Краткая справка:

– документация по EcoRouterOS (Wiki) (https://docs.ecorouter.ru/).

Где изучается?

2 курс:

– Операционные системы и среды;

– Компьютерные сети.

3, 4 курс:

– Организация, принципы построения и функционирования компьютерных систем;

– Организация администрирования компьютерных систем и далее.

Настройка обратного прокси-сервера

Подробное описание пункта задания

Настройте веб-сервер nginx как обратный прокси-сервер на ISP:

• при обращении по доменному имени web.au-team.irpo у клиента должно открываться веб-приложение на HQ-SRV;

• при обращении по доменному имени docker.au-team.irpo клиента должно открываться веб-приложение testapp.

Как делать?

Установите пакет `nginx`:

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

Настроить nginx как реверсивный прокси-сервер, приведя файл `/etc/nginx/sites-available.d/default.conf` к следующему виду любым удобным текстовым редактором, например `vim`:

```
server {
        listen 80;
        server_name web.au-team.irpo;

        location / {
                proxy_pass http://172.16.1.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
        }
}

server {
        listen 80;
        server_name docker.au-team.irpo;

        location / {
                proxy_pass http://172.16.2.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded_For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded_Proto $scheme;
        }
}
~
```

Добавить символическую ссылку на данный файл:

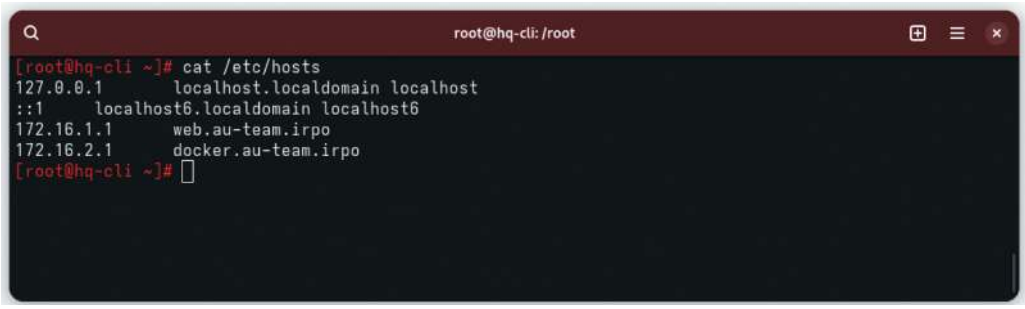
```
ln -s /etc/nginx/sites-available.d/default.conf /etc/nginx/sites-
enabled.d/
```

Запустить и активировать службу `nginx`:

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

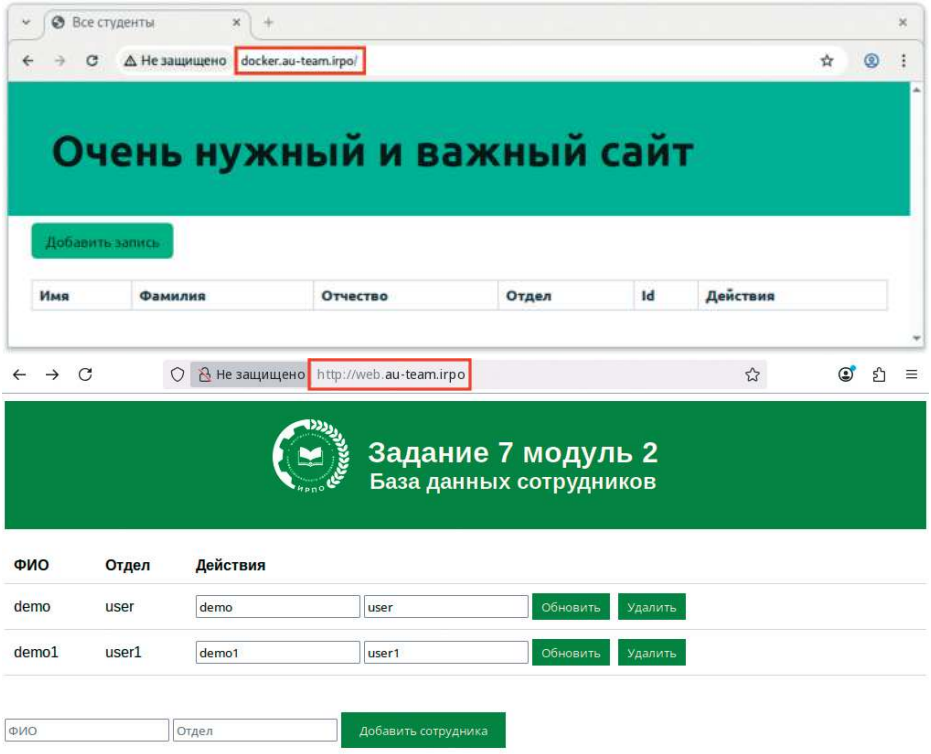
Поскольку в домене SambaDC нет DNS записей, ссылающихся на необходимые имена, а на HQ-CLI в качестве DNS-сервера задан адрес именно контролле-

ра домена, то необходимо добавить записи в файл `/etc/hosts` на виртуальной машине HQ-CLI:



Как проверить?

Проверить возможность доступа до веб-ресурсов из браузера на клиенте:



Где выполнять?

На виртуальной машине: ISP, HQ-CLI.

Дополнительно:

Реверсивный прокси Nginx обладает рядом замечательных характеристик и преимуществ, которые делают его популярным выбором для веб-раз-

работчиков 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);

– Nginx (https://www.altlinux.org/EnterpriseApps/Nginx).

Где изучается?

2 курс:

– Операционные системы и среды.

3 курс:

– Организация администрирования компьютерных систем и далее.

Настройка web-based аутентификации

Подробное описание пункта задания

На маршрутизаторе ISP настройте web-based аутентификацию:

• при обращении к сайту web.au-team.irpo клиенту должно быть предложено ввести аутентификационные данные:

◦ в качестве логина для аутентификации выберите WEB с паролем P@ssw0rd;

◦ выберите файл /etc/nginx/.htpasswd в качестве хранилища учетных записей;

◦ при успешной аутентификации клиент должен перейти на веб-сайт.

Как делать?

Установить пакет `apache2`:

```
apt-get install -y apache2
```

Средствами утилиты `htpasswd` создать пользователя `WEB` и добавить информацию о нем в файл `/etc/nginx/.htpasswd`, задав пароль `P@ssw0rd`:

```
htpasswd –c /etc/nginx/.htpasswd WEB
```

```
[root@ISP ~]# htpasswd -c /etc/nginx/.htpasswd WEB
New password:
Re-type new password:
Adding password for user WEB
[root@ISP ~]#
```

Добавить web-based аутентификацию для доступа к сайту web.au-team.irpo в конфигурационный файл `/etc/nginx/sites-available.d/default.conf` любым удобным текстовым редактором, например `vim`:

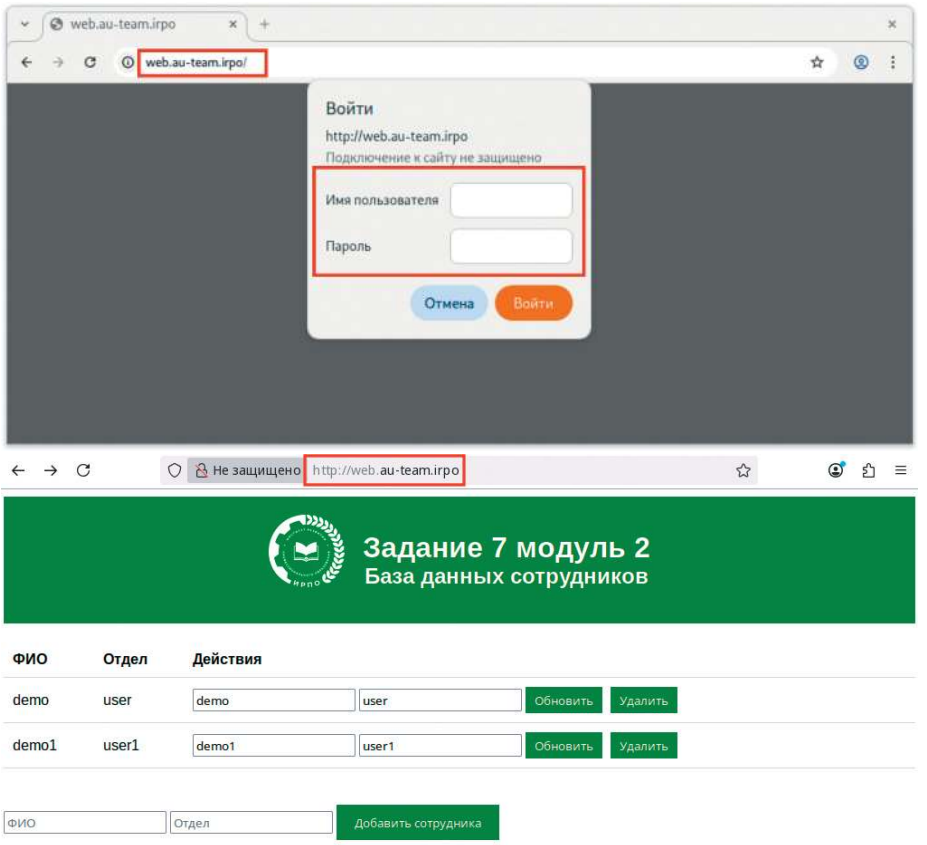
```
server {
        listen 80;
        server_name web.au-team.irpo;

        location / {
                proxy_pass http://172.16.1.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
                auth_basic "Restricted area";
                auth_basic_user_file /etc/nginx/.htpasswd;
        }
}

server {
        listen 80;
        server_name docker.au-team.irpo;

        location / {
                proxy_pass http://172.16.2.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
        }
}
```

Перезапустить службу `nginx`:

```
systemctl restart nginx
```

Как проверить?

Проверить возможность доступа до веб-ресурса из браузера на клиенте:



Где выполнять?

На виртуальной машине: ISP, HQ-CLI.

Дополнительно:

Nginx позволяет настраивать web-based аутентификацию — механизмы, которые защищают веб-ресурсы от неавторизованного доступа. Это позволяет:

• ограничивать доступ к определенным частям сайта (например, к виртуальным хостам или чувствительным страницам);

• интегрироваться с внешними системами аутентификации.

Краткая справка:

– ограничение доступа с помощью базовой HTTP-аутентификации (https://docs.nginx.com/nginx/admin-guide/security-controls/configuring-http-basic-authentication/).

Где изучается?

2 курс:

– Операционные системы и среды.

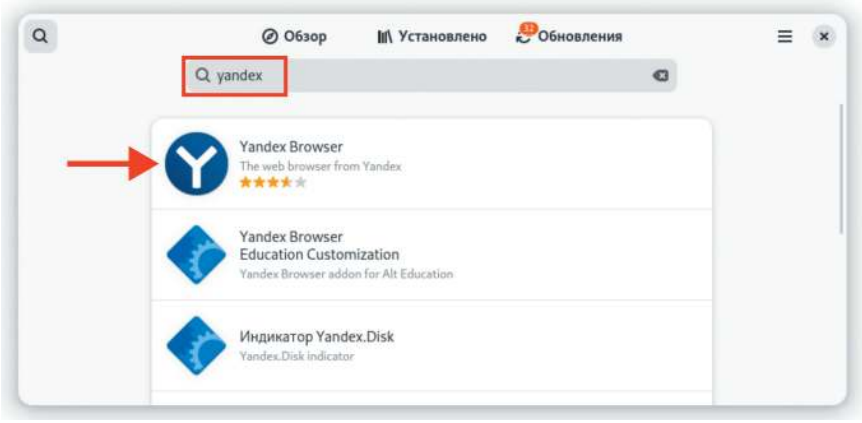
3 курс:
– Организация администрирования компьютерных систем и далее.

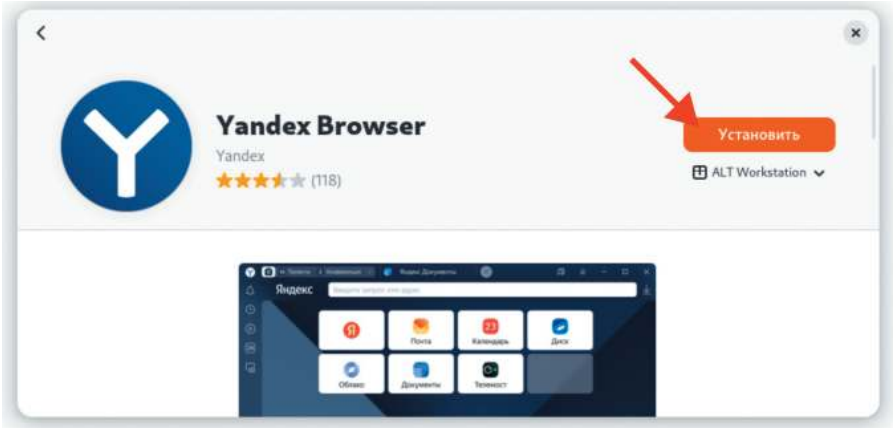
Установка Яндекс Браузера

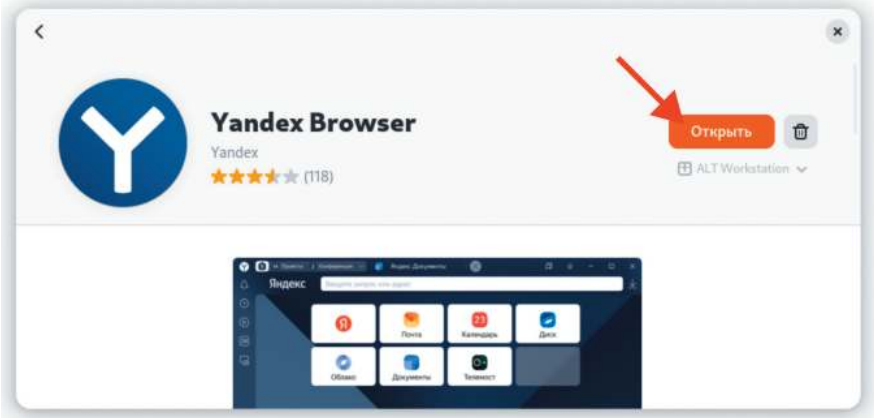
Подробное описание пункта задания
Удобным способом установите приложение Яндекс Браузер на HQ-CLI:
• установку браузера отметьте в отчете.
Как делать?
От имени суперпользователя выполнить:

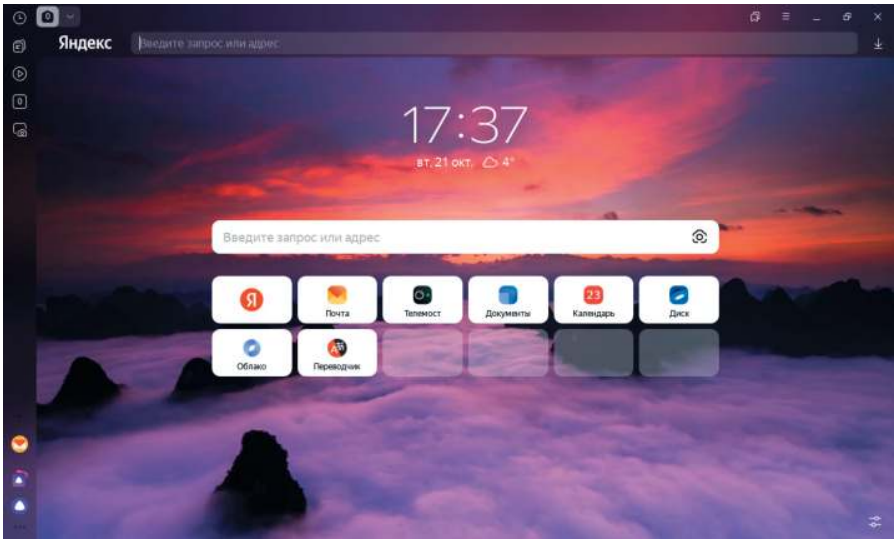
```
apt-get install –y yandex-browser-stable
```

или воспользоваться Центром приложений:









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.

МОДУЛЬ 3. ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Модуль 3
Эксплуатация объектов сетевой инфраструктуры
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. рис. 3.1).

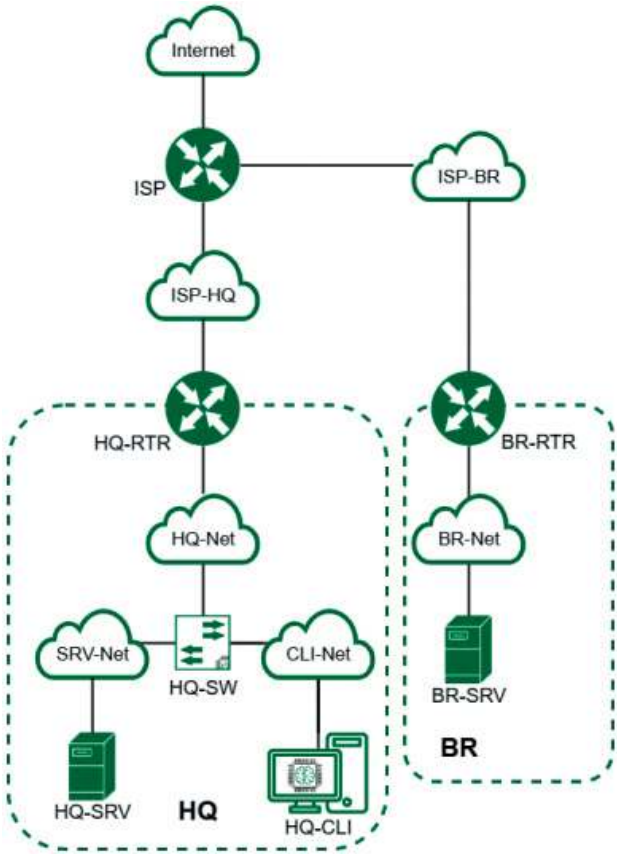


Рис. 3.1. Топология сети

Задание Модуля 3 содержит миграцию пользователей, развертывание и настройку центра сертификации, выдачу сертификатов веб-серверам для шифрования трафика, настройку шифрованного туннеля, настройку межсетевого экрана, принт-сервера, сервера логирования и мониторинга, автомати-

зации на основе инфраструктуры открытых ключей, настройку защиты протокола ssh от перебора, настройку программного обеспечения для создания архивных копий.

В ходе проектирования и настройки сетевой инфраструктуры следует заносить записи в отчет о своих действиях, когда это требуется в задании. Отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла без учета расширения — ФамилияУчастникаМодуль3.

Таблица 3.1

Имя виртуальной машины	**Оперативная память**	**Центральный процессор, ядер**	**Накопитель**	**Операционная система**
ISP	1 ГБ	1 ядро	5 ГБ	Дистрибутив ОС JeOS/Linux или аналог
HQ-RTR	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter 1 ядро в случае использования дистрибутива Linux	10 ГБ	ОС «EcoRouterOS», в случае невозможности использования EcoRouter — дистрибутив ОС JeOS/Linux или аналог
BR-RTR	4 ГБ в случае использования EcoRouter 1 ГБ в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter ядро ГБ в случае использования дистрибутива Linux	10 ГБ	ОС «EcoRouterOS», в случае невозможности использования EcoRouter — дистрибутив ОС JeOS/Linux или аналог
HQ-SRV	2 ГБ	1 ядро	10 ГБ	ОС «Альт Сервер» или аналог
BR-SRV	2 ГБ	1 ядро	10 ГБ	ОС «Альт Сервер» или аналог
HQ-CLI	2 ГБ	2 ядра	20 ГБ	ОС «Альт Рабочая станция» или аналог
Итого	15 (9 в случае использования ОС «Альт» или аналога)	13 (7 в случае использования ОС «Альт» или аналога)	60 ГБ	–

1. Выполните импорт пользователей в домен au-team.irpo:

• в качестве файла источника выберите файл users.csv, располагающийся в образе Additional.iso;

• пользователи должны быть импортированы со своими паролями и другими атрибутами;

• убедитесь, что импортированные пользователи могут войти на машину HQ-CLI.

2. Выполните настройку центра сертификации на базе HQ-SRV:

• необходимо использовать отечественные алгоритмы шифрования;

• сертификаты выдаются на 30 дней;

• обеспечьте доверие сертификату для HQ-CLI;

• выдайте сертификаты веб-серверам;

• перенастройте ранее настроенный реверсивный прокси nginx на протокол https;

• при обращении к веб-серверам https://web.au-team.irpo и https://docker.au-team.irpo у браузера клиента не должно возникать предупреждений.

3. Перенастройте ip-туннель с базового до уровня туннеля, обеспечивающего шифрование трафика:

• настройте защищенный туннель между HQ-RTR и BR-RTR;

• внесите необходимые изменения в конфигурацию динамической маршрутизации, протокол динамической маршрутизации должен возобновить работу после перенастройки туннеля;

• выбранное программное обеспечение, обоснование его выбора и его основные параметры, изменения в конфигурации динамической маршрутизации отметьте в отчете.

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

• обеспечьте работу протоколов http, https, dns, ntp, icmp или дополнительных нужных протоколов;

• запретите остальные подключения из сети Интернет во внутреннюю сеть.

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

• опубликуйте виртуальный pdf-принтер;

• на клиенте HQ-CLI подключите виртуальный принтер как принтер по умолчанию.

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

• сервер сбора логов расположен на HQ-SRV, убедитесь, что сервер не является клиентом самому себе;

• приоритет сообщений должен быть не ниже warning;

• все журналы должны находиться в директории /opt. Для каждого устройства должна выделяться своя поддиректория, которая совпадает с именем машины;

• реализуйте ротацию собранных логов на сервере HQ-SRV:

  ◦ ротируются все логи, находящиеся в директории и поддиректориях /opt;

  ◦ ротация производится один раз в неделю;

- логи необходимо сжимать;
- минимальный размер логов для ротации — 10 МБ.

7. На сервере HQ-SRV реализуйте мониторинг устройств с помощью открытого программного обеспечения:

- обеспечьте доступность по URL — http://mon.au-team.irpo для сетей офиса HQ, внесите изменения в инфраструктуру разрешения доменных имен;
- мониторить нужно устройства HQ-SRV и BR-SRV;
- в мониторинге должны визуально отображаться нагрузка на ЦП, объем занятой ОП и основного накопителя;
- логин и пароль для службы мониторинга admin, P@ssw0rd;
- организуйте доступ к мониторингу для HQ-CLI без внешнего доступа;
- выбор программного обеспечения, основание выбора и основные параметры с указанием порта, на котором работает мониторинг, отметьте в отчете.

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

- плейбук должен собирать информацию о рабочих местах:
  - имя компьютера;
  - IP-адрес компьютера;
- плейбук, должен быть размещен в директории /etc/ansible, отчеты в поддиректории PC-INFO, в формате .yml. Файлы должны называться именем компьютера, который был инвентаризирован;
- файл плейбука располагается в образе Additional.iso в директории playbook.

9. На HQ-SRV настройте программное обеспечение fail2ban для защиты ssh:

- укажите порт ssh;
- при 3 неуспешных авторизациях адрес атакующего попадает в бан;
- бан производится на 1 минуту.

10. Настройка резервного копирования директории сервера HQ-SRV:

- на HQ-SRV развернуть программное обеспечение для резервного копирования и восстановления данных с защитой от вирусов-шифровальщиков;
- в качестве решения рекомендуется использовать программное обеспечение Кибер Бэкап версии 17.4 или аналог;
- настройте организацию irpo;
- настройте пользователя с правами администратора на сервере HQ-SRV, имя пользователя irpoadmin с паролем P@ssw0rd;
- установите на HQ-CLI агент с функциями узла хранилища и подключите его к серверу управления;
- на узле хранилища HQ-CLI создайте директорию /backup и выберите ее в качестве устройства хранения;
- создайте два плана резервного копирования для сервера HQ-SRV:
  - план для резервного копирования директории /etc и всех ее поддиректорий;
  - план для резервного копирования базы данных webdb типа mysql;

• выполните резервное копирование директории /etc и всех ее поддиректорий сервера HQ-SRV на узел хранения HQ-CLI;

• выполните резервное копирование базы данных webdb сервера HQ-SRV на узел хранения HQ-CLI.

Импорт пользователей в домен

Подробное описание пункта задания

Выполните импорт пользователей в домен au-team.irpo:

• в качестве файла источника выберите файл users.csv, располагающийся в образе Additional.iso;

• пользователи должны быть импортированы со своими паролями и другими атрибутами;

• убедитесь, что импортированные пользователи могут войти на машину HQ-CLI.

Как делать?

На сервере HQ-SRV смонтировать образ Additions.iso:

```
mount /dev/sr0 /mnt
```

Скопировать файл Users.csv в директорию /root:

```
cp /mnt/Users.csv /root
```

Переконвертировать файл в utf-8 и избавиться от диакритических знаков, экспортировать в новый файл:

```
iconv -f UTF-8 -t UTF-8//IGNORE /root/Users.csv > /root/Users_fixed.csv
```

Далее перейти в директорию /root, создать в текстовом редакторе скрипт import.sh:

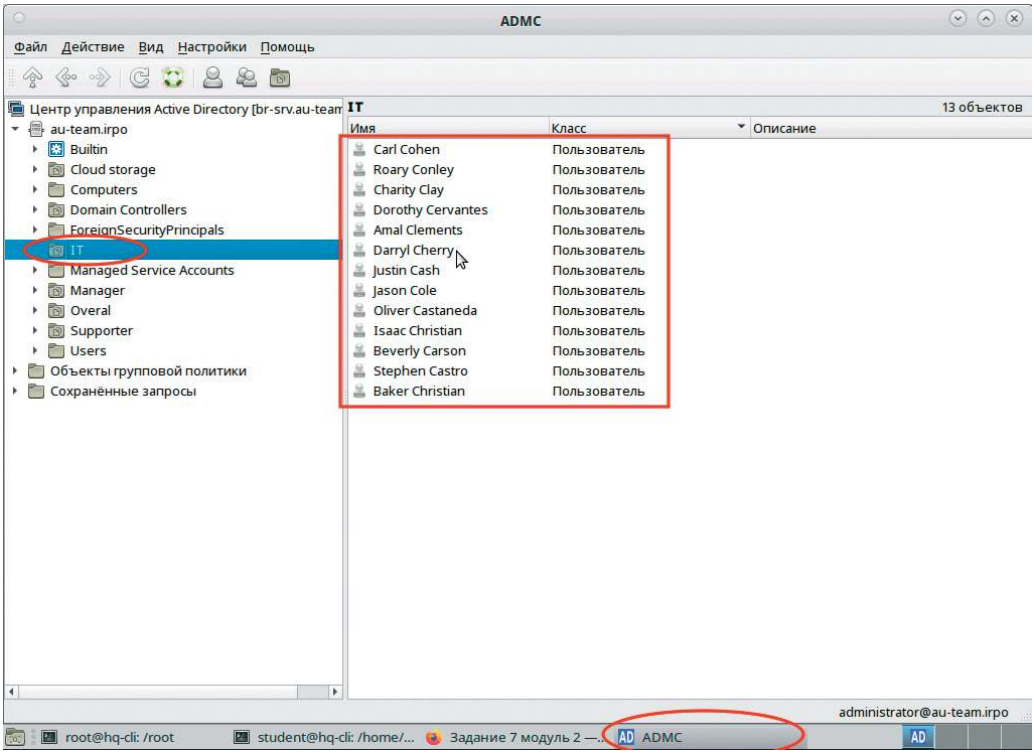
```
#!/bin/bash
while IFS=';' read -r first last role phone ou street zip city
country pass; do
    username="${first:0:1}$last"
      samba-tool user create "${username,,}" "$pass" --given-
name="$first" --surname="$last" --job-title="$role" --telephone-
number="$phone"
    [[ -n "$ou" ]] && samba-tool ou create "OU=$ou" 2>/dev/null
    [[ -n "$ou" ]] && samba-tool user move "${username,,}" "OU=$ou"
2>/dev/null
done < Users_fixed.csv
```

Выполните скрипт:

```
bash /root/import.sh
```

Скрипт во время своей работы выведет информацию о каждом созданном пользователе и подразделении.

Проверить корректность импорта на клиенте с помощью ADMC, предварительно необходимо получить билет kerberos с помощью kinit Administrator@AU-TEAM.IRPO.



Где выполнять?

На виртуальной машине: BR-SRV, проверка на HQ-CLI.

Дополнительно:

Samba-tool позволяет автоматизировать создание пользователей в домене Active Directory через скрипты. Это дает возможность:

• массово импортировать учетные записи из CSV-файлов или корпоративных баз данных;

• стандартизировать атрибуты пользователей (логины, имена, отделы, группы);

• интегрироваться с системами кадрового учета или другими источниками данных.

Краткая справка:
– https://docs.altlinux.org/ru-RU/domain/10.4/html/alt-domain-p10/;
– https://docs.altlinux.org/ru-RU/domain/10.4/html/alt-domain-p10/ch38s02.html.

Где изучается?
3 курс:
– Программное обеспечение компьютерных сетей;
– Организация администрирования компьютерных систем и далее.

Настройка сертификатов ГОСТ

Подробное описание пункта задания
Выполните настройку центра сертификации на базе HQ-SRV:
• необходимо использовать отечественные алгоритмы шифрования;
• сертификаты выдаются на 30 дней;
• обеспечьте доверие сертификату для HQ-CLI;
• выдайте сертификаты веб-серверам;
• перенастройте ранее настроенный реверсивный прокси nginx на протокол https;
• при обращении к веб-серверам https://web.au-team.irpo и https://docker.au-team.irpo у браузера клиента не должно возникать предупреждений.

Как делать?
На сервере HQ-SRV включить поддержку ГОСТ в ОС «Альт»:

```
control openssl-gost enabled
```

С помощью утилиты openssl настроить центр сертификации:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:TCB -out
ca.key
```

Выдать сертификат ЦС на 90 дней:

```
openssl req -new -x509 -md_gost12_256 -days 90 -key ca.key -out ca.crt
```

Затем создать приватный ключ для сервера web:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out
web.au-team.irpo.key
```

Создать запрос для ЦС:

```
openssl req -new -md_gost12_256 -key web.au-team.irpo.key -out web.
au-team.irpo.csr
```

Выдать сертификат на 30 дней:

```
openssl x509 -req -in web.au-team.irpo.csr -CA ca.crt -CAkey ca.key
-CAcreateserial -out web.au-team.irpo.crt -days 30
```

Аналогично для docker:

```
openssl genpkey -algorithm gost2012_256 -pkeyopt paramset:A -out
docker.au-team.irpo.key
```

Создать запрос для ЦС:

```
openssl req –new -md_gost12_256 -key docker.au-team.irpo.key -out
docker.au-team.irpo.csr
```

Выдать сертификат на 30 дней:

```
openssl x509 -req -in docker.au-team.irpo.csr -CA ca.crt -CAkey
ca.key -CAcreateserial -out docker.au-team.irpo.crt -days 30
```

Удобным способом скопировать приватные и публичные ключи с сервера HQ-SRV на ISP в директорию /etc/nginx.

```
scp *.key *.crt root@172.16.1.1:/etc/nginx/
```

Отредактировать конфигурационный файл nginx на ISP, внутри секции http, скопировать секции и server для обоих серверов, дописать к ранее описанной конфигурации параметры работы по протоколу https:

```
server {
        listen 443 ssl;
        server_name web.au-team.irpo;
        ssl_certificate /etc/nginx/web.au-team.irpo.crt;
        ssl_certificate_key /etc/nginx/web.au-team.irpo.key;
        ssl_ciphers GOST2012-KUZNYECHIK-KUZNYECHIKOMAC;
        ssl_protocols TLSv1.2;
        ssl_prefer_server_ciphers on;
location / {
        proxy_pass http://172.16.1.2:8080;
        auth_basic “Authorized access”;
        auth_basic_user_file /etc/nginx/.htpasswd;
        }
}
```

```
server {
        listen 443 ssl;
        server_name docker.au-team.irpo;
        ssl_certificate /etc/nginx/docker.au-team.irpo.crt;
        ssl_certificate_key /etc/nginx/docker.au-team.irpo.key;
        ssl_ciphers GOST2012-KUZNYECHIK-KUZNYECHIKOMAC;
        ssl_protocols TLSv1.2;
        ssl_prefer_server_ciphers on;
location / {
        proxy_pass http://172.16.2.2:8080;
        }
}
```

Проверить конфигурацию nginx на ISP:

```
nginx -t
```

Если конфигурация в порядке, перечитать конфиг или перезапустить сервис на ISP:

```
systemctl reload nginx
```

Передать удобным способом публичный ключ ЦС с сервера HQ-SRV на клиента HQ-CLI:

```
scp ca.crt root@hq-cli:/etc/pki/ca-trust/source/anchors/
```

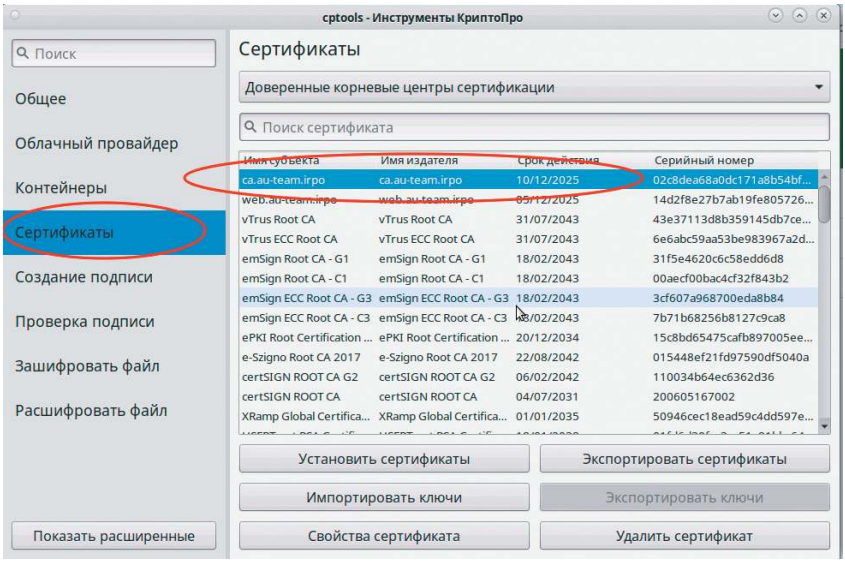
На клиенте HQ-CLI выполнить команду обновления корневых сертификатов:

```
update-ca-trust
```

На клиенте HQ-CLI скачать, распаковать и установить cryptopro csp 5, обязательно установить версию с графикой, поставить галочку напротив пункта «Копировать корневые сертификаты»:

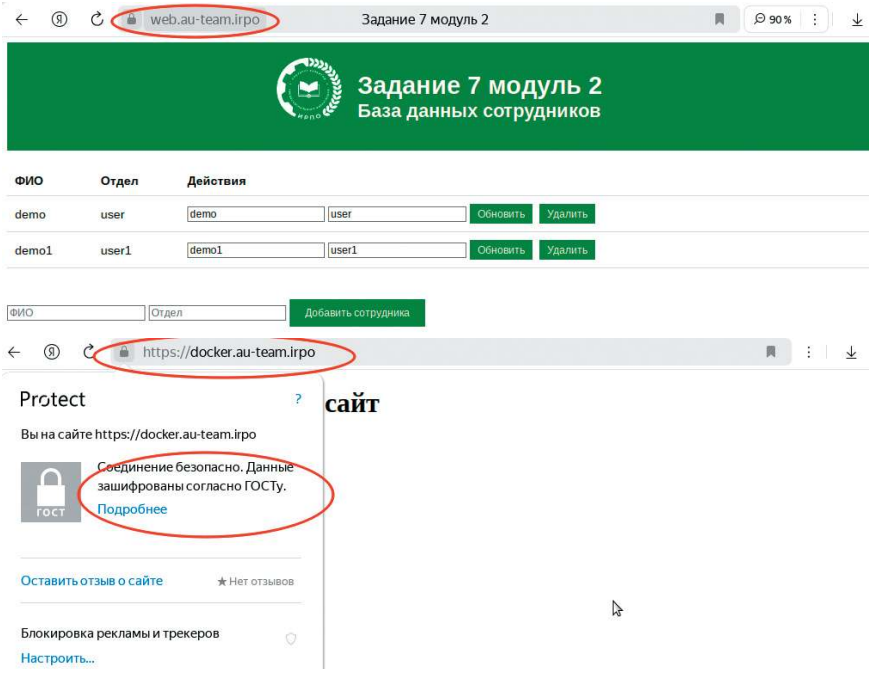
```
bash linux-amd64/install_gui.sh
```

Проверить и убедиться, что появился сертификат в списке доверенных на клиенте, открыв утилиту «Инструменты работы с криптографией», щелкнув на кнопке «Сертификаты»:



В случае, если сертификат отсутствует, добавить его вручную, скопировав его в папку, доступную для чтения пользователем в графике, например /home/user.

Открыть обозреватель Яндекс на странице https://web.au-team.irpo и https://docker.au-team.irpo, согласиться с тем, что сервер использует алгоритмы ГОСТ:



Для проверки алгоритма и соединения выполните команду на клиенте:

```
openssl s_client -connect web.au-team.irpo:443
```

В случае корректной настройки можно увидеть используемый алгоритм (Кузнечик) и информацию о том, что данные шифруются по ГОСТ:

```
x+/Bnw9m7i55RFout2lzkQiiai2iZ9A9OJpAopilK1ER
-----END CERTIFICATE-----
subject=C=RU, ST=Lo, L=Kirovsk, O=au-team, OU=au-team, CN=web.au-team.irpo, emai
lAddress=sa@web.irpo
issuer=C=RU, ST=LO, L=Kirovsk, O=au-team, OU=au-team, CN=ca.au-team.irpo
---
No client certificate CA names sent
---
SSL handshake has read 985 bytes and written 614 bytes
Verification: OK
---
New, TLSv1.2, Cipher is GOST2012-KUZNYECHIK-KUZNYECHIKOMAC
Server public key is 256 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : GOST2012-KUZNYECHIK-KUZNYECHIKOMAC
    Session-ID: 52F4E9D6DEF8F37BFB1139F28D59ADC972264C95767B36C464356CAB3F020D76
    Session-ID-ctx:
    Master-Key: C01D9C34DCBFA3F17700756FA6E7B5B03C851B4529238F5023513164D8AD7488
5A250586AC13061AD251CCEAA51DEF2A
```

Где выполнять?

На виртуальной машине: HQ-SRV.

Дополнительно:

OpenSSL позволяет настраивать SSL/TLS-сертификаты — механизмы, которые обеспечивают криптографическую защиту соединения и аутентификацию сторон. Это позволяет:

• шифровать передаваемые данные, предотвращая перехват трафика;

• идентифицировать веб-сервер, подтверждая его подлинность для пользователей;

• интегрироваться с центрами сертификации (как коммерческими, так и собственными).

Краткая справка:

– https://www.altlinux.org/ГОСТ_в_OpenSSL.

Где изучается?

4 курс:

– Безопасность компьютерных сетей;

– Программное обеспечение компьютерных сетей.

Настройка ipsec на EcoRouter

Подробное описание пункта задания

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

• настройте защищенный туннель между HQ-RTR и BR-RTR;

• внесите необходимые изменения в конфигурацию динамической маршрутизации, протокол динамической маршрутизации должен возобновить работу после перенастройки туннеля;

• выбранное программное обеспечение, обоснование его выбора и его основные параметры, изменения в конфигурации динамической маршрутизации отметьте в отчете.

Как делать?

Описать профиль, криптокарту и криптофильтр, затем применить криптокарту к криптофильтру, затем применить криптофильтр к туннелю. Рекомендуется использовать максимальный размер пакета равный 1360 для работы сети поверх ipsec.

Конфигурацию HQ-RTR и BR-RTR дополнить в соответствии с таблицей, в таблице указаны параметры, что нужно дополнить, без учета предыдущей настройки:

HQ-RTR

crypto-ipsec ike enable
!
crypto-ipsec profile IPSEC ike-v2
 mode tunnel
 nat-traversal
 ike-phase1
  proposal aes256-sha256-modp2048
  auth pre-shared-key P@ssw0rd
 ike-phase2
  protocol esp
  proposal aes256-sha256
  local-ts 172.16.1.2
  remote-ts 172.16.2.2
!
crypto-map CMAP 10
 match peer 172.16.2.2
 set crypto-ipsec profile IPSEC
!

```
filter-map ipv4 FMAP 10
 match gre host 172.16.1.2 host 172.16.2.2
 set crypto-map CMAP peer 172.16.2.2
!
filter-map ipv4 FMAP 20
 match udp host 172.16.2.2 eq 4500 host 172.16.1.2 eq 4500
 set crypto-map CMAP peer 172.16.2.2
!
filter-map ipv4 FMAP 30
 match any any any
 set accept
!
interface tunnel.0
 ip mtu 1360
 set filter-map in FMAP 10
```

Выполнить те же действия, но с другой стороны, указав нужные параметры на BR-RTR:

BR-RTR

```
crypto-ipsec ike enable
!
crypto-ipsec profile IPSEC ike-v2
 mode tunnel
 nat-traversal
 ike-phase1
  proposal aes256-sha256-modp2048
  auth pre-shared-key P@ssw0rd
 ike-phase2
  protocol esp
  proposal aes256-sha256
  local-ts 172.16.1.2
  remote-ts 172.16.2.2
!
crypto-map CMAP 10
 match peer 172.16.2.2
 set crypto-ipsec profile IPSEC
!
filter-map ipv4 FMAP 10
 match gre host 172.16.1.2 host 172.16.2.2
 set crypto-map CMAP peer 172.16.2.2
!
filter-map ipv4 FMAP 20
 match udp host 172.16.2.2 eq 4500 host 172.16.1.2 eq 4500
 set crypto-map CMAP peer 172.16.2.2
!
filter-map ipv4 FMAP 30
 match any any any
```

```
 set accept
!
interface tunnel.0
 ip mtu 1360
 set filter-map in FMAP 10
```

Проверить корректность настройки, выполнив на HQ-RTR:

```
ping 10.10.10.2
```

При корректной настройке BR-RTR ответит на запрос.

Посмотреть параметры шифрованного соединения можно, выполнив команду:

```
show crypto-ipsec ike security-associations
```

Поля state должны иметь состояние ESTABLISHED.

Где выполнять?

На маршрутизаторах: HQ-RTR и BR-RTR.

Дополнительно:

IPsec позволяет настраивать защищенное сетевое взаимодействие — механизмы, которые обеспечивают шифрование и аутентификацию трафика между узлами. Это позволяет:

• создавать зашифрованные туннели между сетями (VPN);

• гарантировать целостность и конфиденциальность передаваемых данных;

• интегрироваться с существующей инфраструктурой (маршрутизаторы, файрволы).

Краткая справка:

– https://docs.ecorouter.ru/Руководство/24-IPsec/04-Настройка-GRE-over-IPsec;

– https://www.altlinux.org/WireGuard опционально;

– https://www.altlinux.org/OpenVPN опционально.

Где изучается?

4 курс:

– Безопасность компьютерных сетей.

Настройка межсетевого экрана на EcoRouter

Подробное описание пункта задания

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

• обеспечьте работу протоколов http, https, dns, ntp, icmp или дополнительных нужных протоколов;

• запретите остальные подключения из сети Интернет во внутреннюю сеть.

Как делать?

Необходимо удалить правило, разрешающее весь остальной трафик, кроме ipsec, описанное в filter-map FMAP с приоритетом 30, рассмотренное в пункте задания 3, на обоих маршрутизаторах, командой:

```
(config)# no filter-map ipv4 FMAP 30
```

Конфигурацию HQ-RTR и BR-RTR дополнить в соответствии с таблицей.

Приведем параметры, которые нужно дополнить, без учета предыдущей настройки:

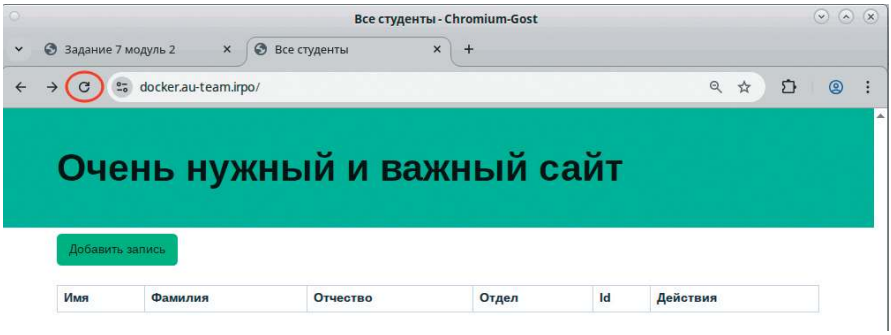
```
filter-map ipv4 FMAP 21
 match tcp any any eq 88
 match udp any any eq 88
 match udp any any eq dns
 match tcp any any range 3268 3269
 match tcp any any eq dns
 match tcp any any eq 389
 match udp any any eq 464
 match tcp any any eq 636
 match tcp any any eq 445
 match udp any any range 137 138
 set accept
!
filter-map ipv4 FMAP 22
 match icmp any any
 match ospf any any
 match tcp any any eq 8080
 match tcp any any eq http
 match tcp any any eq https
 match udp any any eq 123
 match tcp any any eq 2026
 match tcp any any range 32768 60999
 match udp any any range 32768 60999
 set accept
```

Необходимо открыть широкий диапазон портов (32768-60999) для протоколов TCP и UDP, чтобы обеспечить работу не только служб, указанных в задании, но и других служб (ldap, kerberos, smb, netbios):

• для TCP это связано с тем, что клиентские соединения к HTTP/HTTPS-серверам инициируются с высоких случайных портов данного диапазона;

• для UDP диапазон требуется, потому что DNS-клиент отправляет запросы с высокого случайного порта (32768-60999) на серверный порт 53/UDP, а сервер отправляет ответ обратно на этот же высокий порт клиента.

Важно удостовериться, что клиент имеет связь с http, https, ldap, kerberos:




```
[student@hq-cli ~]$ kinit Administrator@AU-TEAM.IRPO
Password for Administrator@AU-TEAM.IRPO:
Warning: Your password will expire in 17 days on [redacted]
[student@hq-cli ~]$
```

Где выполнять?

На виртуальных маршрутизаторах: HQ-RTR и BR-RTR.

Дополнительно:

Межсетевое экранирование позволяет контролировать сетевой трафик — механизмы, которые фильтруют пакеты на основе заданных правил. Это позволяет:

• блокировать нежелательные соединения и атаки из внешних сетей;

• разделять сеть на сегменты с разным уровнем доверия (DMZ, LAN, WAN);

• работать на 4-м (транспортном) уровне модели OSI, фильтруя пакеты по портам и протоколам (TCP/UDP).

Краткая справка:

– https://docs.ecorouter.ru/Руководство/21-Списки-доступа/03-Filter-map/02-Настройка-L3-filter-map.

Где изучается?

2 курс:

– Компьютерные сети (основы).

3 курс:

– Организация, принципы построения и функционирования компьютерных сетей.

4 курс:

– Безопасность компьютерных сетей.

Настройка принт-сервера

Подробное описание пункта задания

Настройте принт-сервер cups на сервере HQ-SRV:

• опубликуйте виртуальный pdf-принтер;

• на клиенте HQ-CLI подключите виртуальный принтер как принтер по умолчанию.

Как делать?

На HQ-SRV выполнить установку cups:

```
apt-get update && apt-get install -y cups cups-pdf
```

В конфигурационном файле cups дописать Allow all в секциях в соответствии с приведенным ниже листингом:

```
<Location />
  Order allow,deny
  Allow all
</Location>
<Location /admin>
  AuthType Default
  Require user @SYSTEM
  Allow all
</Location>
<Location /admin/conf>
  AuthType Default
  Require user @SYSTEM
  Allow all
</Location>
```

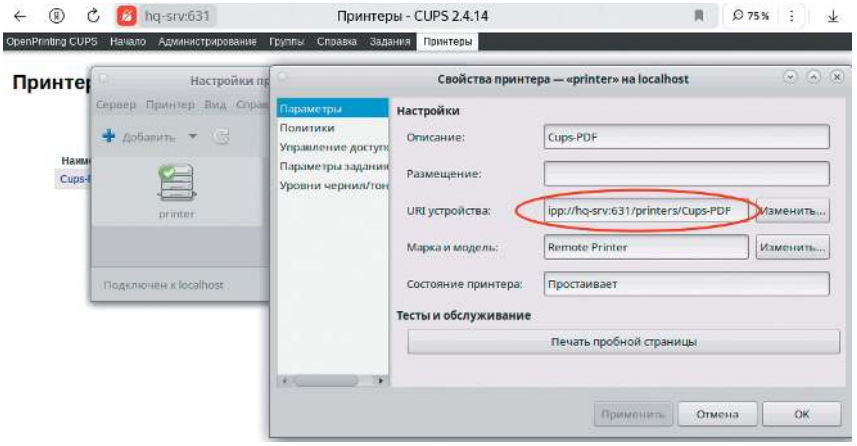
Это позволит управлять сервером cups удаленно с помощью учетной записи root на HQ-SRV.

Затем выполнить запуск и автозагрузку сервера cups:

```
systemctl enable –now cups
```

На клиенте HQ-CLI в веб-обозревателе перейти на страницу https://hq-srv:631/admin/, сделать исключение для самоподписанного сертификата, перейти на вкладку управления принтерами, убедиться, что Cups-PDF опубликован и находится в статусе ожидания. Также можно выполнить добавление принтера вручную:

Удобным способом подключить принтер к клиенту по адресу:
ipp://hq-srv:631/printers/Cups-PDF



Где выполнять?

На виртуальных машинах: HQ-SRV, клиент на HQ-CLI.

Дополнительно:

CUPS позволяет настраивать сетевую печать — механизмы, которые централизуют управление принтерами в сети. Это позволяет:

• предоставлять общий доступ к принтерам для множества пользователей;

• автоматически определять и настраивать драйверы печатающих устройств;

• интегрироваться с различными операционными системами и сетевыми протоколами печати (IPP).

Краткая справка:

– https://docs.altlinux.org/ru-RU/archive/2.4/html-single/master/alt-docs-master/ch06s09.html.

Где изучается?

2 курс:

– Архитектура аппаратных средств;

– Операционные системы и среды.

3 курс:

– Администрирование сетевых операционных систем;

– Программное обеспечение компьютерных сетей.

Логирование, ротация логов

Подробное описание пункта задания

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

• сервер сбора логов расположен на HQ-SRV, убедитесь, что сервер не является клиентом самому себе;

• приоритет сообщений должен быть не ниже warning;

• все журналы должны находиться в директории /opt. Для каждого устройства должна выделяться своя поддиректория, которая совпадает с именем машины;

• реализуйте ротацию собранных логов на сервере HQ-SRV:

◦ ротируются все логи, находящиеся в директории и поддиректориях /opt;

◦ ротация производится один раз в неделю:

◦ логи необходимо сжимать;

◦ минимальный размер логов для ротации — 10 МБ.

Как делать?

Сервер логирования:

На сервера HR-SRV настроить сервер rsyslog, в случае его отсутствия (к примеру, на AltLinux StarterKit) выполнить установку и последующую настройку:

```
apt-get install -y rsyslog
```

Можно привести конфигурационный файл /etc/rsyslog.conf к следующему виду, или создать в директории /etc/rsyslog.conf.d/ свой файл, ввести код:

```
module(load=”imudp”)
$ModLoad imuxsock
authpriv.* /var/log/auth.log

input(type=”imudp” port=”514”)
if $fromhost-ip contains '192.168.100.1' then {
*.warn /opt/hq-rtr/router.log
}
if $fromhost-ip contains '10.10.10.2' then {
*.warn /opt/br-rtr/router.log
}
if $fromhost-ip contains '192.168.0.2' then {
*.warn /opt/br-srv/server.log
}
```

Затем запустить сервер rsyslog:

```
systemctl enable –now rsyslog
```

На маршрутизаторах HQ-RTR и BR-RTR указать сервер rsyslog:

```
rsyslog host 192.168.100.2
```

На BR-SRV установить и запустить rsyslog, прописать в конфигурационном файле (rsyslog.conf или созданном .conf в директории /etc/rsyslog.conf.d):

```
$ModLoad imuxsock
$ModLoad imjournal
*.warn @@192.168.100.2:514
```

При корректной настройке логи типа *.warn будут присылаться с устройств в директорию /opt, в поддиректории, описанные в конфигурации:

```
[root@hq-srv opt]# tree br-srv/
br-srv/
└── server.log

1 directory, 1 file
[root@hq-srv opt]# tree br-rtr
br-rtr
└── router.log

1 directory, 1 file
[root@hq-srv opt]# tree hq-rtr
hq-rtr
└── router.log

1 directory, 1 file
[root@hq-srv opt]#
```

Утилитой logger на BR-SRV можно быстро проверить, высылаются ли логи на сервер:

```
logger warn atencion
```

Ротация логов:

Проверить, установлен ли сервис logrotate. Если не установлен (в случае использования AltLinux StarterKit), выполнить команду:

```
apt-get install –y logrotate
```

Настроить ротацию в конфигурационном файле /etc/logrotate.conf:

```
/opt/br-rtr/*.log
/opt/hq-rtr/*.log
/opt/br-srv/*.log
{
weekly
compress
minsize 10M
}
```

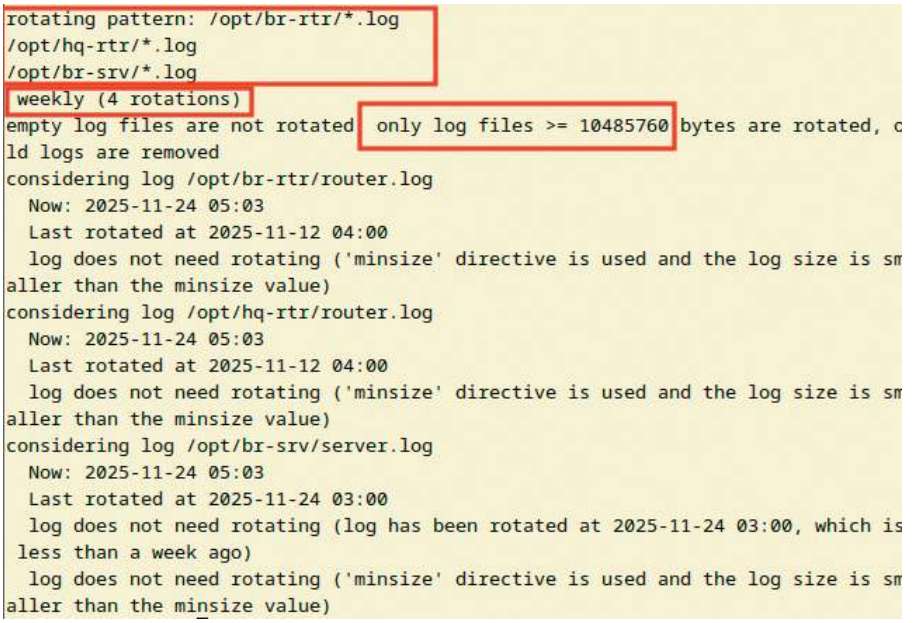
Запустить службу и установить автозапуск сервиса:

```
systemctl enable –now logrotate
```

Проверить конфигурацию командой:

```
logrotate -d /etc/logrotate.conf
```

В конце вывода команды будет описание ротирования указанных директорий:



Где выполнять?

На виртуальных машинах: HQ-SRV — сервер, BR-SRV — клиент.

На маршрутизаторах: HQ-RTR, BR-RTR — клиенты.

Дополнительно:

Системы логирования (rsyslog, journald) позволяют настраивать сбор и анализ системных событий — механизмы, которые централизуют учет работы приложений и ОС. Это позволяет:

• отслеживать ошибки и критические события в реальном времени;

• хранить историю изменений и действий пользователей для аудита;

• интегрироваться с внешними SIEM-системами для анализа безопасности.

Краткая справка:

– https://docs.altlinux.org/ru-RU/domain/10.4/html/alt-domain-p10/ch54s09.html;

– https://www.altlinux.org/Journald.

Где изучается?

2 курс:

– Операционные системы и среды (основы).

3 курс:

– Администрирование сетевых операционных систем;

– Организация, принципы построения и функционирования компьютерных сетей.

Мониторинг с помощью визуализатора grafana и сборщика Prometheus

Подробное описание пункта задания

На сервере HQ-SRV реализуйте мониторинг устройств с помощью открытого программного обеспечения:

• обеспечьте доступность по URL — http://mon.au-team.irpo для сетей офиса HQ, внесите изменения в инфраструктуру разрешения доменных имен;

• мониторить нужно устройства HQ-SRV и BR-SRV;

• в мониторинге должны визуально отображаться нагрузка на ЦП, объем занятой ОП и основного накопителя;

• логин и пароль для службы мониторинга admin, P@ssw0rd;

• организуйте доступ к мониторингу для HQ-CLI без внешнего доступа;

• выбор программного обеспечения, основание выбора и основные параметры с указанием порта, на котором работает мониторинг, отметьте в отчете.

Как делать?

На сервер HQ-SRV установить grafana, prometheus и prometheus-node_exporter. Это можно сделать с помощью команды:

```
apt-get install -y grafana prometheus prometheus-node_exporter
```

На сервер BR-SRV установить только prometheus-node_exporter, запустить и активировать автозапуск:

```
apt-get install –y prometheus-node_exporter
systemctl enable –now prometheus-node_exporter
```

Выполнить настройку сборщика prometheus, в конфигурационном файле /etc/prometheus/prometheus.yml, в секции job_name: 'prometheus' в static_configs дописать в поле targets следующее:

```
    static_configs:
      - targets: ['localhost:9090','hr-srv:9100','br-srv:9100']
```

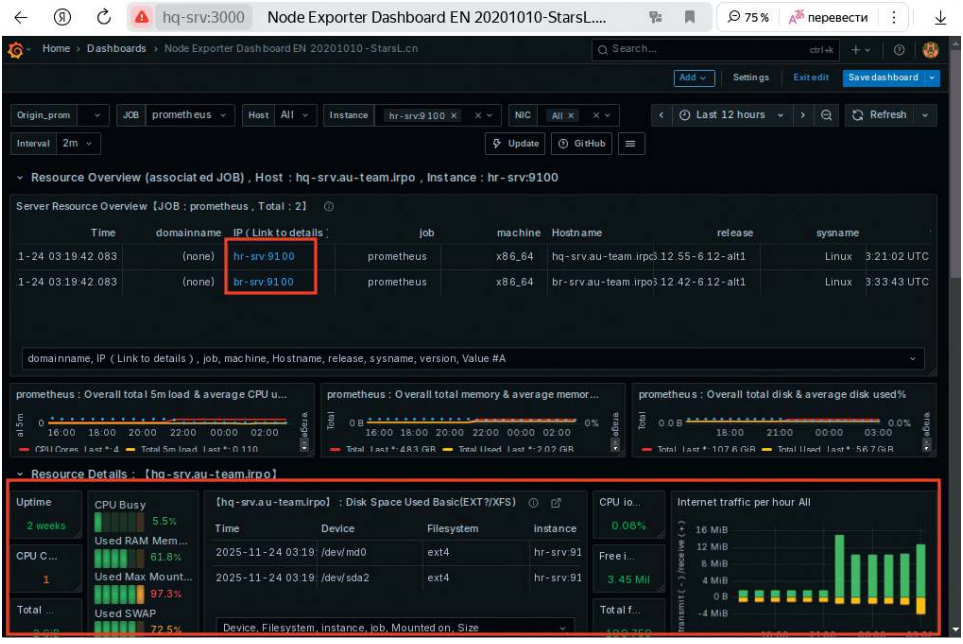
Выполнить запуск и активацию автозапуска grafana-server и prometheus:

```
systemctl enable –now grafana-server
systemctl enable –now prometheus
systemctl enable –now prometheus-node_exporter
```

На клиенте HQ-CLI в веб-обозревателе перейти на сайт http://hq-srv:3000, выполнить вход в grafana с помощью учетной записи: по умолчанию — admin с паролем admin. Заменить пароль по умолчанию на P@ssw0rd.

Добавить источник данных типа prometheus, указать сборщика local-host:9090:

Импортировать дашборд, к примеру 11074 во вкладке dashboards. Перейти в дашборд, убедиться, что нужные данные (цп, оп, хранилища) отображаются корректно:



Где выполнять?

На виртуальных машинах: HQ-SRV — сервер и клиент, BR-SRV — клиент.

Дополнительно:

Системы мониторинга (Zabbix, Prometheus) позволяют настраивать отслеживание работы инфраструктуры — механизмы, которые собирают метрики и анализируют производительность. Это позволяет:

• выявлять сбои и аномалии в реальном времени;

• планировать ресурсы на основе исторических данных и трендов;

• интегрироваться с системами оповещения для оперативного реагирования.

Краткая справка:

– https://www.altlinux.org/Prometheus.

Где изучается?

2 курс:

– Операционные системы и среды.

3 курс:

– Администрирование сетевых операционных систем;

– Организация, принципы построения и функционирования компьютерных сетей.

Инвентаризация с помощью ansible плейбука

Подробное описание пункта задания

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

• плейбук должен собирать информацию о рабочих местах:

  ◦ имя компьютера;

  ◦ IP-адрес компьютера;

• плейбук должен быть размещен в директории /etc/ansible, отчеты в поддиректории PC-INFO, в формате .yml. Файлы должны называться именем компьютера, который был инвентаризирован;

• файл плейбука располагается в образе Additional.iso в директории playbook.

Как делать?

На сервере BR-SRV в директории /etc/ansible/ создать плейбук get_hostname_address.yml со следующим содержимым в формате yaml (заготовку плейбука можно взять с образа Additional.iso в директории playbook):

```
- name: Get_hostname
  hosts: hq-srv,hq-cli
  tasks:
    - name: Save hostname ip
      copy:
        dest: /etc/ansible/PC-INFO/{{ ansible_hostname }}.yml
```

```
        content: |
          Hostname: {{ ansible_hostname }}
          IP_Address: {{ ansible_default_ipv4.address }}
      delegate_to: localhost
```

Выполнить плейбук командой:

```
ansible-playbook get_hostname_address.yml
```

Убедиться, что в поддиректории PC_INFO появились файлы и данные корректны:

```
[root@br-srv ~]# cd /etc/ansible/
[root@br-srv ansible]# tree PC-INFO/
PC-INFO/
|-- hq-cli.yml
`-- hq-srv.yml

1 directory, 2 files
[root@br-srv ansible]# cat PC-INFO/hq-cli.yml
Hostname: hq-cli
IP_Address: 192.168.200.2
[root@br-srv ansible]# cat PC-INFO/hq-srv.yml
Hostname: hq-srv
IP_Address: 192.168.100.2
[root@br-srv ansible]#
```

Где выполнять?

На виртуальных машинах: BR-SRV — сервер, HQ-SRV, HQ-CLI — клиенты.

Дополнительно:

Ansible позволяет настраивать автоматизацию управления инфраструктурой — механизмы, которые унифицируют развертывание и конфигурирование систем. Это позволяет:

• централизованно управлять конфигурациями серверов и сетевых устройств;

• быстро развертывать приложения и обновления без ручного вмешательства;

• интегрироваться с облачными платформами и системами мониторинга.

Краткая справка:

– https://www.altlinux.org/Ansible.

Где изучается?

2 курс:

– Операционные системы и среды (основы).

3 курс:

– Организация администрирования компьютерных систем.

Защита ssh от атак методом перебора пароля

Подробное описание пункта задания

На HQ-SRV настройте программное обеспечение fail2ban для защиты ssh:

- укажите порт ssh;
- при 3 неуспешных авторизациях адрес атакующего попадает в бан;
- бан производится на 1 минуту.

Как делать?

Установить fail2ban и iptables (как блокировщик портов):

```
apt-get install –y fail2ban iptables
```

Настроить сервис ssh на передачу своих логов в службу rsyslog, открыть в конфигурационном файле /etc/opensshd/sshd_config секции:

```
SyslogFacility AUTHPRIV
LogLevel INFO
```

Настроить файл /etc/fail2ban/jail.conf, указав в секции [sshd] параметры защиты:

```
[sshd]
enabled = yes
port    = 2026
logpath = /var/log/auth.log
backend = %(sshd_backend)s
maxretry = 3
bantime = 1m
```

Убедиться, что логи sshd пишутся в /var/log/auth.log. Для настройки auth логов в конфигурационном файле rsyslog должна быть следующая секция:

```
authpriv.* /var/log/auth.log
```

Если логи сервиса sshd ведут в другое место, стоит указать это место (например, /var/log/secure) или оставить параметр `logpath` в jail.conf по умолчанию:

Запустить сервис fail2ban:

```
systemctl enable –now fail2ban
```

Удостовериться в том, что порт 2026 блокируется при 3 неуспешных авторизациях для конкретного ip-адреса, к примеру, выполнив 3 неуспешных попытки авторизации с сервера BR-SRV:

```
fail2ban-client status sshd
```

Для быстрого вывода из бана выполнить:

```
fail2ban-client unban all #всех
fail2ban-client unban 192.168.0.2 #отдельный ip адрес
```

Где выполнять?

На виртуальных машинах: HQ-SRV.

Дополнительно:

Fail2ban позволяет настраивать защиту от bruteforce-атак — механизмы, которые автоматически блокируют подозрительные IP-адреса. Это позволяет:

• анализировать логи сервисов (SSH, FTP, веб-серверы) на предмет неудачных попыток входа;

• динамически добавлять нарушителей в черный список через iptables/firewalld;

• интегрироваться с любыми сервисами, ведущими журналы аутентификации.

Краткая справка:

– https://habr.com/ru/articles/557980/.

Где изучается?

2 курс:

– Операционные системы и среды (основы).

4 курс:

– Безопасность компьютерных сетей.

Резервное копирование

Подробное описание пункта задания

Настройка резервного копирования директории сервера HQ-SRV:

• на HQ-SRV развернуть программное обеспечение для резервного копирования и восстановления данных с защитой от вирусов-шифровальщиков;

• в качестве решения рекомендуется использовать программное обеспечение Кибер Бэкап версии 17.4 или аналог;

• настройте организацию irpo;

• настройте пользователя с правами администратора на сервере HQ-SRV, имя пользователя irpoadmin с паролем P@ssw0rd;

• установите на HQ-CLI агент с функциями узла хранилища и подключите его к серверу управления;

• на узле хранилища HQ-CLI создайте директорию /backup и выберите ее в качестве устройства хранения;

• создайте два плана резервного копирования для сервера HQ-SRV:

◦ план для резервного копирования директории /etc и всех ее поддиректорий;

◦ план для резервного копирования базы данных webdb типа mysql;

• выполните резервное копирование директории /etc и всех ее поддиректорий сервера HQ-SRV на узел хранения HQ-CLI;

• выполните резервное копирование базы данных webdb сервера HQ-SRV на узел хранения HQ-CLI.

Как делать?

Обновить репозитории, обновить ядро операционной системы (затем перезагрузить виртуальную машину), установить нужные пакеты:

```
update-kernel && reboot
apt-get update
apt-get install kernel-source-6.12 kernel-headers-modules-6.12 gcc make
```

Важное замечание: на момент написания руководства новейшее ядро — 6.12.55-6.12-alt1, именно поэтому заголовки ядра и исходные коды ядра устанавливались версии 6.12. В случае другой версии ядра заголовки и исходные коды ядра должны быть версии, совпадающей с версией ядра. В случае отсутствия пакета update-kernel (актуально для AltLinux StarterKit), его стоит установить.

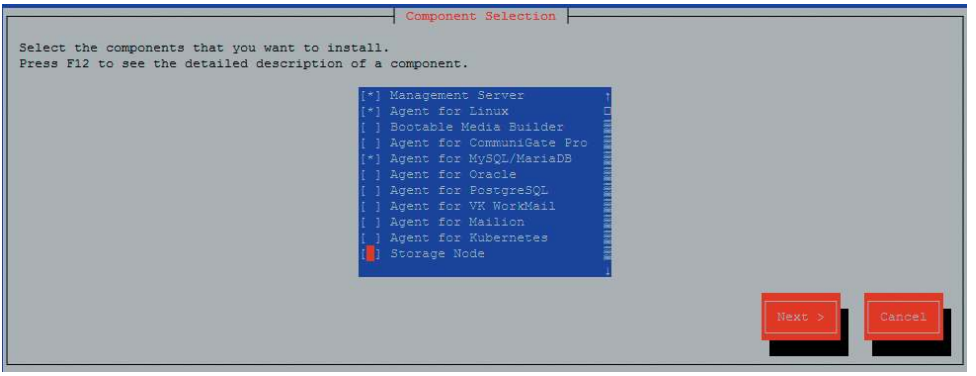
На сервере HQ-SRV смонтировать образ с установщиков Кибер Бекап 18, в примере образ Additional.iso - /dev/sr0, установщик Кибер Бекап 18 - /dev/sr1.

```
mount /dev/sr1 /mnt
```

Запустить установку Кибер Бекап, выполнив команду:

```
bash /mnt/CyberBackup_18_64-bit.x86_64
```

Следуя шагам установщика, на сервере HQ-SRV установить компоненты Management Server, Agent for Linux, Agent for MySQL/MariaDB.



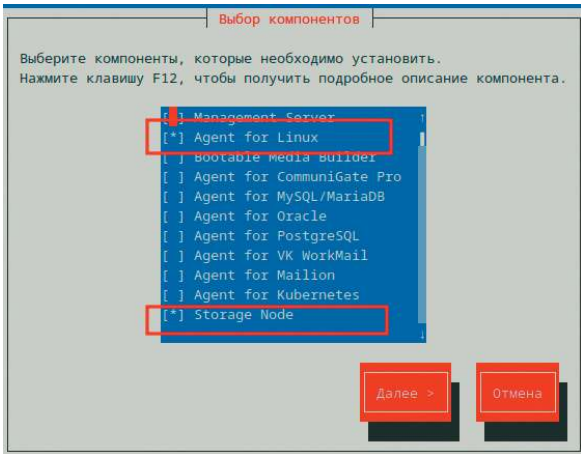
На узле хранилища HQ-CLI смонтировать образ с установщиков Кибер Бекап 18:

```
mount /dev/sr0 /mnt
```

Запустить установку Кибер Бекап, выполнив команду:

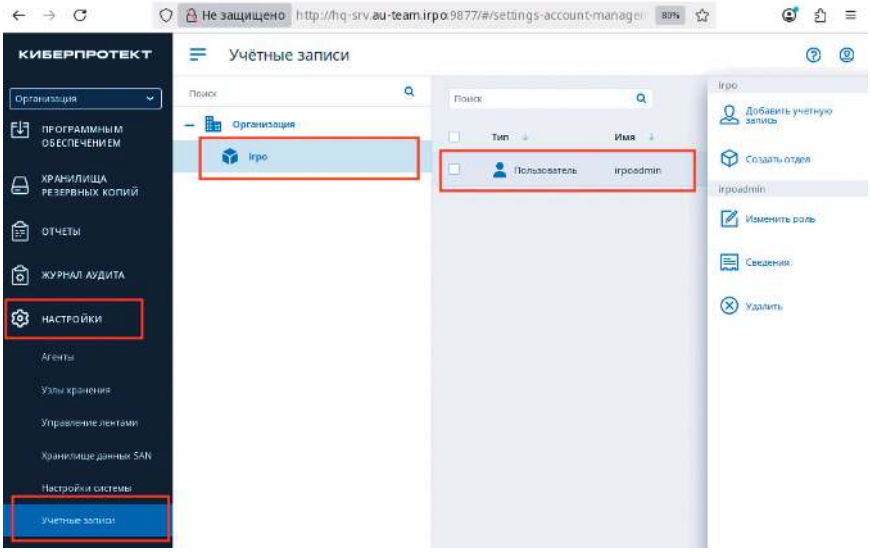
```
bash /mnt/CyberBackup_18_64-bit.x86_64
```

Следуя шагам установщика, на узле хранилища HQ-CLI установить компоненты Agent for Linux, Storage Node.



После установки всех компонентов на сервере HQ-SRV создать учетную запись irpoadmin с паролем P@ssw0rd, затем на клиенте в веб-обозревателе на странице http://hq-srv:9877 авторизоваться учетными данными root с паролем

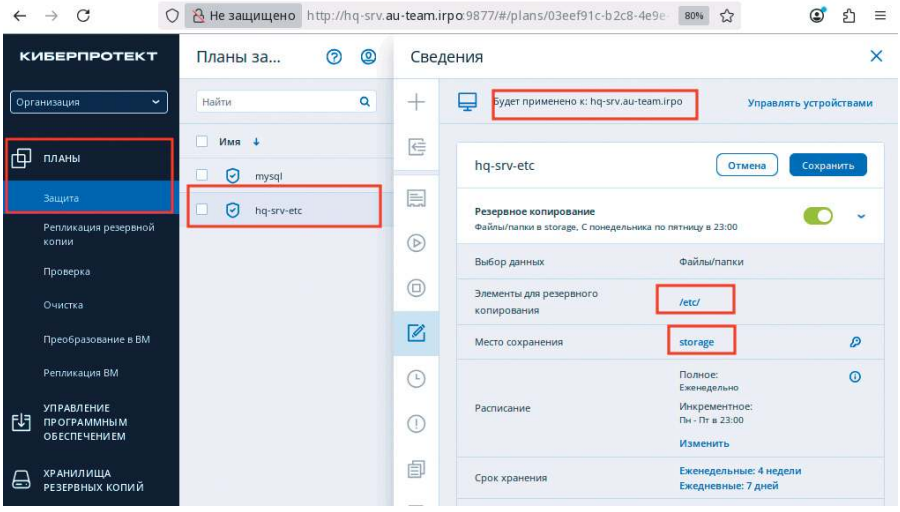
P@ssw0rd (локальный root HQ-SRV), перейти на вкладку «Настройки — учетные записи», создать подразделение irpo, создать учетную запись в подразделении irpoadmin с привилегиями администратора:



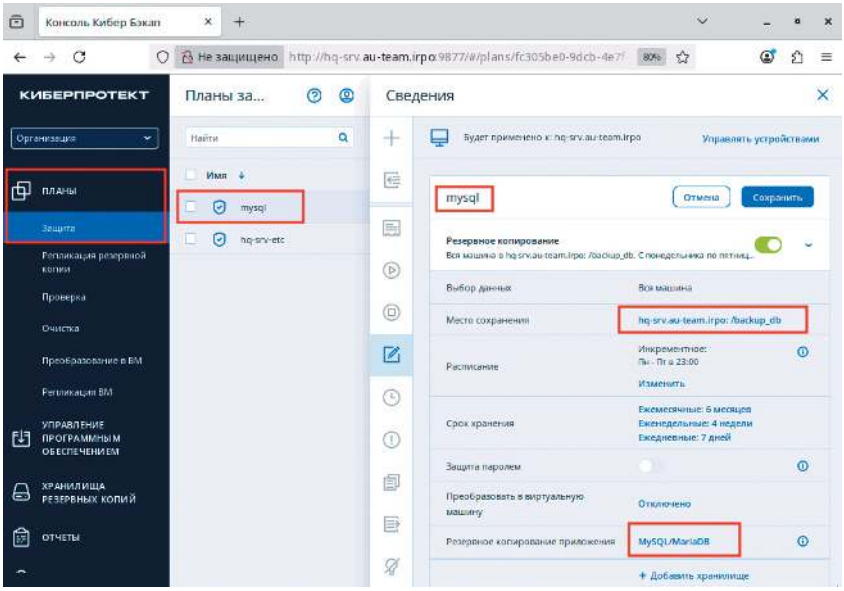
На узле хранилища создать директорию /backup:

```
mkdir /backup
```

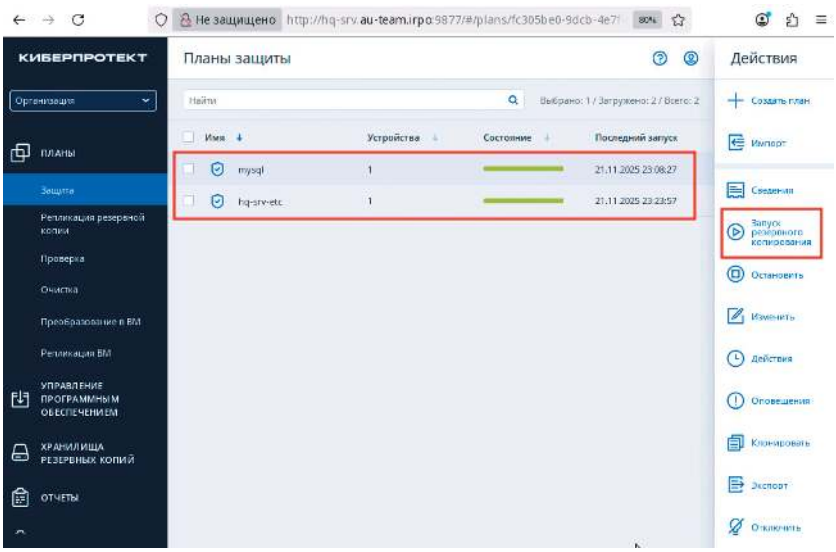
Настроить план резервного копирования для сервера HQ-SRV для директории /etc и всех ее поддиректорий, в качестве места сохранения архивных копий указать узел хранения HQ-CLI (в примере на снимке — storage):



Создать второй план резервного копирования, на сервере HQ-SRV создать директорию /backup_db, указать директорию в качестве места хранения копий:



Выполнить запуск резервного копирования сначала одного, затем другого плана:



Где выполнять?

На виртуальных машинах: HQ-SRV сервер, HQ-CLI — клиент и узел хранилища.

Дополнительно:

Системы резервного копирования позволяют настраивать сохранность данных — механизмы, которые создают и управляют резервными копиями файлов и систем. Это позволяет:

- автоматически создавать инкрементальные бэкапы с дедупликацией;
- восстанавливать данные на определенный момент времени;
- интегрироваться с облачными хранилищами и локальными архивами.

Краткая справка:

Продукт	Ссылка	
Кибер Инфраструктура	https://cyberprotect.ru/forms/forma-trial-infr?education=1	
Кибер Хранилище	https://cyberprotect.ru/forms/forma-trial-storage?education=1	
Кибер Файлы	https://cyberprotect.ru/forms/forma-trial-files?education=1	
Кибер Протего	https://cyberprotect.ru/forms/forma-trial-protego?education=1	
Кибер Бэкап	https://cyberprotect.ru/forms/forma-trial-backup?education=1	

Где изучается?

3 курс:

– Администрирование сетевых операционных систем.

НАЧАЛО РАБОТЫ С КИБЕР ИНФРАСТРУКТУРОЙ

УСТАНОВКА СИСТЕМЫ

О Кибер Инфраструктуре

На схеме, приведенной на рис. 4.1, показаны основные вычислительные компоненты продукта «Кибер Инфраструктура»:

Рис. 4.1. Вычислительные компоненты

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

• файловое хранилище, объектное хранилище S3, блочное хранилище для виртуальных машин или баз данных;

• частные и публичные облака;

• виртуальные машины (ВМ), 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 если в минимальной конфигурации рекомендуется три сервера, можно начать тестировать продукт «Кибер Инфраструктура» всего с одним сервером и добавить остальные серверы позже.

Системные требования

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

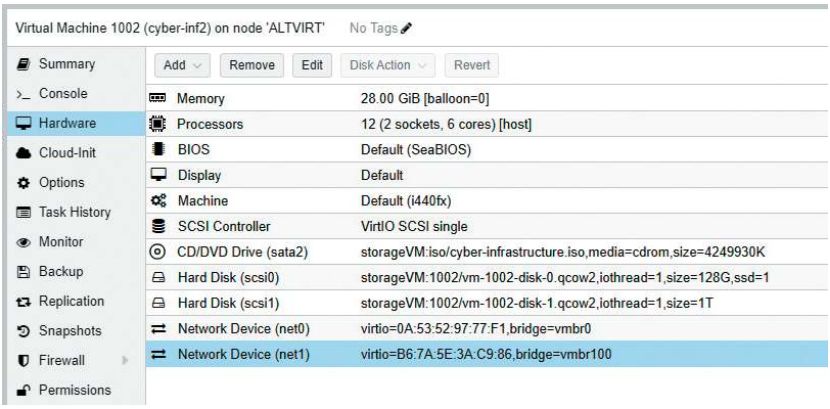
Перейти на сайт компании Киберпротект по ссылке https://cyberprotect.ru/forms/forma-trial-infr?education=1 и корректно заполнить форму-запроса на получение пробной версии продукта.

Свойства стенда

Стенд с «Кибер Инфраструктурой» развернут в среде ОС «Альт Виртуализация». Однако настоятельно советуем устанавливать продукт «Кибер Инфраструктура» на «голое» железо (bare metal).

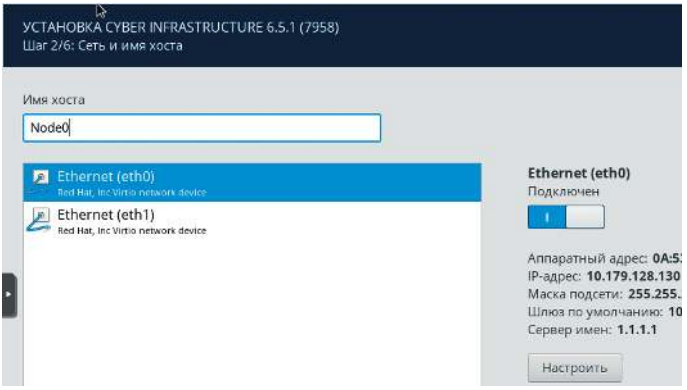
Были выделены следующие ресурсы:

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



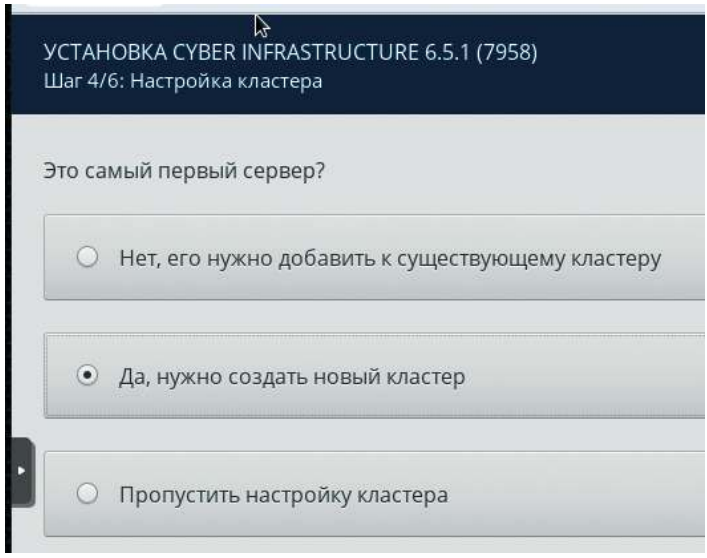
Установка системы

После конфигурирования и запуска ВМ подтвердить установку, принять лицензионное соглашение, перейти на экран настройки «Сети и имени хоста»:

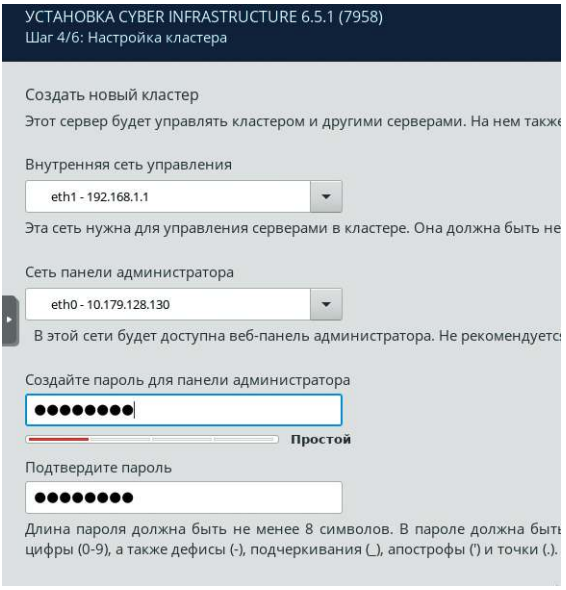


Ввести данные. Не забудьте включить и настроить **ВСЕ** интерфейсы! Далее на следующем шаге необходимо настроить часовой пояс:

На следующем экране выбрать из списка «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 т.п.). Можно использовать простые и словарные пароли, например «Passw0rd», только для экспериментальных и учебных стендов. В таком случае требуется дважды нажать «Далее».

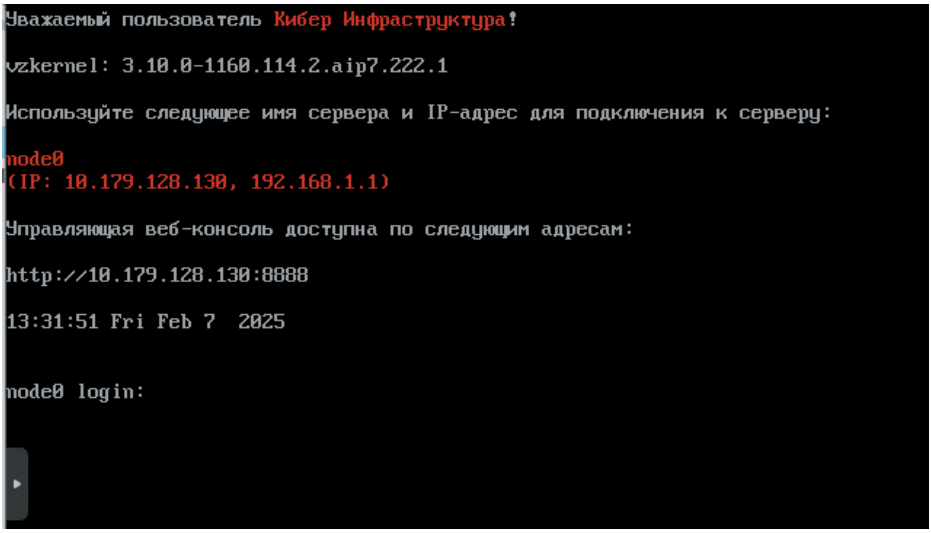
На следующем шаге — настройка дисковой подсистемы:

Должен быть выделен диск под операционную систему. В дальнейшем будет настроен диск под хранилище. После подтверждения операции нажать «Далее».

Начнется установка системы. В зависимости от производительности аппаратного обеспечения (особенно дисков) установка может занять 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, в консоли отобразятся параметры подключения к веб-консоли:

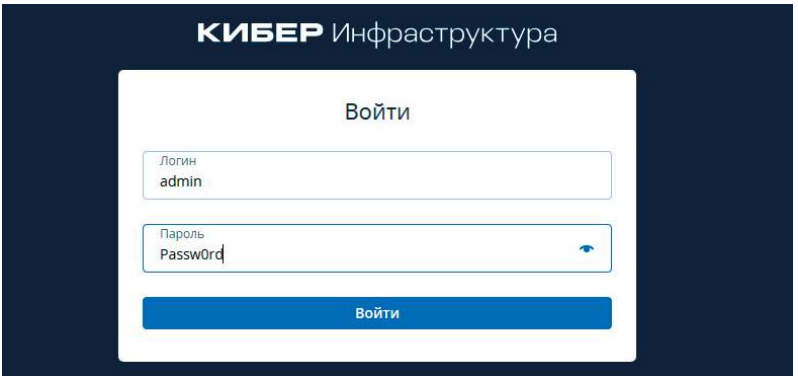


Система установлена.

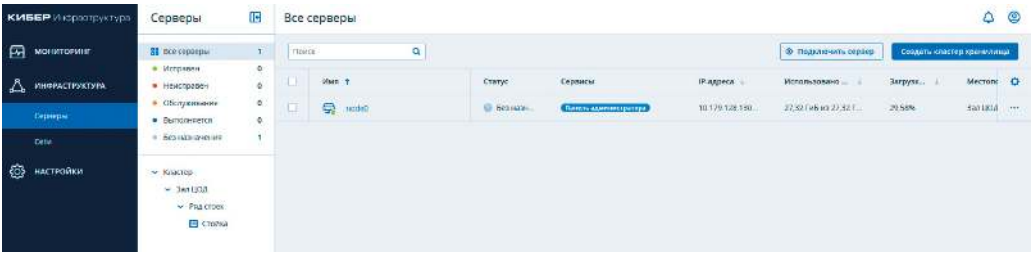
НАСТРОЙКА СИСТЕМЫ

Начало настройки

После ввода параметров веб-консоли и предупреждения о самоподписанном сертификате откроется окно аутентификации:



Далее, после входа в систему, откроется панель администратора:



Напоминаем вам, что решение «Кибер Инфраструктура» является полноценной гиперконвергентной инфраструктурой, объединяющей **вычислительные** ресурсы, **системы хранения** данных и **сетевые технологии** в единую единицу управления. Поэтому для успешной работы необходимо предварительно настроить сетевую подсистему и 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

Перейти к пункту 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, дис-

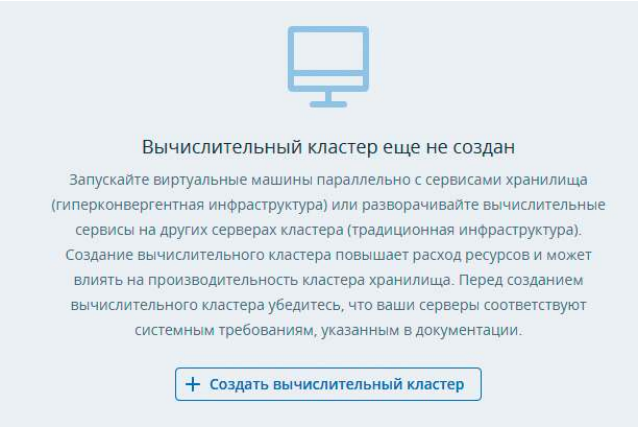
ковых массивов кластера, их следует назначать внутренним сетям. Для этого нужно выбрать пункт справа «Назначить сети», задать тип трафика, выбрать сеть, подтвердить действия.

Типы трафика определяют обычный сетевой трафик и сети управления. Здесь трафик может быть разрешен в обеих сетях. Для настройки используйте пункт «Назначить сетям».

Следует обратить внимание на пункты «Создать сеть» и «Создать тип трафика» в верхней части окна. Первый создает сеть с отдельным адресным пространством, в которой можно выполнить отдельные настройки обоих видов трафика. Второй создает пользовательский тип трафика, связанный с определенным портом. На оба эти пункта можно настроить правила доступа к сетям и портам:

Настройка вычислительного кластера

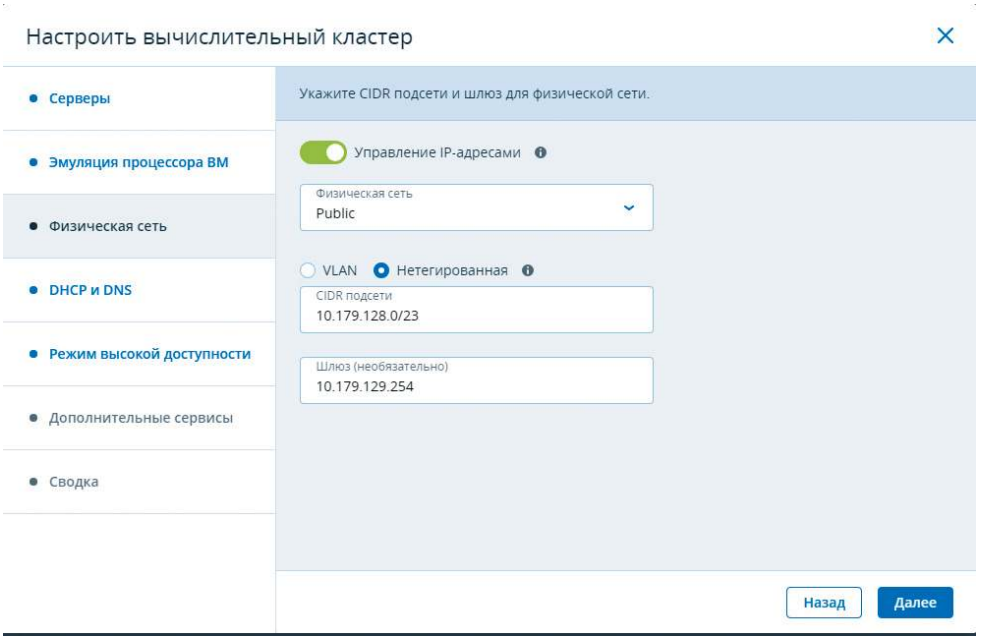
Перейти в пункт «Вычисления»:



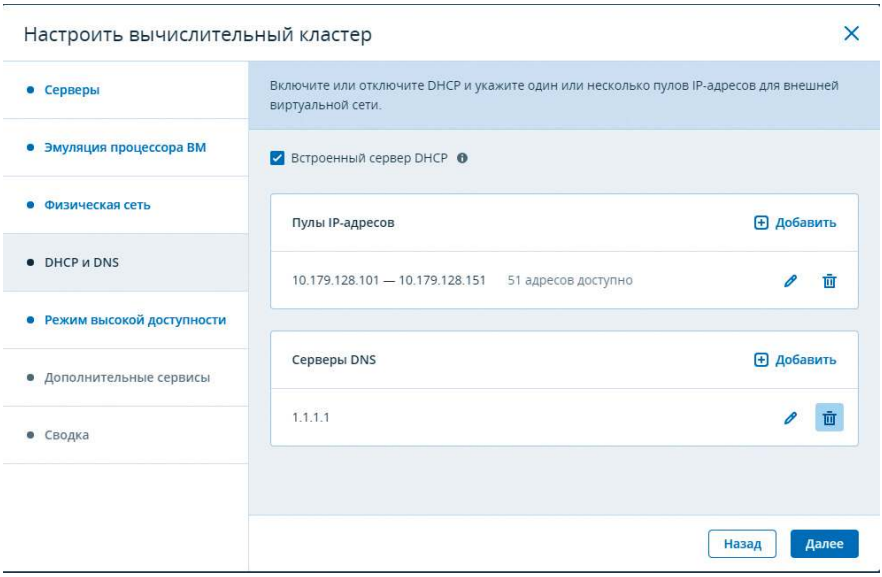
Нажать на кнопку «Создать вычислительный кластер». Выбрать сервер (единственный), тип виртуализации.

При наличии нескольких серверов разных моделей и поколений можно выбрать разную стратегию виртуализации. В нашем случае де-факто все варианты одинаковы. Оставить по умолчанию «Host-Model», нажать на кнопку «Далее».

Перейти к настройке физической сети, с возможностью выдавать виртуальным машинам «белые» IP-адреса для реализации прямого доступа в Интернет:

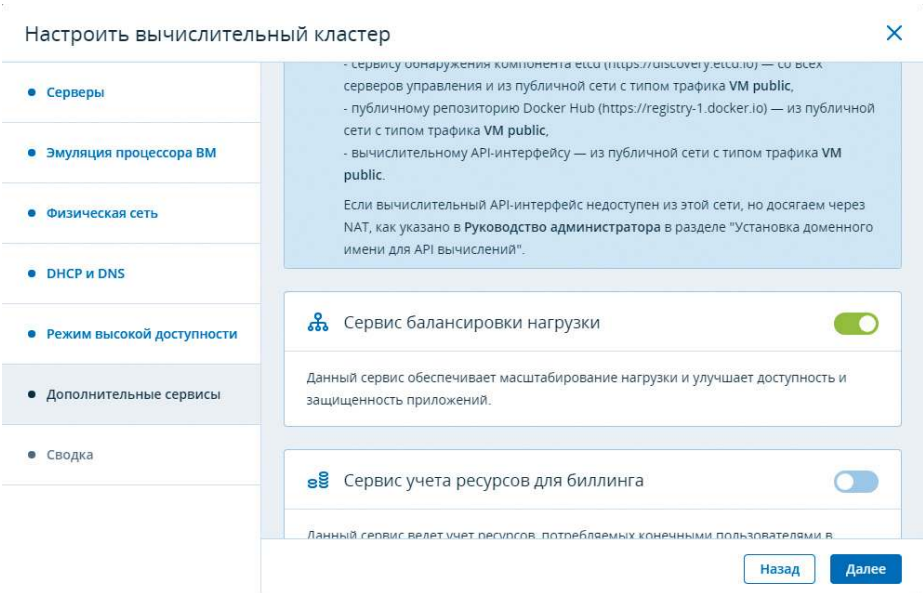


Затем настроить внутренний DHCP-сервер на выдачу адресов и параметров:



Настройки режима «Высокой доступности» оставьте «по умолчанию», поскольку используется только один сервер.

Перейти на вкладку «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.



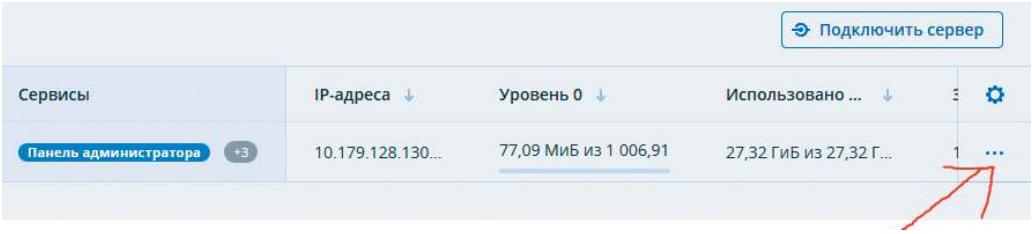
На вкладке последнего пункта «Сводка» будут отображены сводные данные выполненных настроек, проверьте правильность выбранных параметров.

Для завершения процесса создания кластера нажмите на кнопку «Создать кластер». Эта операция может также занять некоторое время, в зависимости от производительности «железа».

Подключение сервера

Теперь необходимо подключить к кластеру нашу ноду (сервер).

Перейти в «Инфраструктура» — «Серверы», выбрать нужный сервер в списке «Сервисы», нажать справа на кнопку с тремя точками, подключить сервер:

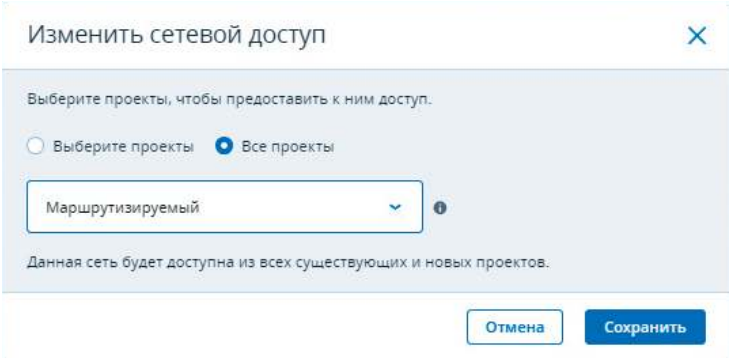


Настройка сети ВМ

В целях ограничения бесконтрольного доступа к физической сети выполните настройку сетевых параметров для виртуальных машин и пользователей проектов. Они будут получать доступ к физической сети на основе маршрутизаторов и плавающего IP.

Перейдите в «Вычисления» — «Сеть», выберите сеть «public», в открывшемся окне справа внизу — «Сетевой доступ» — «Изменить».

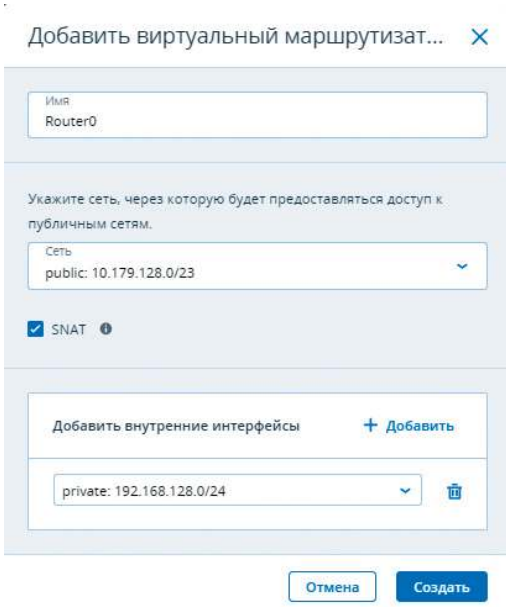
Из предложенных вариантов выбрать «Все проекты», тип доступа — маршрутизируемый, нажать на кнопку «Сохранить».



Перейти к настройке сети «private». Дважды щелкнуть кнопкой мыши на название, в правом нижнем углу открывшегося окна выбрать «Подсети».

Выбрать подходящие для решения нашей задачи параметры пула, DNS-сервера, установить адрес шлюза. Для примера на скриншоте ниже был выбран последний адрес в сети. Шлюз нужен обязательно, иначе не удастся создать маршрутизатор.

Сохранить параметры, вернуться назад, найти пункт меню «Маршрутизаторы», перейти к созданию нового маршрутизатора:



На этом базовая настройка системы закончена. В последующих разделах будут рассмотрены примеры настройки плавающих IP после появления пользователей в системе.

ДОМЕН. ПРОЕКТ. ПОЛЬЗОВАТЕЛИ

Создание домена и проекта

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

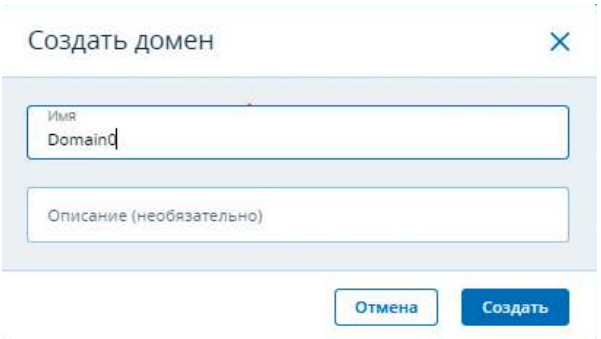
• **администратор** домена может управлять виртуальными объектами во всех проектах внутри назначенного домена, а также назначением проектов и пользователей на панели самообслуживания;

• **участник проекта** играет роль администратора проекта в определенном домене на панели самообслуживания. Участника можно назначить на несколь-

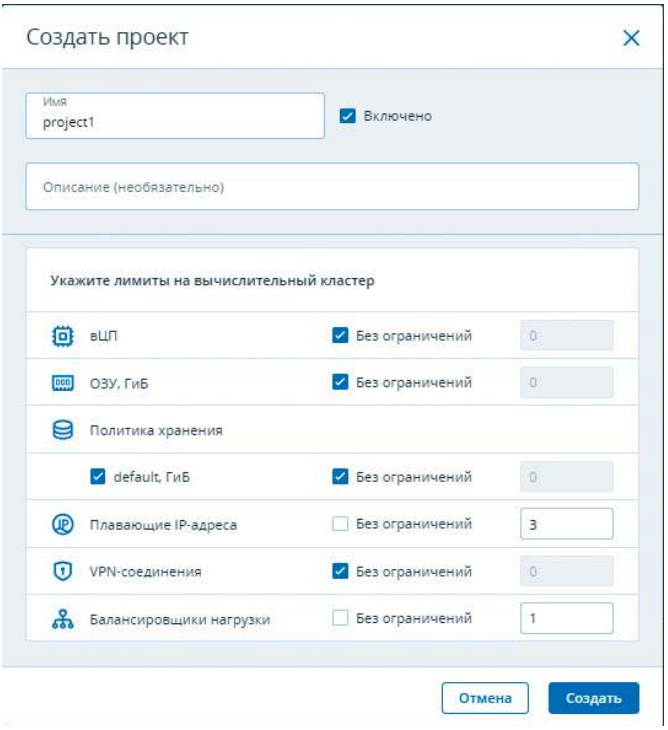
ко проектов, тогда он будет управлять виртуальными объектами во всех этих проектах. С проектами можно выполнить следующие действия:

- просмотреть и назначить квоты проектов;
- назначить участников на проекты.

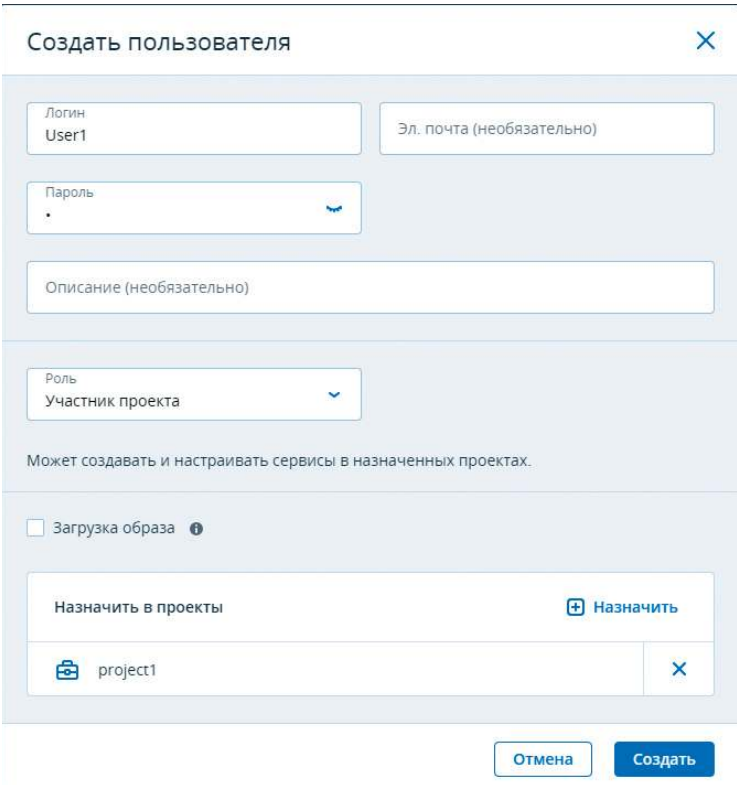
Для создания домена перейдите в меню «Настройки» — «Проекты и пользователи» — «Создать домен». Введите имя домена, нажмите на кнопку «Создать».



Выберите домен, создайте в нем проект: укажите имя, лимиты на ресурсы. На скриншоте ниже выбраны 3 плавающих IP и один балансировщик нагрузки (лимиты впоследствии можно изменить). Нажмите на кнопку «Создать».



Перейдите к диалоговому окну создания пользователя: введите логин, пароль, назначьте его в проект, созданный ранее, с ролью «Участник проекта». Нажмите на кнопку «Создать».



Следует обратить внимание, что при создании пользователя можно разрешить ему загружать образы ОС.

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.

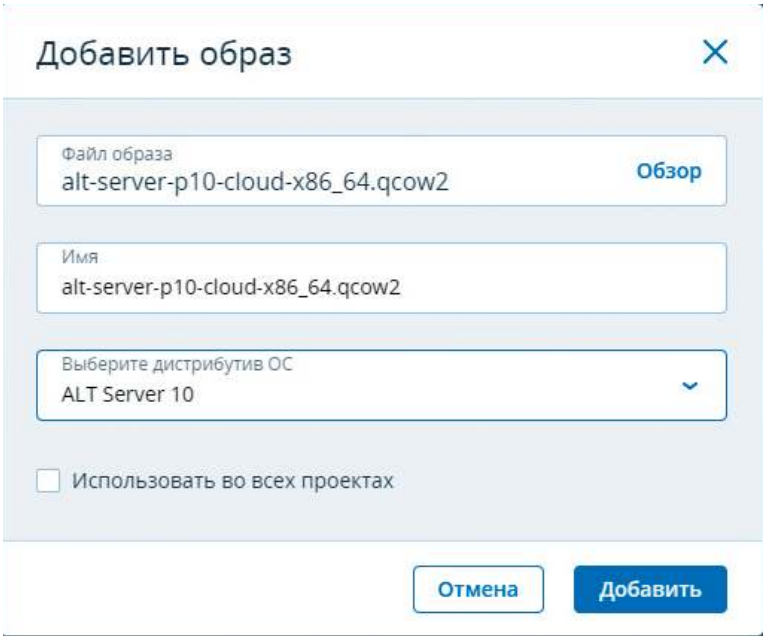
Напомним, что можно дать право скачивать образы и дистрибутивы ОС пользователям. Настройку образов можно выполнить в меню «Вычисления» — «Виртуальные машины», вкладка «Образы».

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:

Компания «Базальт СПО» подготовила удобный образ специально для облачной среды, уже с интегрированными сервисами Cloudbase-Init и OpenSSH Server (https://ftp.altlinux.org/pub/distributions/ALTLinux/p10/images/cloud/x86_64/alt-server-10.4-p10-cloud-x86_64.qcow2).

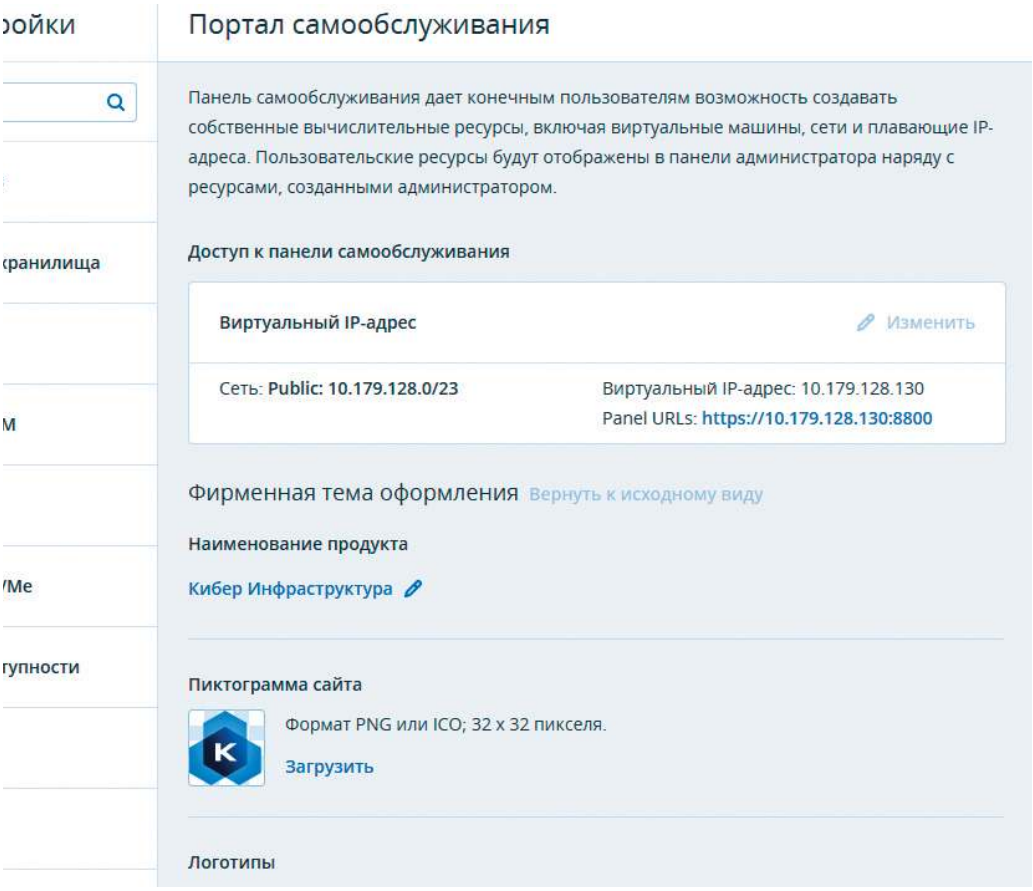
Добавьте образ ОС «Альт Сервер 10» в список доступных для использования или иной другой.



После загрузки образа перейдите в режим пользователя и переключитесь 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):



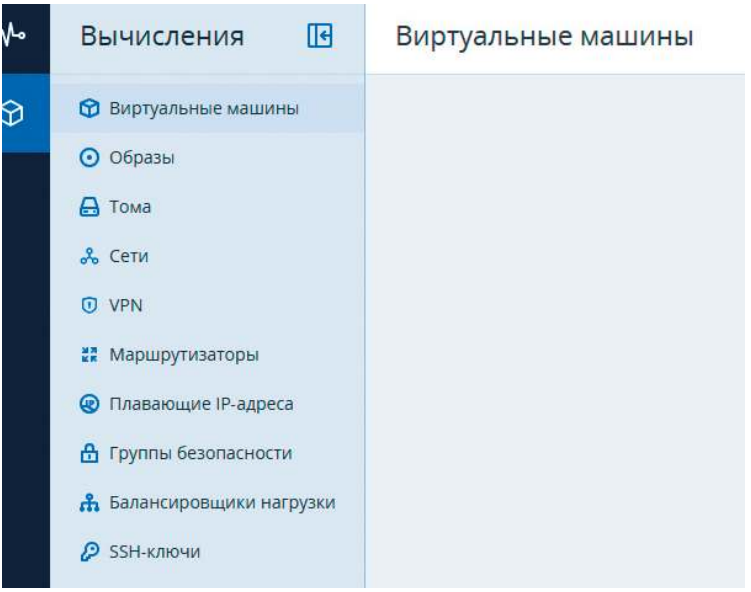
На вкладке «Панель самообслуживания» можно посмотреть адрес IP-панели, на скриншоте, приведенном выше, он совпадает с IP-адресом ноды. Порт по умолчанию — 8 800.

Перейдите по ссылке Panel URLs, откроется окно аутентификации, введите данные для доступа к панели самообслуживания: логин и пароль пользователя. При этом обратите внимание:

- 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, раскрывающихся в подменю: МОНИТОРИНГ (пока пустой) и Вычисления. Вычисления, в свою очередь, дают возможность создавать и управлять всеми доступными пользователю ресурсами.



Рассмотрим кратко 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 технология, 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.

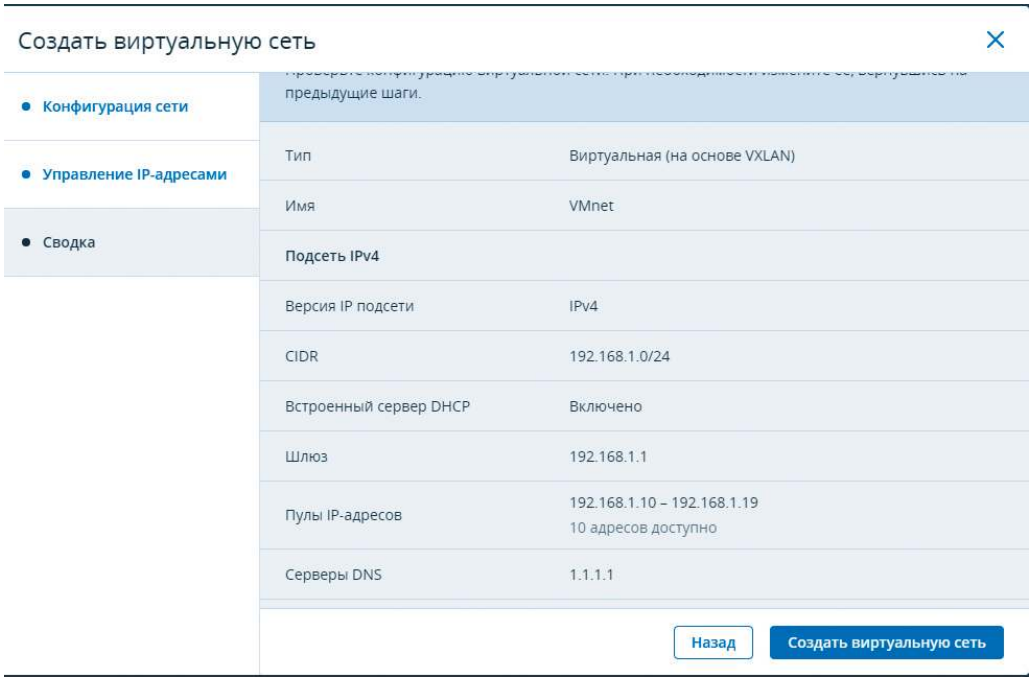
Группы безопасности — это наборы правил сетевого доступа, которые контролируют входящий и исходящий трафик виртуальных машин, назначенных в эту группу.

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

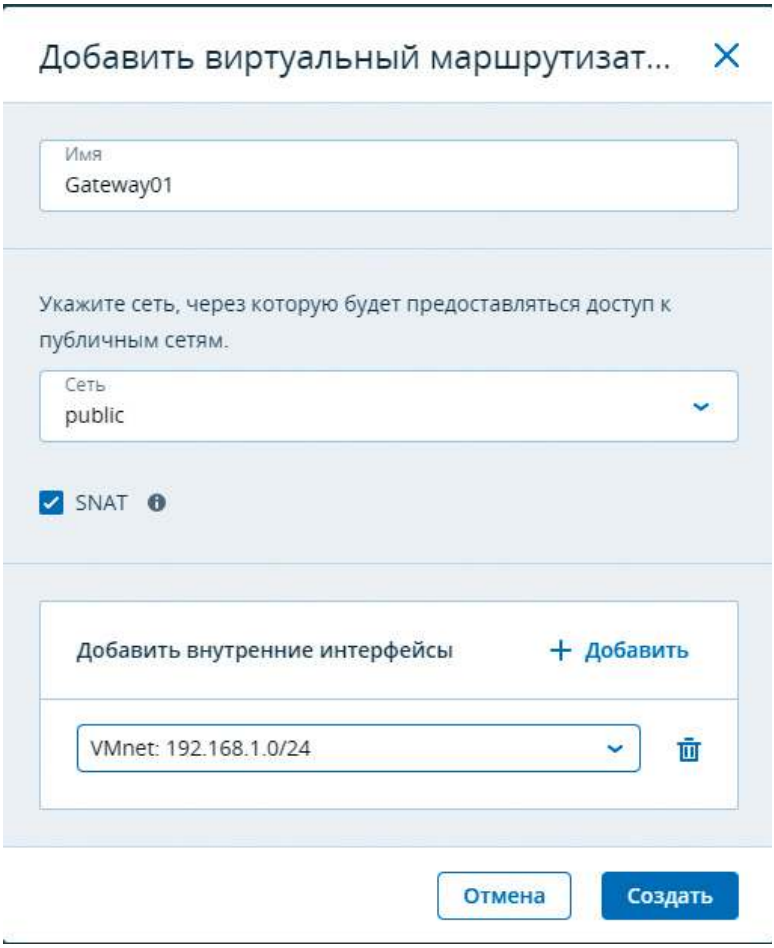
SSH-ключи применяются для защищенного SSH-доступа к виртуальным машинам.

Создание виртуальной машины

Первое, что необходимо сделать — создать внутреннюю виртуальную сеть, в которую будет добавлена ВМ. Перейдем в меню «Создать виртуальную сеть» (см. настройки сети на скриншоте ниже):



На следующем шаге необходимо создать маршрутизатор, через который ВМ будут получать доступ в Интернет:



Перейдите к этапу создания ВМ. Выберите меню «Виртуальные машины» — «Создать виртуальную машину»:

1. Задайте имя ВМ. Укажите, что она будет развернута из образа.

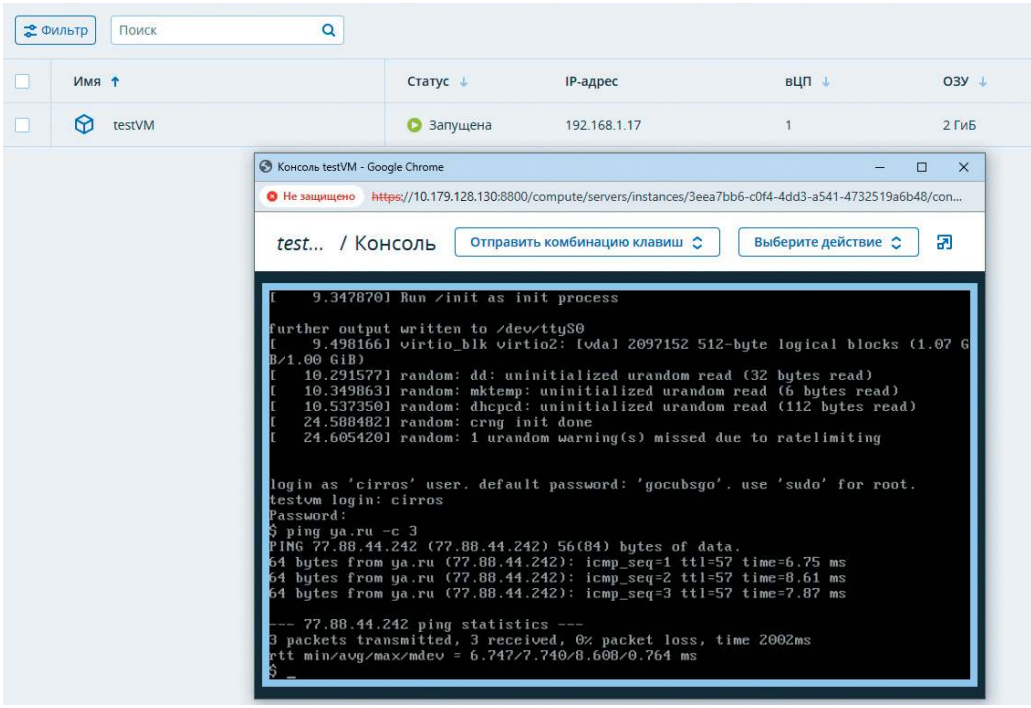
2. Выберите образ cirros.

3. Тип — это «размер» нашей ВМ, то есть количество ресурсов, которое будет выдано данной машине. Выберите small.

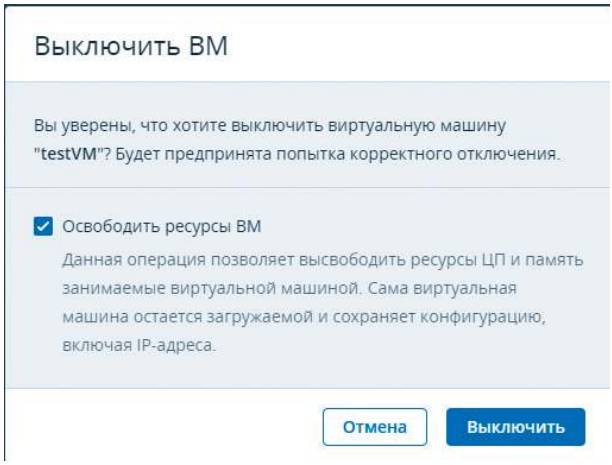
4. Добавьте сетевой интерфейс из созданной виртуальной сети на предыдущем шаге. Остальные параметры пока оставьте без изменения.

Нажмите кнопку «Развернуть». Дождитесь процесса завершения создания виртуальной машины.

Выбрав созданную ВМ, можно войти в консоль, ввести дефолтные логин/пароль (cirros/gocubsgo), войти в интерфейс ВМ и проверить доступ в Интернет:



Выключите ВМ и освободите ресурсы:

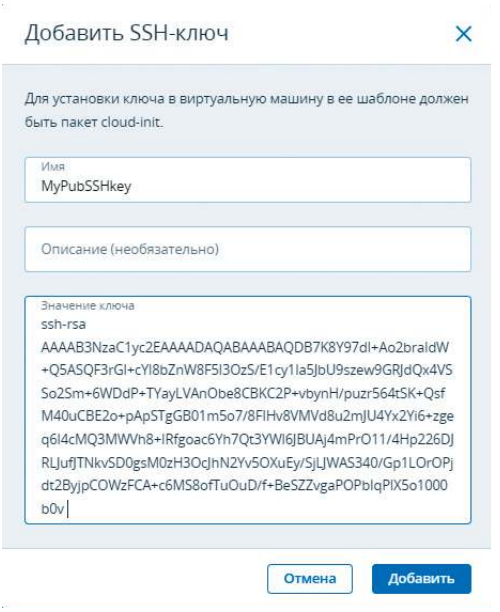


Однако доступ к этой ВМ есть только через виртуальную консоль.

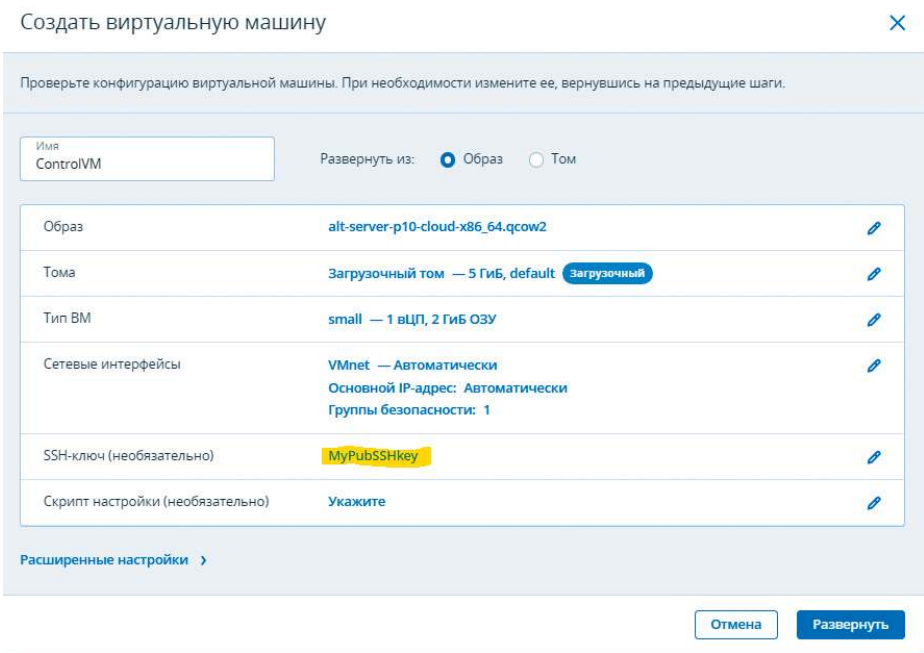
Создайте другую ВМ из образа «Альт Сервер 10», сконфигурируйте доступ к ней по SSH со своего компьютера. Для этоговыполните две дополнительные операции:

- добавьте публичный ключ SSH в виртуальную машину;
- подключите к ней плавающий IP.

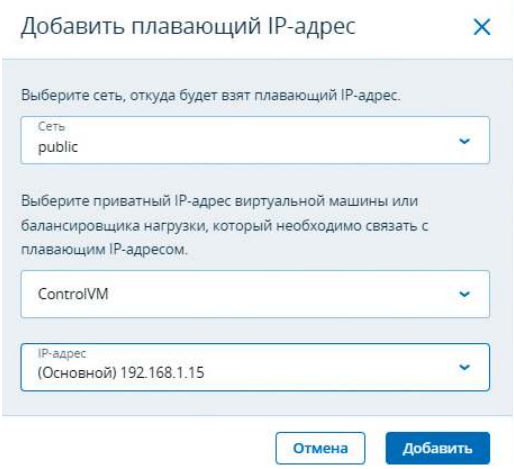
5. Перейдите в пункт меню «SSH ключи», выберите «Добавить SSH ключ», введите требуемые данные заранее созданного публичного ключа (например, командой ssh-keygen -t rsa или любым online генератором):



6. Создайте ВМ из образа «Альт Сервер 10». Добавьте публичный ключ:



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

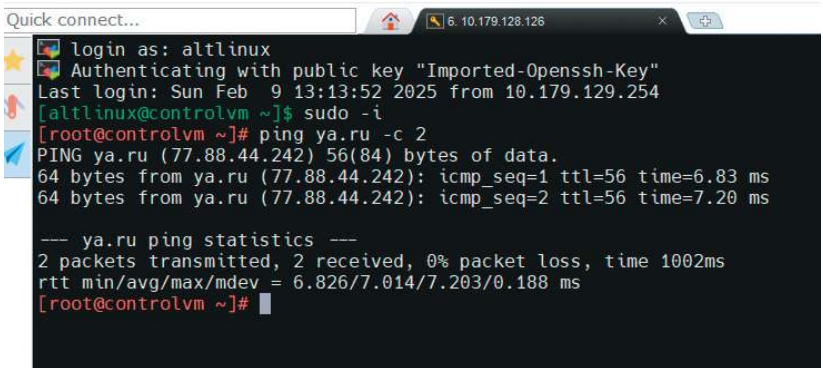


Теперь у нас есть «белый» IP, по которому можно получить доступ к ВМ ControlVM. Обратите внимание, для подключения по SSH необходимо использовать приватный ключ из пары, созданной ранее.

Далее будет использоваться утилита MobaXterm. В облачной версии «Альт Сервер 10» используется учетная запись «altlinux».

Для получения прав суперпользователя введите команду:

```
sudo -i
```

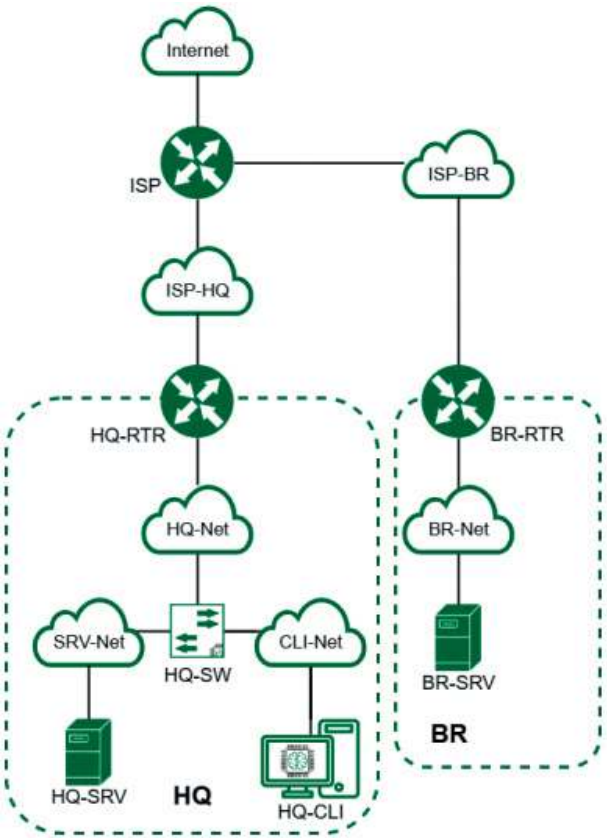


Таким образом, были выполнены настройки доступа к ВМ с рабочего места, виртуальная машина получила доступ в Интернет и, может быть, в дальнейшем использована для автоматизации развертывания инфраструктуры.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1

Инструкция по застройке стенда для Демонстрационного экзамена (ДЭ) КОД 09.02.06-1-2026 «Сетевое и системное администрирование»



Застройка стендов участников

Рекомендуемые действия и лист проверки технического эксперта площадки «Сетевое и системное администрирование» размещены в проверочном листе 1.

На одно рабочее место участника: 8 ядер ЦП, 10 ГБ ОП, крайне рекомендуется твердотельный накопитель, обеспечивающий линейное чтение от 450 МБ/с, скорость сетевого адаптера от 1 ГБ/с. При кластерном подходе к застройке площадки ядра ЦП и объем 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, протестированные на предмет работоспособности, стабильности и выполнимости задания ответственными лицами от застройщика площадки.

Общие рекомендации:

• необходимо обеспечить полную логическую изоляцию стендов участников друг от друга;

• крайне рекомендуется настроить квотирование ресурсов (нагрузка на стенд одного участника не должна 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 учетных записей, последующая проверка на корректность и функциональность;

• блокировка внешних подключений к решению виртуализации на время выполнения участниками задания и проведение экспертной оценки;

• блокировка учетных 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 участникам необходимо остановить виртуальные машины, относящиеся к Модулю 1, и запустить виртуальные машины Модулей 2 и 3.

Виртуальную машину BR-DC для выполнения Модуля 3 в целях оптимизации ресурсов участник включает в тот момент, когда она ему понадобится.

Рекомендуется настроить две учетные записи участникам: одну — для Модуля 1, вторую — для Модулей 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 еще 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, 8 ГБ ОП с частотой от 2,6 ГГц, твердотельный накопитель.

Рекомендуемые действия и лист проверки технического эксперта площадки «Сетевое и системное администрирование» размещены 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 учетные 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, участники также 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 Модулей 2 и 3.

Проверочный лист 2. День Д1:

• пароли учетных записей изменены;

• виртуальные машины Модуля 1 включены, виртуальные машины Модулей 2 и 3 выключены;

• выполнение Модуля 1;

• технический перерыв, дезактивация учетных записей Модуля 1, активация учетных 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 Модулей 2 и 3;
• выполнение 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 российских дистрибутивов Linux: ОС «Альт», 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 приемы 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 оценки 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 одного раза, 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

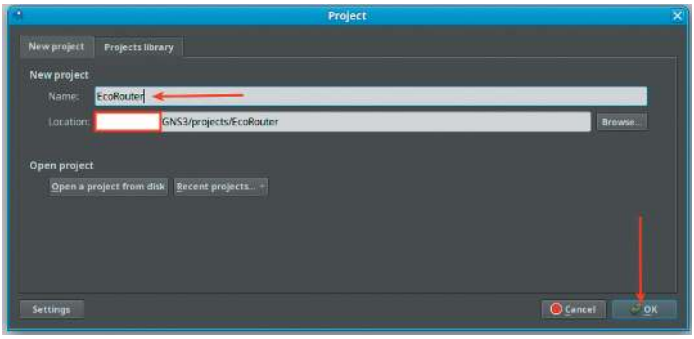
Установка EcoRouter в GNS3

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

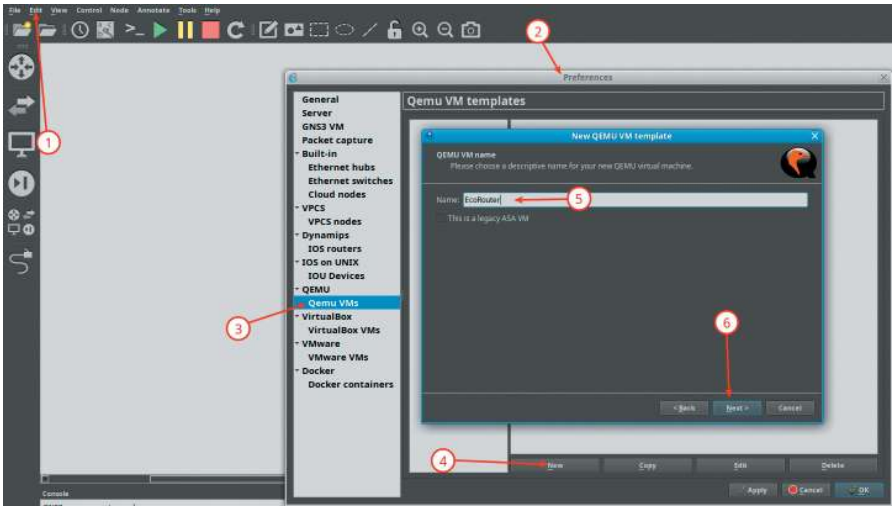
В операционных средах Linux/MAC EcoRouter работает под управлением GNS3.

Рассмотрим пример.

После открытия GNS3 создайте проект:



Далее нажмите Edit, затем выберите Preferences, перейдите на вкладку Qemu VMs. После чего нажмите New, задайте значение поля Name для нового шаблона, нажмите Next:

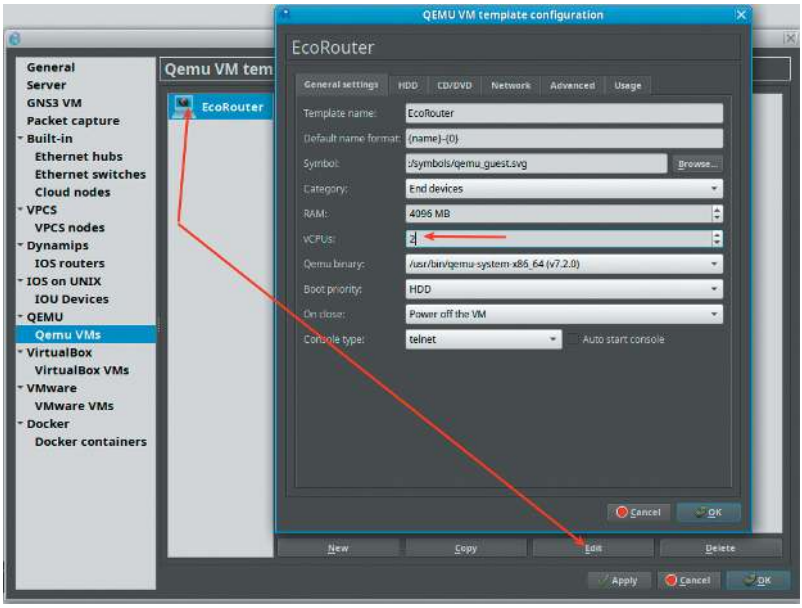


Задайте необходимый объем ОЗУ (минимальное значение 4096) и нажмите Next.

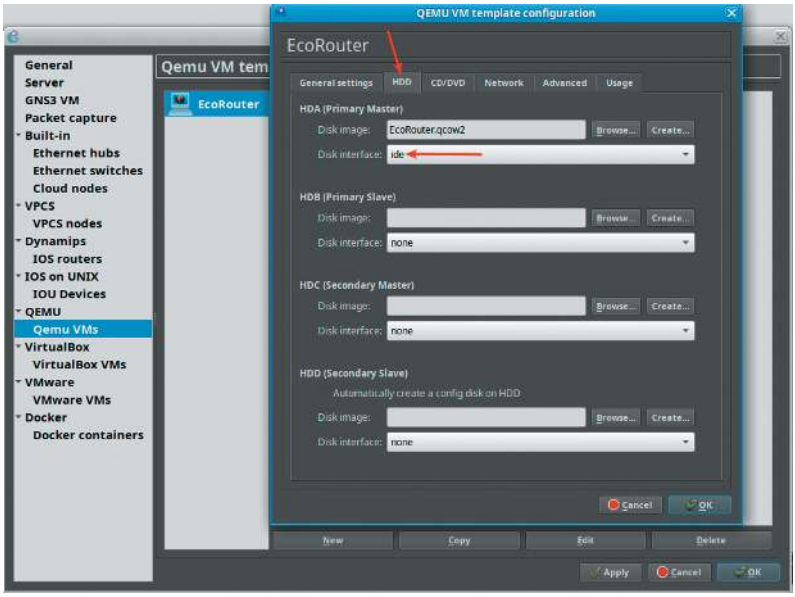
Выберите необходимый тип консоли (telnet) и нажмите Next.

Выберите Existing image (существующий образ ранее был помещен в директорию GNS3/images/QEMU) и нажмите Finish.

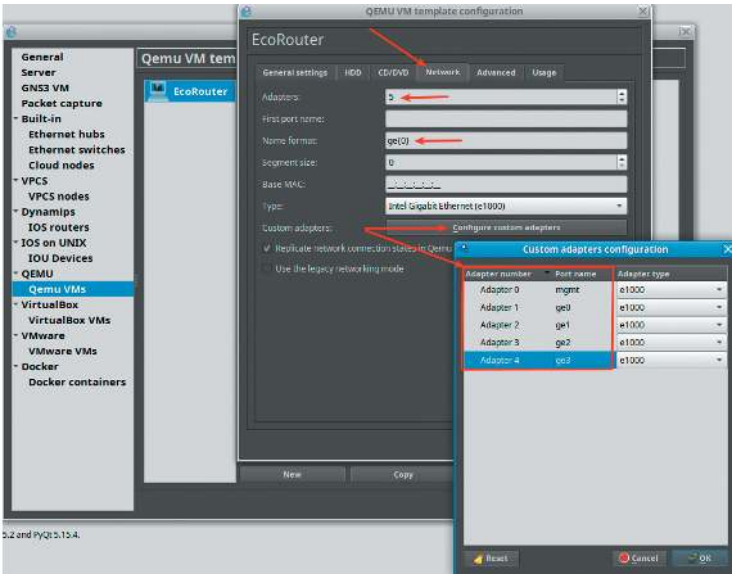
Выберите только что созданный шаблон и нажмите Edit. Далее на вкладке General settings задайте необходимое количество vCPUs (минимально необходимое — 2):



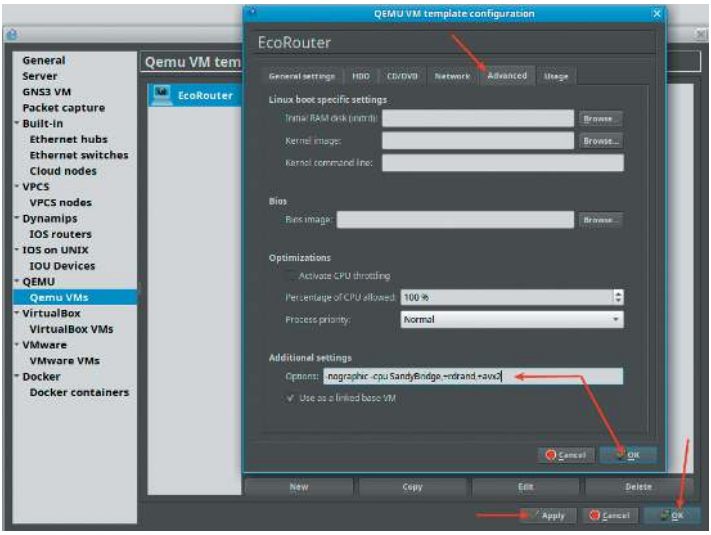
На вкладке HDD выберите в качестве Disk interface — ide:



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



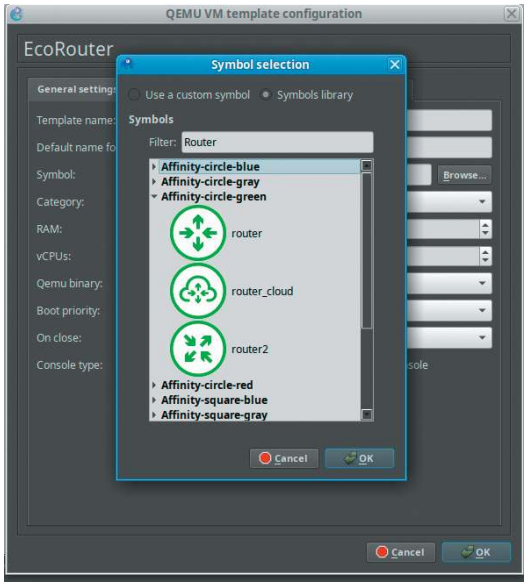
На вкладке Advanced в секции Additional settings передайте правильные Options (-nographic -cpu SandyBridge,+rdrand,+avx2), затем последовательно нажмите кнопки: OK, Apply, OK:



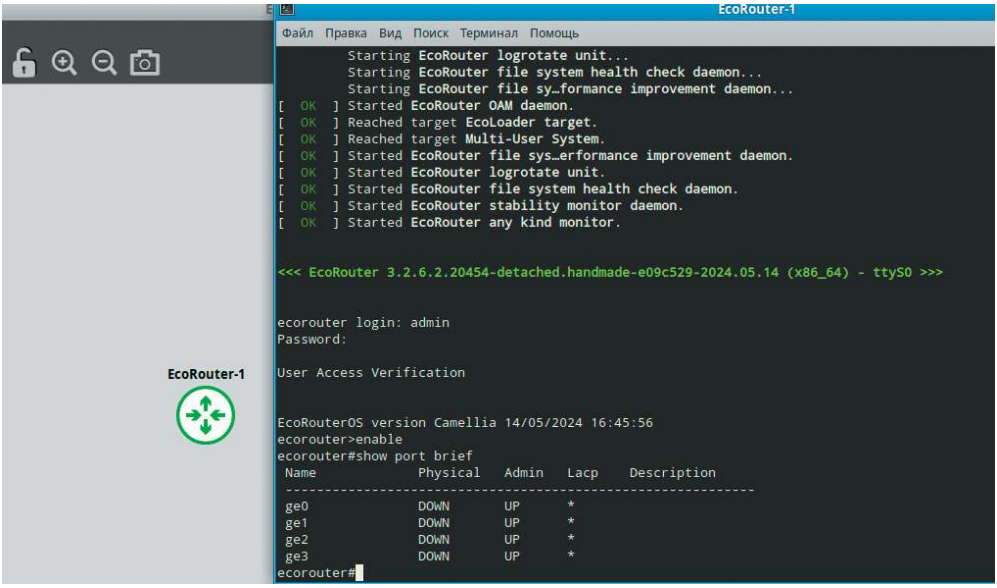
Важное замечание: нужно указать тип BIOS виртуальной материнской платы EcoRouter (-machine pc-q35-6.2), может понадобиться для работы

с более свежими версиями QEMU и GNS3. Тогда на вкладке Advanced в секции Additional settings нужно передать правильные Options (-nographic -cpu SandyBridge,+rdrand,+avx2 -machine pc-q35-6.2).

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



Добавьте EcoRouter в топологию и проверьте работоспособность (логин: пароль по умолчанию admin:admin):



Для того чтобы убедиться, что маршрутизатор загружен верно и дата-плейн загружена корректно, используйте команду:

```
- show hw status | exclude running
```

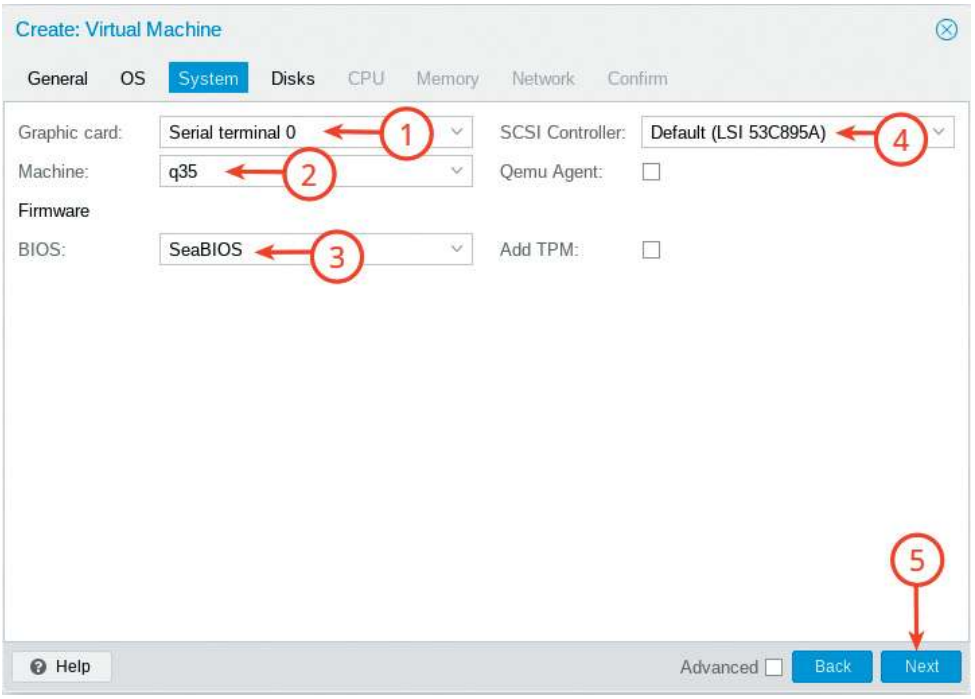
В полном выводе не должно быть failed сервисов. Для тестовых виртуальных машин это может быть важно, так как если не указать 2 vCPU -, то машина загрузится и интерфейсы будут иметь статус «up», но работать не будут.

Установка EcoRouter в «Альт Виртуализация» (редакция PVE)

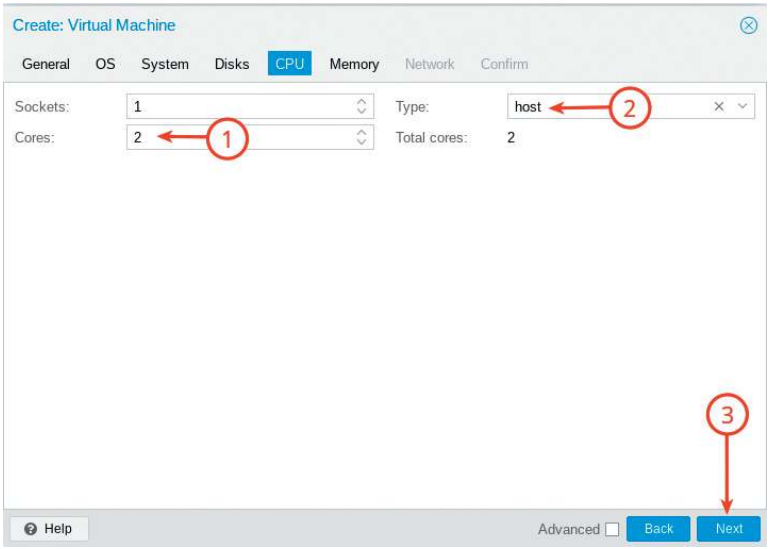
В веб-интерфейсе ОС «Альт Виртуализация» для создания виртуальной машины нажмите Create VM, задайте необходимое имя (Name), нажмите Next.

На следующем этапе (OS) выберите «Do not use any media» (не использовать никаких носителей) и нажмите Next.

На этапе System задайте необходимые для корректной работы настройки и нажмите Next:

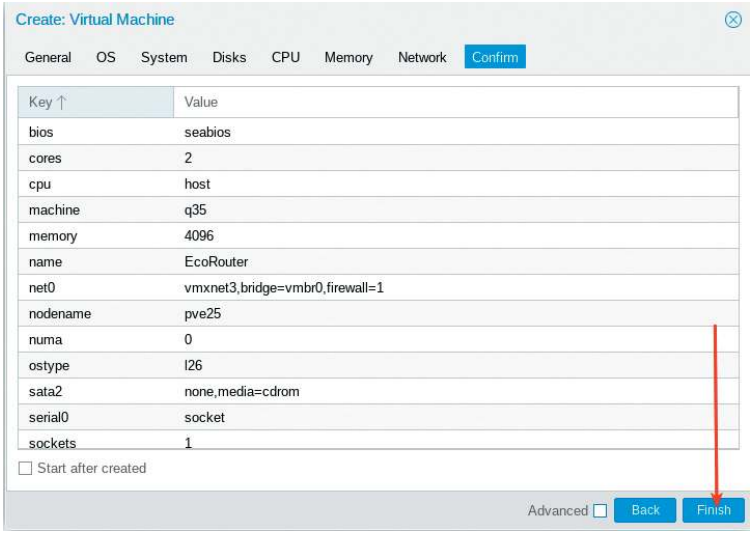


На этапе Disk удалите scsi0 и нажмите Next. На этапе CPU задайте необходимое количество (минимально необходимое для работы — 2), в поле Type выберите значение host, нажмите Next:



На этапе Memory задайте необходимый объем (минимально необходимое для работы — 4 ГБ) и нажмите Next.

Проверьте заданные ранее параметры для создаваемой виртуальной машины и нажмите Finish:

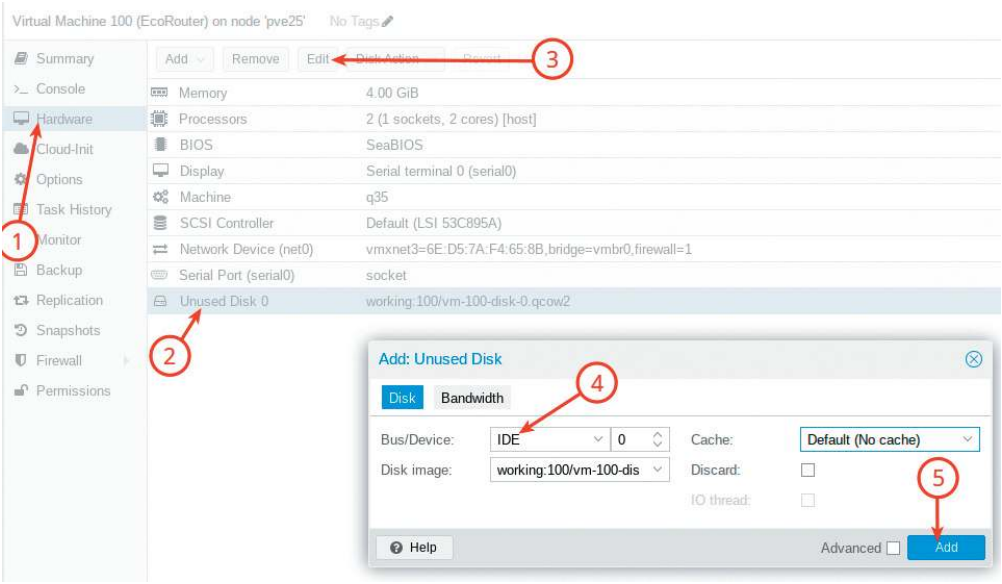


Перейдите в консоль PVE и выполните подключение существующего образа диска EcoRouter к только что созданной ВМ с помощью команды:

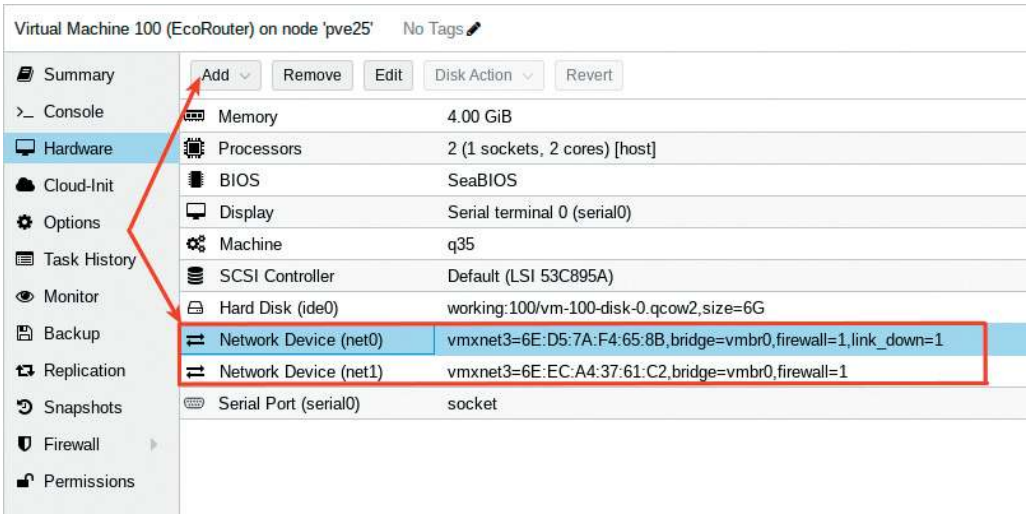
```
qm disk import 100 /home/admin/Загрузки/EcoRouter.qcow2 working
--format qcow2
```

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

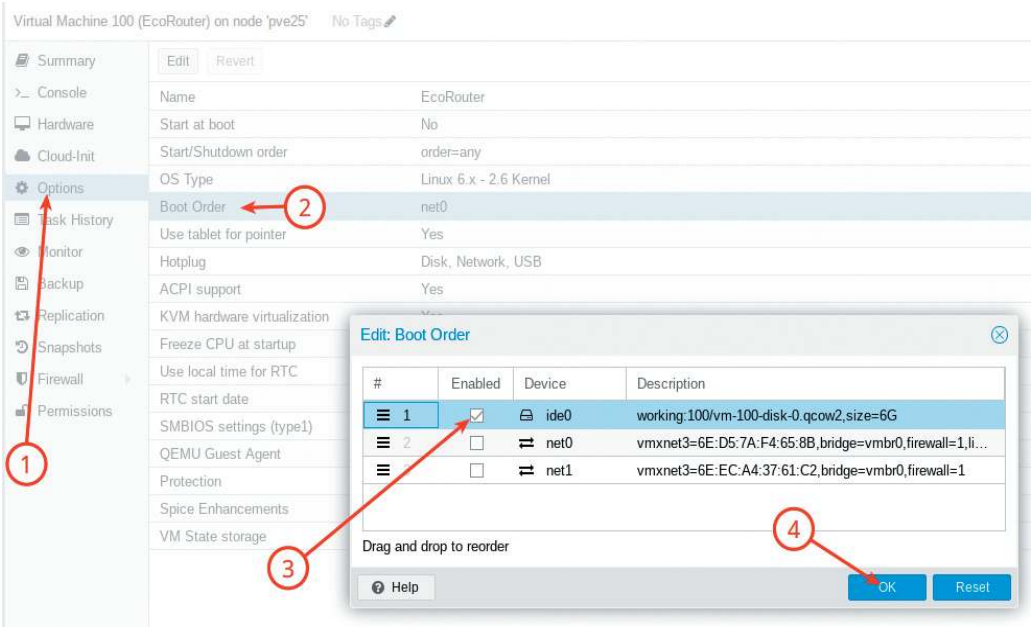
Перейдите в настройки созданной ВМ на вкладке Hardware, выберите только что импортированный диск и нажмите Edit, затем выберите IDE и нажмите Add:



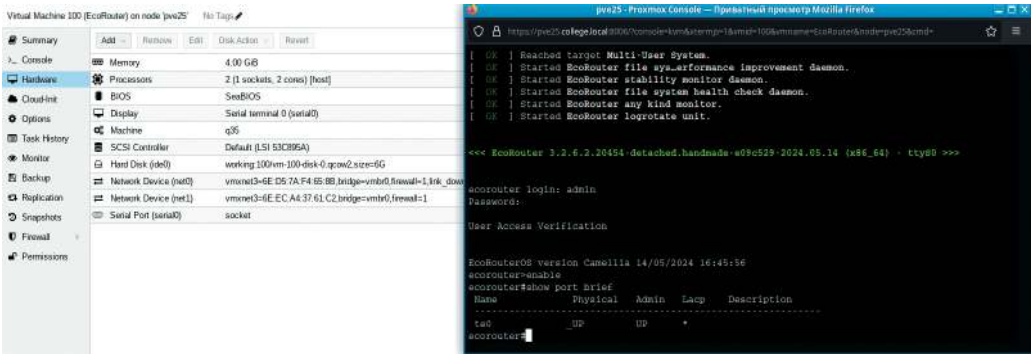
Для корректной работы необходимо добавить еще один интерфейс (который можно выключить), он будет использоваться в EcoRouter в качестве mgmt:



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



Запустите ВМ и проверьте 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 мин.

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 задания баннерного сообщения воспользуйтесь 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 разберемся 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 обрабатывать тегированный или нетегированный 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 удаленного 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
```

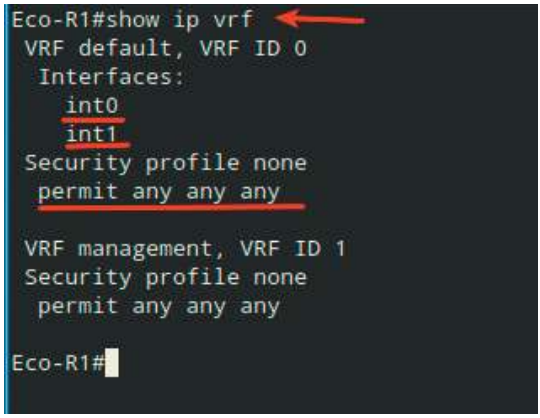
В отличие от профиля безопасности default профиль безопасности none не содержит каких-либо запрещающих правил.

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 расчета 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 условий 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 отключен 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 1 000	Intel Core i7, Xeon-E, Xeon Scalable от 8 ядер или совместимый	32 ГБ	480 ГБ	2 шт.
от 1 000 до 3 000	Intel Xeon Silver 4214R или совместимый	64 ГБ	480 ГБ	2 шт.
от 3 000	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 «Лаборатория Касперского».

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

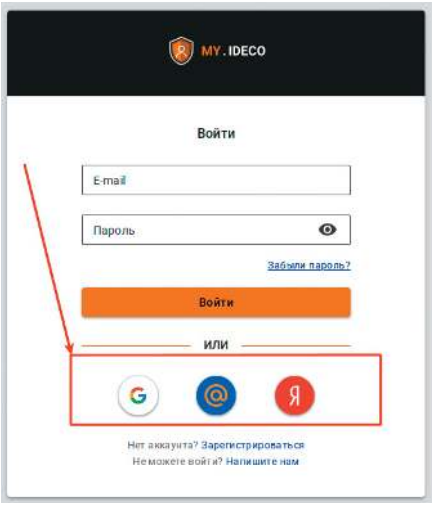
Таким образом, для корректной работы всех модулей фильтрации Ideco NGFW необходимо, чтобы доступ к вышеуказанным ресурсам был разрешен настройками фильтрации.

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.

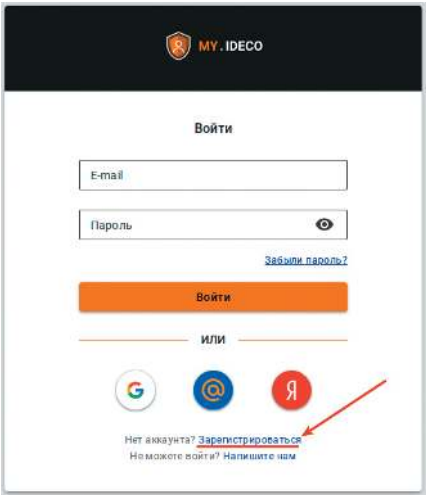
Зарегистрировавшись на my.ideco.ru, вы сможете управлять лицензиями, скачивать загрузочные образы всех продуктов, разрабатываемых компанией Ideco.

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

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

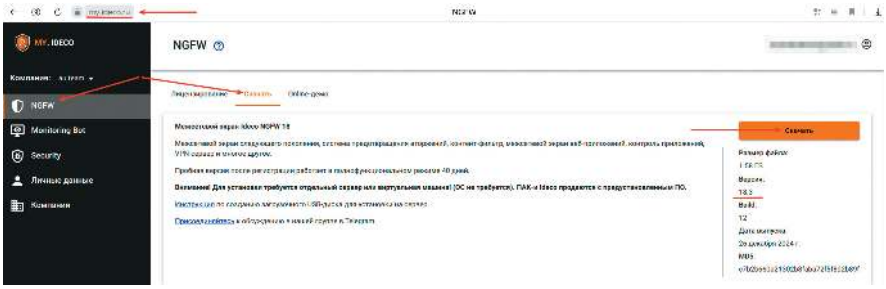


2. Выполнить процедуру полноценной регистрации, нажав на ссылку «Зарегистрироваться»:



После 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 про-

дукта 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:

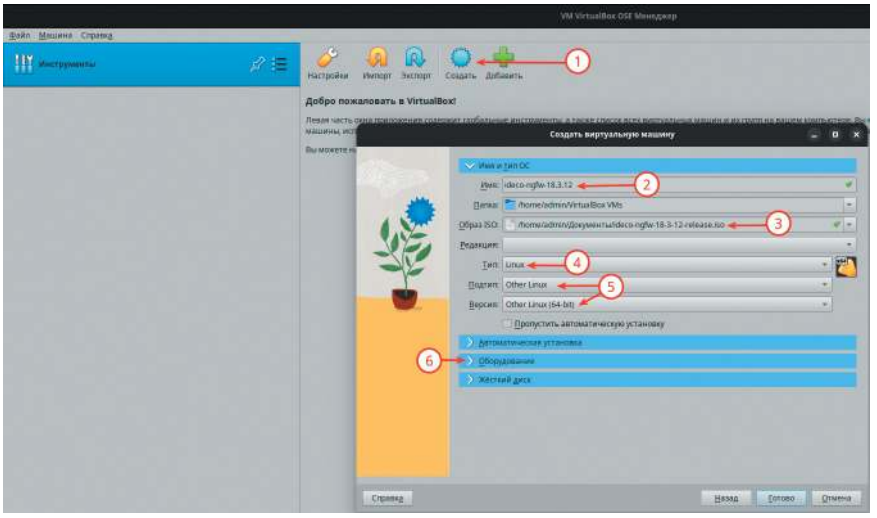
• об имеющихся лицензиях (раздел «Лицензирование»);

• о сроке окончания подписки на обновления модулей и технической поддержки.

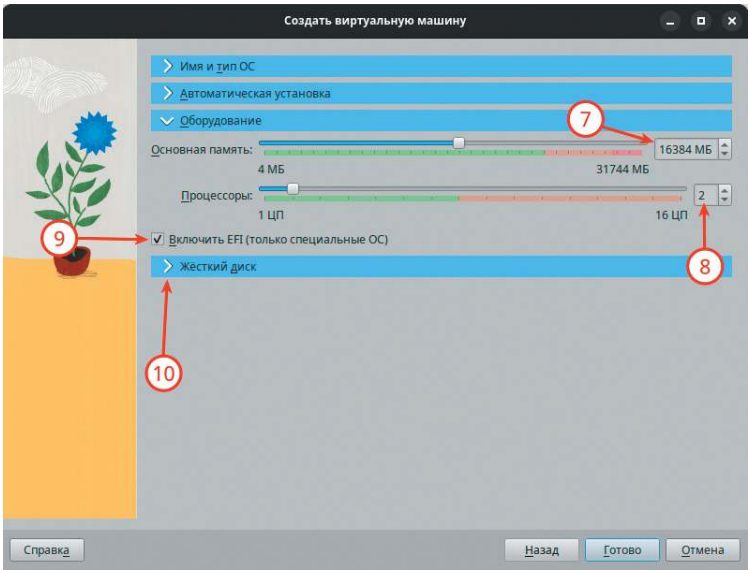
Установка Ideco NGFW в VirtualBox

Рассмотрим пример создания виртуальной машины в VirtualBox для установки Ideco NGFW:

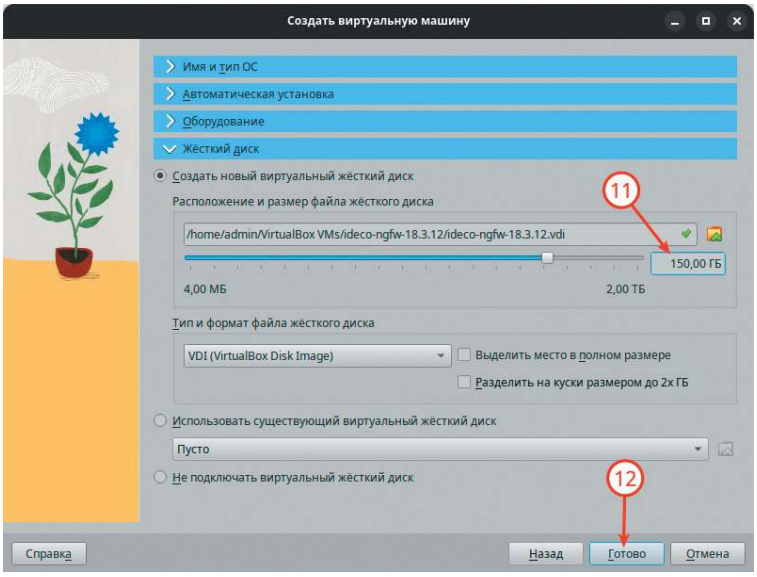
1. В VirtualBox в главном окне «Инструменты» нажмите кнопку «Создать».
2. Задайте имя для создаваемой виртуальной машины, например: ideco-ngfw-18.3.12.
3. Укажите путь до установочного образа с Ideco NGFW в формате iso.
4. В списке «Тип» выберите Linux.
5. В списке «Версия» выберите Other Linux (64-bit).



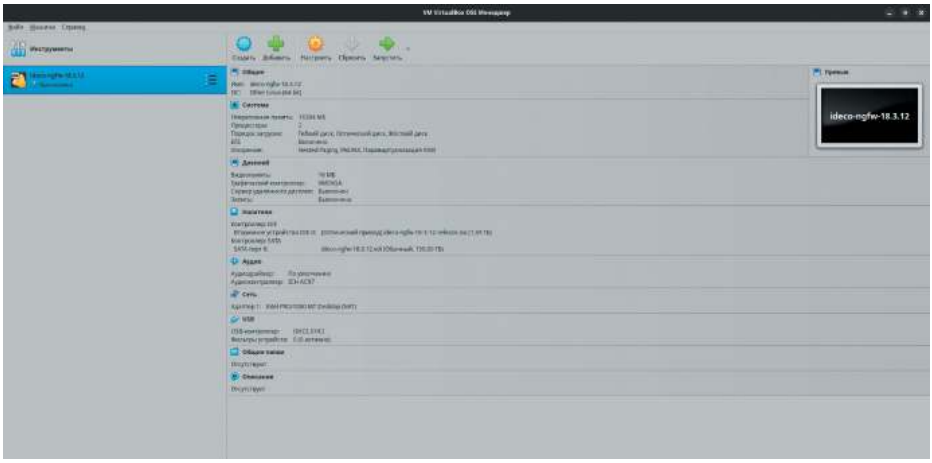
6. Нажмите «Оборудование».
7. Укажите минимально необходимый объем «Основной памяти» (ОЗУ/RAM) 16 ГБ.
8. Задайте произвольное количество vCPU, например 2.
9. Выставите чек-бокс «Включить EFI».
10. Нажмите «Жесткий диск».



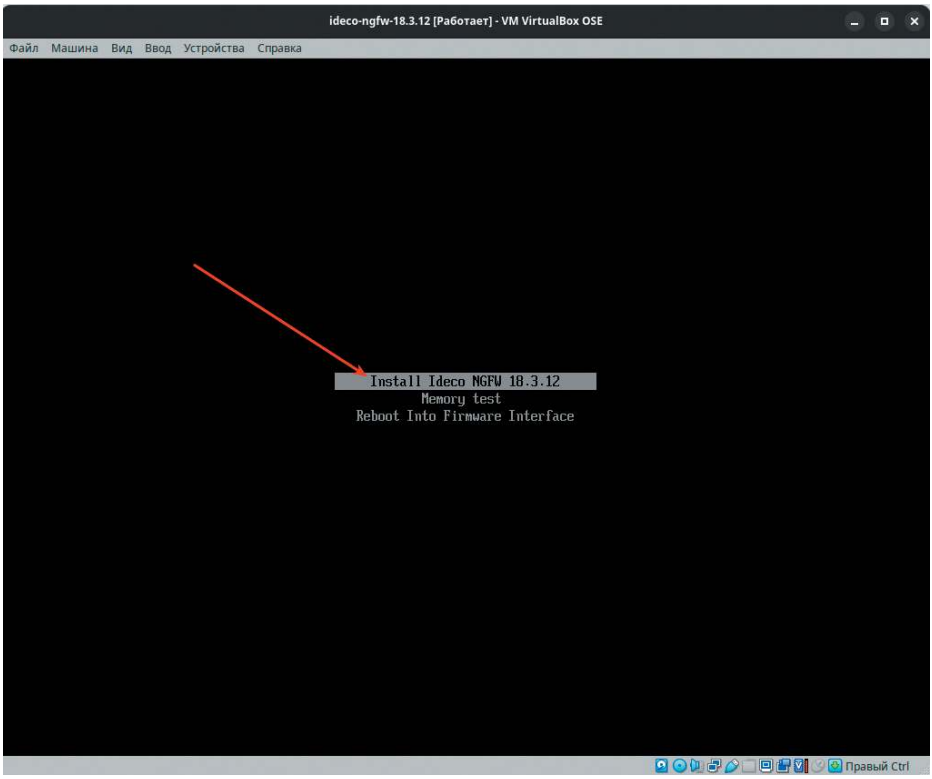
11. Задайте минимально необходимый размер дискового пространства 150 ГБ.
12. Нажмите на кнопку «Готово».



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



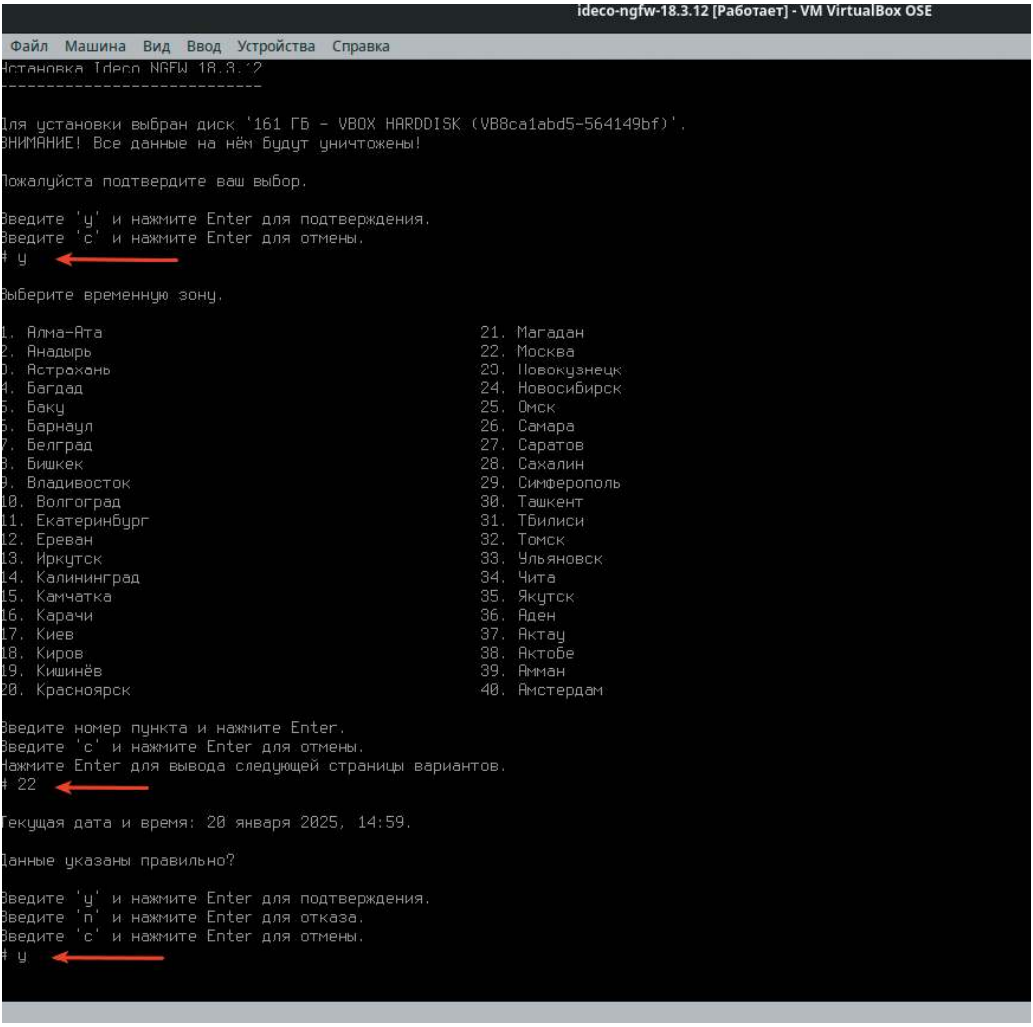
Запустите виртуальную машину. Выберите стрелками на клавиатуре пункт меню Install Ideco NGFW и нажмите Enter (важно, чтобы была отключена опция Secure Boot в UEFI):



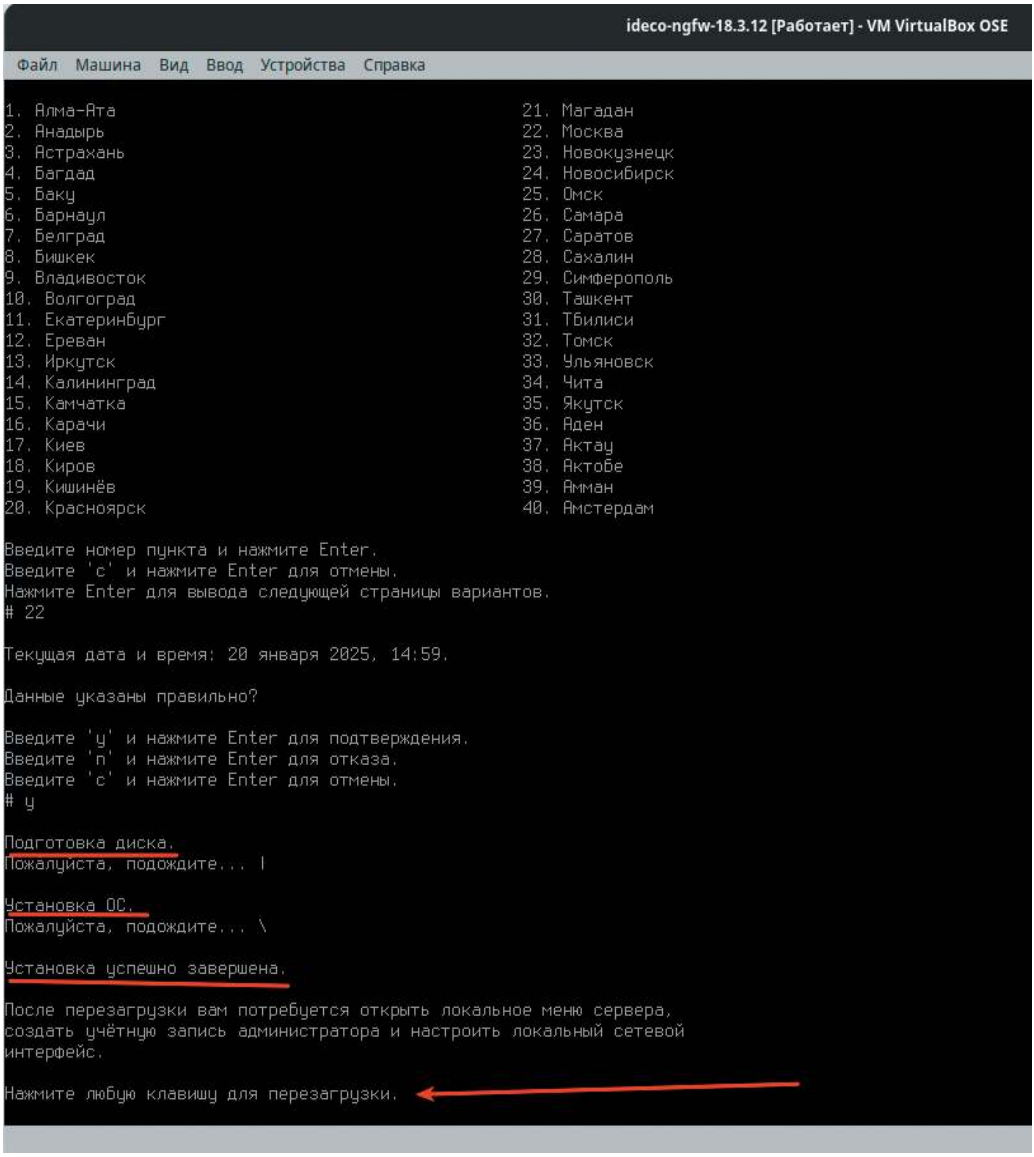
После чего начнется процесс установки Ideco NGFW на виртуальную машину.

На первый вопрос в качестве подтверждения того, что данные на диске будут уничтожены, ответьте утвердительно. Для этого введите с клавиатуры «y» и нажмите Enter.

Выберите необходимую временную зону: для зоны «Москва» введите «22» (на выбор доступны 40 зон, с которыми можно ознакомиться на скриншоте) и нажмите Enter. Проверьте корректность текущей даты и времени, после чего для подтверждения введите с клавиатуры «y» и нажмите Enter.



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



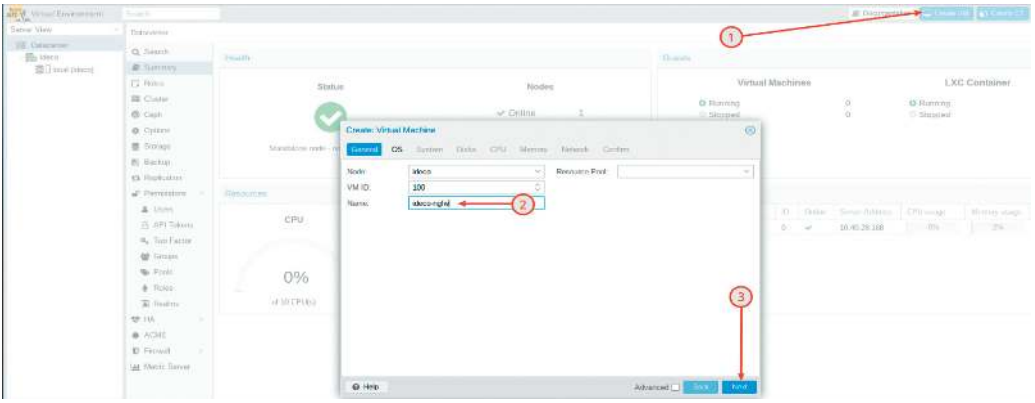
После перезагрузки появится приглашение входа в терминал. Не пытайтесь выполнять вход из-под какого-либо пользователя.

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

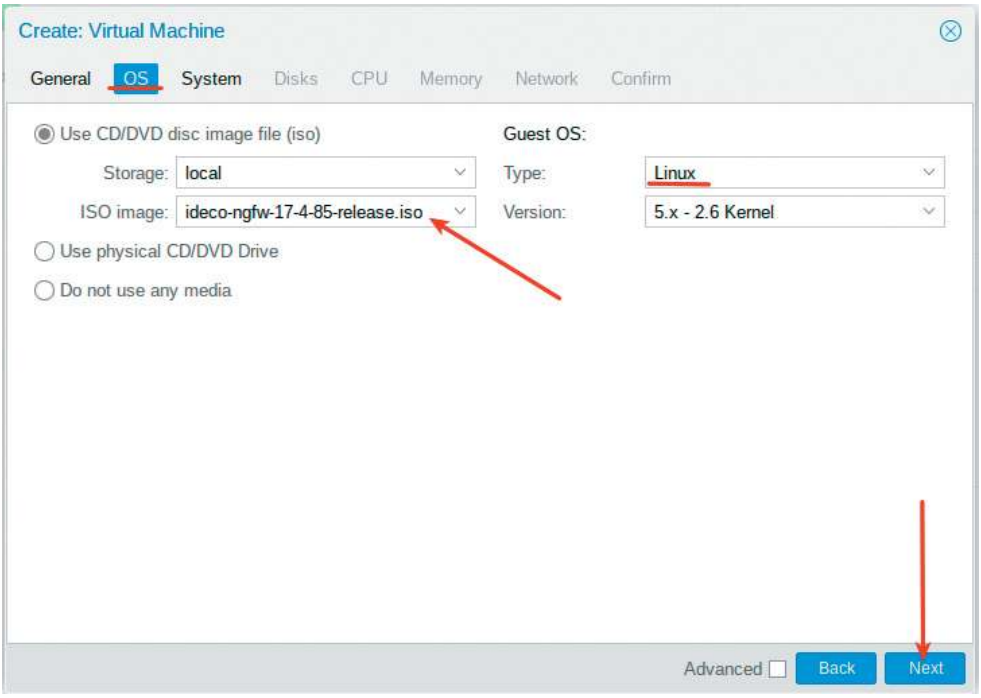
Примечание. На данном этапе при необходимости можно выполнить создание шаблона виртуальной машины с установленным Ideco NGFW, для этого необходимо выключить виртуальную машину. Текущее состояние виртуальной машины наилучшим образом подходит для создания шаблона.

Установка Ideco NGFW в «Альт Виртуализация» (редакция PVE)

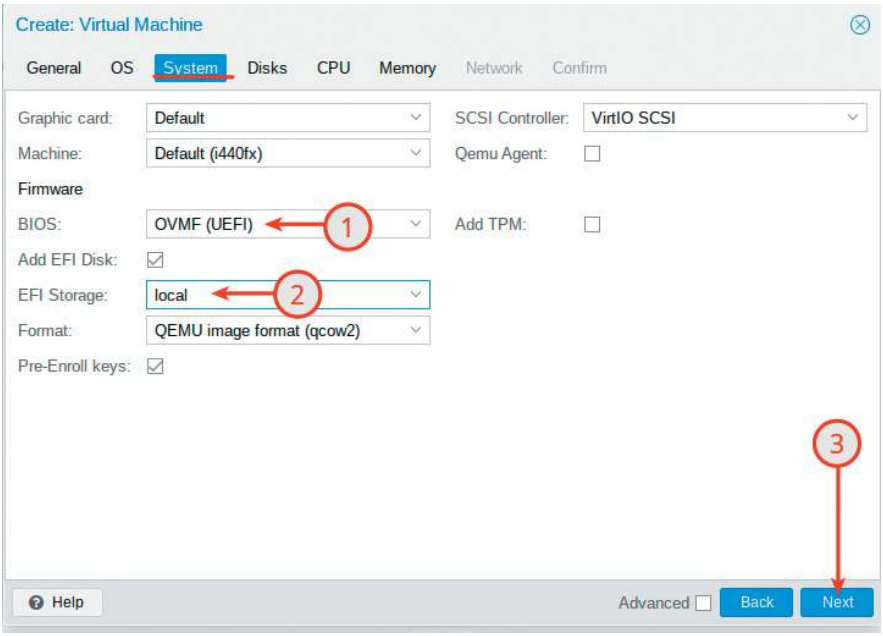
В веб-интерфейсе «Альт Виртуализация» (редакция PVE) нажмите Create VM, после чего задайте имя виртуальной машины (в данном случае имя ideco-ngfw) и нажмите Next:



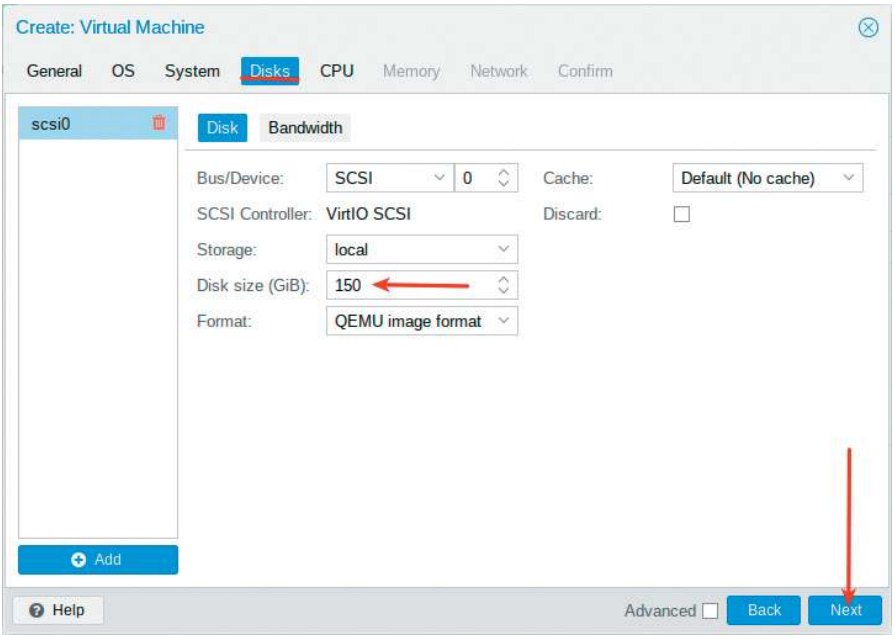
На вкладке OS оставьте в качестве типа гостевой ОС (Guest OS) Linux, а в качестве установочного образа (ISO image) выберите ранее скачанный и загруженный в хранилище «Альт» PVE ISO образ Ideco NGFW:



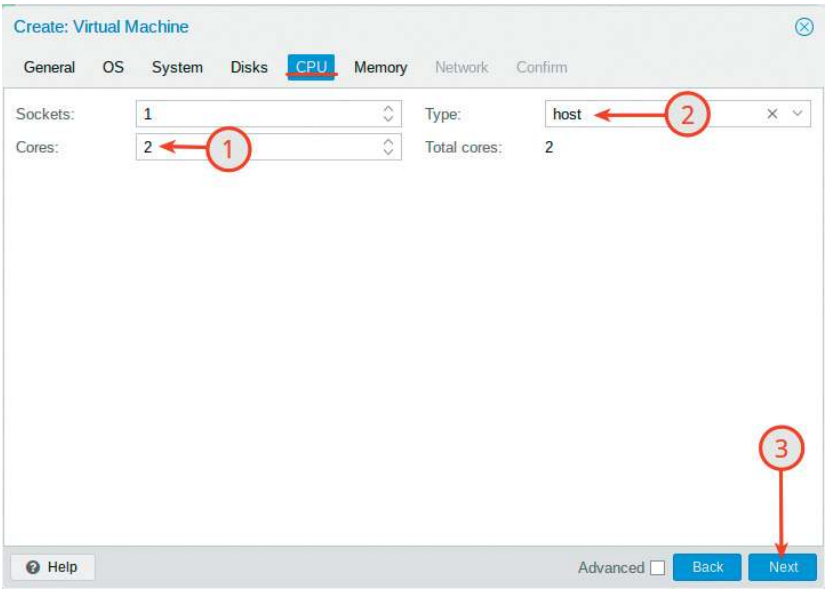
На этапе System выберите в секции BIOS поддержку UEFI, укажите локальное хранилище «Альт» PVE с именем local для хранения диска EFI и нажмите Next:



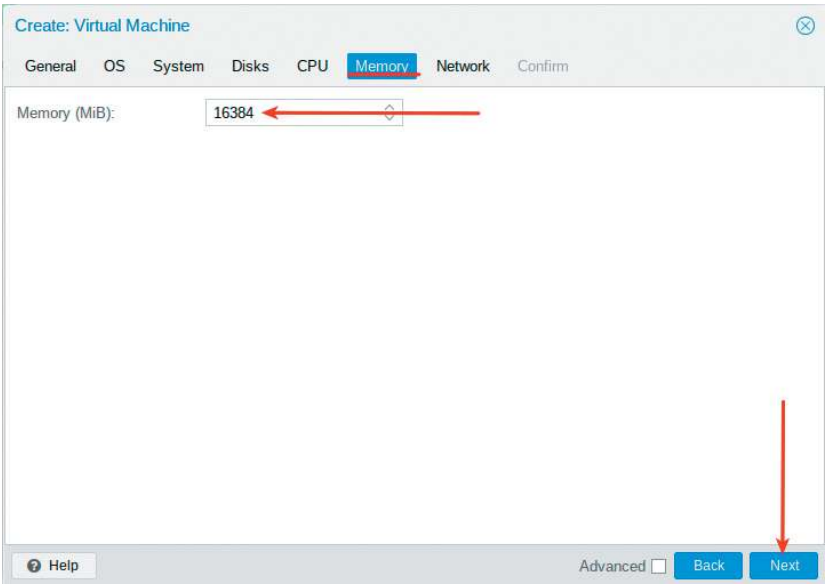
На этапе Disks задайте размер виртуального жесткого диска согласно минимально необходимому объему для установки Ideco NGFW в 150 ГБ и нажмите Next:



На этапе CPU задайте параметр количества ядер (Cores): 2, а в качестве типа выберите host (т.к. необходима поддержка SSE 4.2) и нажмите Next:

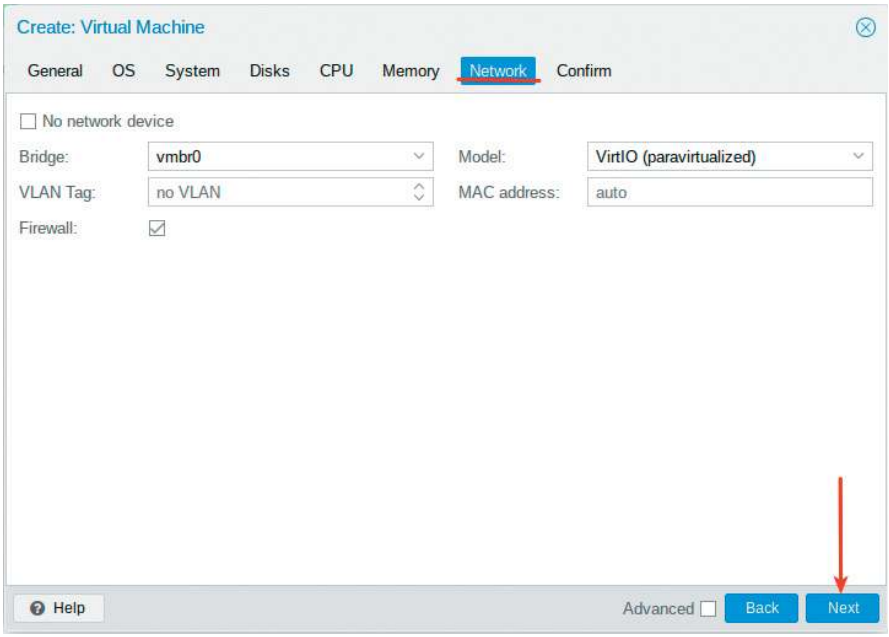


На этапе Memory задайте размер ОЗУ согласно минимально необходимому объему для установки Ideco NGFW в 16 ГБ и нажмите Next:

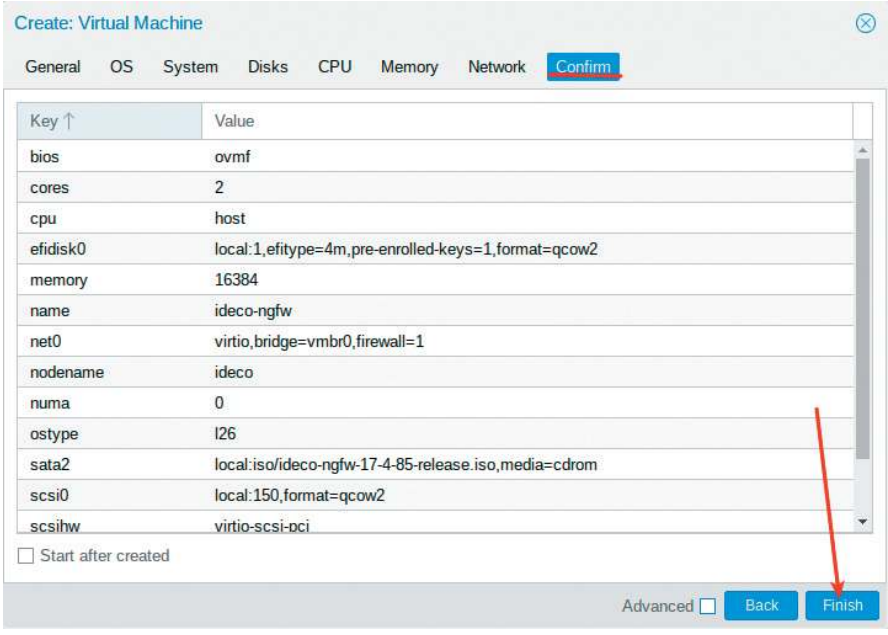


На этапе Network оставьте Bridge vmbr0 по умолчанию и нажмите Next. Далее сетевой интерфейс с именем vmbr0 будет использоваться для доступа

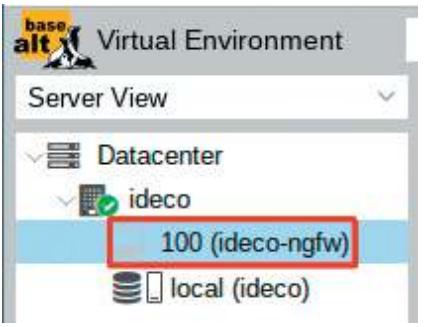
в сеть Интернет. Для локальной сети в дальнейшем необходимо дополнительно добавить Bridge с именем vmbr1.



На этапе Confirm проверьте ранее заданную конфигурацию виртуальной машины и нажмите Finish:



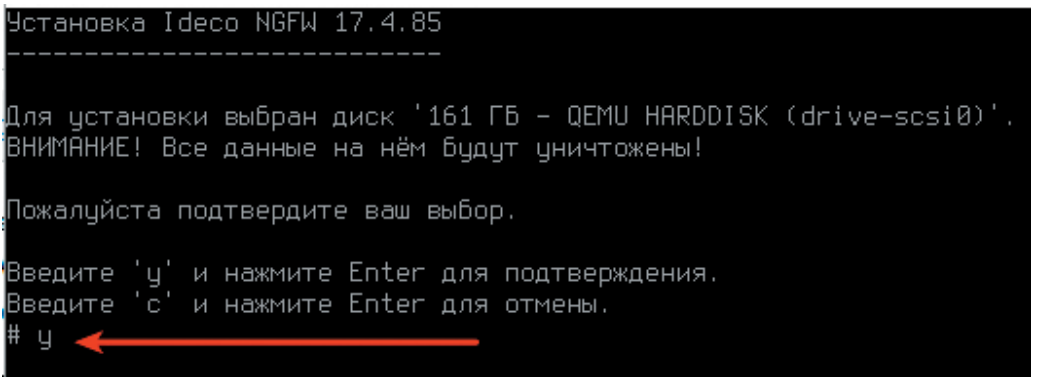
В результате будет создана виртуальная машина с именем ideco-ngfw:



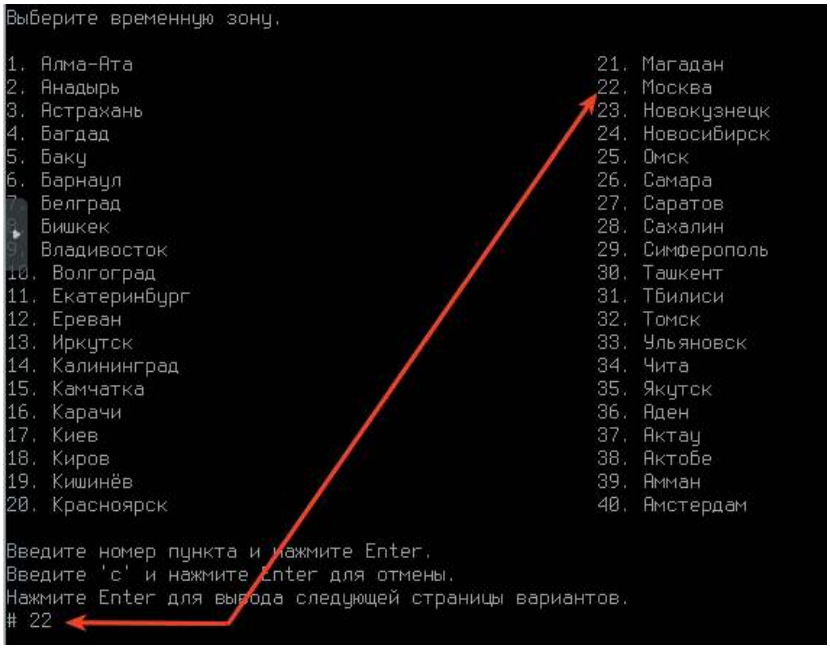
После запуска созданной виртуальной машины выберите стрелками на клавиатуре пункт меню Install Ideco NGFW 17.4.85 и нажмите Enter (важно, чтобы была отключена опция Secure Boot в UEFI):

После этого начнется процесс установки Ideco NGFW на виртуальную машину.

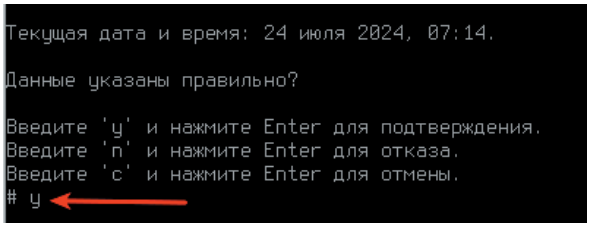
На первый вопрос в качестве подтверждения того, что данные на диске будут уничтожены, ответьте утвердительно и введите для этого с клавиатуры «y», нажмите Enter:



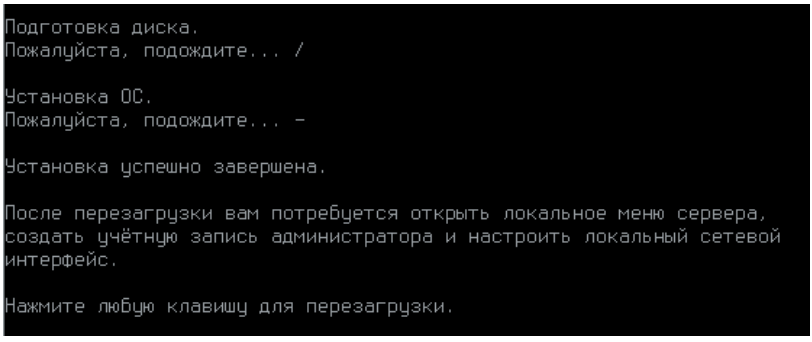
На следующем шаге выберите необходимую временную зону: для зоны «Москва» введите «22» (на выбор доступны 40 зон, с которыми можно ознакомиться на скриншоте) и нажмите Enter:



Проверьте корректность указания текущей даты и времени, после чего для подтверждения введите с клавиатуры «y» и нажмите Enter:



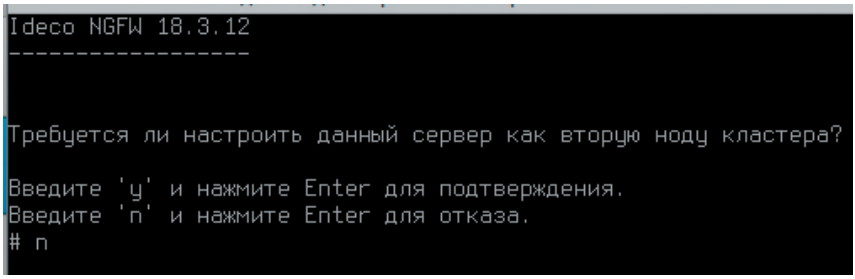
Далее начнется сам процесс установки операционной системы на виртуальную машину. После завершения установки нажмите на любую клавишу на клавиатуре для перезагрузки:



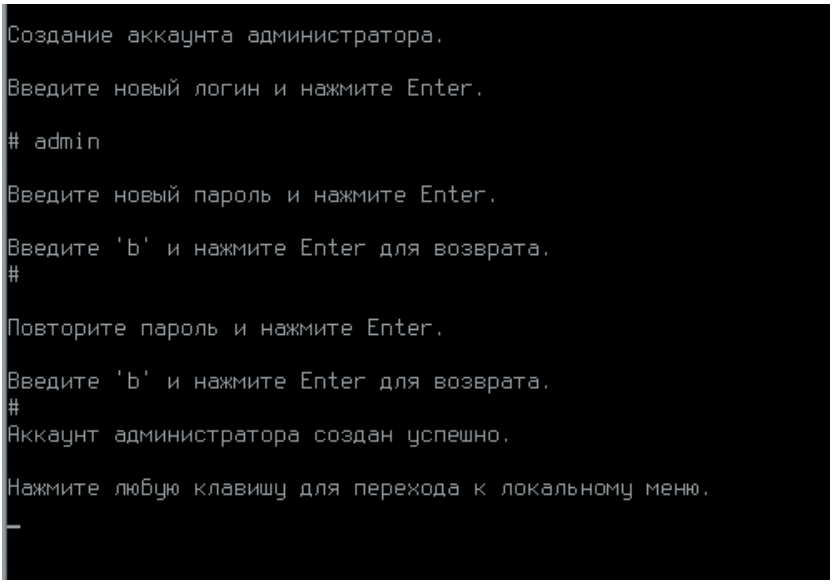
После перезагрузки появится приглашение входа в терминал. Не пытайтесь выполнять вход из-под какого-либо пользователя. Ожидайте несколько минут (время может варьироваться и зависит от вычислительных мощностей), после чего станет доступна локальная консоль Ideco.

Базовая настройка Ideco NGFW

Поскольку в настоящий момент не рассматривается работа в кластерном режиме, то на первый вопрос введите с клавиатуры «n» для отказа и нажмите 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).



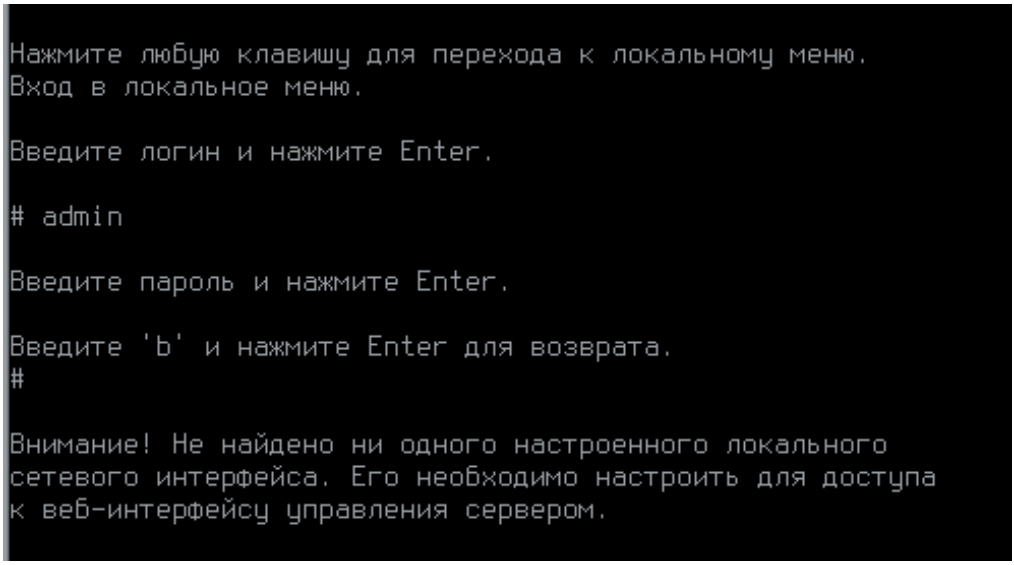
Если пароль не соответствует требованиям политики безопасности, то появится надпись с информацией, что пароль ненадежен. Потребуется ввести новый пароль с учетом требований к нему (описанных выше).

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.

Нажмите любую клавишу на клавиатуре для перехода к локальному меню, после чего выполните вход из-под только что созданного пользователя admin с паролем, который был установлен для данного пользователя (например: idecoP@ssw0rd):



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 нем статический адрес.

Для отказа в настройке локальной сети автоматически через DHCP введите с клавиатуры «n» и нажмите Enter. Назначьте статический адрес на локальный интерфейс в формате IP/префикс. В данном случае назначим первый адрес из сети 10.0.10.0/24:

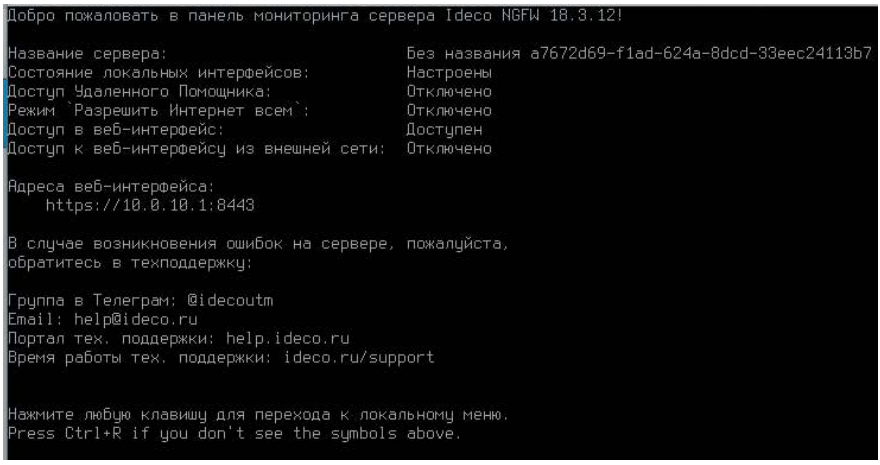
```
Внимание! Не найдено ни одного настроенного локального
сетевого интерфейса. Его необходимо настроить для доступа
к веб-интерфейсу управления сервером.


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.
#
```

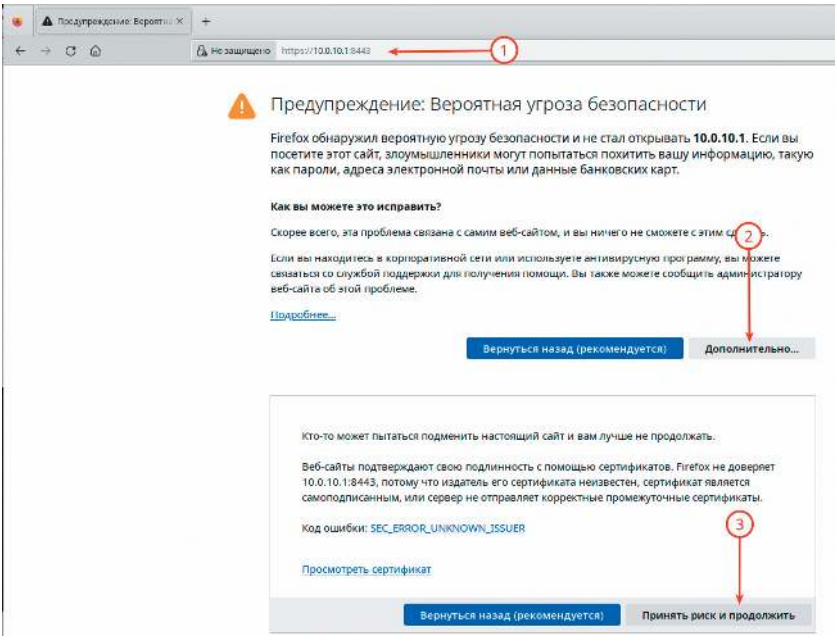
Для выхода введите с клавиатуры номер пункта «Выход»» и нажмите Enter.

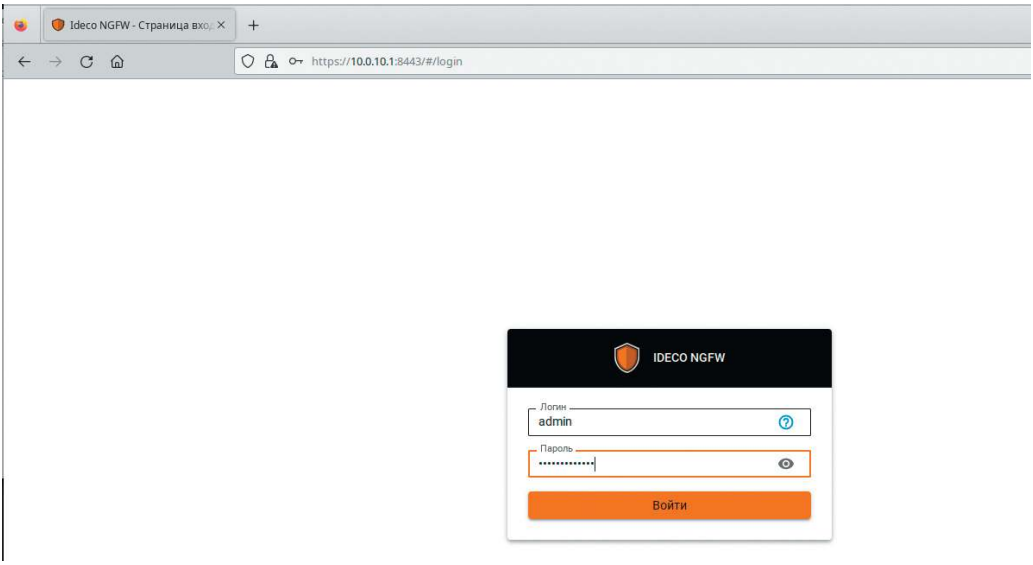
Доступ к веб-интерфейсу Ideco NGFW осуществляется по протоколу https на порт 8443:



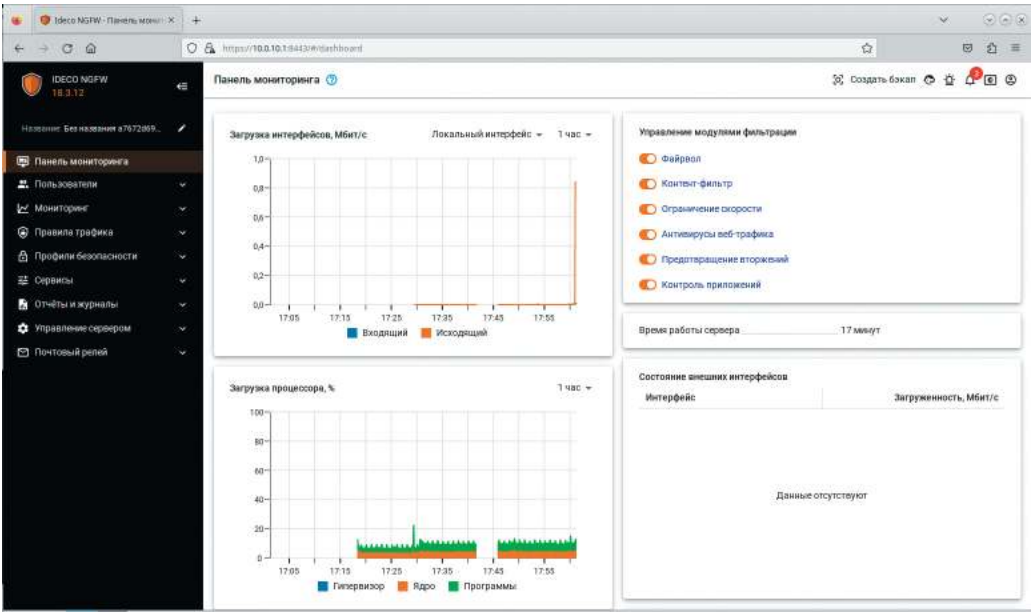
Поддерживаются версии Firefox, Chrome и браузеров, актуальные на текущий момент.

После чего можно выполнять аутентификацию в веб-интерфейсе Ideco NGFW из-под ранее созданного пользователя. Поскольку сертификат на ideco-ngfw является самоподписанным, необходимо добавить исключение: нажмите последовательно кнопки «Дополнительно», «Принять риск и продолжить»:





Результат успешной аутентификации в веб-интерфейсе Ideco NGFW с учетными данными пользователя, созданного в локальной консоли Ideco:



ДЛЯ ЗАМЕТОК

Учебное издание

Носенко Дмитрий Игоревич
Золотарёв Андрей Петрович
Уймин Антон Григорьевич
Дегтярев Сергей Сергеевич
Ефименко Татьяна Ивановна
Морозов Илья Михайлович
Шальнев Владимир Валентинович

СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ.
ПОДГОТОВКА К ДЕМОНСТРАЦИОННОМУ
ЭКЗАМЕНУ КОД 09.02.06-1-2026

Главный редактор *Ю.Б. Захарова*
Выпускающий редактор *Н.Г. Шиндина*
Редакторы *А.А. Гвоздюк, М.В. Леман*
Технический редактор *Е.А. Шугар*
Корректор *А.А. Гвоздюк*
Компьютерная верстка *Ю.Р. Валиахметова*
Обложка *Т.А. Антонова*

ООО «Базальт СПО»
Адрес для переписки: 127015, Москва, Бутырская, 75, оф. 301
Телефон: (495)123-47-99. E-mail: sales@basealt.ru
https://www.basealt.ru/

Подписано в печать 06.03.2026. Бумага офсетная.
Формат 60×90/16. Гарнитура «PT Serif».
Печать цифровая. Печ. л. 13,5.
Тираж 500 экз. (1-й з-д 1–87 экз.). Заказ № 159.

Общество с ограниченной ответственностью Компания «Ай Пи Ар Медиа»,
143405, Московская область, г.о. Красногорск, г. Красногорск,
ш. Ильинское, д. 1А, помещ. 17.17

Акционерное Общество «Т 8 Издательские Технологии» (АО «Т 8»),
109316, г. Москва, Волгоградский пр-т, д. 42, корп. 5

IPR ИЗДАТЕЛЬСКИЙ ЦЕНТР

Актуальный каталог печатных книг

Издательский центр IPR (включает в себя издательства «Ай Пи Ар Медиа» и «Профобразование») создает образовательные ресурсы для университетов и колледжей, с 2005 года комплексно и «под ключ» реализует издательские проекты в сфере образования.

Вместе с нашими партнерами и заказчиками мы разработали более восьми тысяч уникальных изданий, которые выгодно позиционируют университеты, колледжи и отдельных авторов в стране и в мире.

Издавайте вместе с нами:

8-800-555-22-35
izdat@iprmedia.ru

Издание разработано для поддержки реализации образовательных программ СПО в соответствии с требованиями ФГОС 09.02.06 «Сетевое и системное администрирование» (Приказ № 1548 от 09 декабря 2016, Приказ № 519 от 10 июля 2023) и подготовки к демонстрационному экзамену. Направлено на углубление профессиональных знаний и формирование практических умений у студентов укрупненных групп профессий и специальностей «Информатика и вычислительная техника», «Информационная безопасность», «Электроника, радиотехника и системы связи» в области администрирования сетей и систем на платформе отечественных ИТ-решений.

#AU_TEAM

9 785448 829086