ВСЕРОССИЙСКОЕ
ЧЕМПИОНАТНОЕ
ДВИЖЕНИЕ
ПО ПРОФЕССИОНАЛЬНОМУ
МАСТЕРСТВУ

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Региональный этап чемпионата по профессиональному мастерству «Профессионалы» в _____г.

_____

(субъект РФ)

2025-2026 г.

Модуль А. Аудит (вариатив)

Время на выполнение модуля: 4 часа

Задания:

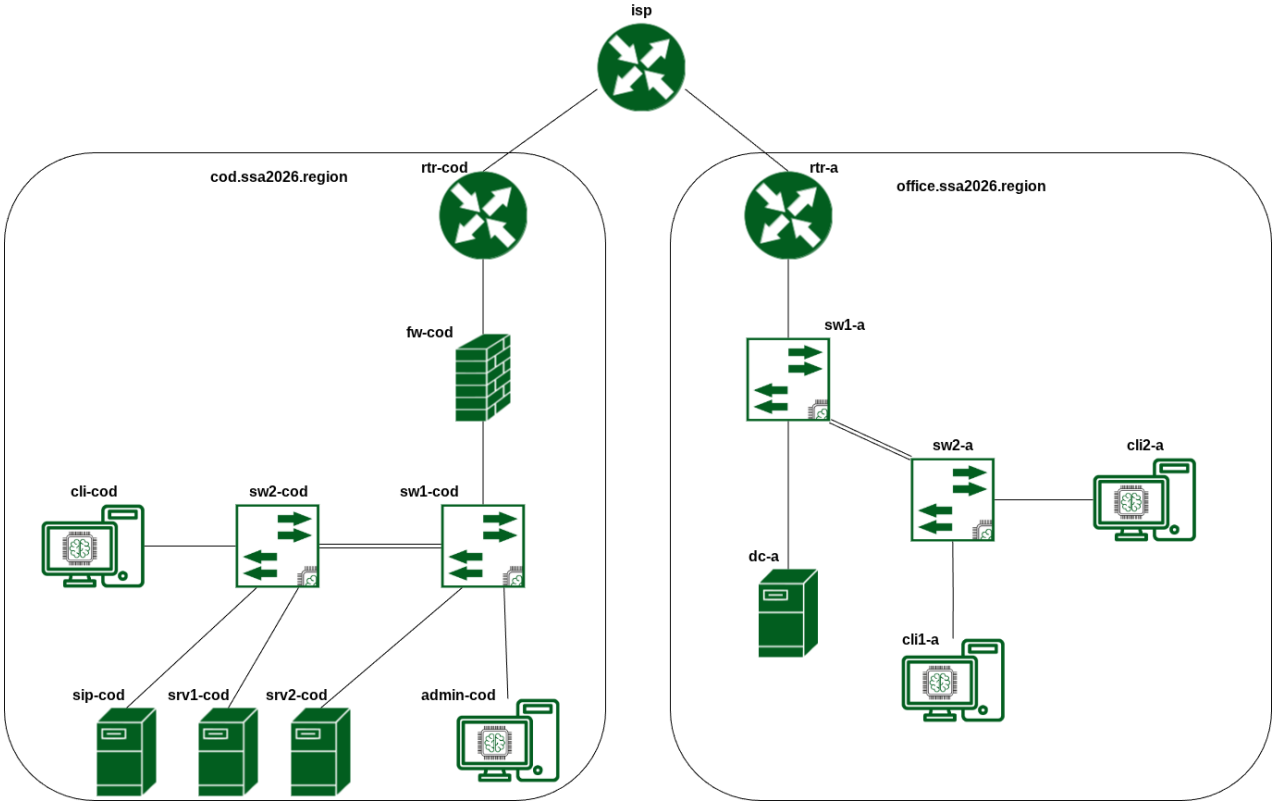
Руководство, в лице непосредственного начальника, поставило вам задачу – произвести независимую оценку результатов выполнения квалификационного испытания вашего возможного коллеги. Комплект документации для проведения испытания включает в себя непосредственно задание и набор оценочных ведомостей. В вашем распоряжении будет и то и другое. Помимо этого, отдел кадров требует от начальника отдела, а значит и он от вас, задокументировать оценку, составив отчёт в текстовом документе формата ODT, где каждый из аспектов оценки (по номерам аспектов оценочного листа) будет иметь подтверждение, в виде снимка фрагмента экрана с информацией, на основании которой вы приняли своё решение и пояснения к ней. Увы, варианта отметить выполнение пунктов задания, не глядя на инфраструктуру вам не оставили – в некотором смысле это и ваша аттестация, сами просили повышения и прибавки к окладу. Шаблон и требования к отчёту расположены на рабочем столе текущего пользователя.

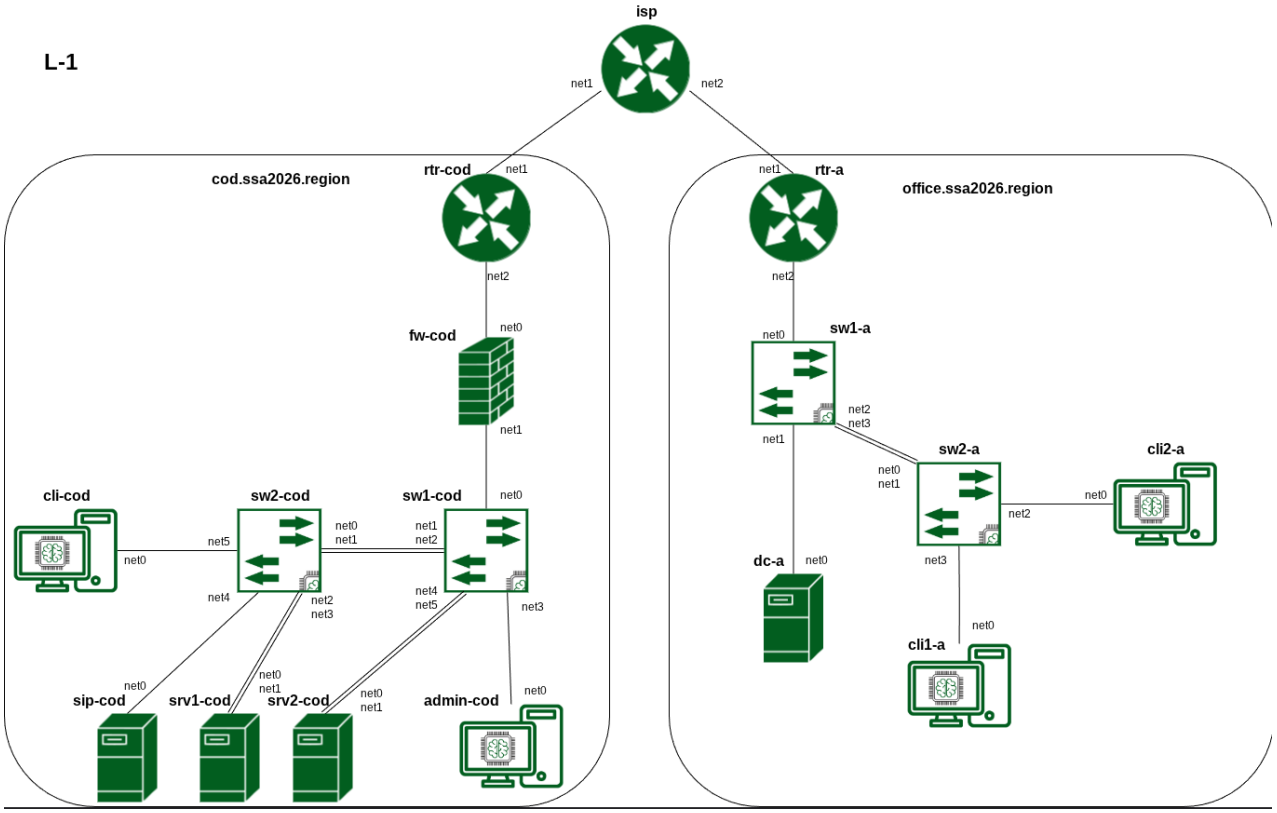
Модуль Б. Настройка технических и программных средств информационно-коммуникационных систем (инвариант)

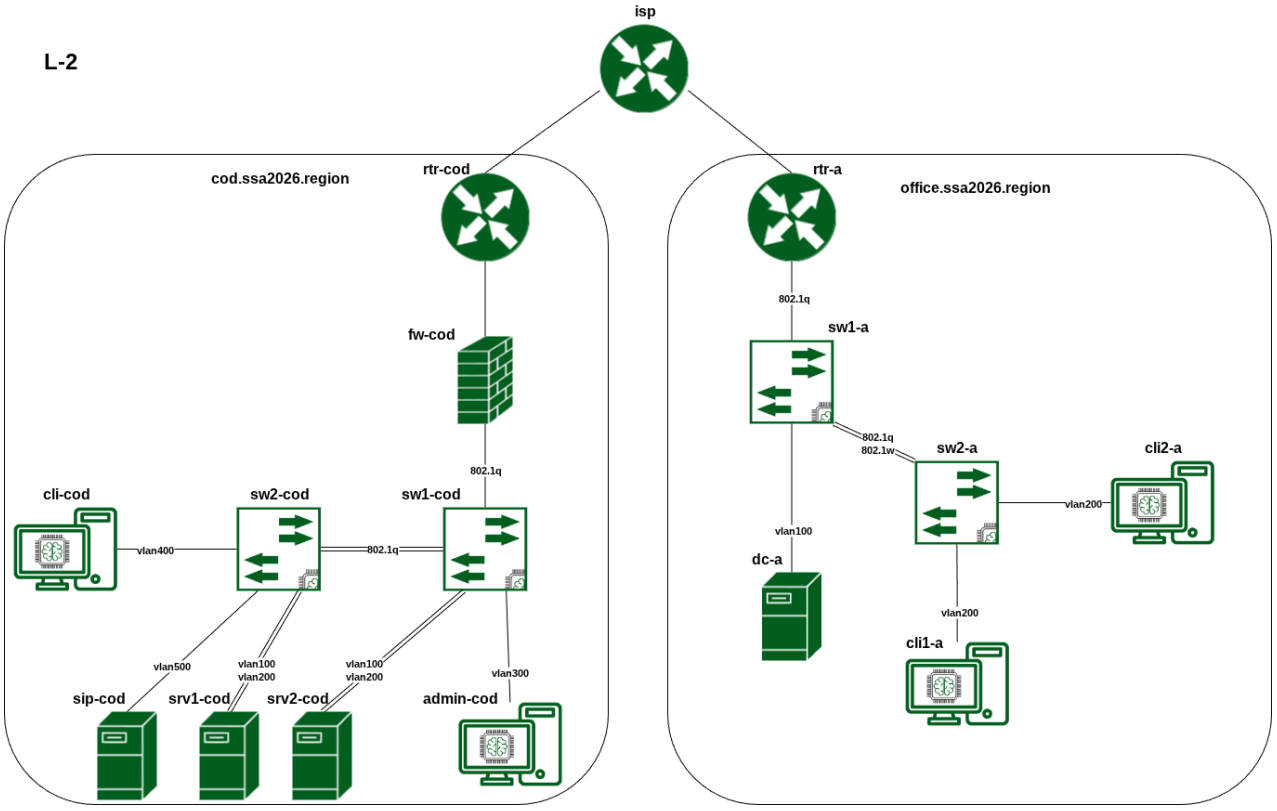
Время на выполнение модуля: 7 часов

Задания:

Схема подключения:




L-1
isp
net1
net2
cod.ssa2026.region
rtr-cod
net1
net2
fw-cod
net0
net1
cli-cod
sw2-cod
sw1-cod
net0
net5
net0
net0
net1
net1
net2
net4
net2
net3
net4
net5
net3
sip-cod
srv1-cod
srv2-cod
admin-cod
net0
net0
net1
net0
net1
net0
office.ssa2026.region
rtr-a
net1
net2
sw1-a
net0
net2
net3
net1
sw2-a
cli2-a
net0
net1
net0
net2
dc-a
net0
net3
cli1-a
net0


L-2
isp
cod.ssa2026.region
rtr-cod
fw-cod
802.1q
cli-cod
sw2-cod
sw1-cod
vlan400
802.1q
vlan500
vlan100
vlan200
vlan100
vlan200
vlan300
sip-cod
srv1-cod
srv2-cod
admin-cod
office.ssa2026.region
rtr-a
802.1q
sw1-a
802.1q
802.1w
sw2-a
cli2-a
vlan200
vlan100
dc-a
vlan200
cli1-a

На виртуальных машинах и оборудовании используются следующие версии ОС и технологические решения:

Название устройства	ОС
rtr-cod	EcoRouterOS (7-jasmine)
fw-cod	Ideco NGFW NOVUM 21
sw1-cod	Альт Сервер 11
sw2-cod	Альт Сервер 11
cli-cod	Альт Рабочая станция 11
srv1-cod	Альт Сервер 11
srv2-cod	Альт Сервер 11
sip-cod	SNG7-PBX16
admin-cod	Альт Рабочая станция 11
rtr-a	EcoRouterOS (7-jasmine)
sw1-a	Альт Сервер 11
sw2-a	Альт Сервер 11
dc-a	Альт Сервер 11
cli1-a	Альт Рабочая станция 11
cli2-a	Альт Рабочая станция 11

Параметры интернет-провайдеров, предоставляющих услуги организации или клиентам

Провайдер	Адрес IPv4/Маска	Шлюз IPv4	AS
GIGAFON COD	178.207.179.4/29	178.207.179.1	31133
GIGAFON A	178.207.179.28/29	178.207.179.25	31133

В сети GIGAFON COD сделаны настройки BGP

1. Соседство устанавливается по IPv4 с адреса шлюза на выделяемый провайдером адрес через физический интерфейс и указанные выше номера автономных систем.

2. Все провайдеры анонсируют делегируемые префиксы в “интернет”.

На DNS-сервере100.100.100.100 настроена зона ssa2026.ru

VLAN - cod:

VLAN	Название	Устройство
100	SRV-COD	srv1-cod, srv2-cod
200	DATA	srv1-cod, srv2-cod
300	MGMT-COD	fw-cod, sw1-cod, sw2-cod, admin-cod
400	CLI	cli-cod
500	VOIP	sip-cod

VLAN - a:

VLAN	Название	Устройство
100	SRV	dc-a
200	CLI	cli1-a, cli2-a
300	MGMT	rtr-a, sw1-a, sw2-a

Проверка будет производиться с использованием доменных имен.

Проверка по IP-адресам выполняться не будет.

Базовая настройка

1. Настройте имена устройств согласно топологии
    a. Используйте fqdn hostname
        i. для ЦОД - cod.ssa2026.region
        ii. для office - office.ssa2026.region
2. Настройте административный доступ
    a. На rtr-cod, sw1-cod и sw2-cod для аутентификации через консоль и по SSH используйте RADIUS-сервер
        i. В качестве RADIUS-сервера используйте srv1-cod
        ii. Используйте пользователя netuser с паролем P@ssw0rd
            1) Для rtr-cod пользователь не должен существовать локально.
            2) Пользователь должен иметь возможность конфигурировать маршрутизатор
        iii. Предусмотрите вход под локальной учетной записью даже при доступности RADIUS-сервера

Настройка коммутации

1. Сконфигурируйте коммутаторы sw1-cod и sw2-cod, sw1-a и sw2-a.

a. Все порты, участвующие в коммутации, должны быть настроены в соответствии с диаграммой L2 и таблицей VLAN-ов.

b. Настройте магистральные каналы в соответствии с диаграммой L2, разрешите только требуемые VLAN.

c. Настройте IP-адреса интерфейсов управления.

i. Для «cod» в качестве сети управления используйте VLAN - MGMT-COD.

ii. Для офиса «a в качестве сети управления используйте VLAN - MGMT.

iii. Для обработки трафика управления используйте NativeVLAN.

iv. Для «cod» трафик VLAN - DATA не должен маршрутизироваться.

2. Настройте агрегацию между устройствами sw1-cod и sw2-cod:

a. Реализуйте агрегированные соединения средствами ядра с последующей передачей интерфейса в управление коммутатору.

b. Используйте active-backup.

3. Настройте протокол STP на коммутаторах sw1-a и sw2-a.

a. Запустите процесс spanning-tree на коммутаторах.

b. Коммутатор sw1-a должен иметь наименьший приоритет.

c. Используйте 802.1w.

Настройка туннелей между офисом «a» и «cod»:

1. Настройте GRE туннель между rtr-a и rtr-cod

a. В качестве сетевого диапазона используйте сеть 10.10.10.0/24

b. Для каждого туннеля используйте минимально возможную маску

Настройка маршрутизации

1. Выполните необходимые настройки сети и маршрутизации BGP с ISP

a. AS ЦОД 64500

b. Анонсировать внутренние сети «cod» в провайдера запрещено.

c. Маршрутизатор ЦОД должен получать маршрут по умолчанию по BGP

i. Ручное создание маршрута по умолчанию ЗАПРЕЩЕНО!

2. Настройте динамическую маршрутизацию между офисом «a» и «cod»

a. Используйте OSPF для маршрутизации между rtr-a, rtr-cod и fw-cod

b. На маршрутизаторах все интерфейсы, кроме туннельных, должны быть переведены в пассивный режим

c. Используйте аутентификацию в OSPF

i. В качестве пароля используйте P@ssw0rd

ii. Пароль должен передаваться с использованием хешированного ключа MD5

Настройка доступа в Интернет

1. Настройте маршрутизаторы для обеспечения доступа в Интернет.

Настройка синхронизации времени между сетевыми устройствами

1. Все устройства должны синхронизировать своё время с сервером точного времени по адресу 100.100.100.100.

2. Используйте на всех устройствах московский часовой пояс.

Настройка службы доменных имен

1. Реализуйте основной DNS сервер сети «cod»

a. В качестве DNS-сервера используйте srv1-cod.

b. Для устройств «cod» необходимо создать записи A и PTR.

2. Реализуйте основной DNS сервер сети офиса «a»

a. В качестве DNS-сервера используйте dc-a.

b. Для устройств офиса «a» необходимо создать записи A и PTR.

3. В качестве DNS сервера пересылки используйте адрес 100.100.100.100

4. Все устройства предприятия должны быть настроены на использование соответствующих их расположению DNS серверов.

5. Настройте взаимосвязь между всеми DNS серверами предприятия.
    a. Настройте перенаправление как прямых, так и обратных зон.
6. Все устройства предприятия должны быть доступы по имени.

Настройка центра сертификации

1. На сервере srv1-cod разверните центр сертификации на базе openssl
    a. Срок жизни корневого сертификата должен составлять 5 лет.
    b. Код страны - RU
    c. Название организации - IRPO
    d. Имя центра сертификации - ssa2026
    e. Все файлы должны храниться в /var/ca
2. Все рабочие станции организации, должны доверять созданному центру сертификации
3. Используйте созданный центр сертификации для выпуска требуемых сертификатов

Настройка сервера баз данных

1. В качестве сервера баз данных используйте srv2-cod
    a. В качестве СУБД используйте PostgreSQL
        i. Используйте версию не ниже 17
    c. Создайте суперпользователя superadmin с паролем P@ssw0rdSQL
        i. Суперпользователь должен иметь полный доступ ко всем базам данных
2. Для администрирования сервера баз данных используйте admin-cod
    a. В качестве программы-клиента для СУБД используйте DBeaver

Настройка устройства хранения данных

1. Используйте хост srv2-cod.
    a. Используйте VLAN DATA.
    b. Настройте iSCSI target.

i. Используйте имя цели iqn.2026-0<№ текущего месяца>.region.ssa2026.cod:data.target

ii. Настройте отдачу по iSCSI свободного (не используемого) диска 2. Используйте хост srv1-cod.

a. Добавьте target iSCSI .

i. Используйте ID с именем iscsi

ii. Для добавления target используйте сеть DATA

iii. Не используйте LUN напрямую

b. Добавьте хранилище LVM.

i. Используйте target iscsi в качестве pv

ii. Используйте vg с именем VG

iii. Используйте 100% дискового пространства для lv с именем DATA

iv. Используйте файловую систему xfs.

v. Настройте автоматическое монтирование тома

vi. Точка монтирования /opt/data

c. Настройте сервер сетевой файловой системы NFS

i. в качестве папки общего доступа выберите /opt/data

ii. доступ для чтения и записи для всей сети MGMT-COD

3. На admin-cod настройте автомонтирование в папку /mnt/nfs

Настройка сервисов в сети офиса «a»

1. Разверните контроллер домена office.ssa2026.region на базе SambaAD.

a. В качестве сервера используйте dc-a.

b. В качестве DNS-сервера используйте dc-a.

i. в качестве DNS backend используйте BIND9_DLZ

c. В качестве пароля доменного администратора используйте P@ssw0rd

2. Для управления контроллером домена используйте ADMC с cli1-a

3. Создайте подразделения, группы и пользователей

a. Создайте подразделения ofadmins и ofusers

b. Создайте группы ofadmins и ofusers

i. Добавьте группы в соответствующие подразделения

c. Создайте пользователей ofadmin1, ofuser1 и user1

i. Добавьте пользователей в соответствующие подразделения и группы

1) Пользователя user1 не добавляете в группы ofadmins и ofusers

ii. В качестве пароля используйте P@ssw0rd

4. Для cli1-a и cli2-a настройте политику изменения рабочего стола на картинку компании, а также запретите использование пользователям изменение сетевых настроек и изменение графических параметров рабочего стола.

5. Введите cli1-a и cli2-a в домен office.ssa2026.region

Настройка системы мониторинга

1. В качестве сервера системы мониторинга используйте srv1-cod

2. В качестве системы мониторинга используйте Zabbix версии не ниже 7.0

a. В качестве СУБД используйте PostgreSQL на srv2-cod

i. Имя базы данных: zabbix

ii. Пользователь базы данных: zabbix_user

iii. Пароль пользователя базы данных: P@ssw0rdZabbix

b. В качестве веб-сервера используйте Apache

3. Система мониторинга должна быть доступна по адресу srv1-cod.cod.ssa2026.region, monitoring.cod.ssa2026.region, <IP адрес srv1-cod>

a. Администратором системы мониторинга должен быть пользователь Admin с паролем P@ssw0rd

b. Часовой пояс по умолчанию должен быть Europe/Moscow

c. Настройте пернаправление с http на https

i. Доступ к Веб-интерфейсу должен производиться по TLS соединению с использованием сертификата выпущенного CA srv1-cod

ii. При обращении к Веб-интерфейсу не должно отображаться ошибок и предупреждений

4. Настройте узлы системы мониторинга

a. В качестве узлов сети используйте

i. Все устройства организации кроме клиентов

b. Имя узла сети должно соответствовать полному имени устройства

c. Все сетевые устройства (маршрутизаторы и коммутаторы) необходимо поместить в группу узлов Network devices

i. Используйте шаблон Cisco IOS by SNMP для маршрутизаторов на EcoRouter

ii. Используйте шаблон Linux by Zabbix agent для fw-cod

iii. Используйте шаблон Linux by Zabbix agent для sw1-cod, sw2-cod, sw1-a и sw2-a

d. Все сервера необходимо поместить в группу узлов Linux servers

i. Используйте шаблон Linux by Zabbix agent для srv1-cod, srv2-cod и dc-a

Настройка IP телефонии

1. На sip-cod установите систему SNG7-PBX16

a. Используйте уже подключенный ISO-образ

2. Для admin-cod должен использоваться внутренний номер 1001

3. Для cli-cod должен использоваться внутренний номер 1002

4. Для cli1-a должен использоваться внутренний номер 2001

5. Для cli2-a должен использоваться внутренний номер 2002

6. На рабочие станции установите любой СофтФон

7. Для реализации внутренних звонков необходимо использовать CHAN_SIP

a. В качестве порта SIP необходимо использовать 5060

b. Сеанс связи должен устанавливаться между всеми рабочими станциями

Модуль Г. Обеспечение отказоустойчивости (инвариант)

Время на выполнение модуля 5 часов

Задания:

1) **Подготовка машины Cloud-ADM.**

a. Создайте виртуальный инстанс с именем **Cloud-ADM**, подключите его к необходимым сетям, ассоциируйте с ним плавающий IP-адрес.

b. Установите следующие параметры для создаваемого инстанса:

1. Тип виртуальной машины: **2 vCPU, 4 ГБ RAM**;

2. Размер диска: **30 ГБ**.

c. В качестве операционной системы используйте Альт Рабочая станция, шаблон **alt-workstation-10.4-p10-cloud**.

d. Настройте внешнее подключение по **SSH** сохранив ключевую пару для доступа с вашего локального ПК на рабочем столе с расширением **.pem**:

1. Создайте в PuTTY профиль с именем **Cloud-ADM**;

2. Реализуйте возможность установления соединения с инстансом Cloud-ADM с локального ПК через PuTTY, **без** необходимости ввода дополнительных параметров.

e. Настройте внешнее подключение по **RDP** сохранив на рабочем столе профиль с именем **Cloud-ADM**:

1. Для подключения используйте имя пользователя **altlinux** и пароль **P@ssw0rd**.

2) **Project_01**

a. На виртуальной машине **Cloud-ADM** создайте скрипт «**deploy_project_01.sh**».

b. В качестве домашней директории используйте путь **/home/altlinux/Projects/Project_01**.

c. Скрипт должен реализовывать следующий функционал:

1. Автоматическое развёртывание виртуальных машин в соответствии с топологией (см. Топология Project_01).

2. Характеристики виртуальных машин: **1vCPU, 1 ГБ ОЗУ, 10 ГБ размер диска**.

3. Образ операционной системы: **alt-p11-cloud-x86_64.qcow2**.

4. Для виртуальной машины **haproxy01** должен создаваться и ассоциироваться **Плавающий-IP**.

d. На виртуальной машине **Cloud-ADM** создайте скрипт «**configure_project_01.sh**».

e. В качестве домашней директории используйте путь **/home/altlinux/Projects/Project_01**.

f. Скрипт должен реализовывать следующий функционал:

1. Установку необходимых компонентов для запуска приложения (см. Приложение Project_01) на виртуальных машинах: **game01, game02, game03** в виде Docker-контейнеров.

2. Образ приложения нужно сделать легковесным через мультистейджинг.

3. На виртуальной машине **haproxy01** настройку распределения входящих запросов через **haproxy**.

4. Настройку доступа к просмотру собранной статистики в веб-интерфейсе с виртуальной машины **Cloud-ADM** по **haproxy01.dev.au.team /haproxy?stats**

5. Приложение должно быть доступно с виртуальной машины **Cloud-ADM** из веб-браузера по именам: **game01.dev.au.team**, **game02.dev.au.team** и **game03.dev.au.team** на **80** порту.

6. Приложение должно быть доступно из вне по **Плавающему-IP** виртуальной машины **haproxy01** на порту **443**.

7. С виртуальной машины Cloud-ADM доступ к приложению должен быть по https://game.au.team.

8. Проблем с сертификатом возникать не должно.

g. На виртуальной машине **Cloud-ADM** создайте скрипт «**destroy_project_01.sh**».

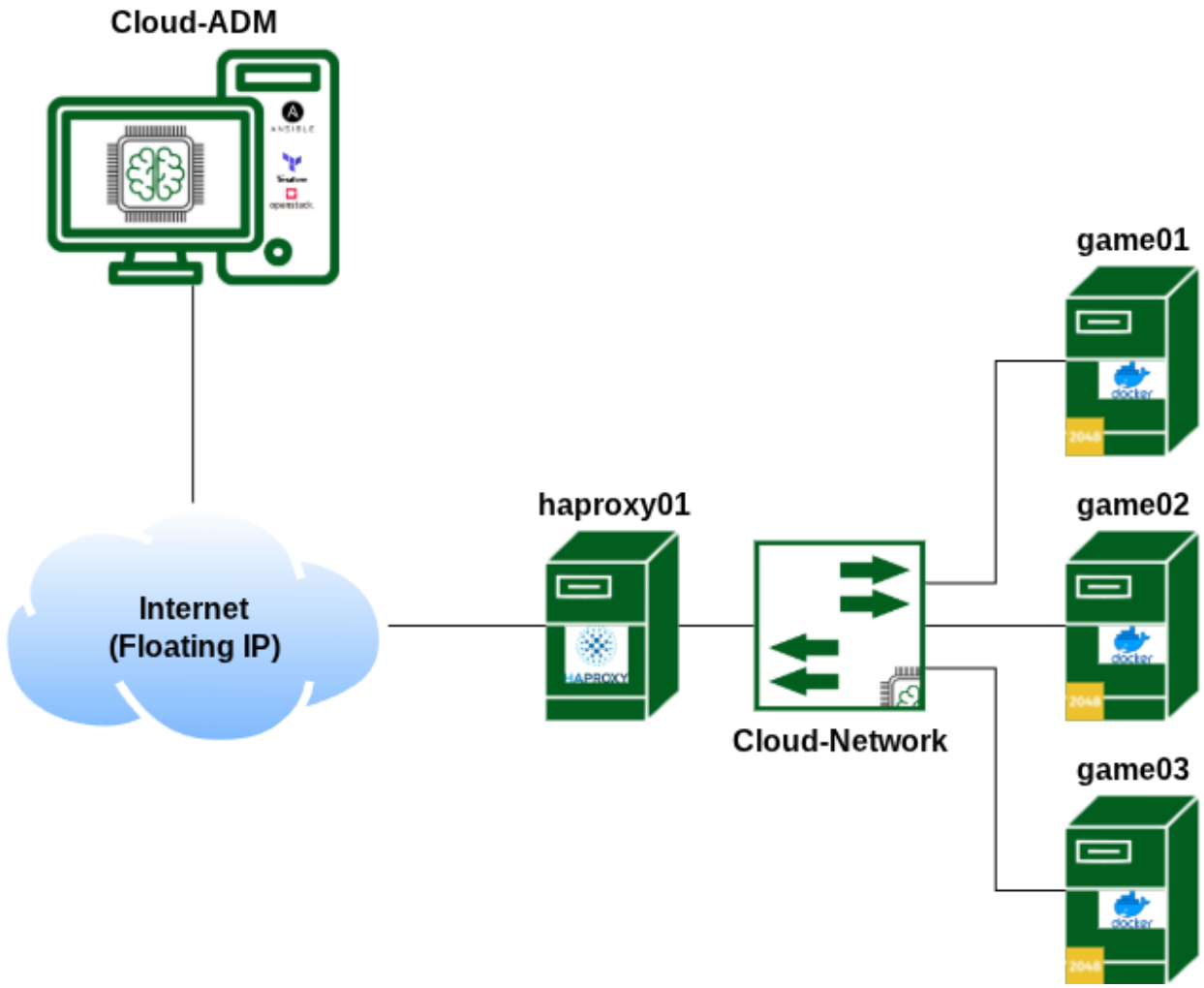
h. В качестве домашней директории используйте путь **/home/altlinux/Projects/Project_01**.

i. Скрипт должен реализовывать следующий функционал:

1. Удалять все автоматически созданные ресурсы через скрипт **deploy_project_01.sh**.

2. Если скрипт **destroy_project_01.sh** не реализован, участник не получит баллов за данный пункт задания, а эксперты вручную выполнят удаление ресурсов.

Топология Project_01:



Приложение Project_01:

https://disk.yandex.ru/d/uhpN6U6UYRK_Nw (у приложения есть README от программиста-разработчика)

3) Project_02

a. Любым способом разверните недостающие виртуальные машины в облаке в соответствии с топологией (см. Топология Project_02).

1. Характеристики виртуальных машин:

- **ACM-Server: 1vCPU, 2 ГБ ОЗУ, 20 ГБ размер диска**.
- **DB-Server: 1vCPU, 1 ГБ ОЗУ, 20 ГБ размер диска.**
- **BAR-Agent01: 1vCPU, 1 ГБ ОЗУ, 10 ГБ размер**

2. Образ операционной системы: **alt-p11-cloud-x86_64.qcow2**.

b. На развёрнутых виртуальных машинах реализуйте следующий функционал:

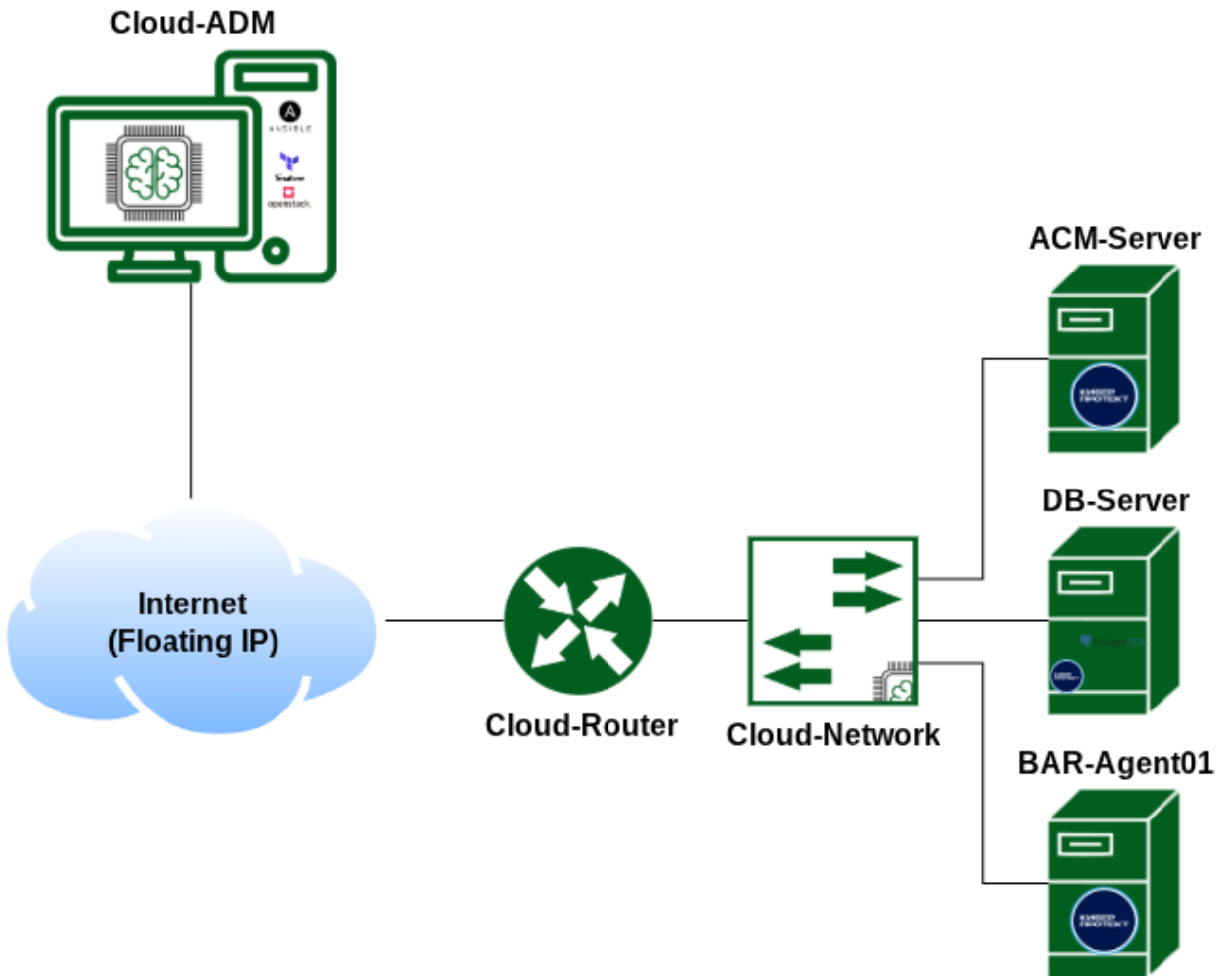
1. Установку сервера управления Кибер Бэкап (версии не ниже 18) на виртуальной машине **ACM-Server**.

- Сервер управления должен быть доступен с **Cloud-ADM** по имени **cb.au.team** на порту **9877**.
- Доступ в веб-интерфейс сервера управления должен быть из-под пользователя **root** с паролем **toor**.
- Для установки сервера управления в качестве СУБД необходимо использовать **PostgreSQL**.

2. Установку агента для Linux на виртуальной машине **BAR-Agent01** с последующей регистрацией на сервере управления.

3. Установку агента для PostgreSQL на виртуальной машине **DB-Server** с последующей регистрацией на сервере управления.

Топология Project_02:



4) Project_03

a. Любым способом разверните недостающие виртуальные машины в облаке в соответствии с топологией (см. Топология Project_03).

1. Характеристики виртуальных машин:

- **master01: 1vCPU, 1 ГБ ОЗУ, 10 ГБ размер диска**.
- **worker01: 1vCPU, 1 ГБ ОЗУ, 10 ГБ размер диска.**
- **worker02: 1vCPU, 1 ГБ ОЗУ, 10 ГБ размер**

2. Образ операционной системы: **alt-p11-cloud-x86_64.qcow2**.

b. На развёрнутых виртуальных машинах реализуйте следующий функционал:

1. Сформируйте кластер Docker Swarm.

- Используйте ВМ **master01** в качестве менеджера кластера, **worker01** и **worker02** - в качестве исполнителей.

- Запускать контейнеры на менеджере запрещено.

2. Разместите в кластере Docker Swarm service для организации собственного хранилища образов контейнеров:

- В качестве образа используйте **registry:3**

- Локальное хранилище образов должно быть доступно со всех узлов кластера на порту **5000**

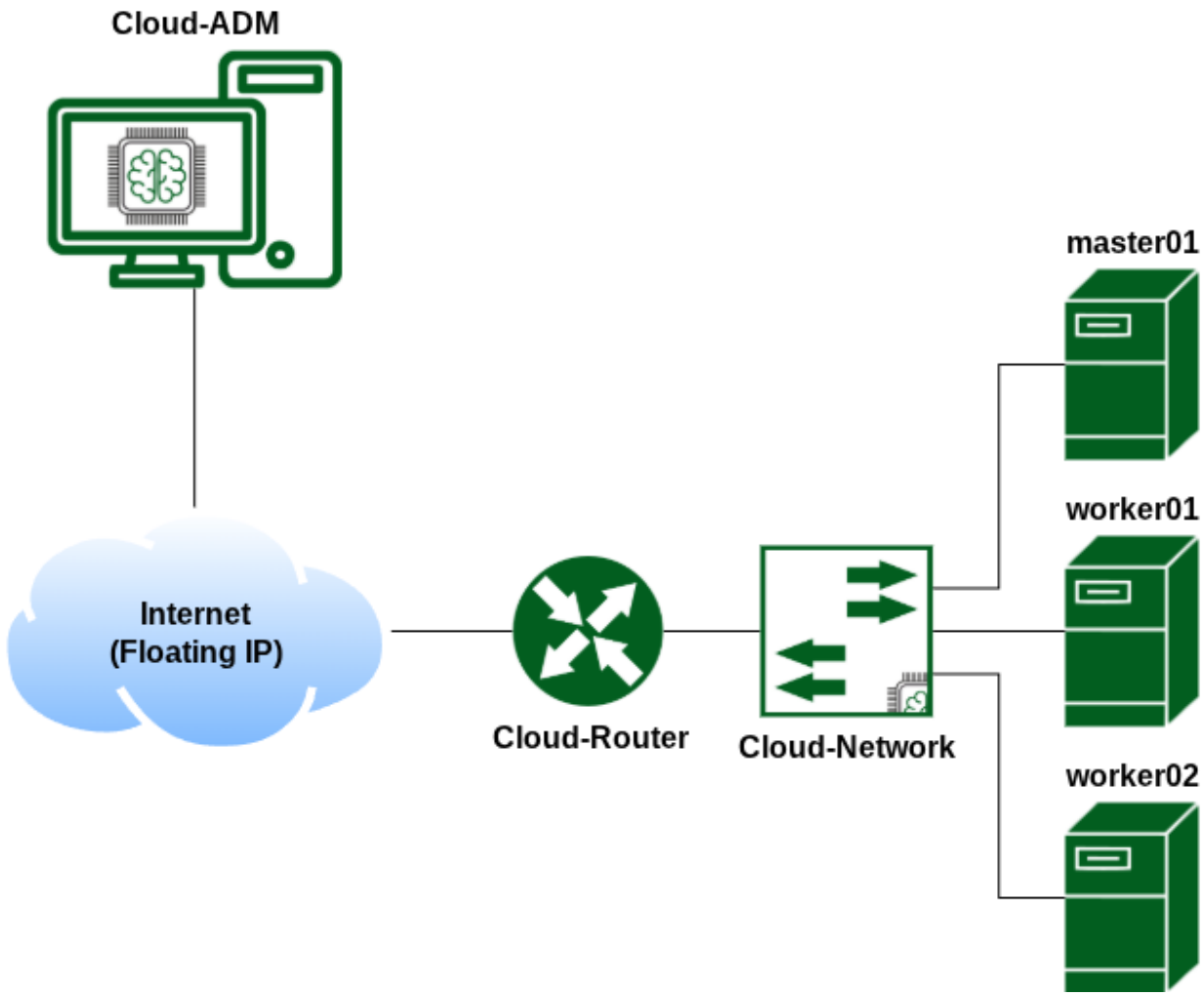
3. Разместите в кластере Docker Swarm stack для организации работы приложения (см. Приложение Project_03)

- В качестве имени для stack используйте **school-site-project**
- Приложение должно быть доступно с **Cloud-ADM** по **http://school-site.au.team** и **https://school-site.au.team**
- В случае доступу по **https**, проблем с сертификатом возникать не должно.

4. На данный момент это просто статический сайт, но стоит предусмотреть возможность развёртывания таких сервисов в стеке как:

- **redis** - для решения задач, требующих быстрой обработки данных
- СУБД: **PostgreSQL** – для хранения данных
- Веб-приложение пока не умеет работать с данными сервисами, но сервисы должны быть развёрнуты в рамках стека **school-site-project** для будущей разработки

Топология Project_03:



Приложение Project_03:

https://disk.yandex.ru/d/ItDZh8DTdK5kAA

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ[1]

1. Конкурсантам при выполнении всех модулей можно использовать интернет-ресурсы, за исключением:

– Систем контроля версий

– Общения посредством форумов/мессенджеров/иных средств коммуникации – видеохостингов

– Средств, требующих авторизацию любой формы

[1] *Указываются особенности компетенции, которые относятся ко всем возрастным категориям и чемпионатным линейкам без исключения.*

2. Конкурсанты имеют право задавать уточняющие вопросы экспертам (кроме эксперта наставника) и вправе получить ответ, если вопрос не предполагает получения информации о реализации конкретной технологии

2.1. Личный инструмент конкурсанта

- Клавиатура, мышь не программируемые
- Средства защиты слуха и глаз

2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Мобильные устройства, устройства фото-видео фиксации, носители информации.