

Разработано главным экспертом по компетенции
«СЕТЕВОЕ И СИСТЕМНОЕ
АДМИНИСТРИРОВАНИЕ»

_____/_____
(подпись) (ФИО главного эксперта)

СОГЛАСОВАНО
Индустриальный эксперт

_____/_____
(подпись) (ФИО)

Менеджер компетенции

_____/_____
(подпись) (ФИО)

**КОНКУРСНОЕ ЗАДАНИЕ
КОМПЕТЕНЦИИ
«СЕТЕВОЕ И СИСТЕМНОЕ
АДМИНИСТРИРОВАНИЕ»
для возрастной категории
Основная**

2024 г.

Чемпионат профессионального мастерства 2024 в рамках Регионального этапа Чемпионата по профессиональному мастерству «Профессионалы»

Конкурсное задание разработано экспертной группой и утверждено индустриальными партнёрами.

Состав экспертной группы:

Морозов Илья Михайлович, инструктор Базальт СПО, инструктор РЭД СОФТ, учебный мастер лаборатории "Сетей и систем передачи информации" РГУ Нефти и Газа им. И.М. Губкина.

Каменецкая Ника Витальевна, эксперт отдела аналитики и архитектуры государственной единой облачной платформы и информационной системы организации АО «КОНСИСТ-ОС».

Мокшанцев Михаил Александрович, эксперт отдела аналитики и архитектуры государственной единой облачной платформы и информационной системы организации АО «КОНСИСТ-ОС».

Уймин Антон Григорьевич, руководитель команды #au_team, инструктор Базальт СПО, инструктор ROSA Linux, инструктор Astra Linux, инструктор РЭД СОФТ, специалист Positive Technologies, Заведующий лабораторией "Сетей и систем передачи информации" РГУ Нефти и Газа им. И.М. Губкина

Консультанты:

Лавров Данил Сергеевич, главный эксперт отдела аналитики и архитектуры государственной единой облачной платформы и информационной системы организации АО «КОНСИСТ-ОС».

Дегтярев Сергей Сергеевич, ГБПОУ РО "Ростовский-на-Дону колледж связи и информатики", преподаватель.

Ефименко Татьяна Ивановна, Санкт-Петербургское государственное автономное профессиональное образовательное учреждение "Колледж туризма и гостиничного сервиса", преподаватель.

Щекотов Владимир Анатольевич, Новочебоксарский химико-механический техникум Минобразования Чувашии, заместитель директора по ИТ.

Терентьева Ольга Арсеньевна, Государственное автономное профессиональное образовательное учреждение Свердловской области "Уральский радиотехнический колледж им. А.С.Попова", преподаватель.

В данном задании установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

Конкурсное задание включает в себя следующие разделы:

Оглавление

1. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ	3
1.2. Структура модулей конкурсного задания	5

1. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №1:

Таблица №1

Оценка конкурсного задания

Критерий		Методика проверки навыков в критерии
А	Аудит	Определена регионом в соответствии с используемыми ОС и сетевым оборудованием: используется виртуализация и скрипты. Задание, указанное в этом документе, является примерным конкурсным заданием. Каждый регион определяет состав этого модуля самостоятельно.
Б	Настройка технических и программных средств информационно-коммуникационных систем	Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен в первый день только один раз и повторная оценка данного аспекта проводиться не будет. Одинаковые пункты могут быть проверены и оценены больше, чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств. Процедура оценки результатов выполнения задания будет производиться в конце дня конкретного модуля.
В	Обеспечение отказоустойчивости	Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен в первый день только один раз и повторная оценка данного аспекта проводиться не будет. Одинаковые пункты могут быть проверены и оценены больше, чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств. Процедура оценки результатов выполнения задания будет производиться в конце дня конкретного модуля.

1.1. КОНКУРСНОЕ ЗАДАНИЕ

Формат участия: индивидуальный

Возрастной ценз: от 16 лет

Общая продолжительность Конкурсного задания¹: 15 ч.

¹ Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом/командой.

Количество конкурсных дней: 3 дня.

Вне зависимости от количества модулей, Конкурсное задание должно включать оценку по каждому из разделов требований по компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний/оценки квалификации.

Конкурсное задание состоит из 3 модулей, общее количество баллов конкурсного задания составляет 100.

1.2. Структура модулей конкурсного задания

Модуль А. (Аудит)

Время на выполнение модуля 5 часов.

Задания:

Руководство компании «au.team» из-за низкой квалификации бывшего системного администратора столкнулось с рядом проблем. Было принято решение пригласить Вас, как высококлассного специалиста, для их решения. Перед Вами поставлены задачи, описанные в техническом задании, которые нужно решить в течение короткого промежутка времени. К сожалению, поскольку технического специалиста в организации не осталось, некоторые из требований могут звучать не очень внятно. Но вы являетесь профессионалом и, конечно, поймёте о чём идёт речь.

УДАЧИ!

Преыдуший специалист имел настолько низкую квалификацию, что за всё время обслуживания существующей локальной сети так и не собрал необходимую сетевую документацию. Это стало серьёзной проблемой, когда пользователи стали обращаться с жалобами на некачественную работу некоторых сервисов.

Ваша первая задача – составить всю необходимую для обслуживания сети документацию. Самостоятельно разработайте формат документации, который будет удобно использовать, примеры оформления представлены в приложении. Необходимо собрать следующую информацию об инфраструктуре:

- Схема подключений
- Схема топологии канального уровня
- Схема топологии сетевого уровня
- Таблица адресации
 - Имя устройства
 - Тип устройства
 - Операционная система, версия
 - Сетевой интерфейс
 - IP-конфигурация
- Таблица сетевых сервисов
 - Имя устройства
 - Название сервиса
 - Роль в инфраструктуре

Документ сохраните на рабочем столе рабочего компьютера с именем “Документация к инфраструктуре <Номер рабочего места>” в формате **PDF**.

Ваша вторая задача - отреагировать на жалобы пользователей, связанные с работой некоторых приложений. Предыдущий администратор с пользователями уже пообщался и записал результаты опроса в отдельный бланк в приложении. Определите причины проблем, запишите их в предоставленный бланк и примите меры для устранения.

В выполнении задания есть один серьезный нюанс – Вы работаете удалённо, поэтому физически обнаружить устройства не представляется возможным, а все операции придется выполнять с компьютера администратора. Реквизиты для доступа к машинам где-то на рабочем столе компьютера администратора, единственный пароль который Вам известен - **P@ssw0rd**.

Спецификация оценки

В рамках данного модуля оцениваются навыки аудита имеющейся сетевой сервисной инфраструктуры.

Проверка результатов выполнения задания осуществляется оценивающими экспертами сразу по окончании выделенного на модуль времени. В дальнейшем проверка данного модуля осуществляться не будет.

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

Время на выполнение модуля 5 часов.

На всех устройствах с ОС ALT Linux созданы учётные записи (логин/пароль):
 root/toor и user/resu, если Вам нужно установить пароль - используйте
 P@ssw0rd. Доступ к ISP вы не имеете!!

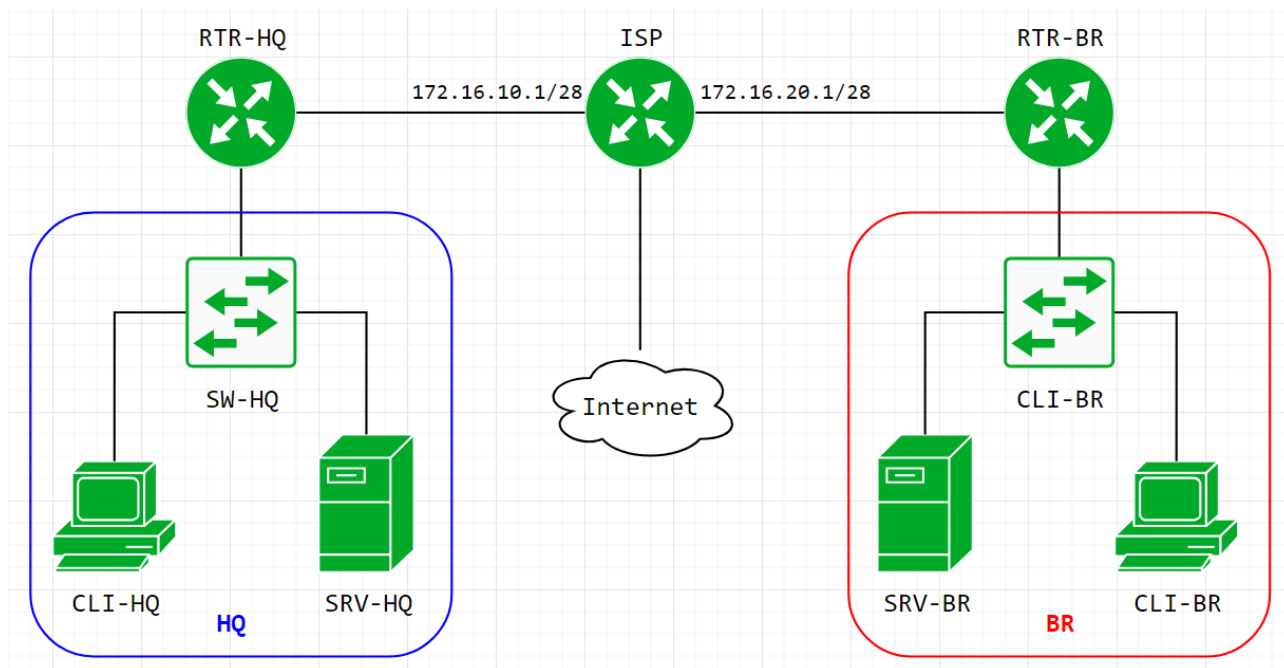


Рисунок 1. Топология

Таблица 1. Операционные системы в топологии

Название устройства	ОС
RTR-HQ	Eltex vESR
RTR-BR	Eltex vESR
SRV-HQ	Альт Сервер 10
SRV-BR	Альт Сервер 10
CLI-HQ	Альт Рабочая станция 10
CLI-BR	Альт Рабочая станция 10
SW-HQ	Альт Сервер 10
SW-BR	Альт Сервер 10

Таблица 2. Записи доменных имен

Запись	Тип записи
rtr-hq.company.prof	A
rtr-br.company.prof	A
sw-hq.company.prof	A
sw-br.company.prof	A
srv-hq.company.prof	A
srv-br.company.prof	A
cli-hq.company.prof	A
cli-br.company.prof	A
dbms.company.prof	CNAME
test.company.prof	A

Задания:

Базовая настройка

1. Настройте имена устройств согласно топологии и таблицы
 - a. Используйте полное доменное имя
2. Сконфигурируйте адреса устройств на свое усмотрение. Для офиса **HQ** выделена сеть 10.0.10.0/24, для офиса **BR** выделена сеть 10.0.20.0/24. Данные сети необходимо разделить на подсети для каждого vlan.
3. На **SRV-HQ** и **SRV-BR**, создайте пользователя **sshuser** с паролем **P@ssw0rd**
 - a. Пользователь **sshuser** должен иметь возможность запуска утилиты **sudo** без ввода пароля.
 - b. Аутентификация пользователя **sshuser** должна происходить только при помощи ключей. Запретите парольную аутентификацию.
 - c. Измените стандартный **ssh** порт на **2023**.
 - d. На **CLI-HQ** сконфигурируйте клиент для автоматического подключения к **SRV-HQ** и **SRV-BR** под пользователем **sshuser**. При подключении автоматически должен выбираться корректный порт. Создайте пользователя **sshuser** на **CLI-HQ** для обеспечения такого сетевого доступа.

Настройка дисковой подсистемы

1. На **SRV-HQ** настройте зеркалируемый LVM том
 - a. Используйте два неразмеченных жестких диска.
 - b. Настройте автоматическое монтирование логического тома.
 - c. Точка монтирования **/opt/data**.
2. На **SRV-BR** сконфигурируйте чередующийся LVM том.
 - a. Используйте два неразмеченных жестких диска.
 - b. Настройте автоматическое монтирование тома.
 - c. Обеспечьте шифрование тома средствами **dm-crypt**. Диск должен монтироваться при загрузке ОС без запроса пароля.
 - d. Точка монтирования **/opt/data**.

Настройка коммутации

1. В качестве коммутаторов используются **SW-HQ** и **SW-BR**.
2. В обоих офисах серверы должны находиться во `vlan100`, клиенты – во `vlan200`, management подсеть – во `vlan300`.
3. Создайте management интерфейсы на коммутаторах.
4. Для каждого `vlan` рассчитайте подсети, выданные для офисов. Количество хостов в каждой подсети не должно превышать 30-ти.

Установка и настройка сервера баз данных

1. В качестве серверов баз данных используйте сервера **SRV-HQ** и **SRV-BR**
2. Разверните сервер баз данных на базе PostgreSQL
 - a. Разрешите внешние подключения для всех пользователей.
 - b. Создайте пользователя БД **dbadmin** с паролем **P@ssw0rd**.
 - c. Создайте базы данных `prod`, `test`, `dev`
 - i. Разрешите полный доступ пользователю `dbadmin`
 - ii. Заполните базы данных тестовыми данными при помощи утилиты `pgbench`. Коэффициент масштабирования сохраните по умолчанию.
 - d. Сконфигурируйте репликацию с **SRV-HQ** на **SRV-BR**
 - e. Обеспечьте отказоустойчивость СУБД при помощи HAProxy.
 - i. HAProxy установите на **SW-HQ**.
 - ii. Режим балансировки – Hot-Standby: Активным необходимо сделать только **SRV-HQ**. В случае отказа **SRV-HQ** активным сервером должен становиться **SRV-BR**.
 - iii. Выбор `standby` режима (RO/RW) остается на усмотрение участника.
 - iv. Обеспечьте единую точку подключения к СУБД по имени `dbms.company.prof`

Настройка динамической трансляции адресов

1. Настройте динамическую трансляцию адресов для обоих офисов. Доступ к интернету необходимо разрешить со всех устройств.

Настройка протокола динамической конфигурации хостов

1. Настройте протокол динамической конфигурации хостов на обоих маршрутизаторах **RTR**:
 - a. Адрес сети – согласно топологии
 - b. Адрес шлюза по умолчанию – адрес маршрутизатора
 - c. DNS-суффикс – company.prof
2. Клиентские машины **CLI** получают адрес динамически из соответствующей подсети.

Настройка DNS для **SRV-HQ** и **SRV-BR**

1. Реализуйте основной DNS сервер компании на **SRV-HQ**
 - a. Для всех устройств обоих офисов необходимо создать записи **A** и **PTR**.
 - b. Для всех сервисов предприятия необходимо создать записи **CNAME**.
 - c. Создайте запись **test** таким образом, чтобы при разрешении имени из левого офиса имя разрешалось в адрес **SRV-HQ**, а из правого – в адрес **SRV-BR**.
 - d. Сконфигурируйте **SRV-BR**, как резервный DNS сервер. Загрузка записей с **SRV-HQ** должна быть разрешена только для **SRV-BR**.
 - e. Клиенты предприятия должны быть настроены на использование внутренних DNS серверов.

Настройка узла управления **Ansible**

1. Настройте узел управления на базе **SRV-BR**
 - a. Установите **Ansible**.
2. Сконфигурируйте инвентарь по пути **/etc/ansible/inventory**. Инвентарь должен содержать три группы устройств:
 - a. **networking**
 - b. **servers**

c. clients

3. Напишите плейбук в `/etc/ansible/gathering.yml` для сбора информации об IP адресах и именах всех устройств (и клиенты, и серверы, и роутеры). Отчет должен быть сохранен в `/etc/ansible/output.yml`, в формате ПОЛНОЕ_ДОМЕННОЕ_ИМЯ – АДРЕС

Между маршрутизаторами RTR-HQ и RTR-BR сконфигурируйте защищенное соединение

1. Все параметры на усмотрение участника.
2. Используйте парольную аутентификацию.
3. Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса.
4. Для обеспечения динамической маршрутизации используйте протокол OSPF.

На сервере SRV-HQ сконфигурируйте основной доменный контроллер на базе FreeIPA

1. Создайте 30 пользователей user1-user30.
2. Пользователи user1-user10 должны входить в состав группы group1.
3. Пользователи user11-user20 должны входить в состав группы group2.
4. Пользователи user21-user30 должны входить в состав группы group3.
5. Разрешите аутентификацию с использованием доменных учетных данных на клиентских машинах.
6. Установите сертификат центра сертификации FreeIPA в качестве доверенного на обоих клиентских ПК.

На SRV-BR сконфигурируйте проxy-сервер со следующими параметрами

1. Настройте клиенты офисов на использование прокси сервера предприятия
2. Пользователям group1 разрешен доступ в сеть Интернет, но не на какие-либо сервисы предприятия
3. Пользователям group2 разрешен доступ только на сервисы предприятия

4. Пользователям group3 не разрешен доступ никуда, также, как и пользователям, не прошедшим аутентификацию
5. Любым пользователям компьютера **СЛ-НЦ** разрешен доступ в сеть Интернет и на все сервисы предприятия, кроме доменов vk.com, mail.yandex.ru и worldskills.org
6. Авторизация для проху спрашивается браузером, SSO не ожидается

Модуль В. (Обеспечение отказоустойчивости)

Время на выполнение модуля 5 часов

Задания:

Данный модуль содержит задачи, основанные на практиках DevOps при разработке и эксплуатации информационных систем в сфере разработки современного программного обеспечения.

Главной задачей данного модуля является создание элементов автоматизированной инфраструктуры с помощью инструментов для работы с облачными средами и управления контейнерами. В рамках задания вам будет предоставлен доступ к инфраструктуре облачного провайдера. В качестве основной задачи необходимо подготовить инструкции для полностью автоматического развертывания приложения вместе со всеми необходимыми службами в облаке.

Для выполнения задания на ваших локальных компьютерах будет обеспечен доступ к сети Интернет.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

Доступ к облачному провайдеру и авторизацию на сервере выполняет экспертная группа. Главный эксперт сам определяет провайдера облачной инфраструктуры. В качестве платформы облачных вычислений используется OpenNebula - платформа с открытым исходным кодом для управления ресурсами разнородных центров обработки данных.

Все пункты задания необходимо реализовать на стороне провайдера облачной инфраструктуры. Эксперты будут ожидать наличие работоспособных элементов инфраструктуры согласно заданию.

Пункты задания, касающиеся настройки облака, потребуют от Вас написания автоматизированных сценариев развёртывания инфраструктуры согласно заданию. Конкретные инструменты выбираются на Ваше усмотрение. По завершении выполнения задания, ожидается, что будут полностью удалены автоматически созданные машины, сетевые и другие настройки в облачной инфраструктуре. Эксперты при проверке будут выполнять скрипт и проверять, что за отведённое (20 минут) время вся инфраструктура создаётся и работает должным образом.

Для проверки работоспособности скриптов автоматического развертывания инфраструктуры, эксперты могут проверять их работу в отдельной учётной записи того же облачного провайдера. Вам необходимо предусмотреть возможность указания необходимых параметров для работы скриптов с другой учетной записью облачного провайдера.

Проверка будет выполняться с инстанса ControlVM, вы можете установить все необходимые для вашей работы инструменты на указанную машину.

Подготовка машины ControlVM

1. Вся проверка выполнения задания будет проводиться с машины ControlVM.
2. НЕ удаляйте ControlVM по завершении задания.
3. Создайте инстанс с именем ControlVM и подключите его к сети интернет.
 - a. Тип виртуальной машины: 2 vCPU, Доля vCPU 50%, 2 RAM.
 - b. Размер диска: 10 ГБ.
 - c. Отключите мониторинг и резервное копирование.
 - d. Операционная система: ALT Linux 10.
 - e. Разрешите внешние подключения по протоколу SSH.
 - f. Сохраните ключевую пару для доступа на рабочем столе вашего локального ПК с расширением .pem
4. Настройте внешнее подключение к ControlVM.
 - a. На локальном ПК используйте клиент SSH PuTTY.
 - b. Создайте в PuTTY профиль с именем ONCloud.
 - c. Убедитесь в возможности установления соединения с ControlVM с локального ПК с помощью клиента PuTTY без ввода дополнительных параметров.
 - d. Используйте для подключения имя пользователя altlinux и загруженную ключевую пару.

Подготовка облачной инфраструктуры

1. Подготовьте сценарий автоматизации развёртывания облачной инфраструктуры.
 - a. Виртуальные машины и сети должны быть созданы согласно Топологии.

- b. Имена виртуальных машин и сетей должны соответствовать Топологии.
 - c. Обеспечьте подключение виртуальных машин к соответствующим сетям.
 - d. В случае предоставления внешнего доступа к созданным виртуальным машинам, он должен быть разрешён только по протоколу ssh.
 - e. Разрешите трафик по протоколу ICMP.
 - f. Вы можете назначить глобальные IP адреса для управления созданными виртуальными машинами.
 - g. Используйте аутентификацию на основе открытых ключей, аутентификация с использованием пароля должна быть отключена для SSH.
 - h. Создайте балансировщик нагрузки.
 - i. Сохраните внешний адрес балансировщика нагрузки в файле `/home/altlinux/lb.ip`.
 - ii. Ограничьте внешний доступ протоколами http и https.
 - iii. Балансировка нагрузки должна использовать алгоритм round robin.
 - iv. При обращении на внешний адрес балансировщика нагрузки должен выводиться ответ от приложения на внутреннем сервере.
2. Виртуальные машины должны соответствовать следующим характеристикам.
- a. Операционная система: ALT Linux 10.
 - b. Количество vCPU: 1.
 - c. Объём оперативной памяти: 1024 МБ.
 - d. Объём диска: 15 ГБ.
3. На машине ControlVM создайте скрипт `cloudinit.sh`.
- a. В качестве рабочей директории используйте путь `/home/altlinux/bin`.

- b. Используйте файл `/home/altlinux/bin/cloud.conf` для указания настроек для подключения к облачному провайдеру.
- c. При выполнении проверки, эксперты могут изменить настройки только в файле `cloud.conf`. Другие файлы редактироваться не будут.
- d. Вы можете оставить любые понятные комментарии в файле `cloud.conf`.
- e. Скрипт должен выполняться из любой директории без явного указания пути к исполняемому файлу.
- f. Выполнение задания ожидается с использованием инструментов Terraform и/или OpenStack CLI. Однако, вы вправе выбрать другие инструменты, не противоречащие условиям задания и правилам соревнования.

Развертывание приложений в Docker

1. На машине ControlVM.
 - a. Установите Docker и Docker Compose.
 - b. Создайте локальный Docker Registry.
 - c. В домашней директории хоста создайте файл `name.txt` и запишите в него строку `experts`.
 - d. Напишите Dockerfile для приложения HelloFIRPO.
 - i. В качестве базового образа используйте `alpine`
 - ii. Сделайте рабочей директорию `/hello` и скопируйте в неё `name.txt`
 - iii. Контейнер при запуске должен выполнять команду `echo`, которая выводит сообщение "Hello, FIRPO! Greetings from " и затем содержимое файла `name.txt`, после чего завершать свою работу.
 - iv. Соберите образ приложения и загрузите его в ваш Registry.
 1. Используйте название приложения `App2`
 2. Используйте номер версии `1.0` для вашего приложения

3. Образ должен быть доступен для скачивания и дальнейшего запуска на локальной машине.
- e. Создайте в домашней директории пользователя ubuntu файл `wiki.yml` для приложения MediaWiki.
- i. Средствами `docker compose` должен создаваться стек контейнеров с приложением MediaWiki и базой данных.
 - ii. Основной контейнер MediaWiki должен называться `wiki` и использовать образ `mediawiki`
 1. Файл `LocalSettings.php` с корректными настройками должен находиться в домашней папке пользователя ubuntu и автоматически монтироваться в образ.
 2. MediaWiki должна быть доступна извне через порт 80.
 - iii. Контейнер с базой данных должен называться `db` и использовать образ `mysql`
 1. Он должен создавать базу с названием `mediawiki`, доступную по стандартному порту, для пользователя `wiki` с паролем `P@ssw0rd`
 2. База должна храниться в отдельном `volume` с названием `dbvolume`
 3. База данных не должна быть доступна извне.
- f. Настройте мониторинг с помощью `NodeExporter`, `Prometheus` и `Grafana`.
- i. Создайте в домашней директории пользователя ubuntu файл `monitoring.yml` для `Docker Compose`
 - ii. Используйте контейнеры `NodeExporter`, `Prometheus` и `Grafana` для сбора, обработки и отображения метрик.
 - iii. Настройте `Dashboard` в `Grafana`, в котором будет отображаться загрузка CPU, объем свободной оперативной памяти и места на диске.

- iv. Интерфейс Grafana должен быть доступен по внешнему адресу на порту 3000.

Развёртывания облачных сервисов

1. На машине ControlVM создайте скрипт /home/ubuntu/bin/DeployApp.sh.
 - a. Скрипт должен выполняться из любой директории без явного указания пути к исполняемому файлу.
 - b. Подготовьте web-приложение App1
 - i. Скачайте файлы app1.py и Dockerfile по адресу: <https://github.com/auteam-usr/moscow39>
 - ii. Соберите образ приложения и загрузите его в ваш Docker Registry.
 - c. Команда DeployApp.sh должна запускать средства автоматизации для настройки операционных систем.
 - d. Разверните web-приложение App1 из репозитория Docker на виртуальных машинах Web1 и Web2.
 - e. Обеспечьте балансировку нагрузки между Web1 и Web2.
 - f. Обеспечьте внешний доступ к web-приложению по протоколу https.
 - g. При обращении по протоколу http должно выполняться автоматическое перенаправления на протокол https.
 - h. Обеспечивать доверие сертификату не требуется.

По завершении рабочего времени

- Высвободите выделенные ресурсы облачного провайдера для автоматически созданных объектов.
- Удалите все автоматически созданные виртуальные машины, сети, объекты, ресурсы.
- НЕ удаляйте ControlVM и необходимые для её работы ресурсы.

Обратите внимание, что при наличии в облачной инфраструктуре существующих объектов, за исключением объектов, необходимых для работы ControlVM, объектов по умолчанию проверка осуществляться не будет.

Топология виртуальной сети

