ВСЕРОССИЙСКОЕ
ЧЕМПИОНАТНОЕ
ДВИЖЕНИЕ
ПО ПРОФЕССИОНАЛЬНОМУ
МАСТЕРСТВУ

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Региональный этап чемпионата

по профессиональному мастерству

«Профессионалы»

(субъект РФ)

2027 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

Конкурсное задание включает в себя следующие разделы:

1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ……4
1.1. Общие сведения о требованиях компетенции……...4
1.2. Перечень профессиональных задач специалиста по компетенции «_____»……4
1.3. Требования к схеме оценки……5
1.4. Спецификация оценки компетенции……..5
1.5. Содержание конкурсного задания……..6
1.5.1. Разработка/выбор конкурсного задания……..6
1.5.2. Структура модулей конкурсного задания (инвариант/вариатив)…….7
2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ……8
2.1. Личный инструмент конкурсанта……...8
2.2.Материалы, оборудование и инструменты, запрещенные на площадке…..8
3. ПРИЛОЖЕНИЯ……...8

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

1. ФГОС – Федеральный государственный образовательный стандарт
2. ПС – Профессиональный стандарт
3. КЗ – Конкурсное задание
4. ИЛ – Инфраструктурный лист
5. ИКС – Информационно коммуникационная система
6. КС – Компьютерная сеть
7. ОС – Операционная система

1.ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

1.1. Общие сведения о требованиях компетенции

Требования компетенции (ТК) «Сетевое и системное администрирование» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

1.2. Перечень профессиональных задач специалиста по компетенции «Сетевое и системное администрирование»

Перечень видов профессиональной деятельности, умений, знаний и профессиональных трудовых функций специалиста (*из ФГОС/ПС/ЕТКС*) базируется на требованиях современного рынка труда к данному специалисту.

Таблица 1

Перечень профессиональных задач специалиста

№ п/п	Раздел	Важность в %
1	**Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах**	**20**
	Специалист должен знать и понимать: – Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения	

№ п/п	Раздел	Важность в %
	– Основы архитектуры, устройства и функционирования вычислительных систем – Принципы организации, состав и схемы работы операционных систем – Стандарты информационного взаимодействия систем – Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе – Инструкции по установке администрируемых сетевых устройств – Инструкции по эксплуатации администрируемых сетевых устройств – Инструкции по установке администрируемого программного обеспечения – Инструкции по эксплуатации администрируемого программного обеспечения – Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.	
	Специалист должен уметь: – Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки – Оценивать степень критичности инцидентов при работе прикладного программного обеспечения – Устранять возникающие инциденты – Локализовать отказ и инициировать корректирующие действия – Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий – Производить мониторинг администрируемой информационно-коммуникационной системы – Конфигурировать операционные системы сетевых устройств – Пользоваться контрольно-измерительными приборами и аппаратурой – Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику	
2	**Обеспечение работы технических и программных средств информационно-коммуникационных систем**	**25**
	Специалист должен знать и понимать – Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети – Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети	

№ п/п	Раздел	Важность в %
	– Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств – Инструкции по установке администрируемого программного обеспечения – Инструкции по эксплуатации администрируемого программного обеспечения – Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем – Базовая эталонная модель взаимодействия открытых систем; – Международные стандарты локальных вычислительных сетей; – Модели информационно-телекоммуникационной сети «Интернет» – Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе – Устройство и принцип работы кабельных и сетевых анализаторов – Средства глубокого анализа информационно-коммуникационной системы – Метрики производительности администрируемой информационно-коммуникационной системы – Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе – Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы	
	Специалист должен уметь: – Использовать современные методы контроля производительности информационно-коммуникационной системы – Анализировать сообщения об ошибках в сетевых устройствах и операционных системах – Локализовать отказ и инициировать корректирующие действия; – Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств – Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы – Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы	
3	**Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам**	**20**

№ п/п	Раздел	Важность в %
	Специалист должен знать и понимать: – Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы – Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы – Инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы – Инструкции по эксплуатации администрируемых сетевых устройств информационно-коммуникационной системы – Инструкции по установке администрируемого программного обеспечения – Инструкции по эксплуатации администрируемого программного обеспечения – Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем – Базовая эталонная модель взаимодействия открытых систем для управления сетевым трафиком – Международные стандарты локальных вычислительных сетей – Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе – Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы	
	Специалист должен уметь: – Использовать процедуры восстановления данных – Определять точки восстановления данных; работать с серверами архивирования и средствами управления операционных систем – Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий – Выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику	
4	**Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ**	**25**
	Специалист должен знать и понимать: – Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети – Основы архитектуры, устройства и функционирования вычислительных систем	

№ п/п	Раздел	Важность в %
	– Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств – Инструкции по установке администрируемого программного обеспечения – Лицензионные требования по настройке устанавливаемого программного обеспечения – Инструкции по эксплуатации администрируемого программного обеспечения – Типовые причины инцидентов, возникающих при установке программного обеспечения – Стандарты информационного взаимодействия систем – Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем – Принципы организации, состав и схемы работы операционных систем – Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы	
	Специалист должен уметь: – Использовать современные методы контроля производительности информационно-коммуникационной системы – Анализировать сообщения об ошибках в сетевых устройствах и операционных системах – Соблюдать процедуру установки прикладного программного обеспечения в соответствии с требованиями организации-производителя – Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение по изменению процедуры установки – Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств – Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы – Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы – Соблюдать процедуру установки прикладного программного обеспечения в соответствии с требованиями организации-производителя	
5	**Бережливое производство**	**5**
	Специалист должен знать и понимать:	

№ п/п	Раздел	Важность в %
	– Принципы функционирования информационно-коммуникационных системы	
	Специалист должен уметь: – Выполнять мероприятия модернизации информационно-коммуникационной системы, способствующие сокращению электропотребления	
6	**Охрана труда**	**5**
	Специалист должен знать и понимать: – Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы	
	Специалист должен уметь: – Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий	

Проверить/соотнести с ФГОС, ПС, Отраслевыми стандартами

1.3. Требования к схеме оценки

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице 2.

Таблица 2

Матрица пересчета требований компетенции в критерии оценки

Критерий/Модуль					**Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ**
Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ		**А**	**Б**	**Д**	
	1	5	15	-	20
	2	5	15	5	25
	3	5	5	10	20
	4	-	5	20	25
	5	-	-	5	5
	6	5	-	-	5
Итого баллов за критерий/модуль		20	40	40	**100**

1.4. Спецификация оценки компетенции

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице 3.

Таблица 3

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.
Д	**DevOps**	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.

1.5. Содержание конкурсного задания

Общая продолжительность Конкурсного задания[1]: 15 часов 0 минут

Количество конкурсных дней: 3 дня

Вне зависимости от количества модулей, КЗ включает оценку по каждому из разделов требований компетенции.

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

1.5.1. Разработка/выбор конкурсного задания

Конкурсное задание состоит из 3 модулей, включает обязательную к выполнению часть (инвариант) - 2 модулей, и вариативную часть - 1 модуль. Общее количество баллов конкурсного задания составляет 100.

Обязательная к выполнению часть (инвариант) выполняется всеми регионами без исключения на всех уровнях чемпионатов.

Модули вариативной части выбираются регионом самостоятельно в зависимости от потребностей работодателей региона в соответствующих специалистах. Регионы могут использовать вариативные модули, представленные в типовом конкурсном задании. В случае если ни один из модулей вариативной части не подходит под запрос работодателя конкретного региона, то вариативный(е) модуль(и) формируется регионом самостоятельно под запрос работодателя. При этом, время на выполнение модуля(ей) и количество баллов в критериях оценки по аспектам не меняются.

Исключать вариативные модули из конкурсного задания запрещено.

[1] *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.*

1.5.2. Структура модулей конкурсного задания

Модуль А. Аудит (вариатив)

Время на выполнение модуля: 4 часа 0 минут

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: 6 часов 0 минут

Задания:

Таблица ОС:

VM	OS
GW-CORE	Альт Сервер 11/или аналог
GW-1	EcoRouterOS Pesto/или аналог
GW-2	EcoRouterOS Pesto/или аналог
GW-3	EcoRouterOS Pesto/или аналог
PROVIDER-GW	Eltex (vESR)/или аналог
PROVIDER-SW	Eltex (vESR)/или аналог
ZSPD-FW	Ideco NGFW NOVUM 22/или аналог
ZSPD-SW	Альт Сервер 11/или аналог
COD-GW	EcoRouterOS Pesto/или аналог
COD-SRV-1	Альт Сервер 11/или аналог
COD-SRV-2	Альт Сервер 11/или аналог
COD-ADMIN	Альт Рабочая станция 11/или аналог
PUB	Альт Сервер 11/или аналог
DATA	Альт Сервер 11/или аналог

Таблица 1 - VLAN в COD:

Описание сети	Служебное имя	VLAN
Магистральный трафик провайдера	ISP	untagged
Трафик инфраструктуры	COD	10
Внутренний трафик СХД	DATA	20
Анонсируемые другим AS адреса	PUBLIC	30

Таблица 2 - VLAN в PROVIDER:

Описание сети	Служебное имя	VLAN
Магистральный трафик провайдера	ISP	25

Таблица 3 - VLAN в ZSPD:

Описание сети	Служебное имя	VLAN
Магистральный трафик провайдера	ISP	17

Таблица 4 – Описание доменной зоны ssa.prof:

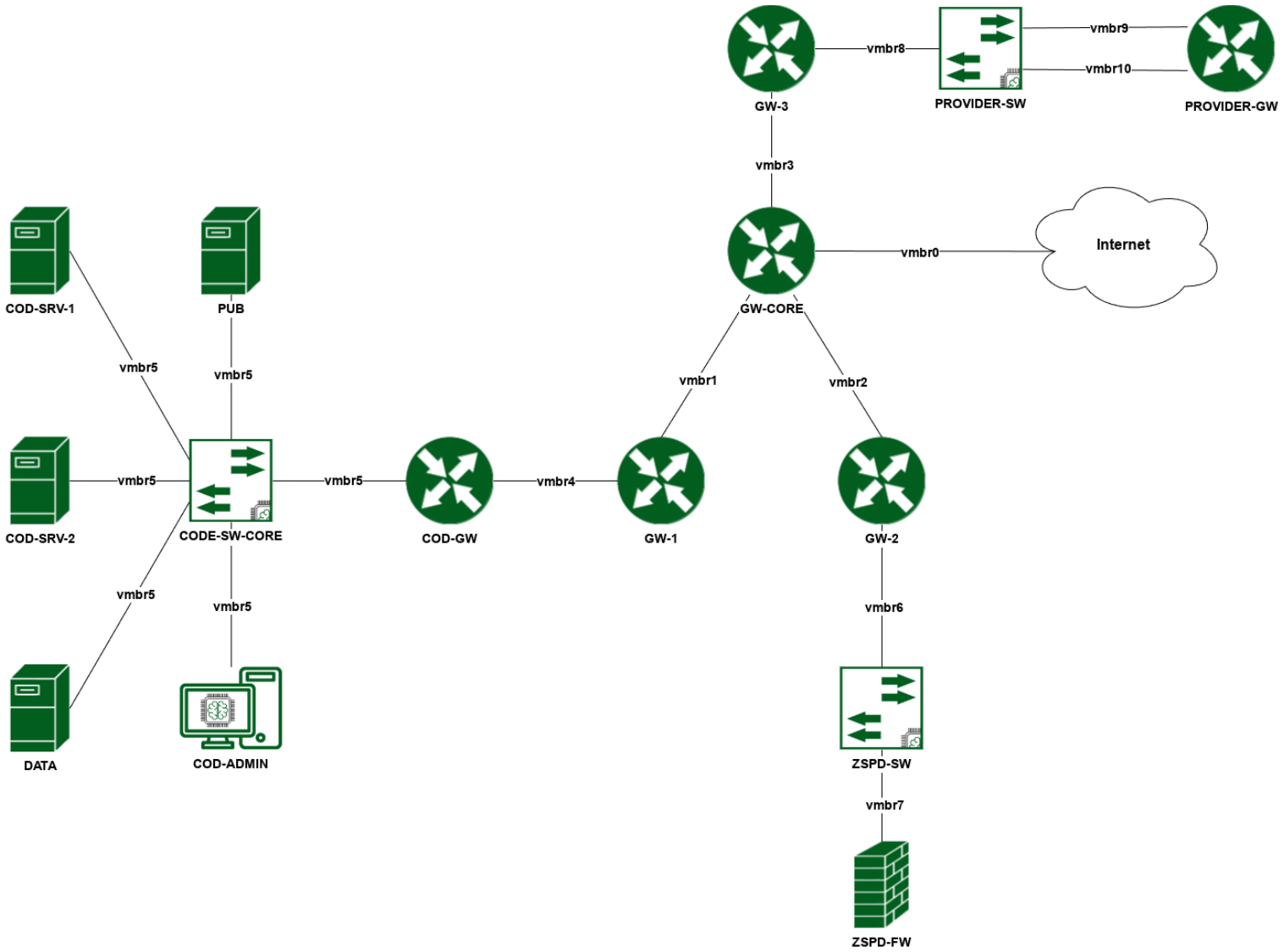
Устройство	Полное доменное имя	Тип записи	Адрес, который был назначен на интерфейс

GW-CORE	gw-core.ssa.prof	A	dummy/loopback
GW-1	gw-1.ssa.prof	A	loopback
GW-2	gw-2.ssa.prof	A	loopback
GW-3	gw-3.ssa.prof	A	loopback
COD-GW	cod-gw.ssa.prof	A	loopback
PROVIDER-GW	provider-gw.ssa.prof	A	подключенный к внешней сети
ZSPD-FW	zspd-fw.ssa.prof	A	подключенный к внешней сети
ZSPD-SW	zspd-sw.ssa.prof	A	MGMT
PUB	pub.ssa.prof	A	из сети PUBLIC

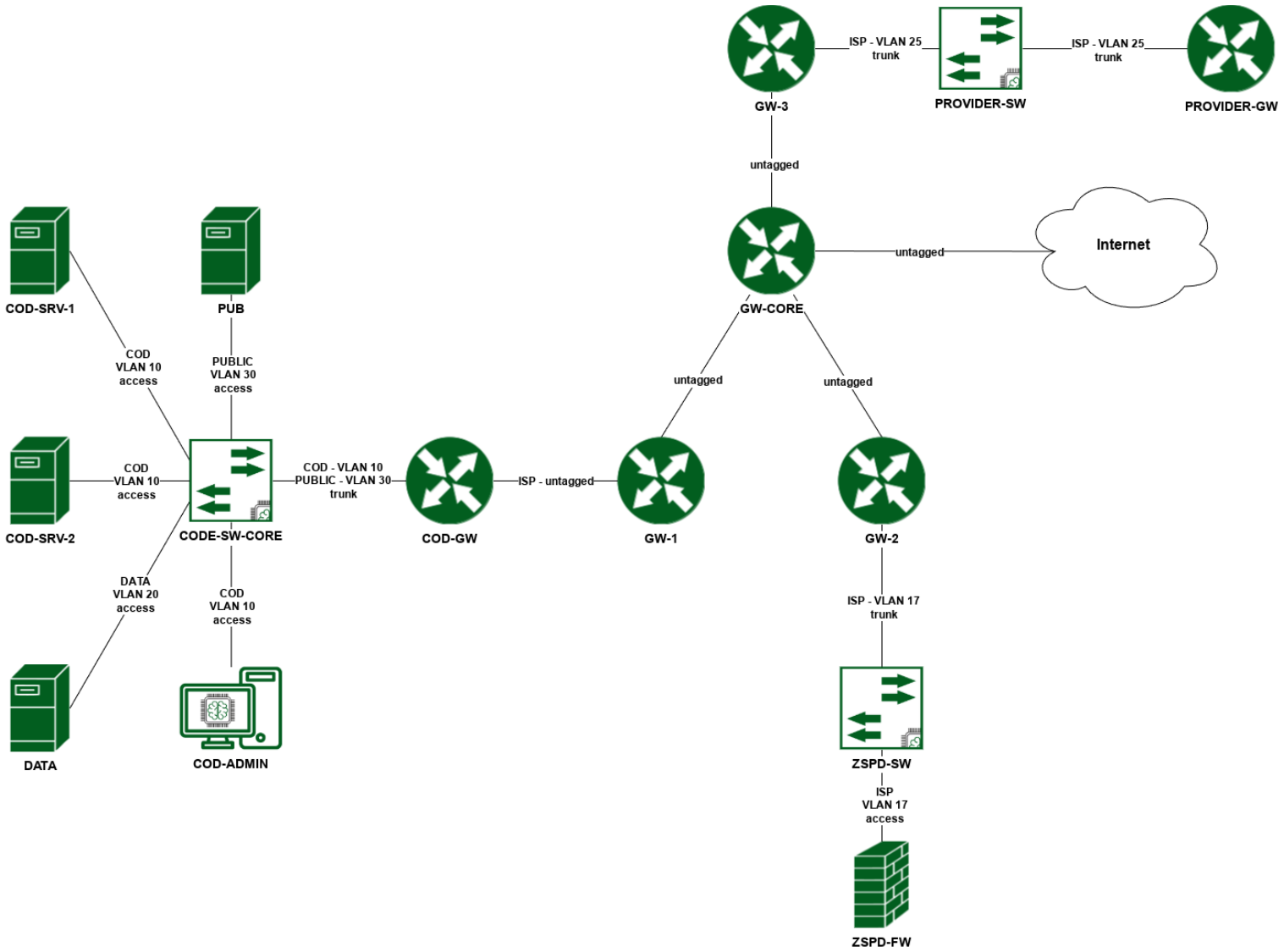
Таблица 5 – Описание доменной зоны cod.ssa.prof :

Устройство	Полное доменное имя	Тип записи	Адрес, который был назначен на интерфейс
COD-SRV-1	cod-srv-1.cod.ssa.prof	A,PTR	из сети COD
COD-SRV-2	cod-srv-2.cod.ssa.prof	A,PTR	из сети COD
DATA	data.cod.ssa.prof	A,PTR	из сети DATA
COD-ADMIN	cod-admin.cod.ssa.prof	A,PTR	DHCP

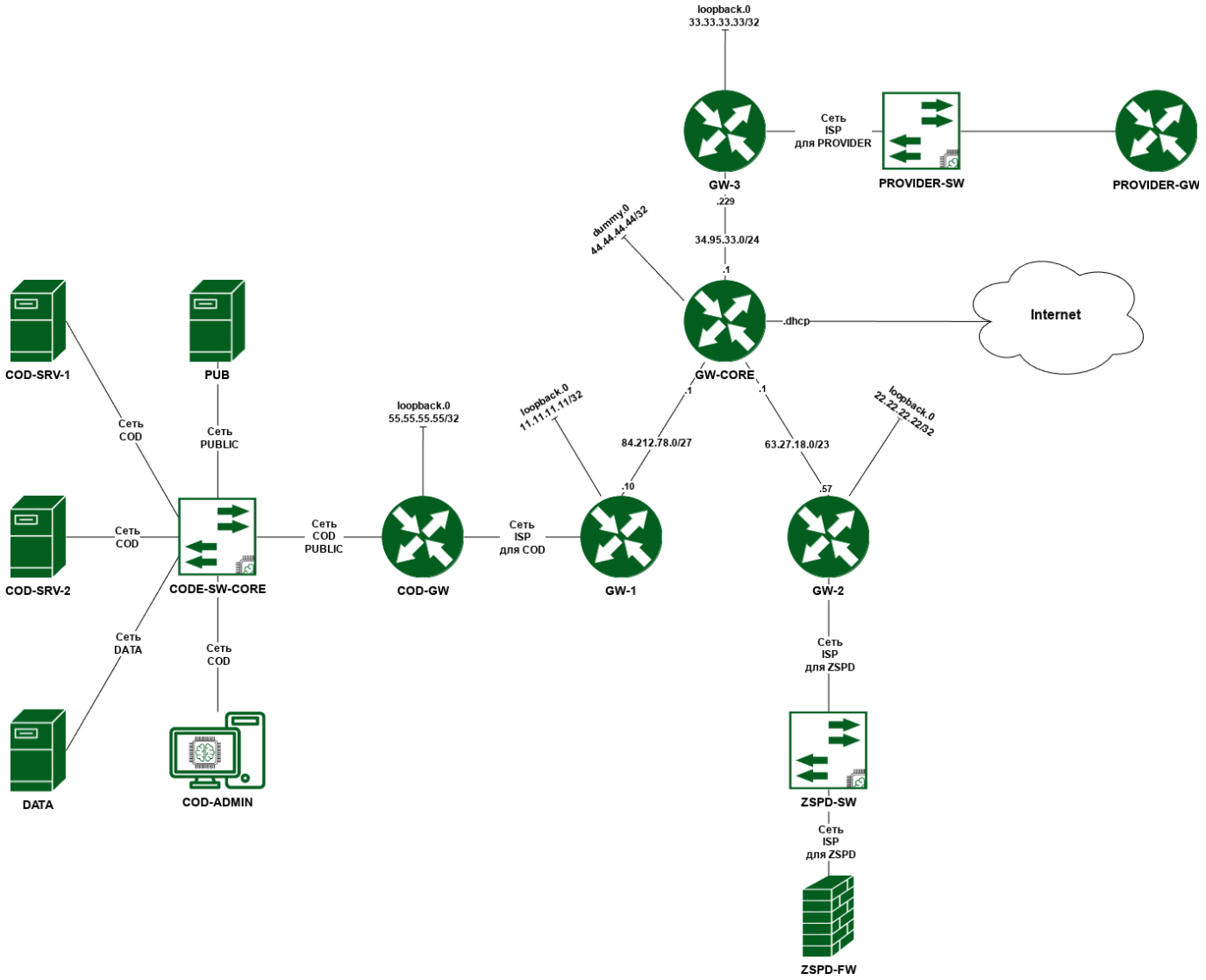
Топология L1:



Топология L2:



Топология L3:



1. **Настройка базовых параметров:**

a. Настройте имена устройств в соответствии с топологией:

i. На устройствах GW-*, PROVIDER-*, ZSPD-* в качестве доменного имени используйте ssa.prof;

ii. На устройствах COD-* в качестве доменного имени используйте cod.ssa.prof;

iii. На остальных устройствах использовать доменное имя не требуется.

b. На устройствах COD-*, GW-*, PROVIDER-*, ZSPD-SW добавьте административную учетную запись master с паролем P@ssw0rd:

i. На устройстве GW-CORE необходимо обеспечить выполнение утилиты sudo без запроса пароля;

ii. На устройстве ZSPD-SW необходимо обеспечить выполнение утилиты sudo с вводом пароля;

iii. На маршрутизаторах EcoRouter сконфигурируйте хранение паролей в защищенном виде.

iv. На маршрутизаторе COD-GW выполните настройку пароля для enable режима. В качестве пароля используйте P@ssw0rd. В конфигурации пароль должен хранится в виде результата хэш функции.

v. На маршрутизаторах GW-* деактивируйте встроенную учетную запись администратора.

c. Обеспечьте административный доступ по протоколу SSH:

i. Для доступа используйте доменные имена согласно таблице 4;

ii. Требуется возможность подключения к сетевым устройствам с COD-ADMIN:

1. Используйте встроенную консоль (cmd).

d. Настройте адресацию в соответствии с топологией и требованиями пунктов ниже:

i. Если в задании не указаны IP адреса для той или иной сети – настройте адресацию на ваше усмотрение.

ii. В случае настройки адресации на ваше усмотрение не забудьте обеспечить доступ к устройству с использованием системы доменных имен.

iii. Заказчик не будет заниматься аудитом инфраструктуры, и в случае недоступности сервиса или устройства по доменному имени, его проверка произведена не будет.

e. Для доступа в интернет следует получить IP адрес по DHCP на устройстве GW-CORE.

2. Настройка обмена маршрутной информацией по протоколу BGP между маршрутизаторами GW-*:

a. В качестве ASN используйте 64499 (AS Провайдера);

b. Доступ в Интернет предоставляется через GW-CORE. Маршруты необходимо передавать по iBGP;

c. Используйте dummy/loopback интерфейсы для установления соседства по iBGP;

d. В качестве IGP используйте протокол IS-IS;

i. Используйте маршрутизацию в пределах одной зоны;

ii. Используйте выбранные Вами адреса dummy/loopback в качестве SYSTEM ID;

e. RID BGP должен соответствовать адресу dummy/loopback интерфейса устройства, использующегося для обмена по iBGP;

f. Передавать все маршруты запрещено.

3. Настройка коммутации:

a. COD-SW-CORE является виртуальными коммутаторами на уровне гипервизора. Необходимо настроить VID (тег) на портах (Network Device в Hardware BM) оконечных устройств (виртуальных машин).

b. Для настройки коммутации на ZSPD-SW используйте Open vSwitch

i. Имя коммутатора должно совпадать с коротким именем устройства.

1. Используйте заглавные буквы.

ii. Добавьте все физические порты в коммутатор.

iii. Разрешите на магистральных каналах только используемые VLAN.

iv. Создайте интерфейс управления с именем MGMT

1. Для интерфейса управления используйте сеть ISP (таблица 3)

c. Для настройки коммутации на PROVIDER-SW

i. Разрешите на магистральных каналах только используемые VLAN.

d. Агрегируйте каналы между PROVIDER-GW и PROVIDER-SW.

i. Используйте протокол LACP.

4. Настройка оптимальной адресации для клиентских маршрутизаторов и хостов из PA-диапазона 78.23.0.0/24 с учётом максимального количества полезных IPv4-адресов:

a. COD-GW – 6 адресов;

b. ZSPD-FW – 30 адресов;

c. PROVIDER-GW - 62 адреса.

5. Настройка сети COD:

a. Сегментируйте сетевое пространство в соответствии с таблицей 1 и топологией:

b. В качестве ASN используйте 65005 (AS ЦОД-А);

c. В качестве IGP используйте протокол OSPF;

i. Интерфейсы, не участвующие в процессе OSPF, должны быть переведены в пассивный режим.

ii. COD-GW по OSPF должен получать только маршрут до адреса интерфейса loopback на GW-1;

iii. На GW-1 настройте перераспределение OSPF маршрутов в BGP;

d. Используйте loopback интерфейсы для установления соседства по BGP;

e. RID OSPF и BGP должен соответствовать адресу loopback интерфейса устройства, использующегося для обмена по OSPF/BGP;

f. Обеспечьте передачу необходимой маршрутной информации и трафика для взаимодействия COD с внешними сетями.

i. COD-GW маршрут по умолчанию должны получать по BGP

ii. Анонсируйте Провайдеру по BGP подсеть 212.78.93.0/24 для дальнейшей публикации ресурсов.

iii. Передача внутренних подсетей Провайдеру не допускается.

6. Настройка технологии трансляции адресов на устройствах:

a. На GW-CORE обеспечьте трансляцию PA-диапазона 78.23.0.0/16 и PI-диапазона 212.78.93.0/24 для предоставления доступа в сеть Интернет;

b. Использование технологии допускается только на COD-GW и GW-CORE;

7. Настройка службы доменных имен:

a. Настройте GW-CORE в качестве DNS сервера:

i. DNS сервер должен быть доступен только по адресам 127.0.0.1 и dummy/loopback интерфейса;

ii. DNS-сервер должен обслуживать зону ssa.prof:

1. Обеспечьте определение имён в соответствии с таблицей 4.

iii. В качестве DNS сервера пересылки используйте 77.88.8.8;

iv. Все устройства, где требуется выход Интернет и нет особых требований, должны использовать данный сервер в качестве основного DNS.

b. Настройте ZSPD-FW в качестве DNS сервера:

i. В качестве внешнего DNS сервера используйте GW-CORE.

c. Настройте COD-SRV-1 в качестве DNS сервера:

i. DNS-сервер должен обслуживать зону cod.ssa.prof:

1. Обеспечьте определение имён в соответствии с таблицей 5.

ii. В качестве внешнего DNS сервера используйте GW-CORE;

8. Настройка протокола динамической конфигурации хостов:

a. На COD-SRV-1 реализуйте DHCP-сервер на базе Kea-DHCPv4:

i. DHCP-сервер должен обслуживать подсеть COD;

ii. В качестве диапазона раздаваемых IP-адресов используйте адреса с 100 по 200 включительно;

iii. В качестве адреса шлюза по умолчанию используйте адрес соответствующего маршрутизатора в требуемой сети;

iv. В качестве адреса DNS-сервера используйте адрес COD-SRV-1;

v. В качестве DNS-суффикса используйте cod.ssa.prof;

vi. COD-ADMIN должен получать все необходимые сетевые параметры автоматически;

vii. DNS-записи типа A и PTR соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.

9. Настройка синхронизации времени между сетевыми устройствами:

a. В качестве сервера времени должен выступать GW-CORE

i. Используйте стратум 5;

ii. Используйте ntp2.vniiftri.ru в качестве внешнего сервера синхронизации времени;

iii. Используйте московский часовой пояс.

b. Устройства ZSPD-SW и ZSPD-FW должны синхронизировать время с GW-CORE:

i. Используйте московский часовой пояс;

ii. Используйте chrony где это возможно.

10. Настройка устройства хранения данных:

a. Используйте хост DATA;

b. Диски сгруппируйте в исполнении RAID 0;

c. Настройте iSCSI target:

i. Используйте имя цели iqn.<№ текущего года>-<№ текущего месяца>.prof.ssa.cod:data;

ii. Настройте отдачу RAID-массива по iSCSI .

11. Настройка центра сертификации:

a. На COD-SRV-1 разверните центр сертификации на базе openssl:

i. Используйте директорию /etc/openssl/CA для файлов

ii. Срок жизни корневого сертификата должен составлять 5 лет;

iii. Код страны – RU;

iv. Название организации – PROF;

v. Название подразделения – SSA;

vi. Имя центра сертификации – COD;

b. COD-ADMIN должен доверять центру сертификации;

c. Используйте созданный центр сертификации для выпуска требуемых сертификатов.

12. Настройка сервера баз данных:

a. В качестве сервера баз данных используйте COD-SRV-1:

i. В качестве СУБД используйте PostgreSQL:

1. Используйте версию 18;

2. Для пользователя postgres используйте пароль P@ssw0rd.

ii. Создайте суперпользователя superadmin с паролем P@ssw0rdSQL:

1. Суперпользователь должен иметь полный доступ ко всем базам данных.

13. Настройка системы мониторинга:

a. В качестве сервера системы мониторинга используйте COD-SRV-1;

b. В качестве системы мониторинга используйте Zabbix версии не ниже 7.0:

i. В качестве СУБД используйте PostgreSQL на COD-SRV-1:

1. Имя базы данных: zabbix;

2. Пользователь базы данных: zabbix_user;

3. Пароль пользователя базы данных: P@ssw0rdZabbix.

ii. В качестве веб-сервера используйте NGINX.

c. Система мониторинга должна быть доступна по по адресу https://srv-cod.cod.ssa.prof:8080:

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

ii. Часовой пояс по умолчанию должен быть Europe/Moscow;

iii. При обращении к Системе мониторинга по адресу http://srv-cod-1.cod.ssa.prof:8080, должно перенаправлять на адрес https://srv-cod-1.cod.ssa.prof:8080 и не должно отображаться ошибок и предупреждений.

d. Настройте узлы системы мониторинга:

i. В качестве узлов сети используйте устройства PUB, DATA и COD-GW;

ii. Имя узла сети должно соответствовать короткому имени устройства:

1. Используйте заглавные буквы.

iii. При настройке интерфейса узла сети используйте DNS имя;

iv. PUB и DATA необходимо поместить в группу узлов Servers:

1. Используйте шаблон Linux by Zabbix agent.

v. COD-GW необходимо поместить в группу узлов Network devices:

1. Используйте шаблон Cisco IOS by SNMP.

14. Настройка системы резервного копирования:

a. Установку сервера управления Кибер Бэкап (версии не ниже 18) выполните на хосте DATA;

i. Сервер управления должен быть доступен с COD-ADMIN по имени cb.cod.ssa.prof на порту 9877.

ii. Доступ в веб-интерфейс сервера управления должен быть из-под пользователя root с паролем toor;

iii. Для установки сервера управления в качестве СУБД необходимо использовать PostgreSQL на хосте COD-SRV-1.

b. Установку агента для PostgreSQL выполните на хосте COD-SRV-1 с последующей регистрацией на сервере управления;

c. Установку агента для Linux выполните на хосте COD-ADMIN с последующей регистрацией на сервере управления.

Модуль Д. DevOps (инвариант)

Время на выполнение модуля: 5 часов 0 минут

Задания:

Выполняется на базе инфраструктуры модуля Б.

15. Настройка управления СУБД:

a. Для администрирования сервера баз данных используйте pgAdmin4 на COD-SRV-1:

i. Установите pgAdmin4 в режиме веб-сервера;

ii. Веб-интерфейс pgAdmin4 должен быть доступен по адресу https://cod-srv-1.cod.ssa.prof:5050:

1. При обращении к Веб-интерфейсу по адресу http://cod-srv-1.cod.ssa.prof:5050, должно перенаправлять на адрес https://cod-srv-1.cod.ssa.prof:5050 и не должно отображаться ошибок и предупреждений.

iii. Для авторизации используйте пользователя pgadmin@cod.ssa.prof с паролем P@ssw0rd;

iv. В pgAdmin4 зарегистрируйте сервер баз данных используя суперпользователя superadmin.

16. Настройка менеджера репозиториев для централизованного хранения и управления артефактами:

a. Установите Docker на COD-SRV-2;

b. Напишите файл compose.yml для развёртывания настроенного и готового к работе Nexus:

i. Настройте volume для сохранения данных сервиса Nexus с именем nexus-data;

ii. В качестве СУБД используйте PostgreSQL на COD-SRV-1;

1. Имя базы данных: nexus;

2. Пользователь базы данных: nexus_user;

3. Пароль пользователя базы данных: P@ssw0rdNexus.

iii. Веб-интерфейс сервиса Nexus должен быть доступен по адресу nexus.cod.ssa.prof

1. При обращении к Веб-интерфейсу по адресу http://nexus.cod.ssa.prof, должно перенаправлять на адрес https://nexus.cod.ssa.prof и не должно отображаться ошибок и предупреждений;

iv. Создайте учётную запись в Nexus:

1. Имя учётной записи: devops, пароль: P@ssw0rd;

2. Пользователь devops должен обладать правами администратора.

v. Создайте в Nexus Docker hosted репозиторий для хранения Docker-образов доступный на порту 8083.

20. Настройка платформы для работы с кодом:

a. На сервере PUB установите GitFlic в режиме Self-Hosted:

i. В качестве СУБД используйте PostgreSQL на COD-SRV-1:

1. Имя базы данных: gitflic;

2. Пользователь базы данных: gitflic_user;

3. Пароль пользователя базы данных: P@ssw0rdGitFlic.

ii. Веб-интерфейс сервиса GitFlic должен быть доступен по адресу git.ssa.prof:

1. При обращении к Веб-интерфейсу по адресу http://git.ssa.prof, должно перенаправлять на адрес https://git.ssa.prof и не должно отображаться ошибок и предупреждений;

2. Измените пароль для пользователя adminuser@admin.local на P@ssw0rd.

b. Зарегистрируйте пользователя Devops Master:

i. Используйте почтовый адрес devops@ssa.prof;

ii. В качестве пароля используйте P@ssw0rd;

iii. Создайте приватный проект с именем app.

c. На PUB и COD-SRV-2 установите GitFlic Runner в режиме Shell:

i. Не используйте запуск GitFlic Runner в контейнере.

ii. Зарегистрируйте установленные GitFlic Runner в проекте app:

1. GitFlic Runner установленный на PUB должен иметь имя PUB и тег prod;

2. GitFlic Runner установленный на COD-SRV-2 должен иметь имя COD-SRV-2 и тег test.

21. Настройка приложения:

a. На хосте COD-SRV-2 напишите Dockerfile для приложения django-girls-wo-docker (https://disk.yandex.ru/d/eyDpftUg5ncrPA):

i. В качестве базового образа используйте python:3.9-alpine;

ii. В качестве рабочей директории используйте /app;

iii. Для связи используйте порт 8000

b. Запустите приложение на COD-SRV-2:

i. Веб-интерфейс приложения должен быть доступен по адресу http://cod-srv-2.cod.ssa.prof:8000

c. Исходный код приложения разместите в приватном проекте app в системе контроля версий.

d. Собранный образ запушьте в Nexus Docker hosted репозиторий:

i. Имя образа должно быть django-girls;

ii. Тег образа должен быть v.0.1.

22. Настройка платформы наблюдаемости:

a. На хосте PUB установите Grafana, Loki, Tempo (single-binary) и Prometheus:

i. Обеспечьте доступ:

1. Grafana – http://grafana.ssa.prof:3000;

2. Prometheus – http://prometheus.ssa.prof:9090;

ii. Loki должен принимать логи на порту 3100, Tempo – OTLP-трейсы на порту 3200;

iii. На GW-CORE добавьте A-записи в зону ssa.prof для имён grafana, loki, tempo, prometheus.

b. На хосте COD-SRV-2:

i. Напишите Dockerfile для Jaeger HotROD (https://disk.yandex.ru/d/hgAR6Fz55WnH_A - Демо-приложение HotROD генерирует три сигнала (логи/метрики/трейсы), по которым видно ошибки и латентность бизнес-операций) и запустите контейнер;

ii. Веб-интерфейс приложения должен быть доступен по адресу http://hotrod.cod.ssa.prof:8080;

iii. Установите Grafana Alloy и настройте:

1. Сбор логов контейнера HotROD и отправку в Loki (http://loki.ssa.prof:3100);

2. Сбор метрик узла и контейнеров (экспортеры unix и cadvisor) с remote_write в Prometheus;

3. OTLP-приём трейсов и форвардинг в Tempo (http://tempo.ssa.prof:3200);

iv. Убедитесь, что трейсы приложения поступают в Tempo.

c. В Grafana настройте источники данных Prometheus, Loki, Tempo и корреляцию Trace-to-Logs.

d. Создайте дашборды и алерты:

i. Базовые дашборды инфраструктуры (CPU, RAM, диск) и приложения (ошибки, задержки);

ii. Настройте алерты: высокая загрузка, заполнение диска, недоступность узла, рост ошибок/латентности приложения.

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ[2]

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

– Систем контроля версий, если это не раздел с документацией

– Общения посредством форумов/мессенджеров/иных средств коммуникации – видеохостингов, а также помощь 3-х лиц

– Средств, требующих авторизацию любой формы, а также вход на ресурс под гостевой учётной записью

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.

3. ПРИЛОЖЕНИЯ

Приложение 1. Инструкция по заполнению матрицы конкурсного задания

Приложение 2. Матрица конкурсного задания

Приложение 3. Инструкция по охране труда

Приложение 4. Чек-лист компетенции

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