



ЧЕМПИОНАТ
ПО ПРОФЕССИОНАЛЬНОМУ
МАСТЕРСТВУ

ЧЕМПИОНАТ
ПРОФЕССИОНАЛЬНОГО МАСТЕРСТВА
ГОРОДА МОСКВЫ

МОСКОВСКИЕ
МАСТЕРА
2025



КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «Сетевое и системное администрирование»

Чемпионата профессионального мастерства города Москвы «Московские мастера» регионального этапа Чемпионата по профессиональному мастерству «Профессионалы» в 2025 г.

Основная категория

2025 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	3
1.1. Общие сведения о требованиях компетенции	3
1.2. Перечень профессиональных задач специалиста по компетенции «_____»	3
1.3. Требования к схеме оценки	9
1.4. Спецификация оценки компетенции	9
1.5. Конкурсное задание	10
1.5.1. Разработка/выбор конкурсного задания	10
1.5.2. Структура модулей конкурсного задания (инвариант/вариатив)	11
2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ	30
2.1. Личный инструмент конкурсанта	30
2.2. Материалы, оборудование и инструменты, запрещенные на площадке	30
3. ПРИЛОЖЕНИЯ	30

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 и знаний и профессиональных трудовых функций специалиста (из ФГОС/ПС/ЕТКС..) и 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	25
	- Специалист должен знать и понимать:	

	<p>Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения</p> <p>Основы архитектуры, устройства и функционирования вычислительных систем</p> <p>Принципы организации, состав и схемы работы операционных систем</p> <p>Стандарты информационного взаимодействия систем</p> <p>Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе</p> <p>Инструкции по установке администрируемых сетевых устройств</p> <p>Инструкции по эксплуатации администрируемых сетевых устройств</p> <p>Инструкции по установке администрируемого программного обеспечения</p> <p>Инструкции по эксплуатации администрируемого программного обеспечения</p> <p>Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.</p>	
	<p>- Специалист должен уметь:</p> <p>Идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки</p> <p>Оценивать степень критичности инцидентов при работе прикладного программного обеспечения</p> <p>Устранять возникающие инциденты</p> <p>Локализовать отказ и инициировать корректирующие действия</p> <p>Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий</p> <p>Производить мониторинг администрируемой информационно-коммуникационной системы</p> <p>Конфигурировать операционные системы сетевых устройств</p> <p>Пользоваться контрольно-измерительными приборами и аппаратурой</p>	

	Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику	
	Обеспечение работы технических и программных средств информационно-коммуникационных систем	
	- Специалист должен знать и понимать Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах; Локализовывать 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;	
2	- Специалист должен уметь: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; 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	25

	<p>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;</p>	
3	<p>Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам</p> <p>- 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</p>	25

	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: Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах; Локализовывать 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;	
	- Специалист должен уметь: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого	

	<p>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;</p>	
--	---	--

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		Б	Г	
	1	25	0	25
	2	25	0	25
	3	5	20	25
	4	5	20	25
Итого баллов за критерий/модуль		60	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
Б	Настройка технических и программных средств информационно-коммуникационных систем	В соответствии с используемыми ОС и Сетевым оборудованием
Г	Обеспечение отказоустойчивости	В соответствии с используемыми ОС и Сетевым оборудованием

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Общая продолжительность Конкурсного задания: 15 ч.

Количество конкурсных дней: 3 дня (1 и 2 день – Модуль Б; 3 день – Модуль Г).

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

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания.

1.5.1. Разработка/выбор конкурсного задания

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

1.5.2. Структура модулей конкурсного задания

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

Время на выполнение модуля 10 часов

Задания:

Часть 1 (1 день - 5 часов)

1) Базовая настройка

а) Настройте имена устройств согласно топологии

1. Используйте полное доменное имя

```
EcoRouter: conf t
```

```
hostname (имя домена)
```

```
Alt Server: nano /etc/hostname
```

б) Сконфигурируйте адреса устройств на свое усмотрение.

1. Для офиса HQ выделена сеть 192.168.11.0/24

```
EcoRouter:
```

```
en
```

```
conf
```

```
int R-HQ
```

```
ip add 192.168.11.1/24
```

```
no sh
```

```
port ge0 (какой будет)
```

```
service-instance R-HQ
```

```
encapsulation untagged
```

```
connect ip int R-HQ
```

```
AltServer - client:
```

```
nano /etc/net/ifaces/<имя интерфейса>/options
```

```

BOOTPROTO=dhcp
TYPE=eth
NM_CONTROLLED=yes no
DISABLED=yes no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp static
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no

```

```
echo 192.168.11.2/24 >> /etc/net/ifaces/<имя интерфейса>/ipv4address
```

2. Для офиса DT выделена сеть 192.168.33.0/24

EcoRouter:

```

en
conf
int R-DT
ip add 192.168.33.1/24
no sh
port ge0 (какой будет)
service-instance R-DT
encapsulation untagged
connect ip int R-DT

```

AltServer - client:

```
nano /etc/net/ifaces/<имя интерфейса>/options
```

```

BOOTPROTO=dhcp
TYPE=eth
NM_CONTROLLED=yes no
DISABLED=yes no
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp static
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no

```

```
echo 192.168.33.2/24 >> /etc/net/ifaces/<имя интерфейса>/ipv4address
```

3. Для туннелей между офисами выделена сеть 10.10.10.0/24

i. Туннель должен вмещать минимально возможное количество адресов

```
en
```

```
conf t
int tunnel.0
ip add 10.10.10.1/30 (ip add 10.10.10.2/30)
ip tunnel 10.10.10.1 10.10.10.2 mode gre (ip tunnel 10.10.10.2 10.10.10.1
mode gre)
no sh
port ge0
service-instance tunnel.0
encapsulation untagged
connect ip int tunnel.r
ex
ex
```

4. Данные сети необходимо разделить на подсети для каждого vlan.

i. VLAN110 должна вмещать не более 64 адресов

```
int (нужный интерфейс)
ip add (Нужный адрес)/26
port (нужный порт)
service-instance ge(номер порта)
encapsulation dot1q 110 exact
rewrite pop 1
connect ip interface (нужный интерфейс)
```

ii. VLAN220 должна вмещать не более 16 адресов

```
int (нужный интерфейс)
ip add (Нужный адрес)/28
port (нужный порт)
service-instance ge(номер порта)
encapsulation dot1q 220 exact
rewrite pop 1
```

```
connect ip interface (нужный интерфейс)
```

iii. VLAN330 должна вмещать не более 8 адресов

```
int (нужный интерфейс)
```

```
ip add (Нужный адрес)/29
```

```
port (нужный порт)
```

```
service-instance ge(номер порта)
```

```
encapsulation dot1q 330 exact
```

```
rewrite pop 1
```

```
connect ip interface (нужный интерфейс)
```

с) На всех устройства (кроме FW-DT) создайте пользователя sshuser с паролем P@ssw0rd

1. Пользователь sshuser должен иметь возможность запуска утилиты sudo без дополнительной аутентификации.

```
useradd sshuser
```

```
passwd sshuser <P@ssw0rd>
```

```
usermod -aG wheel sshuser
```

```
nano /etc/sudoers #WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL
```

```
su - sshuser
```

```
sudo ls
```

2. На маршрутизаторах пользователь sshuser должен обладать максимальными привилегиями.

```
EcoRouter: username sshuser
```

```
role admin
```

2) Настройка коммутации

а) Настройте коммутаторы SW1-HQ, SW2-HQ, SW3-HQ.

1. Используйте Open vSwitch

2. Имя коммутатора должно совпадать с коротким именем устройства

i. Используйте заглавные буквы

hostnamectl set-hostname (имя хоста)

3. Передайте все физические порты коммутатору.

```
ovs-vsctl add-br br-mgmt
```

```
ovs-vsctl add-port br-mgmt ens33
```

4. Обеспечьте включение портов, если это необходимо

```
ip link set ens33 up
```

```
ovs-vsctl set Interface ens33 admin_state=up
```

5. Создайте на коммутаторах интерфейсы управления и именем MGMT.

i. Для интерфейсов управления используйте vlan330.

```
ovs-vsctl set port ens33 tag=330
```

```
ip link add mgmt type veth peer name mgmt-br
```

```
ovs-vsctl add-port br-mgmt mgmt-br
```

```
ip addr add 192.168.1.2/29 dev mgmt
```

```
ip link set mgmt up
```

6. Настройте протокол основного дерева

i. Корнем дерева должен выступать SW1-HQ.

```
ovs-vsctl set bridge br-mgmt stp_enable=true
```

```
ovs-vsctl set bridge br-mgmt other_config:stp-priority=0
```

b) Настройте коммутатор SW-DT

1. В качестве коммутатора используйте соответствующий виртуальный коммутатор.

c) Для каждого офиса устройства должны находиться в соответствующих VLAN

1. Клиенты - vlan110,

2. Сервера – в vlan220,

3. Администраторы – в vlan330.

3) Настройте подключения маршрутизаторов к провайдеру

a) Для подключения R-DT к провайдеру необходимо использовать последний адрес из сети 172.16.4.0/28.

б) Для подключения R-HQ к провайдеру необходимо должен использовать последний адрес из сети 172.16.5.0/28.

с) Провайдер использует первый адрес из каждой сети

4) Настройка динамической трансляции адресов

а) Настройте на маршрутизаторах динамическую трансляцию адресов.

б) Все устройства во всех офисах должны иметь доступ к сети Интернет

5) Настройка протокола динамической конфигурации хостов

а) На R-HQ и R-DT настройте протокол динамической конфигурации хостов для клиентов (CLI)

1. Адрес сети – согласно топологии

i. Исключите адрес шлюза по умолчанию из диапазона выдаваемых адресов

2. Адрес шлюза по умолчанию – в соответствии с топологией

i. Шлюзом для сети HQ является маршрутизатор R-HQ

ii. Шлюзом для сети DT является межсетевой экран FW-DT

3. DNS-суффикс – au.team

4. Настройте клиентов на получение динамических адресов.

6) Между офисами DT и HQ необходимо сконфигурировать ip туннель

а) Используйте GRE

7) Настройте динамическую маршрутизацию OSPF

а) Между офисами DT и HQ

1. Маршрутизаторы должны быть защищены от вброса маршрутов с любых интерфейсов, кроме тех, на которых обмен маршрутами явно требуется.

2. Обеспечьте защиту протокола маршрутизации посредством парольной защиты

i. Используйте пароль P@ssw0rd

b) Между R-DT и FW-DT

1. R-DT должен узнавать о сетях, подключенных к FW-DT по OSPF.
2. FW-DT должен получать маршрут по умолчанию и другие необходимые маршруты от R-DT через OSPF.
3. R-DT должен быть защищен от вброса маршрутов с любых интерфейсов, кроме тех, на которых обмен маршрутами явно требуется.

8) Настройка DNS для SRV1-HQ и SRV1-DT

a) Реализуйте основной DNS сервер компании на SRV1-HQ

1. Для всех устройств обоих офисов необходимо создать записи A и PTR.
2. Для всех сервисов предприятия необходимо создать записи CNAME.
3. Загрузка записей с SRV1-HQ должна быть разрешена только для SRV1-DT

b) Сконфигурируйте SRV1-DT, как резервный DNS сервер.

c) Все устройства должны быть настроены на использование обоих внутренних DNS серверов.

1. Для офиса HQ основным DNS сервером является SRV1-HQ
2. Для офиса DT основным DNS сервером является SRV1-DT

d) В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

9) Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP.

a) В качестве сервера должен выступать SRV1-HQ

1. Используйте стратум 5
2. Используйте ntp2.vniiftri.ru в качестве внешнего сервера синхронизации времени

b) Все устройства должны синхронизировать своё время с SRV1-HQ.

1. Используйте chrony, где это возможно

c) Используйте на всех устройствах московский часовой пояс.

10) Реализация доменной инфраструктуры SAMBA AD

а) Сконфигурируйте основной доменный контроллер на SRV1-HQ

1. Используйте модуль BIND9_DLZ
2. Создайте 30 пользователей user1-user30 с паролем P@ssw0rd.
3. Пользователи user1-user10 должны входить в состав группы group1.
4. Пользователи user11-user20 должны входить в состав группы group2.
5. Пользователи user21-user30 должны входить в состав группы group3.
6. Создайте подразделения CLI и ADMIN
 - i. Поместите клиентов в подразделения в зависимости от их роли.
7. Клиентами домена являются ADMIN-DT, CLI-DT, ADMIN-HQ, CLI-HQ.

ф) В качестве резервного контроллера домена используйте SRV1-DT.

1. Используйте модуль BIND9_DLZ

h) Реализуйте общую папку на SRV1-HQ

1. Используйте название SAMBA
2. Используйте расположение /opt/data

Часть 2 (2 день - 5 часов)

11) Управление доменом с помощью ADMS

а) Управление доменом с помощью ADMS осуществляться с ADMIN-HQ

б) Для подразделения CLI настройте политику изменения рабочего стола на картинку компании, а также запретите использование пользователям изменение сетевых настроек и изменение графических параметров рабочего стола.

с) Для подразделения ADMIN реализуйте подключение общей папки SAMBA с использованием доменных политик.

12. Настройка межсетевого экрана

1. Сервера и Администраторы офиса DT должны иметь доступ ко всем устройствам

2. Клиенты офиса DT должны иметь доступ только к серверам
3. Разрешите ICMP-запросы администраторами офиса DT на внутренние интерфейсы межсетевого экрана

13) Реализация бекапа общей папки на сервере SRV1-HQ с использованием systemctl

а) Бекап должен архивировать все данные в формат tar.gz и хранить в директории /var/bac/.

1. Архивация должна производиться благодаря юниту типа service с названием backup.

2. Сервис должен включаться автоматический при загрузке.

б) Время выполнения бекапа каждый день в 8 часов вечера.

1. Используйте юнит типа timer для выполнения.

2. Если устройство будет выключено, то архивация производится сразу после запуска.

14) Развертывание приложений в Docker на SRV2-DT

а) Создайте локальный Docker Registry.

б) Напишите Dockerfile для приложения web.

1. В качестве базового образа используйте nginx:alpine

2. Содержание index.html

```
<html>
```

```
<body>
```

```
<center><h1><b>WEB</b></h1></center>
```

```
</body>
```

```
</html>
```

3. Соберите образ приложения web и загрузите его в ваш Registry.

- i. Используйте номер версии 1.0 для вашего приложения

- ii. Образ должен быть доступен для скачивания и дальнейшего запуска на локальной машине

с) Разверните Docker контейнер используя образ из локального Registry.

1. Имя контейнера web
2. Контейнер должно работать на порту 80
3. Обеспечьте запуск контейнера после перезагрузки компьютера

15) Настройка системы централизованного мониторинга

а) В качестве сервера системы централизованного мониторинга используйте SRV3-DT

б) В качестве системы централизованного мониторинга используйте Zabbix

1. В качестве сервера баз данных используйте PostgreSQL

- i. Имя базы данных: zabbix
- ii. Пользователь базы данных: zabbix
- iii. Пароль пользователя базы данных: zabbixpwd

2. В качестве веб-сервера используйте Apache

с) Система централизованного мониторинга должна быть доступна для внутренних пользователей по адресу <http://<IP адрес SRV3-DT>/zabbix>

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

2. Часовой пояс по умолчанию должен быть Europe/Moscow

д) Настройте узел системы централизованного мониторинга

1. В качестве узлов сети используйте устройства SRV1-DT, SRV2-DT, SRV3-DT, SRV-HQ.

2. Имя узла сети должно соответствовать полному имени устройства

16) Настройте веб-сервер nginx как обратный прокси-сервер на SRV1-DT

а) При обращении по доменному имени www.au.team, клиента должно перенаправлять на SRV2-DT на контейнер web

б) При обращении по доменному имени zabbix.au.team клиента должно перенаправлять на SRV3-DT на сервис Zabbix

с) Если необходимо, настройте сетевое оборудование для обеспечения работы требуемых сервисов.

18) Настройка узла управления Ansible

a) Настройте узел управления на базе ADMIN-DT

1. Используйте стандартную пакетную версию ansible.

b) Сконфигурируйте инвентарь

1. Инвентарь должен располагаться по пути `/etc/ansible/inventory`.
 - i. Настройте запуск данного инвентаря по умолчанию
2. Инвентарь должен содержать три группы устройств:
 - i. Networking (R-DT, R-HQ)
 - ii. Servers (SRV1-HQ, SRV1-DT, SRV2-DT, SRV3-DT)
 - iii. Clients (ADMIN-HQ, ADMIN-DT, CLI-HQ, CLI-DT)
3. Реализуйте доступ ко всем устройствам с учетом настроек SSH
 - i. Подключение осуществляется по пользователю `sshuser`
 - ii. Используйте корректный интерпретатор Python
 - iii. Отключите проверку SSH-ключа на хосте

c) Выполните тестовую команду “ping” средствами ansible

1. Убедитесь, что все устройства отвечают “pong” без предупреждающих сообщений
2. Убедитесь, что команды ansible выполняются от пользователя `user` без использования `sudo`

18) Настройка резервного копирования

- a) На ADMIN-HQ развернуть Кибер Бекап 17 версии
- b) Настроить организацию `wsg`
- c) Настроить пользователя с правами администратора на сервере Кибер Бекап `wsradmin` с паролем `P@ssw0rd`
- d) Установить на CLI-HQ агент Кибер Бекап с функциями узла хранилища и подключить его при помощи токена
- e) Подключить в качестве устройства хранения блочное устройство `sdb` в формате `xfs` (устройство должно быть примонтировано в папку `/backups`)
- f) Создать план полного резервного копирования для сервера ADMIN-HQ
- g) Выполнить полное резервное копирование ADMIN-HQ на узел хранения

Модуль Г. (*Обеспечение отказоустойчивости*) (вариант)

Время на выполнение модуля 5 часов

Задания:

1) Подготовка машины ControlVM

а) Общие указания:

1. Вся проверка выполнения задания будет осуществляться с машины ControlVM.

2. НЕ удаляйте инстанс ControlVM после завершения задания.

б) Создание и настройка инстанса ControlVM:

1. Создайте виртуальный инстанс с именем **ControlVM** и подключите его к сети интернет.

2. Установите следующие параметры для виртуальной машины:

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

ii. **Размер диска:** 30 ГБ.

iii. **Тип диска:** SSD.

3. Отключите функции мониторинга и резервного копирования для данного инстанса.

4. В качестве операционной системы выберите **Альт Сервер 10**.

5. Настройте инстанс для разрешения внешних подключений по протоколу SSH.

6. Сохраните ключевую пару для доступа на вашем локальном ПК на рабочем столе с расширением **.pem**.

в) Настройка внешнего подключения к ControlVM:

1. Установите на локальный ПК клиент SSH **PuTTY**.

2. Создайте в PuTTY профиль с именем **cloud**.

3. Убедитесь в возможности установления соединения с инстансом ControlVM с локального ПК через PuTTY, без необходимости ввода дополнительных параметров.

4. Для подключения используйте имя пользователя **altlinux** и ранее сохранённую ключевую пару.

2) Подготовка облачной инфраструктуры:

а) Требования к виртуальным машинам:

1. Основные характеристики:

- i. Операционная система: Альт p10 StarterKit/Альт Сервер p10-cloud
- ii. Количество vCPU: 1.
- iii. Объём оперативной памяти: 1024 МБ.
- iv. Объём диска: 10 ГБ./30 ГБ
- v. Тип диска: HDD.

б) Подготовьте сценарий автоматизации развёртывания облачной инфраструктуры:

1. Создание виртуальных машин и сетей:

- i. Виртуальные машины и сети должны быть созданы строго в соответствии с предложенной топологией (см. Топология ниже).
- ii. Имена виртуальных машин, сетей, подсетей и маршрутизаторов должны соответствовать именованиям, указанным в Топологии.
- iii. Обеспечьте правильное подключение виртуальных машин к соответствующим сетям в рамках заданной топологии.

2. Безопасность и доступ:

- i. Разрешите трафик по протоколу ICMP для всех виртуальных машин для диагностики сетевых подключений.
- ii. Назначьте IP-адреса всем машинам. Сохраните внешние IP-адреса всех машин в файле /home/altlinux/white.ip на машине ControlVM.
- iii. Настройте аутентификацию на основе открытых ключей для SSH.
- iv. В случае предоставления внешнего доступа к виртуальным машинам, разрешите его только по протоколу SSH (публичный ключ, пароль отключён) и только с соответствующих IP-адресов.

3. Балансировка нагрузки:

- i. Создайте балансировщик нагрузки и распределите трафик между серверами Web1 и Web2 (см. Топология).
- ii. Ограничьте внешний доступ к балансировщику только протоколами HTTP и HTTPS. Все остальные порты должны быть закрыты.
- iii. Балансировка нагрузки должна использовать алгоритм round robin.
- iv. При обращении на внешний адрес балансировщика нагрузки должен выводиться ответ от приложения, работающего на внутренних серверах Web1 и Web2.

4. Настройка подключения:

- i. Настройте машину WebAdm так, чтобы она могла подключаться по SSH с использованием пользователя altlinux и пароля «P@ssw0rd» к серверам Web1 и Web2 с помощью VPN туннеля.
- ii. Убедитесь, что машина ControlVM может подключаться к машине WebAdm используя ключевую пару пользователя altlinux по SSH через её глобальный IP-адрес.

3) Создание и настройка скрипта на машине ControlVM:

а) Создание скрипта автоматизации:

- 1. На машине ControlVM создайте скрипт cloudinit.sh.
- 2. В качестве рабочей директории используйте путь /home/altlinux/bin.
- 3. Скрипт должен использовать файл конфигурации /home/altlinux/bin/cloud.conf для настройки подключения к облачному провайдеру.
- 4. При проверке задания, эксперты могут изменить настройки только в файле cloud.conf. Другие файлы редактироваться не будут.

В файле cloud.conf допускается оставление комментариев, поясняющих назначение параметров.

б) Требования к скрипту:

1. Скрипт должен быть разработан таким образом, чтобы его можно было выполнять из любой директории без необходимости указания полного пути к исполняемому файлу.

2. Для выполнения задания используйте инструменты для автоматизации развёртывания инфраструктуры.

3. Скрипт должен включать механизмы проверки доступности созданных ресурсов и их правильного функционирования, включая доступность Web-серверов через балансировщик нагрузки.

4) Развертывание приложений в Docker

а) Общие требования:

Все действия выполняются на машине ControlVM. Выполнить развертывание Python-скрипта в Docker, настроить WordPress с использованием Docker Compose и развернуть базовый стек ELK для сбора и отображения логов.

б) Развертывание Python-скрипта в Docker

1. Напишите Python-скрипт в домашней директории пользователя ru.py, который выполняет следующие задачи:

- i. Проверяет наличие файла input.txt в рабочей директории root.
- ii. Выводит сообщение с содержимым.
- iii. Если файла input.txt нет, выводит сообщение об ошибке.

2. Создайте Dockerfile для Python-скрипта file-copy-python:

- i. Используйте базовый образ python:3.8-alpine.
- ii. Python-скрипт ru.py должен выполняться внутри контейнера.
- iii. Реализуйте копирование файла input.txt в контейнер (этот файл может содержать произвольный текст).
- iv. Контейнер при запуске должен выводит содержимое файла input.txt, после чего завершать свою работу.

3. Сборка и запуск контейнера:

- i. Соберите Docker-образ с именем file-copy-python.yml.

ii. Запустите контейнер и убедитесь, что содержимое файла выводится файл input.txt.

с) Развертывание WordPress с использованием Docker Compose

3.1. Создание файла wordpress.yml:

i. В домашней директории пользователя создайте файл `wordpress.yml`, описывающий стек контейнеров для WordPress и MySQL.

3.2. Конфигурация стека Docker Compose:

i. Определите два сервиса:

1) **wordpress:**

- Используйте образ **wordpress:latest**.
- Свяжите с сетью `wordpress-network`.
- Прокиньте порт 80 для доступа к WordPress извне.
- Настройте необходимые переменные окружения (`WORDPRESS_DB_HOST`, `WORDPRESS_DB_USER`, `WORDPRESS_DB_PASSWORD`, `WORDPRESS_DB_NAME` и тд.).

2) **mysql:**

- Используйте образ **mysql:5.7**.
- Свяжите с сетью `wordpress-network`.
- Создайте volume для хранения данных базы данных.
- Настройте необходимые переменные окружения (`MYSQL_DATABASE`, `MYSQL_USER`, `MYSQL_PASSWORD`, `MYSQL_ROOT_PASSWORD` и тд.).

3.3. Запуск стека:

i. Запустите Docker Compose с файлом `wordpress.yml`.

ii. Убедитесь, что WordPress доступен по указанному порту и готов к настройке.

4) Развертывание базового стека ELK

а) Создание файла `elk.yml`:

1. В домашней директории пользователя создайте файл `elk.yml`, описывающий стек контейнеров для Elasticsearch, Logstash и Kibana.

b) Конфигурация стека Docker Compose:

1. Определите три сервиса:

1) elasticsearch:

- Используйте образ **elasticsearch:7.10.1**.
- Прокиньте порт 9200 для доступа к Elasticsearch API.

2) logstash:

- Используйте образ **logstash:7.10.1**.
- Настройте Logstash для получения данных и отправки их в Elasticsearch.

3) kibana:

- Используйте образ **kibana:7.10.1**.
- Прокиньте порт 5601 для доступа к веб-интерфейсу Kibana.

c) Запуск стека:

1. Запустите Docker Compose с файлом `elk.yml`.
2. Убедитесь, что все сервисы работают и Kibana доступна по порту 5601.

5) Развёртывания облачных сервисов

a) На машине ControlVM создайте скрипт `/home/altlinux/bin/DeployApp.sh`.

1. Скрипт должен выполняться из любой директории без явного указания пути к исполняемому файлу.

b) Подготовьте web-приложение App1

1. Скачайте файлы `app1.py` и `Dockerfile` по адресу:

<https://github.com/auteam-usr/moscow39>

2. Соберите образ приложения и загрузите его в локальный репозиторий Docker на ваше усмотрение.

c) Команда `DeployApp.sh` должна запускать средства автоматизации для настройки операционных систем.

1. Разверните web-приложение App1 из репозитория Docker на виртуальных машинах Web1 и Web2.
2. Обеспечьте балансировку нагрузки между Web1 и Web2.
3. Обеспечьте внешний доступ к web-приложению по протоколу https.
4. При обращении по протоколу http должно выполняться автоматическое перенаправления на протокол https.
5. Обеспечивать доверие сертификату не требуется.

б) Завершение работы

- a) По окончании рабочего времени освободите ресурсы облачного провайдера, использованные для автоматически созданных объектов.
- b) Удалите все автоматически созданные виртуальные машины, сети, объекты и другие ресурсы.
- c) **Внимание:** НЕ удаляйте **ControlVM** и ресурсы, необходимые для её функционирования.
- d) Важно: если в облачной инфраструктуре останутся объекты, кроме тех, которые необходимы для работы **ControlVM** или создаются по умолчанию, проверка выполнения задания не будет проводиться.

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ

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

- Систем контроля версий
- Общения посредством форумов/мессенджеров/иных средств коммуникации – видеохостингов

2. Участники 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

Нулевой - нельзя ничего привозить.

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. Чертежи, технологические карты, алгоритмы, схемы