ВСЕРОССИЙСКОЕ
ЧЕМПИОНАТНОЕ
ДВИЖЕНИЕ
ПО ПРОФЕССИОНАЛЬНОМУ
МАСТЕРСТВУ

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«Сетевое и системное администрирование»

Регионального чемпионата Ленинградской области по профессиональному мастерству «Профессионалы» в 2024 г.

г. Кировск, 2024 г.

Конкурсное задание включает в себя следующие разделы:

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

1. ИКС – Информационно коммуникационная система

2. КС – Компьютерная сеть

3. 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: Лицензионные требования по настройке и	

	эксплуатации устанавливаемого программного обеспечения 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 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 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;	
3	Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам	25
	- 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: 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 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;	

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**	**В**	**Г**	
	1	5	5	10	20
	2	5	5	10	20
	3	10	10	10	30
	4	10	10	10	30
Итого баллов за критерий/модуль		30	30	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**	В соответствии с используемыми ОС и Сетевым оборудованием
Б	**Настройка технических и программных средств информационно-коммуникационных систем**	В соответствии с используемыми ОС и Сетевым оборудованием
В	**Автоматизация**	В соответствии с используемыми ОС и Сетевым оборудованием
Г	**Обеспечение отказоустойчивости**	В соответствии с используемыми ОС и Сетевым оборудованием
Д	**Миграция**	В соответствии с используемыми ОС и Сетевым

		оборудованием

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Общая продолжительность Конкурсного задания[1]: 15 ч.

Количество конкурсных дней: 3 дня

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. 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) – 1 модуль, и вариативную часть – 2 модуля. Общее количество баллов конкурсного задания составляет 100.

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

Количество модулей из вариативной части, выбирается регионом самостоятельно в зависимости от материальных возможностей площадки соревнований и потребностей работодателей региона в соответствующих специалистах. 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.

Таблица №4

Матрица конкурсного задания

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

Обобщенная трудовая функция	Трудовая функция	Нормативный документ/ЗУН	Модуль	Константа/вариатив	ИЛ	КО
1	2	3	4	5	6	7

Инструкция по заполнению матрицы конкурсного задания **(Приложение № 1)**

1.5.2. Структура модулей конкурсного задания (инвариант/вариатив)

Модуль А. (*Аудит*)

Время на выполнение модуля

Задания:

На текущем чемпионате модуль не применяется

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

Время на выполнение модуля 4 часа.

Задания:

1. **Базовая настройка устройств**

a) Настройте имена устройств согласно топологии
   a. Используйте полное доменное имя, кроме ISP
   b. Используйте строчные буквы, кроме ISP
b) Настройте адресацию устройств согласно топологии
   a. Адрес сети – согласно топологии
      i. Для RTR1 – последний адрес сети минус 1
      ii. Для RTR2 – последний адрес сети минус 2
      iii. Для SRV1 – первый адрес сети плюс 1
      iv. Для SRV2 – первый адрес сети плюс 2
      v. Для CLI1 – десятый адрес сети
      vi. Для CLI2 – двадцатый адрес сети
   b. Адрес шлюза по умолчанию:
      i. Для SRV1 – адрес маршрутизатора RTR1

ii. Для SRV2 – адрес маршрутизатора RTR2
iii. Для CLI1 – адрес маршрутизатора RTR1
iv. Для CLI2 – адрес маршрутизатора RTR2

c. DNS-суффикс – company.prof
i. Используйте в качестве домена поиска

d. Адрес DNS-сервера:
i. Для RTR1 – адрес 77.88.8.8
ii. Для RTR2 – адрес 77.88.8.1
iii. Для SRV1 – адрес маршрутизатора RTR1
iv. Для SRV2 – адрес маршрутизатора RTR2
v. Для CLI1 – адрес маршрутизатора RTR1
vi. Для CLI2 – адрес маршрутизатора RTR2

c) На всех устройствах, кроме CLI1 и CLI2, создайте пользователя sshuser с паролем P@ssw0rd
a. Пользователь sshuser должен иметь возможность запуска утилиты sudo без дополнительной аутентификации(без ввода даже своего пароля).

2. Настройка ISP

a) Настройте адресацию на интерфейсах:
a. Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
b. Интерфейс, к которому подключен RTR1, имеет адрес 11.11.11.1/24
c. Интерфейс, к которому подключен RTR2, имеет адрес 22.22.22.1/24

b) Настройте DHCP сервер:
a. Пул INET1
i. Адрес сети – 11.11.11.0/24
ii. Выдаваемые адреса – 11.11.11.100 – 11.11.11.200
iii. Адрес шлюза по умолчанию – 11.11.11.1
iv. Адрес DNS-сервера – 11.11.11.1

b. Пул INET2
i. Адрес сети – 22.22.22.0/24
ii. Выдаваемые адреса – 22.22.22.100 – 22.22.22.200
iii. Адрес шлюза по умолчанию – 22.22.22.1
iv. Адрес DNS-сервера – 22.22.22.1

c) Настройте перенаправляющий DNS сервер:

a. Все запросы должны пересылаться на внешний DNS сервер по адресу 8.8.8.8
b. DNS сервер должен быть доступен по адресу 11.11.11.1 для RTR1
c. DNS сервер должен быть доступен по адресу 22.22.22.1 для RTR2

d) Настройте динамическую трансляцию адресов для сети 11.11.11.0/24 и 22.22.22.0/24
   a. RTR1 и RTR2 должны иметь выход в Интернет
e) Настройте возможность удаленного подключения по SSH с RTR1 и RTR2
   a. Пользователь для подключения sshuser с паролем P@ssw0rd
   b. Адрес для подключения:
      i. 11.11.11.1 для RTR1
      ii. 22.22.22.1 для RTR2
f) Настройте возможность отправки и получения ICMP запросов между RTR1 и RTR2 по внешним адресам
   a. Отправка и получение ICMP запросов на ISP должна быть запрещена

3. Настройка коммутации

a) В качестве коммутатора используйте виртуальный коммутатор opennebula
b) Убедитесь, что устройства достижимы друг друга

4. Настройка дисковой подсистемы

a) На RTR1 настройте RAID массив
   a. Уровень дискового массива RAID 1.
   b. Используйте имя дискового массива md0.
   c. Используйте два неразмеченных жестких диска.
   d. Используйте 100% дискового пространства
   e. Используйте файловую систему ext4.
   f. Настройте автоматическое монтирование дискового массива.
   g. Точка монтирования /opt/data.
b) На RTR2 сконфигурируйте LVM
   a. Используйте два неразмеченных жестких диска.
   b. Создайте группу логических томов VG
   c. Создайте логический том DATA
   d. Используйте 100% дискового пространства
   e. Используйте файловую систему ext4.

f. Настройте автоматическое монтирование тома
g. Точка монтирования /opt/data

5. Установка и настройка сервера баз данных

a) В качестве сервера баз данных используйте маршрутизатор RTR2
b) Разверните сервер баз данных на базе MariaDB
    a. Пользователь root сервера баз данных должен иметь пароль P@ssw0rd
    b. Настройте возможность удаленного подключения к серверу баз данных пользователю root с паролем P@ssw0rd с любых адресов
c) Разверните программное обеспечение для визуального управление базами данных adminer
d) Проверьте корректность входа в adminer пользователя root с паролем P@ssw0rd

6. Настройка системы централизованного журналирования

a) В качестве сервера системы централизованного журналирования используйте RTR2
b) В качестве системы централизованного журналирования используйте Rsyslog совместно с веб панелью LogAnalyzer
    a. Настройте Rsyslog
        i. Настройте взаимосвязь сервера баз данных с Rsyslog
            1. В качестве сервера баз данных используйте MariaDB на RTR2
            2. Имя базы данных: Syslog
            3. Пользователь базы данных: rsyslog
            4. Пароль пользователя базы данных: rsyslogpwd
            5. В базу данных должны записываться только сообщения об ошибках и более важные
        ii. Настройте возможность приема сообщений по протоколам TCP и UDP по порту 514
    b. Установите LogAnalyzer
        i. В качестве веб-сервера используйте Apache
        ii. Файлы LogAnalyzer должны располагаться в папке /var/www/html/loganalyzer
            1. Установочные файлы находятся в addons_final.iso
        iii. Используйте базу данных, с которой работает Rsyslog

iv. Веб панель LogAnalyzer должна быть доступна по адресу http://<IP адрес RTR2>/loganalyzer

v. Для авторизации в веб панели LogAnalyzer необходимо использовать пользователя admin с паролем P@ssw0rd

1. Требовать, чтобы пользователь вошел в систему

c) Настройте централизованный сбор журналов с хостов RTR1, SRV1, SRV2
   a. Уровень журналирования – сообщения об ошибках и более важные
   b. RTR1 использует протокол UDP
   c. SRV1 и SRV2 использует протокол TCP

7. Настройка системы централизованного мониторинга

a) В качестве сервера системы централизованного мониторинга используйте RTR1
b) В качестве системы централизованного мониторинга используйте сборщика prometheus и визуализатор grafana
c) Система централизованного мониторинга должна быть доступна по адресу http://<IP адрес RTR1>:3000
   a. Администратором системы мониторинга должен быть пользователь admin с паролем P@ssw0rd
   b. Часовой пояс по умолчанию должен быть Europe/Moscow
   c. Разрешите самостоятельную регистрацию новых пользователей
d) Настройте узел системы централизованного мониторинга, в качестве сборщика используйте prometheus node exporter
   a. В качестве узлов сети используйте устройства RTR2, SRV1, SRV2
   b. Имя узла сети должно соответствовать имени устройства
   c. Используйте дашборд, в котором будет видна загрузка ЦП, использование ОП, дисковой подсистемы всех перечисленных устройств. Остальные параметры мониторинга по желанию

8. Настройка SSH на управляемых серверах

a) В качестве управляемых серверов используйте все устройства, кроме клиентов
   a. Доступ разрешен только пользователю sshuser.
   b. Доступ пользователю root запрещен в явном виде
   c. Доступ по паролю запрещен
b) На CLI1 в каталоге /opt/keys сгенерируйте пару ключей с именем ans.priv и ans.pub Скопируйте публичный ключ на устройства

c) Настройте подключение по SSH для пользователя sshuser по соответствующему ключу.

----------ВНИМАНИЕ!!! ----------

После окончания настройки модуля Б,

НЕОБХОДИМО сделать SNAPSHOT на всех устройствах, кроме ISP и клиентов

---------- ВНИМАНИЕ!!! ----------

Модуль В. (*Автоматизация*)

Время на выполнение модуля 4 часа

Задания:

6. Настройка узла управления Ansible

a) Настройте узел управления на базе CLI1
   a. Вам доступна документация на сайте https://docs.ansible.com/
b) Сформируйте инвентарь:
   a. В каталоге /opt/ansible создайте файл инвентаря с именем hosts
      i. Настройте запуск данного инвентаря по умолчанию
   b. Сформируйте группы серверов
      i. RTR1 – включается маршрутизатор RTR1
      ii. RTR2 – включается маршрутизатор RTR2
      iii. Router – включаются группы серверов RTR1 и RTR2
      iv. SRV1 – включается сервер SRV1
      v. SRV2 – включается сервер SRV2
      vi. Server – включаются группы серверов SRV1 и SRV2
   c. Реализуйте доступ к серверам с учетом настроек SSH
      i. Подключение осуществляется по пользователю sshuser
      ii. Подключение осуществляется по ключу

iii. Проверка ключей при подключении по SSH должна быть отключена

iv. Для исключения предупреждений укажите корректный интерпретатор Python

v. Все параметры должны быть размещены в папке group_vars в качестве переменных

vi. Выполните тестовые подключения, добавьте хосты в список известных.

d. Выполните тестовую команду “ping” средствами ansible

i. Убедитесь, что все сервера отвечают “pong” без предупреждающих сообщений

ii. Убедитесь, что команды ansible выполняются от пользователя user без использования sudo

c) Создайте структуру каталогов

a. В каталоге /opt/ansible создайте папку project_1

i. В папке project_1 создайте файл playbook_1.yml

ii. В папке project_1 создайте файл playbook_2.yml

b. В каталоге /opt/ansible создайте папку project_2

i. В папке project_2 создайте файл playbook_1.yml

c. В каталоге /opt/ansible создайте папку project_3

i. В папке project_3 создайте файл playbook_1.yml

ii. В папке project_3 создайте файл playbook_2.yml

d. В каталоге /opt/ansible создайте папку project_4

i. В папке project_4 создайте файл playbook_1.yml

ii. В папке project_4 создайте файл playbook_2.yml

e. В каталоге /opt/ansible создайте папку project_5

i. В папке project_5 создайте файл playbook_1.yml

ii. В папке project_5 создайте файл playbook_2.yml

7. Настройка динамической трансляции адресов

a) Настройте динамическую трансляцию адресов средствами Ansible для группы серверов RTR1

a. В качестве плейбука используйте файл playbook_1.yml в каталоге project_1

b. Плейбук должен содержать действия по настройке динамической трансляцию адресов

i. Используйте firewalld
ii. Для внешнего интерфейса используйте зону external
iii. Обеспечьте автоматическое восстановление правил после перезагрузки
iv. Использование плагина shell и command НЕ допускается
a. Использование запрещенных плагинов обнулит весь пункт при проверке

b) Настройте динамическую трансляцию адресов средствами Ansible для группы серверов RTR2
c. В качестве плейбука используйте файл playbook_2.yml в каталоге project_1
d. Плейбук должен содержать действия по настройке динамической трансляцию адресов
i. Используйте iptables
ii. Обеспечьте автоматическое восстановление правил после перезагрузки
iii. Использование плагина shell и command НЕ допускается
a. Использование запрещенных плагинов обнулит весь пункт при проверке

8. Настройка перенаправляющего DNS

a) Настройте перенаправляющий DNS средствами Ansible для группы серверов Router
a. В качестве плейбука используйте файл playbook_1.yml в каталоге project_2
b. Плейбук должен содержать действия по настройке перенаправляющего DNS
i. Используйте bind9
ii. Прослушивается только адрес 127.0.0.1 и адрес внутреннего интерфейса
iii. Все запросы должны пересылаться внешнему DNS-серверу
a. Для RTR1 на 77.88.8.8
b. Для RTR2 на 77.88.8.1
iv. Сервер должен только перенаправлять все запросы и не пытаться разрешить их самостоятельно
v. Использование плагина shell и command НЕ допускается

        a. Использование запрещенных плагинов обнулит весь пункт при проверке
    c. Плейбук должен содержать действия по перенастройке адреса DNS-сервера на маршрутизаторах на 127.0.0.1
        i. Использование плагина shell и command НЕ допускается
            a. Использование запрещенных плагинов обнулит весь пункт при проверке

9. Настройка протокола динамической конфигурации хостов

a) Настройте протокол динамической конфигурации хостов средствами Ansible для группы серверов RTR1
    a. В качестве плейбука используйте файл playbook_1.yml в каталоге project_3
    b. Плейбук должен содержать действия по настройке протокола динамической конфигурации хостов
        i. Адрес сети – согласно топологии
        ii. Адрес шлюза по умолчанию – адрес маршрутизатора RTR1
        iii. DNS-суффикс – company.prof
        iv. Адрес DNS-сервера – адрес маршрутизатора RTR1
        v. Адрес NTP-сервера – адрес маршрутизатора RTR1
        vi. Выдаваемые адреса:
            a. Первый адрес – первый адрес сети плюс 5
            b. Последний адрес – общее количество адресов в сети разделенное на 2
        vii. Использование плагина shell и command НЕ допускается
            a. Использование запрещенных плагинов обнулит весь пункт при проверке
b) Настройте протокол динамической конфигурации хостов средствами Ansible для группы серверов RTR2
    a. В качестве плейбука используйте файл playbook_2.yml в каталоге project_3
    b. Плейбук должен содержать действия по настройке протокола динамической конфигурации хостов
        i. Адрес сети – согласно топологии
        ii. Адрес шлюза по умолчанию – адрес маршрутизатора RTR2
        iii. DNS-суффикс – company.prof
        iv. Адрес DNS-сервера – адрес маршрутизатора RTR2

v. Адрес NTP-сервера – адрес маршрутизатора RTR2
vi. Выдаваемые адреса:
    a. Первый адрес – общее количество адресов в сети разделенное на 2 плюс 1
    b. Последний адрес – последний адрес сети минус 5
vii. Использование плагина shell и command НЕ допускается
    a. Использование запрещенных плагинов обнулит весь пункт при проверке

c) Переконфигурируйте сетевые настройки на CLI2 для получения сетевых параметров по DHCP
    a. Применение Ansible НЕ требуется

10. Настройка сервера времени

a) Настройте сервер времени средствами Ansible для группы серверов Router
    a. В качестве плейбука используйте файл playbook_1.yml в каталоге project_4
    b. Плейбук должен содержать действия по установке и настройке сервера времени
        i. Используйте сервер времени на базе Chrony
        ii. Используйте стратум 4
        iii. Используйте внешний сервер синхронизации времени
            a. ntp2.vniiftri.ru для RTR1
            b. ntp3.vniiftri.ru для RTR2
        iv. Сервер допускает синхронизацию времени только для сети LAN.
        v. Используйте часовой пояс Europe/Moscow
        vi. Использование плагина shell и command НЕ допускается
            a. Использование запрещенных плагинов обнулит весь пункт при проверке

11. Настройка NTP клиента

a) Настройте NTP клиента средствами Ansible для группы серверов Server
    a. В качестве плейбука используйте файл playbook_2.yml в каталоге project_4
    b. Проект должен содержать действия по установке и настройке NTP клиента
        i. Используйте NTP клиент на базе Chrony
        ii. Используйте часовой пояс Europe/Moscow

iii. Устройства должны синхронизировать время:
    a. Первый сервер RTR1
    b. Второй сервер RTR2
iv. Использование плагина shell и command НЕ допускается
    a. Использование запрещенных плагинов обнулит весь пункт при проверке

12. Настройка NFS сервера

a) Настройте NFS сервер средствами Ansible для группы маршрутизаторов Router
    a. В качестве плейбука используйте файл playbook_1.yml в каталоге project_5
    b. Плейбук должен содержать действия по настройке NFS сервера
        i. Настройте общий доступ к директории /opt/data
        ii. Общий доступ должен быть обеспечен для чтения и записи только для устройств локальной сети

13. Настройка NFS клиента

a) Настройте NFS клиента средствами Ansible для группы серверов Server
    a. В качестве плейбука используйте файл playbook_2.yml в каталоге project_5
    b. Плейбук должен содержать действия по настройке NFS клиента
        i. На SRV1 настройте автоматическое подключение NFS каталога
            1. Используйте локальную точку монтирования /mnt/data
            2. Используйте общую папку на RTR1
        ii. На SRV2 настройте автоматическое подключение NFS каталога
            1. Используйте локальную точку монтирования /mnt/data
            2. Используйте общую папку на RTR2

----------ВНИМАНИЕ!!! ----------

После окончания настройки пунктов, связанных с модулем B, НЕОБХОДИМО сбросить все устройства, используя имеющийся SNAPSHOT

---------- ВНИМАНИЕ!!! ----------

Модуль Г. (*Обеспечение отказоустойчивости*)

Время на выполнение модуля 4 часа

Задания:

14. Настройка отказоустойчивости динамической трансляции адресов

a) Группа серверов VRRP включает в себя маршрутизаторы RTR1 и RTR2
b) Создайте группу серверов Keepalived со следующими параметрами:
    a. Имя группы – NAT
    b. Иерархия группы - RTR1 -> RTR2
    c. Идентификатор группы – 69
    d. Приоритет - 110 и 100 соответственно
    e. Виртуальный адрес группы - последний адрес сети
    f. Интервал рассылки сообщений - 1 секунда
    g. Время, после которого сервер с более высоким приоритетом заберет обратно себе роль мастера – 30 секунд
c) Обеспечьте автозапуск конфигурации
d) Переконфигурируйте сетевые настройки SRV1 и SRV2 с учетом настроек отказоустойчивости динамической трансляции адресов

15. Настройка отказоустойчивости перенаправляющего DNS

a) Группа серверов VRRP включает в себя маршрутизаторы RTR1 и RTR2
b) Создайте группу серверов Keepalived со следующими параметрами:
    a. Имя группы – DNS
    b. Иерархия группы - RTR1 -> RTR2
    c. Идентификатор группы – 53
    d. Приоритет - 110 и 100 соответственно
    e. Виртуальный адрес группы - последний адрес сети
    f. Интервал рассылки сообщений - 1 секунда
    g. Время, после которого сервер с более высоким приоритетом заберет обратно себе роль мастера – 30 секунд
c) Обеспечьте автозапуск конфигурации
d) Внесите изменения в настройки перенаправляющих DNS с учетом работы keepalived

16. Настройка отказоустойчивости сервера времени

a) Группа серверов VRRP включает в себя маршрутизаторы RTR1 и RTR2
b) Создайте группу серверов Keepalived со следующими параметрами:
    a. Имя группы – NTP
    b. Иерархия группы – RTR1 -> RTR2
    c. Идентификатор группы – 123
    d. Приоритет - 110 и 100 соответственно
    e. Виртуальный адрес группы - последний адрес сети
    f. Интервал рассылки сообщений - 1 секунда
    g. Время, после которого сервер с более высоким приоритетом заберет обратно себе роль мастера – 30 секунд
c) Обеспечьте автозапуск конфигурации

17. Настройка балансировки и отказоустойчивости DHCP сервера

a) Используйте внутренние сервисы для управления коллективной работой службы DHCPD (failover)
b) Используйте следующие роли для DHCP серверов:
    a. RTR1 – primary
    b. RTR2 – secondary

c) Используйте следующую конфигурацию взаимодействия DHCP серверов
    a. Таймаут, по истечении которого сервер считается не рабочим - 60 секунд
    b. Количество запросов, которые могут быть отправлены без обязательного подтверждения – 10
    c. Время, в течение которого DHCP сервер будет ждать восстановления канала связи с партнёром – 3600 секунд
    d. Индекс разделения работы между DHCP серверами – 128
    e. Время, по истечении которого прекращается работа балансировки и сервер отвечает самостоятельно - 3 секунды
d) Переконфигурируйте DHCP сервера для работы failover с учетом отказоустойчивости NAT, DNS, NTP и FreeIPA
    a. Имя пира – DHCP
    b. Выдаваемые адреса:
        i. Первый адрес – первый адрес сети плюс 5
        ii. Последний адрес – последний адрес сети минус 5
    c. Адрес NTP-сервера – адреса доменных NTP серверов
e) Переконфигурируйте сетевые настройки на CLI1 и CLI2 для получения сетевых параметров по DHCP
    a. Проверьте работоспособность DHCP failover на клиентах
f) Клиенты CLI1 и CLI2 должны получать параметры NTP сервера по DHCP
    a. Используйте NTP клиент на базе Chrony
    b. Используйте часовой пояс Europe/Moscow

18. Настройка отказоустойчивой системы централизованного управления авторизацией пользователей

a) Разверните систему централизованного управления авторизацией пользователей
    a. Разверните домен на базе FreeIPA
        i. Основной сервер - SRV1
        ii. Дополнительный сервер (реплика) - SRV2
    b. Имя домена - company.prof
    c. DNS сервер - интегрированный с IPA
        i. Запросы, которые выходят за рамки зоны, пересылаются на виртуальный адрес перенаправляющего DNS-сервера
        ii. Обратная зона - согласно топологии
        iii. Все устройства сети должны быть доступны по имени

d. CA сервер - интегрированный с IPA
    i. Клиенты домена должны доверять центру сертификации
e. NTP сервер - интегрированный с IPA
    i. NTP сервер должен синхронизировать время с отказоустойчивым сервером времени
f. Пароль администратора домена - P@ssw0rd

b) Настройте систему централизованного управления авторизацией пользователей
    a. Создайте пользователей user1, user2 и mon с паролем P@ssw0rd,
    b. Пользователей user1, user2 включите в группу prof
    c. Пользователя mon включите в группу admins
    d. Создайте правило admin_sudo, разрешающее группе пользователей admins использовать sudo на всех компьютерах в домене без ограничения.
    e. Обеспечьте доменному пользователю admin, после успешной авторизации на клиентах, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
        i. Используйте Яндекс браузер
c) Клиентов CLI1 и CLI2 введите в домен FreeIPA
d) Настройте подключение к системе централизованного мониторинга с использованием FreeIPA
    a. Используйте адрес системы централизованного мониторинга http://mon.company.prof:3000
    b. Используйте LDAP в качестве аутентификацию по умолчанию
        i. В настройках LDAP укажите все имеющиеся серверы
    c. Используйте доменного пользователя mon
        i. Группа – grafana_admin
        ii. Тип пользователя – admin

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ[2]

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

– Систем контроля версий

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

– 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 Критерии оценки

Приложение №4 Инструкция по охране труда и технике безопасности по компетенции «Сетевое и системное администрирование».

Приложение №5 Чертежи, технологические карты, алгоритмы, схемы и т.д.