ВСЕРОССИЙСКОЕ
ЧЕМПИОНАТНОЕ
ДВИЖЕНИЕ
ПО ПРОФЕССИОНАЛЬНОМУ
МАСТЕРСТВУ

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ
«Сетевое и системное администрирование»
Итогового (межрегионального) этапа чемпионата
по профессиональному мастерству
«Профессионалы» в 2026 г.

(субъект РФ)

2026 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:

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	

№ п/п	Раздел	Важность в %
	~ 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 ~ 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;	

№ п/п	Раздел	Важность в %
	~ 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**
	Специалист должен знать и понимать: ~ Общие принципы функционирования аппаратных, программных	

№ п/п	Раздел	Важность в %
	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 ~ Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств ~ Инструкции по установке администрируемого программного обеспечения	

№ п/п	Раздел	Важность в %
	~ 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: ~ Принципы функционирования информационно-коммуникационных системы	
	Специалист должен уметь: ~ Выполнять мероприятия модернизации информационно-коммуникационной системы, способствующие сокращению электропотребления	

№ п/п	Раздел	Важность в %
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	

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
		Б	Д		
Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ	1	10			
	2	10	10		
	3	10	10		
	4	10	10		
	5	10	10		
	6		10		
Итого баллов за критерий/модуль		**50**	**50**		**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. Содержание конкурсного задания

Общая продолжительность Конкурсного задания[1]: 15 часов

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 2 модулей, включает обязательную к выполнению часть (инвариант) – 2 модулей. Общее количество баллов конкурсного задания по всем модулям составляет 100.

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

1.5.2. Структура модулей конкурсного задания

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

Время на выполнение модуля: 5 часов (день 1)

Задания:

Структурная топология:

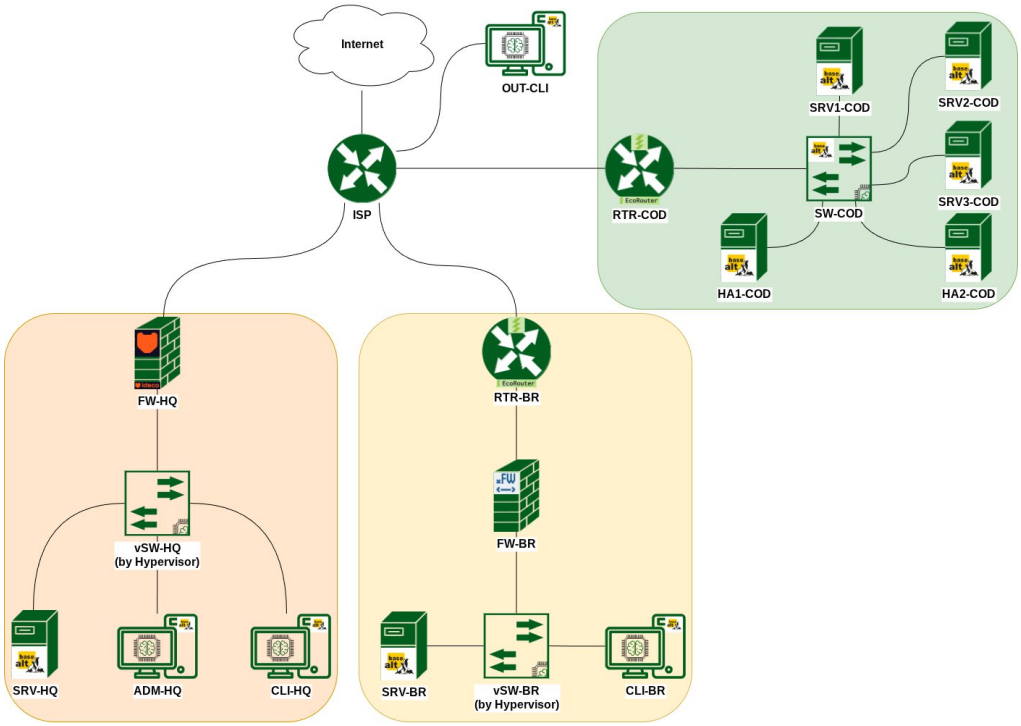
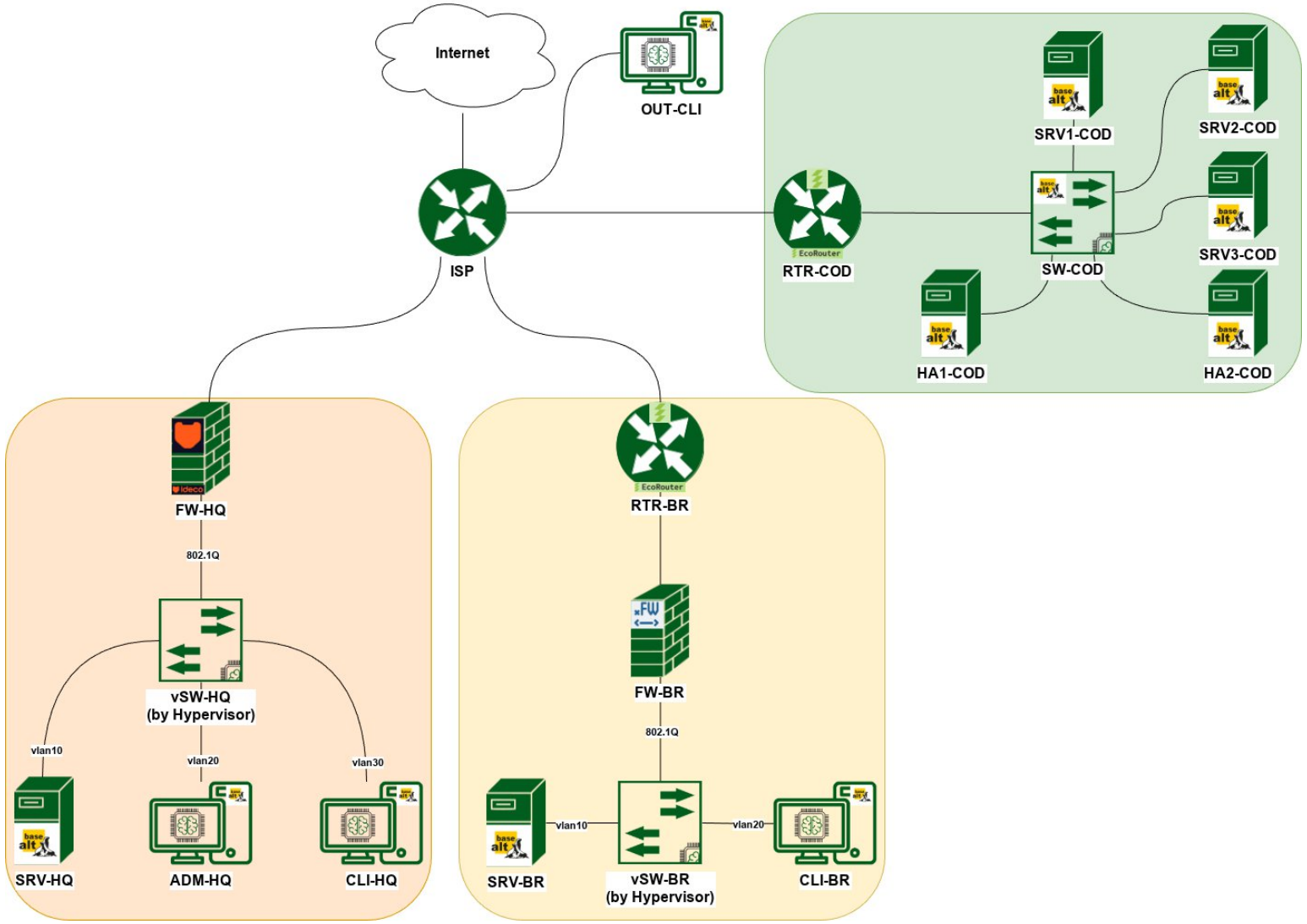


Таблица используемых операционных систем (ОС):

ВМ	ОС
ISP	Стартовый набор (Starterkit) jeos-systemd (p11)
FW-HQ	Ideco NGFW Novum 21
SRV-HQ	Альт Сервер 11
ADM-HQ	Альт Рабочая станция 11
CLI-HQ	Альт Рабочая станция 11
RTR-BR	EcoRouterOS не ниже jasmine
FW-BR	ViPNet xFirewall xF-VA
SRV-BR	Альт Сервер 11
CLI-BR	Альт Рабочая станция 11
RTR-COD	EcoRouterOS не ниже jasmine
SW-COD	Альт Сервер 11
HA1-COD	Альт Сервер 11
HA2-COD	Альт Сервер 11
SRV1-COD	Альт Сервер 11
SRV2-COD	Альт Сервер 11
SRV3-COD	Альт Сервер 11
OUT-CLI	Симпли Линукс 11

Топология L-2:



Топология L-3:

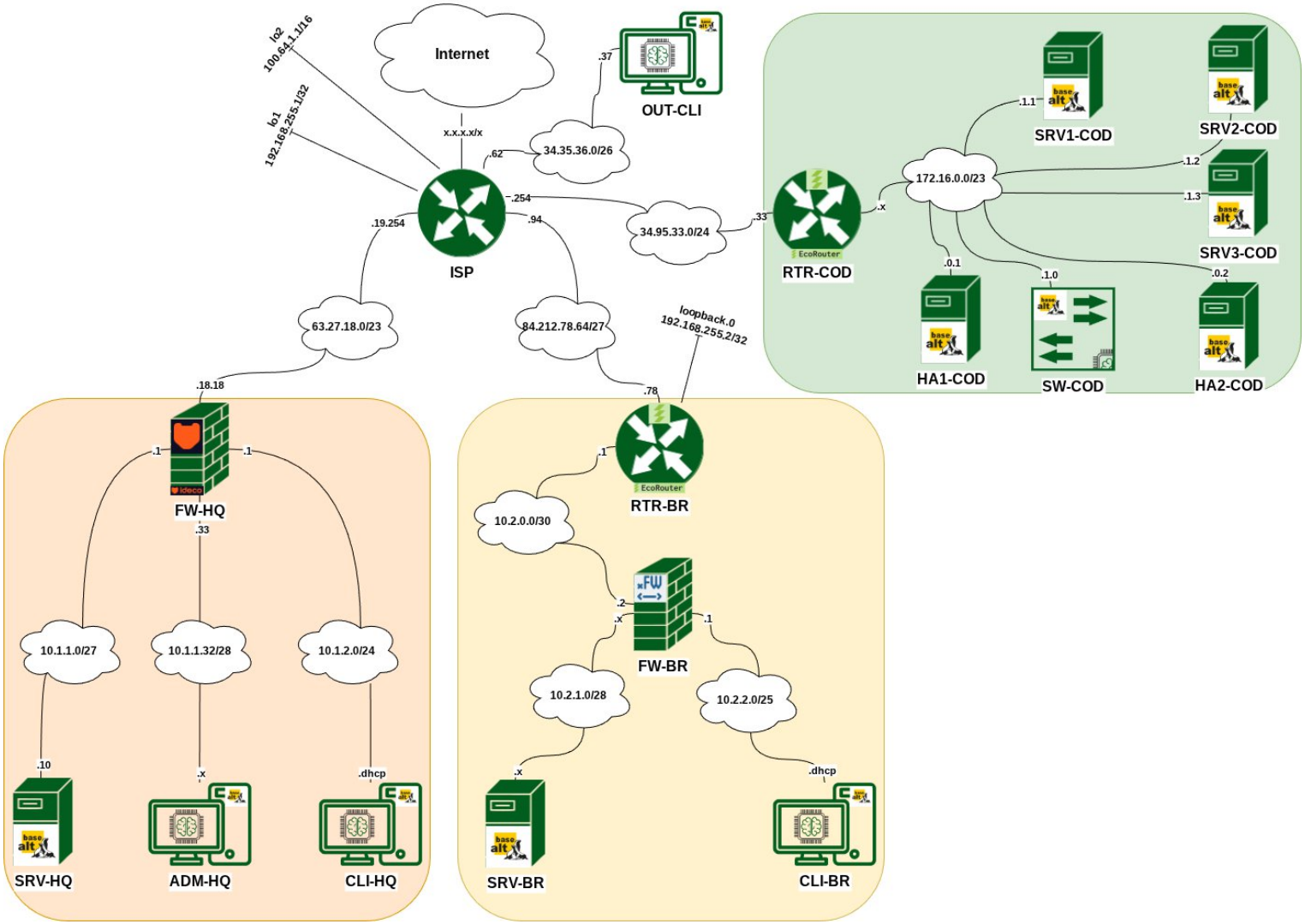


Таблица адресации:

ВМ	NIC	Сеть	IP-адрес	Шлюз
ISP	Internet	x.x.x.x/x	x.x.x.x	x.x.x.x
	ISP <-> FW-HQ	63.27.18.0/23	63.27.19.254	
	ISP <-> RTR-BR	84.212.78.64/27	84.212.78.94	
	ISP <-> RTR-COD	34.95.33.0/24	34.95.33.254	
	ISP <-> OUT-CLI	34.35.36.0/26	34.35.36.62	
	lo1	192.168.255.1/32	192.168.255.1	
	lo2	100.64.0.0/16	100.64.1.1	
FW-HQ	ISP <-> FW-HQ	63.27.18.0/23	63.27.18.18	63.27.19.254
	vlan10	10.1.1.0/27	10.1.1.1	
	vlan20	10.1.1.32/28	10.1.1.33	
	vlan30	10.1.2.0/24	10.1.2.1	
SRV-HQ	vlan10	10.1.1.0/27	10.1.1.10	10.1.1.1
ADM-HQ	vlan20	10.1.1.32/28	10.1.1.x	10.1.1.33
CLI-HQ	vlan30	10.1.2.0/24	dhcp	dhcp
RTR-BR	ISP <-> RTR-BR	84.212.78.64/27	84.212.78.78	84.212.78.94
	RTR-BR <-> FW-BR	10.2.0.0/30	10.2.0.1	
	loopback.0	192.168.255.2/32	192.168.255.2	
FW-BR	RTR-BR <-> FW-BR	10.2.0.0/30	10.2.0.2	10.2.0.1
	vlan10	10.2.1.0/28	10.2.1.x	
	vlan20	10.2.2.0/25	10.2.2.1	
SRV-BR	vlan10	10.2.1.0/28	10.2.1.x	10.2.1.x
CLI-BR	vlan20	10.2.2.0/25	dhcp	dhcp
RTR-COD	ISP <-> RTR-COD	34.95.33.0/24	34.95.33.33	34.95.33.254
	RTR-COD <-> SW-COD	172.16.0.0/23	172.16.x.x	
SW-COD	RTR-COD <-> SW-COD	172.16.0.0/23	172.16.1.0	172.16.0.x
HA1-COD	SW-COD <-> HA1-COD	172.16.0.0/23	172.16.0.1	172.16.0.x
HA2-COD	SW-COD <-> HA2-COD	172.16.0.0/23	172.16.0.2	172.16.0.x
SRV1-COD	SW-COD <-> SRV1-COD	172.16.0.0/23	172.16.1.1	172.16.0.x
SRV2-COD	SW-COD <-> SRV2-COD	172.16.0.0/23	172.16.1.2	172.16.0.x
SRV3-COD	SW-COD <-> SRV3-COD	172.16.0.0/23	172.16.1.3	172.16.0.x
OUT-CLI	ISP <-> OUT-CLI	34.35.36.0/26	34.35.36.37	34.35.36.62

Предварительные условия:

Маршрутизатор ISP уже настроен (доступ для участника - не предусматривается):

- **ASN:** 64499
- **Loopback (lo1):** 192.168.255.1/32
- **IS-IS SYSTEM ID:** 1921.6825.5001, уровень L2
    - **идентификатор зоны (area):** 49.0001

- **идентификатор процесса:** .00

- **Анонсируемые маршруты (lo2: 100.64.1.1/16):** 100.64.0.0/16 и 0.0.0.0/0
- **SNAT**

Пароли на все случаи необходимо использовать **P@ssw0rd**, если в задании не сказано явным образом иное.

Реализация инфраструктуры выпуска необходимых сертификатов для требуемых служб и сервисов, а также их дальнейшая публикация – на усмотрение участника, если в задании не сказано явным образом иное.

1. **Настройка базовых параметров**

a. Настройте имена устройств в соответствии с топологией. В качестве доменного имени используйте au.team.

b. На устройствах RTR-BR, RTR-COD и SW-COD добавьте административную учётную запись net_admin с паролем P@ssw0rd.

i. При настройке ОС на базе Linux пользователь должен иметь возможность выполнять sudo без ввода пароля.

ii. При настройке ОС, отличных от Linux, пользователь должен обладать максимальными привилегиями.

c. Настройте адресацию в соответствии с топологией L3.

i. Для ADM-HQ используйте последний возможный IP-адрес узла из соответствующей подсети.

ii. Для FW-BR используйте последний возможный IP-адрес узла в сторону сети SRV-BR.

iii. Для SRV-BR используйте десятый возможный IP-адрес узла из соответствующей подсети.

iv. Для RTR-COD используйте последний возможный IP-адрес узла в сторону локальной сети центра обработки данных.

d. Настройте коммутацию в соответствии с топологией L2.

i. vSW-HQ и vSW-BR являются виртуальными коммутаторами на уровне гипервизора. Необходимо настроить VID (тег) на портах (Network Device в Hardware BM) оконечных устройств (виртуальных машин).

ii. Для SW-COD для организации виртуального коммутатора необходимо использовать Open vSwitch.

1. Имя коммутатора должно совпадать с коротким именем устройства.
2. Добавьте все физические порты в коммутатор.
3. Обеспечьте включение портов (при необходимости).

e. Веб-интерфейсы управления межсетевыми экранами FW-HQ и FW-BR должны быть доступны с ADM-HQ.

2. Настройка обмена маршрутной информацией по протоколу BGP

a. Настройте обмен маршрутной информацией по протоколу BGP на маршрутизаторе RTR-BR.

i. Доступ в Интернет предоставляется через ISP, поэтому маршруты необходимо передавать по iBGP.

ii. Используйте интерфейс loopback.0 для установления соседства по iBGP.

iii. В качестве IGP используйте протокол IS-IS:

1. Используйте маршрутизацию в пределах одной зоны (area).
2. Используйте адрес интерфейса loopback в качестве System ID (см. таблицу адресации).

iv. Router ID (RID) для BGP должен соответствовать адресу интерфейса loopback (см. таблицу адресации).

b. Настройте обмен маршрутной информацией по протоколу BGP на маршрутизаторе RTR-COD.

c. В качестве номера автономной системы (ASN) используйте 64499 (AS провайдера).

d. Анонсировать внутренние сети в провайдера запрещено.

e. Маршрутизаторы должны получать маршрут по умолчанию через BGP от провайдера. Ручное создание статического маршрута по умолчанию не допускается.

3. Настройка доступа в Интернет

a. Настройте динамическую трансляцию адресов (NAT) для обоих офисов и центра обработки данных в сторону ISP.
b. Все устройства в офисах и центре обработки данных должны иметь доступ к сети Интернет.
c. Настройте авторизацию на межсетевом экране FW-HQ для доступа в сеть Интернет:

i. Для доступа в сеть Интернет с SRV-HQ должна быть настроена авторизация с использованием соответствующего IP-адреса от имени пользователя hq.user5.

ii. Для доступа в сеть Интернет с ADM-HQ должна быть настроена авторизация с использованием соответствующих IP- и MAC-адресов от имени пользователя hq.user4.

iii. Для доступа в сеть Интернет с CLI-HQ должен быть установлен Ideco Client и создан профиль для пользователя hq.user3.

4. Настройка контроллера домена

a. Разверните контроллер домена au.team на базе FreeIPA.
   i. В качестве сервера используйте SRV-HQ.
   ii. Выполните установку FreeIPA с интегрированным DNS.
      1. Для всех устройств двух офисов и центра обработки данных должны быть созданы записи типа A и PTR.
b. Создайте группы и пользователей.
   i. Создайте группы hq, br и cod.
   ii. Создайте по 5 пользователей для каждой группы.
      1. Имена пользователей должны быть в формате hq.user1 – hq.user5, br.user1 – br.user5, cod.user1 – cod.user5.

2.В качестве пароля для всех пользователей используйте P@ssw0rd.

3.Добавьте пользователей в соответствующие группы.

c. Добавьте ADM-HQ, CLI-HQ, CLI-BR и FW-HQ в домен au.team.

i. На FW-HQ необходимо организовать импорт пользователей из домена.

1.Создайте родительскую группу FreeIPA-Users.

2.Создайте в родительской группе одноимённые группы hq, br и cod.

3.Выполните импорт пользователей из домена в одноимённые группы на FW-HQ.

d. Все необходимые зоны обратного просмотра, а также записи типа A и PTR должны создаваться с помощью Terraform.

i. Terraform версии 1.14.5 необходимо установить на ADM-HQ.

ii. Все файлы, необходимые для работы Terraform, должны быть размещены в директории /home/user/terraform.

iii. Используйте в качестве провайдера: camptocamp/freeipa версии 1.0.0.

iv. Исключением могут являться записи для CLI-HQ и CLI-BR.

5. Настройка протокола динамической конфигурации хостов

a. На SRV-HQ реализуйте DHCP-сервер на базе Kea-DHCPv4.

i. В качестве раздаваемой сети используйте подсеть CLI-HQ.

ii. В качестве диапазона раздаваемых IP-адресов используйте адреса с 128 по 254 включительно из соответствующей подсети.

iii. В качестве адреса шлюза по умолчанию используйте адрес FW-HQ.

iv. В качестве адреса DNS-сервера используйте адрес сервера SRV-HQ.

v. В качестве DNS-суффикса используйте au.team.

vi. CLI-HQ должен получать все необходимые сетевые параметры автоматически.

b. На FW-HQ необходимо реализовать DHCP-Relay.

c. На FW-BR реализуйте DHCP-сервер.

i. В качестве раздаваемой сети используйте подсеть CLI-BR.

ii. В качестве диапазона раздаваемых IP-адресов используйте все возможные адреса узлов из соответствующей подсети, за исключением адреса FW-BR.

iii. В качестве адреса шлюза по умолчанию используйте адрес FW-BR.

iv. В качестве адреса DNS-сервера используйте адрес сервера SRV-HQ.

v. В качестве DNS-суффикса используйте au.team.

vi. CLI-BR должен получать все необходимые сетевые параметры автоматически.

6. Настройка туннелей

a. Настройте GRE-туннель между FW-HQ и RTR-BR.

i. В качестве сетевого диапазона используйте сеть 10.0.1.0/30.

ii. Имя туннельных интерфейсов должно быть tunnel.1.

b. Настройте GRE-туннель между FW-HQ и RTR-COD.

i. В качестве сетевого диапазона используйте сеть 10.0.2.0/30.

ii. Имя туннельных интерфейсов должно быть tunnel.2.

c. Настройте GRE-туннель между RTR-BR и RTR-COD.

i. В качестве сетевого диапазона используйте сеть 10.0.3.0/30.

ii. Имя туннельных интерфейсов должно быть tunnel.3.

7. Настройка маршрутизации

a. Настройте динамическую маршрутизацию между офисом BR и центром обработки данных COD.

i. Используйте протокол OSPF для маршрутизации между FW-BR, RTR-BR и RTR-COD.

ii. Межсетевой экран FW-BR должен получать маршрут по умолчанию и другие необходимые маршруты от RTR-BR через OSPF. Ручное создание статического маршрута по умолчанию на FW-BR не допускается.

iii. На всех маршрутизаторах интерфейсы, не участвующие в процессе OSPF, должны быть переведены в пассивный режим.

b. Настройте статическую маршрутизацию между офисом HQ и офисом BR, а также между офисом HQ и центром обработки данных COD, чтобы обеспечить полную связность всех трёх площадок.
c. Убедитесь, что сети одного офиса доступны из другого офиса и из центра обработки данных, и наоборот.

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

Время на выполнение модуля: 4 часа (день 2)

Задания:

8. **Настройка облачного хранилища**
   a. На сервере SRV-BR выполните установку облачного хранилища Nextcloud версии 33.0.0.
      i. Установка с использованием контейнеризации не допускается.
      ii. В качестве веб-сервера необходимо использовать Apache2.
      iii. В качестве СУБД необходимо использовать PostgreSQL.
   b. Доступ к платформе из любых сетей должен осуществляться по протоколу HTTPS.
      i. При обращении по протоколу HTTP должно автоматически выполняться перенаправление на HTTPS.
      ii. При обращении по HTTP с любого клиентского устройства не должно возникать проблем с сертификатами.
   c. Сервис должен быть доступен по имени ncloud.au.team.
   d. Аутентификация в облачном хранилище должна быть реализована для доменных пользователей из групп hq, br и cod.
9. **Настройка системы управления конфигурацией**
   a. На ADM-HQ установите Ansible.
      i. Ansible должен быть установлен через pip внутри виртуального окружения с именем venv/ansible, расположенного в каталоге /home/user/ansible.
   b. Создайте инвентарный файл по пути /home/user/ansible/inventories/production/hosts.
      i. Файл инвентаря должен быть написан в формате YAML.
      ii. Файл инвентаря должен содержать две группы устройств с именами proxy и server.

iii. Узлы, входящие в группу proxy: ha1-cod и ha2-cod.

iv. Узлы, входящие в группу server: srv1-cod, srv2-cod и srv3-cod.

v. Доступ ко всем узлам должен осуществляться на основе ключевой пары; доступ по паролю не допускается.

c. При использовании команды ansible -i inventories/production/hosts -m ping all никаких проблем, ошибок и уведомлений возникать не должно, все узлы должны отвечать pong.

10. Настройка веб-портала в центре обработки данных

a. На ADM-HQ напишите playbook playbook1_keepalived.yml в директории /home/user/ansible.

i. Данный playbook должен использовать инвентарный файл /home/user/ansible/inventories/production/hosts и выполняться на группе узлов proxy.

ii. Playbook должен реализовывать установку и настройку keepalived таким образом, чтобы MASTER был ha1-cod, а BACKUP — ha2-cod. В качестве VIP необходимо использовать адрес 172.16.1.253/23.

b. На ADM-HQ напишите playbook playbook2_web.yml в директории /home/user/ansible.

i. Playbook должен использовать инвентарный файл /home/user/ansible/inventories/production/hosts и выполняться на группе узлов server.

ii. Playbook должен реализовывать установку и настройку веб-сервера Angie таким образом, чтобы каждый узел из группы публиковал файл index.html с содержимым <ИМЯ_СЕРВЕРА> by Angie!.

c. На ADM-HQ напишите playbook playbook3_haproxy.yml в директории /home/user/ansible.

i. Playbook должен использовать инвентарный файл /home/user/ansible/inventories/production/hosts и выполняться на группе узлов proxy.

ii. Playbook должен реализовывать установку и настройку haproxy таким образом, чтобы при обращении к VIP происходило перенаправление на узлы группы server. В качестве режима балансировки необходимо использовать roundrobin.

iii. Также должна быть настроена статистика haproxy, доступная при обращении к VIP на порт 9000 и URI /haproxy_stats.

d. Каждый playbook должен быть идемпотентным.

i. При повторном запуске ansible-playbook статус всех задач должен быть OK.

e. Доступ к веб-порталу из любых сетей должен осуществляться по протоколу HTTPS.

i. При обращении по протоколу HTTP должно автоматически выполняться перенаправление на HTTPS.

ii. При обращении по HTTP с любого клиентского устройства не должно возникать проблем с сертификатами.

f. Сервис должен быть доступен по имени www.au.team.

11. Настройка личного кабинета и портала SSL VPN

a. На FW-HQ опубликуйте личный кабинет пользователя.

i. Доступ к веб-порталу из любых сетей должен осуществляться по протоколу HTTPS.

ii. При обращении по протоколу HTTP должно автоматически выполняться перенаправление на HTTPS.

iii. Доступ должен осуществляться как по имени lk.au.team, так и по публичному IP-адресу FW-HQ.

b. На FW-HQ настройте ресурсы SSL VPN для доступа к ним из личного кабинета пользователя.

i. При входе в личный кабинет из любой сети офисов HQ и BR от имени доменного пользователя должны быть доступны ресурсы ncloud.au.team и www.au.team.

ii. При входе в личный кабинет из сети OUT-CLI от имени доменного пользователя должен быть доступен только ресурс www.au.team.

12. Настройка удалённого доступа

a. На FW-HQ настройте возможность VPN-подключения с использованием Ideco Client

i. Доступ по данному типу VPN должен предоставляться только доменным пользователям

b. На OUT-CLI установите Ideco Client

i. Создайте профиль для подключения к HQ-FW

ii. Используйте для подключения учётные данные пользователя br.user4

Модуль Д. Миграция (вариатив)

Время на выполнение модуля: 6 часов

Задания:

Таблица адресации:

ВМ	IP address
ISP	192.168.1.1/24
WIN-DC	192.168.1.2/24
WIN-CLI1	DHCP
WIN-CLI2	DHCP
LIN-DC1	192.168.1.3/24
LIN-DC2	192.168.1.2/24
ADM	192.168.1.99/24
LIN-CLI1	DHCP
LIN-SRV1	192.168.1.4/24
LIN-SRV2	192.168.1.5/24

Текущие роли хостов, в существующей инфраструктуре:

Хост WIN-DC:

Развернут первоначальный контроллер домена semifinal.irpo. Установлены и настроены такие роли как: ADDS, DNS, DHCP, хранилище базы данных LDAP. Созданы доменные пользователи, группы и подразделения, учетные записи компьютеров, реализованы GPO на основе административных шаблонов. Реализовано файловое хранилище для профилей пользователей домена

Хост WIN-CLI1:

Введен в домен, вход доменным пользователем, применены GPO.

Хост WIN-CLI2:

Выполнена первоначальная настройка сетевых параметров. В домен не введен, участник к данной машине доступа не имеет. Будет введен в домен во время проверки стенда группой экспертов.

Хосты LIN-DC1 и LIN-DC2:

Предназначены для контроллеров домена на основе Samba-DC

Хост ADM:

Машина администратора. В домены не вводится!

Хост Lin-Cli1:

Должен быть введен в домен Samba.

Хосты LIN-SRV1 и LIN-SRV2:

Для инфраструктурных и дополнительных служб.

Ваша цель – перевести инфраструктуру на Альт Домен, дополнительно настроив необходимые сервисы и службы.

Существует ряд требований и ограничений:

- Параметры и свойства объектов домена должны быть сохранены.
- Идентификаторы клиентов (SUID), элементов инфраструктуры (GUID) не должны измениться, необходимо выполнить полную миграцию существующего домена на Альт.
- Клиентские машины на Windows должны продолжить работать в домене. Устанавливать какое-либо стороннее ПО на них нельзя. Можно пользоваться только штатным ПО Microsoft.
- Все существующие групповые политики (GPO) должны быть перенесены на Альт, их уникальные коды (GUID) должны остаться прежними.
- Хост WIN-DC по факту перевода инфраструктуры должен быть выключен, информация о контроллере домена WIN-DC должна быть удалена из домена.

Для достижения цели вам необходимо решить ряд задач:

Сервер времени

- Настройте NTP-сервера chrony - на хосте LIN-DC1. Все остальные работающие хосты должны быть его клиентами.

Контроллеры домена

- Установите контроллеры домена на основе Samba-DC на хосты LIN-DC1 и LIN-DC2. Введите их в домен semifinal.irpo.
- На хосте LIN-DC1 настройте:
  - PDC Samba-DC. LDAP и SYSVOL, роль DNS. Синхронизируете с LIN-DC2. Передайте все роли FSMO данному контроллеру.
- На хосте LIN-DC2 настройте: дополнительный DC.
  - Синхронизируете с LIN-DC1 по базам данных LDAP и DNS.
  - Установите сервис DHCP и настройте его для обновления DNS-записей.
  - На обоих контроллерах должен быть реализован уровень домена (функциональный уровень) AD не ниже чем Windows Server 2016.
  - На обоих контроллерах должна быть настроена двунаправленная репликации SYSVOL по выбранному вами методу.

Настройка DNS

- Для решения задач необходимо создать необходимые DNS записи включенных хостов и используемых служб. Это надо сделать как для зоны прямого, так и обратного просмотра.

Объекты домена

- Создать пользователей LinUser1 и LinUser2 с паролем P@ssw0rd.
- Создать доменную группу LinUsers, поместить в нее созданных пользователей.
- Создать подразделение LinOU, поместить в него пользователей, УЗ компьютера LIN-CLI1.

Групповые политики

- Поскольку корпоративными требованиями разрешена только темная тема стиля оформления на клиентских хостах, вам необходимо создать групповую политику, которая установит темную тему оформления по умолчанию, и запретит пользователю менять стиль оформления. Политику назовите IrpoStyle.

Инфраструктурные службы

- На хосте LIN-SRV1 настройте:
  - Общий анонимный файловый ресурс Share, доступный всем пользователям без аутентификации.
  - Хранилище профилей доменных пользователей Windows (рекомендуем в каталоге /opt). Каждый доменный пользователь, к которому применен перемещаемый профиль, должен видеть только свой ресурс.
  - Общий ресурс с именем UserDocs, (рекомендуем в каталоге /opt) для доменных пользователей.
  - Пользователи Linux должны хранить важные корпоративные документы в каталоге ~/DomainDocs своей учетной записи. Обеспечьте автоматическое монтирование файлового ресурса UserDocs для доменного пользователя на хостах с ОС «Альт» без повторного ввода пароля (SSO, Single Sign-On) к данному каталогу. Используйте механизм pam_mount.

Веб службы

- Установите веб-сервере Apache2 на хост LIN-SRV1, создайте сайт web.semifinal.irpo. Используйте html документ login.html, размещенный в каталоге /template.

- Вам необходимо обеспечить прозрачную авторизацию пользователей домена на этом веб-сайте. Напоминаем вам, для решения этой задачи необходимо настроить как веб-сервер, так и браузер на клиентских хостах.
- Для настройки браузера Chromium в Альт предусмотрен пакет групповых политик admx-chromium. Используйте соответствующие шаблоны для создания политики GPO. Политику назовите ChromiumSSO. Важно! Пользователь не должен вводить никакие аутентификационные данные для подключения просмотра страницы.

Мониторинг

- На хосте LIN-SRV2 сконфигурируйте сервер мониторинга на основе свободного ПО (Prometheus+Grafana). Клиентами мониторинга являются LIN-DC1, LIN-DC2 и LIN-SRV1.
- На дашборде Grafana по адресу http://mon.semifinal.irpo должны отображаться как минимум:
  - загрузка ЦП
  - свободная оперативная память
  - свободное место на диске.

Резервное копирование

- Необходимо настроить резервное копирование каталога, где хранятся профили пользователей Windows и общий ресурс UserDocs на машину ADM.
- Используйте программный комплекс Кибер Бекап, доступный вам в формате iso. Сервер управления установите на LIN-SRV1. Агент с функциями узла хранилища установите на ADM и подключите его к серверу управления. На узле хранилища ADM создайте директорию /backup и выберите её в качестве хранилища с именем BackUpFolder. Создайте план резервного копирования для решения задачи, назовите его DomDataBackUp.

Интерфейс сервера должен быть доступен по адресу http://backup.semifinal.irpo.

- Сохранять нужно только документы и профили доменных пользователей.

Администрирование

- На хост WIN-CLI1 необходимо установить набор инструментов RSAT, для управления доменом.
- На хост ADM необходимо установить компонент удаленного управления базой данных конфигурации ADMC и модуль редактирования настроек клиентской конфигурации (GPUI), а также все необходимые наборы шаблонов групповых политик.
    - Напоминаем вам, что вводить хост ADM в домен нельзя!

  Управление доменом должно быть доступно из обоих хостов с помощью перечисленных инструментов одновременно.

Чек-лист функциональной проверки со стороны заказчика:

- ✓ Синхронизация времени всех хостов с NTP-сервером.
- ✓ Разрешение имён хостов в прямой и обратной зонах DNS.
- ✓ Выдача DHCP-клиентам настроек и регистрация их в DNS.
- ✓ Отсутствие в домене контроллера Windows (WIN-DC выключен, записи удалены).
- ✓ Владение всеми ролями FSMO контроллером LIN-DC1.
- ✓ Уровень функциональности домена не ниже Windows Server 2016.
- ✓ Двунаправленная репликация SYSVOL между LIN-DC1 и LIN-DC2.
- ✓ Вход в домен пользователей, существовавших до миграции (сохранение учётных записей).
- ✓ Сохранение GUID групповых политик, перенесённых из домена WIN-DC.

✓ Применение перенесённых групповых политик на клиентах Windows.

✓ Наличие в домене пользователей LinUser1, LinUser2 и группы LinUsers.

✓ Наличие подразделения LinOU с размещёнными в нём пользователями и компьютером LIN-CLI1.

✓ Применение групповой политики IrpoStyle (тёмная тема, запрет смены) на клиенте Windows.

✓ Действие политики ChromiumSSO (прозрачная авторизация на web.semifinal.irpo).

✓ Доступность анонимного файлового ресурса Share на LIN-SRV1.

✓ Работа перемещаемых профилей пользователей Windows (сохранение данных между сеансами).

✓ Разграничение доступа к общему ресурсу UserDocs (каждый пользователь видит только свой каталог).

✓ Автоматическое монтирование каталога DomainDocs для пользователей Linux.

✓ Доступность дашборда мониторинга с метриками CPU, RAM, диска для LIN-DC1, LIN-DC2, LIN-SRV1.

✓ Наличие плана резервного копирования DomDataBackUp в сервере управления Кибер Бэкап.

✓ Наличие успешных резервных копий данных профилей и UserDocs на хосте ADM.

✓ Возможность управления доменом с WIN-CLI1 с помощью RSAT (создание/изменение объектов).

✓ Возможность управления доменом с ADM (вне домена) с помощью GPUI и ADMC.

✓ Ввод клиента WIN-CLI2 в домен и применение к нему групповых политик.

✓ Наличие DNS-записей (A и PTR) для всех включённых хостов.

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

– 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.*