****

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

*Время на выполнение модуля 3 часа.*

Задания:

**1. Произведите базовую настройку устройств**

• Настройте имена устройств согласно топологии. Используйте полное доменное имя.

• На L2 и L3 устройствах необходимо создать пользователя sshuser с паролем P@$$w0rd.

• На маршрутизаторах данный пользователь должен иметь максимальные привилегии и с устройства ISP должен быть реализован вход без пароля от пользователя root.

• На коммутаторах данный пользователь должен иметь возможность запуска sudo без дополнительной аутентификации.

**2. Настройка ISP**

• Настройте адресацию на интерфейсах:

• Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP

• Интерфейс, к которому подключен HQ-RTR, имеет адрес 4.4.4.1/28

• Интерфейс, к которому подключен BR-RTR, имеет адрес 5.5.5.1/26

• Настройте динамическую трансляцию адресов для всех сетей.

**3. Для офиса HQ используется сеть 192.168.100.0/23, для офиса BR - 192.168.200.0/25.**

• Сеть в офисе HQ и BR необходимо разделить на подсети для каждой VLAN.

**4. Настройка коммутации.**

• Настройка коммутаторов осуществляется при помощи Open vSwitch.

• Имена коммутаторов должны совпадать с коротким именем устройства

• Сервера в офисах HQ и BR должны находиться во VLAN10, клиенты - VLAN20, также создайте подсеть управления VLAN99.

• Для серверов офиса HQ выделяется подсеть на не менее 25 устройств, для клиентов офиса HQ - не менее 230 устройств, подсеть управления не более 10 устройств.

• Для серверов офиса BR выделяется подсеть на не менее 10 устройств, для клиентов офиса BR - не менее 60 устройств, подсеть управления не более 10 устройств.

• Шлюзом по умолчания для устройств необходимо указывать первый доступный адрес подсети.

**5. На коммутаторе BR-SW необходимо настроить уровень сервиса для клиента и сервера. Для сервера ограничьте скорость до 10 Mbps, а для клиентов 1 Mbps.**

**6. Между офисами HQ и BR необходимо сконфигурировать туннель:**

 Настройте GRE;

 Задание значения максимального размера пакета, для интерфейса 1400;

 Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса.

**7. Настройка динамической трансляции адресов**

• Настройте динамическую трансляцию адресов для обоих офисов.

• Заблокируйте доступ к Интернету для коммутаторов.

• Остальные устройства должны иметь доступ к Интернету.

**8. Настройка межсетевого экрана.**

• Реализуйте функционал межсетевого экрана на HQ-RTR и BR-RTR.

• Запретите ICMP трафик на пограничные маршрутизаторы из внешних сетей. Трафик из внутренних сетей обоих офисов должен быть разрешен.

• Обеспечьте доступ по SSH к серверу BR-SRV из внешних сетей. В качестве внешнего порта используйте 65000 на маршрутизаторе BR-RTR.

• Заблокируйте доступ к youtube и bittorrent на двух маршрутизаторах.

**9. Настройка протокола динамической конфигурации хостов.**

• Для офиса HQ в качестве сервера DHCP выступает машина HQ-SRV1, офиса BR - BR-SRV.

• Клиентами являются машины HQ-CLI, BR-CLI.

• Адрес шлюза по умолчанию - адреса маршрутизаторов HQ-RTR и BR-RTR

• Адрес DNS-сервера для машины HQ-CLI - адрес сервера HQ-SRV2, для машины BR-CLI - адрес сервера BR-SRV.

• DNS-суффикс для офисов HQ и BR - au.team

**10. Настройка DNS для офисов HQ и BR.**

• Основной DNS-сервер реализован на HQ-SRV2.

• BR-SRV является подчиненным DNS сервером.

• Для всех устройств используется доменное имя au.team.

• Для всех устройств двух офисов необходимо создать записи A и PTR.

• В качестве DNS сервера пересылки используйте сервера 94.232.137.104

|  |  |
| --- | --- |
| **Машина** | **Запись А** |
| ISP | isp.au.team |
| HQ-RTR | hq-rtr.au.team |
| BR-RTR | br-rtr.au.team |
| HQ-SW | hq-sw.au.team |
| BR-SW | br-sw.au.team |
| HQ-SRV1 | hq-srv1.au.team |
| HQ-SRV2 | hq-srv2.au.team |
| BR-SRV | br-srv.au.team |
| HQ-CLI | hq-cli.au.team |
| BR-CLI | br-cli.au.team |

**Модуль Г. *Автоматизация*. (Вариатив)**

*Время на выполнение модуля 3 часа*.

**Задания:**

**1. Настройте доменный контроллер Samba на машине HQ-SRV2.**

* Создайте 15 пользователей для офиса HQ, имена пользователей формата user№.hq.
* Создайте 10 пользователей для офиса BR, имена пользователей формата user№.br.
* Пользователи группы hq имеют право аутентифицироваться на любом клиентском ПК.
* На BR-CLI могут аутентифицироваться только пользователи группы br и локальные пользователи.
* Пользователи группы br должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id.
* Для всех пользователей домена должны быть реализованы общие каталоги по пути /mnt/Adsamba

**2. Настройка безопасного удаленного доступа SRV-HQ, SRV-BR.**

* Для подключения используйте порт 2024;
* Запретите любое подключение к пользователю root;
* Ограничьте количество попыток входа до двух;
* Настройте произвольный баннер при входе.

**3. Реализуйте механизм инвентаризации ПК через Ansible на BR-SRV:**

* Плейбук должен собирать информацию о рабочих местах:
	+ Имя компьютера
	+ Версию ПО - Vim, Chromium. Если ПО отсуствует, плейбук в отчете уведомит об этом фразой - “Программа не установлена”
	+ IP-адрес на компьютере
* Отчеты, собранные с машин должны быть размещены в том же каталоге на сервере, где и плейбук в папке PC\_INFO, в формате .yml. Файл называется именем компьютера, который был инвентаризован
* Рабочий каталог Ansible (плейбуки, роли, inventory и т.д.) должны располагаться в /etc/ansible
* Плейбук должен собирать информацию о сетевых устройствах:
	+ Создавать резервную копию конфигураций.
	+ Информацию сохранять в папку NETWORK\_INFO

**4. Разверните Zabbix (Server+Web) на хосте BR-SRV**

* Для хранения информации используйте базу данных PostgreSQL на хостe HQ-SRV1
* Обеспечьте мониторинг доступности всех Linux-узлов сети
* Доступ к Web-интерфейсу должен производиться по TLS соединению

**5. Выполните настройку центра сертификации на базе HQ-SRV1:**

* Необходимо использовать отечественные алгоритмы шифрования;
* Сертификаты выдаются на 365 дней;
* Выдайте сертификаты для всех веб-серверов;

**6. Запустите сервис MediaWiki на сервере HQ-SRV1.**

* Используйте веб-сервер Apache. В качестве системы управления базами данных используйте MySQL.
* Создайте базу данных ‘mediawiki’ для использования с MediaWiki.
* Создайте пользователя ‘wiki’ с паролем ‘WikiP@ssw0rd’ и предоставьте ему права доступа к этой базе данных.
* Установите последнюю версию MediaWiki/
* MediaWiki должна быть доступна на порту 8080.
* Сервер должен быть доступен по HTTPS. Используйте самоподписанные сертификаты.

**7. Настройка проксирования**

* Проксирование необходимо настроить на маршрутизаторах HQ-RTR и BR-RTR
* При попытке перехода на https://www.wikipedia.org/ происходит перенаправление на https://mediawiki.au.team:8080

**8. Реализуйте мониторинг по средствам rsyslog.**

* Сервер сбора логов расположен на HQ-SRV1
* Собирать логи необходимо со всех устройств двух офисов
* Приоритет сообщений должен быть не ниже warning.
* Все журналы должны находиться в директории /opt. Для каждого хоста должна выделяться своя директория, которая совпадает с именем машины, например, для сервера HQ-SRV2 должна создаваться директория hq-srv2.au.team.
* Реализуйте ротацию логов:
	+ Ротация производится один раз в неделю
	+ Логи необходимо сжимать
	+ Минимальный размер логов для ротации – 100 МБ

**

**Модуль Д. (*DevOps*)** **(вариатив)**

*Время на выполнение модуля 3 часа*.

*DC-RTR, DC-SRV1, DC-SRV2 и DC-SRV3 уже предустановлены имеют статический адрес и доменные имена.*

*Установлен компьютер администратора с графическим интерфейсом PC-ADMIN.*

**Задания:**

1. **Реализуйте систему HA proxmox на серверах  DC-SRV1, DC-SRV2 и DC-SRV3**
* Обеспечьте перенос LXC контейнеров и ВМ при отказе одного из серверов
* Реализуйте общее хранилище на базе CIFS из дополнительных дисков которые подключены к хостам (60 гб) для реализации HA

**2. Развертывание приложений в Docker**

* Создайте ВМ Docker с OC Альт Сервер 10.1
	+ CPU 2
	+ OZU 4 гб
	+ Storage 30 гб
* Установите Docker и Docker Compose.
* Создайте локальный Docker Registry.
	+ В домашней директории хоста создайте файл name.txt и запишите в него строку experts.
	+ Напишите Dockerfile для приложения Hello.
		- В качестве базового образа используйте alpine
		- Сделайте рабочей директорию /hello и скопируйте в неё name.txt
		- Контейнер при запуске должен выполнять команду echo, которая выводит сообщение "Hello! Greetings from" и затем содержимое файла name.txt, после чего завершать свою работу.
	+ Соберите образ приложения App и загрузите его в ваш Registry.
		- Используйте номер версии 1.0 для вашего приложения
		- Образ должен быть доступен для скачивания и дальнейшего запуска на локальной машине.
* Настройте мониторинг с помощью NodeExporter, Prometheus и Grafana в Docker.
	+ Создайте в домашней директории пользователя файл monitoring.yml для Docker Compose:
	+ Используйте контейнеры NodeExporter, Prometheus и Grafana для сбора, обработки и отображения метрик.
	+ Настройте Dashboard для центра обработки данных DC в Grafana, в котором будет отображаться загрузка CPU, объём свободной оперативной памяти и места на диске. Для всех серверов.
	+ Интерфейс Grafana должен быть доступен по внешнему адресу на порту 3000 с PC-ADMIN.

**3. Конфигурация внутренней системы обучения**

* Создайте ВМ MOODLE с OC Альт Сервер 10.1
	+ CPU 2
	+ OZU 2 гб
	+ Storage 30 гб
* На PC-ADMIN создайте локального пользователя programmer с паролем P@$$w0rd.
* Обеспечьте данного пользователя ключом ssh чтобы он входил без пароля на данную ВМ.
* Сконфигурируйте веб-сервер LMS Apache на сервере ВМ MOODLE:
	+ На главной странице должен отражаться номер места
	+ Используйте базу данных SQL
	+ Создайте пользователей в соответствии с таблицей, пароли у всех пользователей «P@ssw0rd»
* Добавьте данной ВМ доменное имя (moodle) чтобы пользователи с клиентских устройств (PC-ADMIN) имели доступ по доменному имени и защищенному доверенным сертификатом.



**4. Реализация системы обработки заявок**

* Реализайте развёртывание LXC контейнеров OTRS (Znuny). Подключите к клиентам OTRS пользователей SAMBA AD.
* Создайте пользователей support который имеет возможность отвечать на заявки.
* Добавьте данному контейнеру доменное имя (otrs) чтобы пользователи с клиентских устройств (PC-ADMIN) имели доступ по доменному имени и защищенному доверенным сертификатом.