Базовая настройка

1) Настройте имена хостов в соответствии с **диаграммой**
   Назначьте для всех хостов доменное имя **sirius2022.lin**
2) **Если необходимо**, сформируйте файл /etc/hosts. Он будет использоваться при проверке, в случае некорректной работы сервиса DNS. Конфигурация данного пункта остается на усмотрение участника и оцениваться **НЕ БУДЕТ.**
3) В случае корректной работы сервисов DNS, ответы от DNS сервера должны иметь более высокий приоритет.

Конфигурация сетевой инфраструктуры

1) На HQ-LinSRV1 настройте службу разрешения доменных имен для внутренней сети
   a) Сервер должен обслуживать зону **sirius2022.lin**
   b) Создайте записи типа A для всех хостов офисов Branch и HQ
   c) Реализуйте поддержку обратного разрешения имен. Добавьте необходимые записи для всех хостов офисов Branch и HQ
   d) Создайте необходимые записи для WEB сервисов
   e) Для прямой зоны разрешите динамическое обновление записей. Обновление должно быть разрешено только с хоста HQ-LinRTR
   f) Создайте запись test. Реализуйте следующие правила разрешения записи:
      i) Если клиент пытается разрешить запись из внутренней сети офисов HQ и Branch, то запись должна разрешаться в адрес 1.1.1.1
      ii) Если клиент пытается разрешить запись из VPN подсети, то запись должна разрешатся в 2.2.2.2
   g) При обращении к зоне sirius2022.ru запрос должен пересылатся на сервер ISP. При обращении к любой другой неизвестной зоне запрос должен пересылаться на адрес 10.113.38.100. Для проверки пересылки на sirius2022.ru используйте test.sirius2022.ru

2) Сконфигурируйте сервис для автоматической выдачи адресов клиентским машинам на HQ-LinRTR
    a) В качестве диапазона используйте 192.168.0.100-200/24
    b) Сконфигурируйте выдачу корректного адреса DNS сервера и доменного имени.
    c) Сконфигурируйте отправку обновлений для зоны sirius2022.lin
    d) Сконфигурируйте опцию для выдачи адреса TFTP сервера. В качестве адреса TFTP сервера используйте адрес HQ-LinSRV1

Конфигурация служб мониторинга, резервного копирования, журналирования

1. На маршрутизаторе HQ-LinRTR настройте возможность удаленного мониторинга по протоколу SNMP v3.
    a. Задайте местоположение устройств “Moscow, Russia ”
    b. Задайте контакт admin@sirius2022.lin
    c. Используйте имя группы “WSRSKILLZ”.
    d. Создайте профиль только для чтения с именем “WSR”.
    e. Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
    f. Используйте имя пользователя: **snmpuser** и пароль: **snmppass**
    g. Задайте команду для проверки snmp_test на HQ-LinCLI:
        i. Команда должна выполняться из любой директории.
        ii. Скрипт должен быть размещен в /opt/script/.
        iii. Скрипт должен принимать имя устройства, имя пользователя, пароль и тип шифрования в качестве параметров. Если параметры не указаны, то параметры должны запрашиваться интерактивно
        iv. При вызове команды с параметрами -h или --help должна выводиться справка о команде.

2. Разверните Zabbix (Server+Web) на хосте HQ-LinSRV2

a. Для хранения информации используйте базу данных PostgreSQL на хосте HQ-LinSRV1
b. Обеспечьте мониторинг доступности всех узлов сети
c. Доступ к Web-интерфейсу должен производиться по защищённому соединению
    i. Сервис должен быть доступен по имени **zbx.sirius2022.lin**
d. Обеспечьте возможность доступа с использованием учётных записей службы LDAP
    i. Только членам группы **Sysadmins** разрешён доступ к Web-интерфейсу
    ii. Группа sysadmins должна быть членом группы администраторов Zabbix
    i. Обеспечьте мониторинг всех Linux-серверов стандартными шаблонами с использованием Zabbix-agent
    ii. Обмен данными должен производиться по защищённому соединению с использованием sha256-хэша строки **W3RSK1LZ2021**

3. Разверните Grafana на хосте HQ-LinSRV2
    a. Обеспечьте получение данных из Zabbix посредством API
    b. Создайте дашборд для мониторинга следующих показателей Linux-хостов:
        i. Загрузка ЦП по ядрам
        ii. Общая и занятая ОЗУ
        iii. Общее и занятое дисковое пространство
        iiii. Должна быть возможность выбрать необходимый хост из выпадающего списка
    c. Доступ к Web-интерфейсу должен производиться по защищённому соединению
        i. Сервис должен быть доступен по имени **grafana.sirius2022.lin**
    ci. Обеспечьте возможность доступа с использованием учётных записей службы LDAP

ii. Группа Sysadmins должна иметь права администраторов Grafana

4. Обеспечьте централизованный сбор журналов со всех клиентских хостов и серверов в базу данных на HQ-LinSRV1
5. На BR-LinSRV разверните приложение LogAnalyzer
    a. В качестве источника данных используйте базу данных на HQ-LinSRV1
    b. Доступ должен осуществляться по имени logs.sirius2022.lin, по протоколу https.
    c. Реализуйте перенаправление http->https

Конфигурация систем централизованного управления пользователями и компьютерами

1) Реализуйте LDAP-сервер на хосте HQ-LinSRV1 для хранения учётных записей пользователей и групп
    a) Имя домена - **sirius2022.lin**
    b) Создайте учётные записи и группы в соответствии с **таблицей 1**
        i) Учётные записи должны входить в OU users, группы - OU groups
        ii) Задайте пароль **P@ssw0rd** для всех УЗ
    c) Все виртуальные Linux-хосты должны поддерживать авторизацию через данный сервер
        i) Только группам **Sysadmins** и **Uzvers** разрешено авторизовываться на хостах

2) Укажите, с помощью чего реализован LDAP сервер. Оценка за выполнение будет одинакова, вне зависимости от выбранного решения.
    a) FreeIPA
    b) OpenLDAP
    c) SambaAD
    d) 389 Directory Server

Конфигурация служб удаленного доступа

1) На BR-LinRTR настройте сервер удаленного доступа на основе технологии OpenConnect
    a) Сервер должен работать на порту 4443 для tcp и udp
    b) В качестве сертификатов используйте сертификаты, выданные HQ-LinSRV1
    c) Разрешите исследование mtu
    d) Если клиент не активен в течении 30 минут, подключение должно быть разорвано
    e) В качестве адресного пространства для клиентов используйте 10.8.8.0/24
    f) Настройте использование DNS серверов предприятия и выдачу корректного доменного имени
    g) Все DNS запросы должны проходить через VPN туннель
    h) Сконфигурируйте пользователя vpnuser с паролем vpnpass. В качестве места хранения пользователя используйте локальную базу данных
    i) Обеспечьте доступ к сетям и сервисам обоих офисов

2) На Remote-LinCLI настройте клиент удаленного доступа на основе технологии OpenConnect
    a) Реализуйте автоматическое подключение к VPN сервису предприятия
        i) Создайте юнит connect.service
        ii) В качестве описания юнита задайте “VPN Connector to branch office”
        iii) Добавлять юнит в автозагрузку не нужно.

3) Между HQ-LinRTR и BR-LinRTR должен функционировать GRE over IPSEC
    a) В качестве адресного пространства используйте подсеть 10.5.5.0/30
    b) Для защиты используйте IKEv1 IPSEC с аутентификацией по общему ключу.
    c) Параметры IPSEC произвольные

4) Между HQ-LinRTR и BR-LinRTR настройте динамическую маршрутизацию по протоколу OSPF.
    a) Обьявите сети, необходимые для полной связанности
    b) Используйте GRE туннель для формирования соседства

Конфигурация служб хранения данных

1) Преобразуйте в физические тома LVM все свободные носители на BR-LinSRV.
    a) Создайте группу логических томов WSR_LVM
    b) Создайте следующие логические тома.
        i. Users, 200 Мб.
        ii. Shares, 40% от оставшегося свободного места.
    c) Обеспечьте создание снапшотов тома Shares раз в час.
        i. Снапшоты создаются в формате SNAP-XX, где XX - номер снапшота, (01, 02 и т.д.)
        ii. Снапшоту выделяется 5% от общего объема группы томов.
        iii. Снапшоты должны создаваться при помощи скрипта /root/create_snap.sh
    d) Создайте снапшот чистого тома Users с названием CLEAR
        i. Снимок должен позволять хранение 30% изменений указанного логического тома.
    e) Обеспечьте монтирование тома Users в каталог /opt/Users
    f) Обеспечьте монтирование тома Shares в каталог /opt/Shares
    g) Монтирование должно происходить во время загрузки системы.

1) Реализуйте файловый сервер на BR-LinSRV
    a) Создайте 2 общие папки shares и users
    b) В папке shares создайте каталог workfolders. Внутри каталога workfolders создайте папки Work1 и Work2
        i. Обеспечьте возможность монтирования каталога workfolders по протоколу nfs на BR-LinCLI и HQ-LinCLI
        ii. Создайте специального пользователя automount с паролем P@ssw0rd
        iii. Обеспечьте автоматическое монтирование разделяемого ресурса на машины HQ-LinCLI и BR-LinCLI при входе пользователя в систему.
    c) Обеспечьте автоматическое подключение катлога /opt/Users на машины HQ-LinCLI и BR-LinCLI по протоколу NFS в директорию /home

Конфигурация web и почтовых служб

1) На HQ-LinSRV1 разверните веб сайт
    a) Используйте порт 8088

b) Используйте директорию /opt/web/ в качестве корневой директории сайта
c) В качетсве содержимого сконфигурируйте файл index.html со следующим содержимым: “Welcom to SIRIUS. Server HQ-LinSRV1”

2) На HQ-LinSRV2 разверните веб сайт
   a) Используйте порт 8088
   b) Используйте директорию /opt/web/ в качестве корневой директории сайта
   c) В качетсве содержимого сконфигурируйте файл index.html со следующим содержимым: “Welcom to SIRIUS. Server HQ-LinSRV2”

3) На сервере HQ-LinSRV3 настройте haproxy
   a) В качестве бэкэндов используйте HQ-LinSRV1 и HQ-LinSRV2
   b) Обеспечьте балансировку нагрузки между бэкэндами, с использованием алгоритма Round Robin
   c) Доступ должен производится по имени www.sirius2022.lin
   d) Сконфигурируйте https и автоматическое перенаправление на https.

Конфигурация параметров безопасности и служб аутентификации

1) Реализуйте корневой центр сертификации на сервере HQ-LinSRV1
   a) Корневой директорией для УЦ должна служить /etc/ca
   b) Используйте следующие атрибуты:
      i) CN - WSRSKILLZ CA
      ii) Country - RU
      iii) Organization - WSR ITNSA 39
   c) Все сертификаты, использованные при выполнении задания, должны быть выпущены данным УЦ
   d) Все системы должны доверять данному УЦ

e) Сконфигурируйте автоматическое добавление сертификатов из системного хранилища в браузер firefox для всех пользователей.

2) На BR-LinSRV настройте удаленный доступ по протоколу SSH:
   a) Доступ ограничен пользователями **ssh_p, root** и **ssh_c**
      i) В качестве пароля пользователь (кроме root) использовать **ssh_pass.**
      ii) root использует стандартный пароль
   b) SSH-сервер должен работать на порту **22**

3) На Remote-LinCLI настройте клиент удаленного доступа SSH:
   a) Доступ к BR-LinSRV из под локальной учетной записи root под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.
   b) Произведите необходимые настройки на BR-LinRTR для получения доступа по SSH на BR-LinSRV1. При подключении на внешний адрес BR-LinRTR, на порт 2222 должно производится перенаправление соеденения на BR-LinSRV1, порт 22.
   c) Отключите необходимость строгой проверки ключа при подключении к BR-LinSRV

Конфигурация СУБД

1) Реализуйте сервер СУБД на базе PostgreSQL на хосте HQ-LinSRV1
   a) Разрешите локальные и удалённые подключения с хоста HQ-LinSRV2
      i) Подключения, не требуемые для выполнения задания, должны быть явно запрещены средствами PostgreSQL
   b) Подготовьте сервер для запуска потоковой репликации в режиме Hot-Standby
      i) Обеспечьте репликацию на сервер HQ-LinSRV3

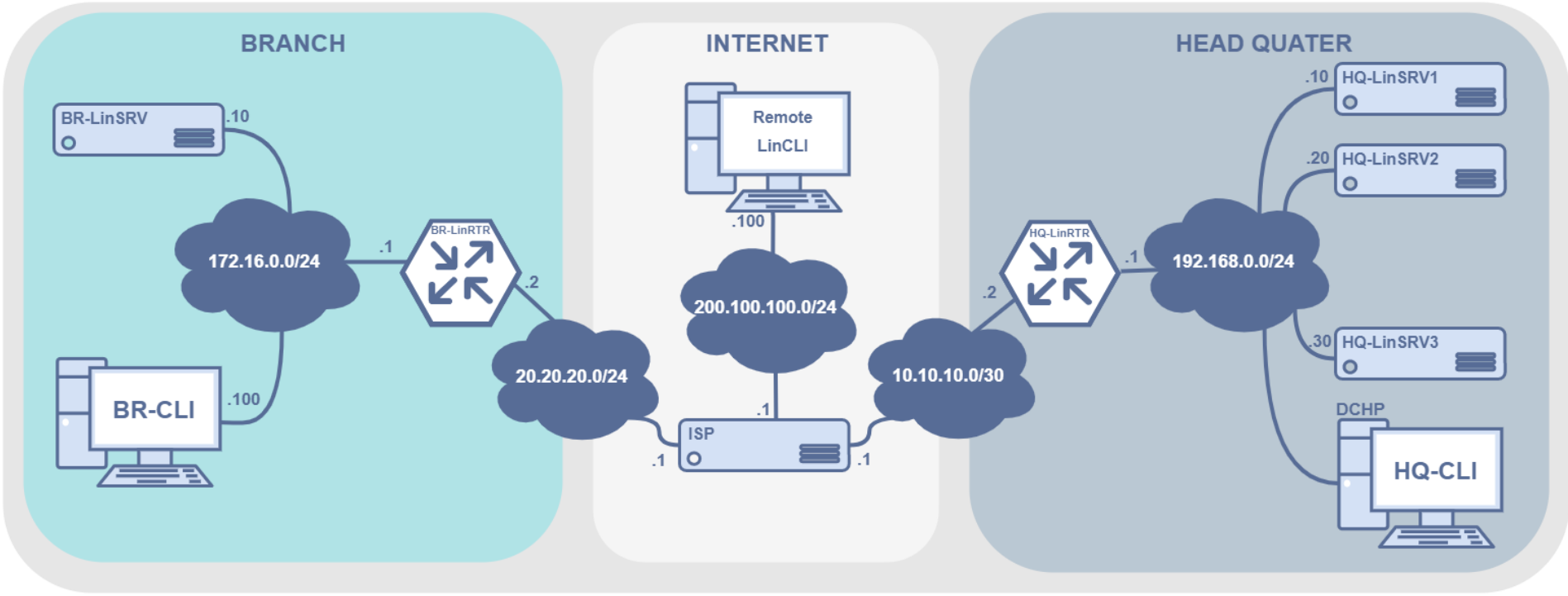
Таблица №1 – Группы и пользователи LDAP

Группы	Пользователи
Sysadmins	HyperAdmin
Uzvers	NotSoSmallUser
Experts	Stallman
Allies	IvanPetrov

Таблица №2 – DNS-имена

Хост	DNS-имя
BR-LinSRV	A,PTR: br-linsrv.sirius2022.lin CNAME: logs.sirius2022.lin
BR-CLI	A,PTR: br-cli.sirius2022.lin
HQ-LinSRV1	A,PTR: hq-linsrv1.sirius2022.lin
HQ-LinSRV2	A,PTR: hq-linsrv2.sirius2022.lin CNAME: zbx.sirius2022.lin CNAME: grafana.sirius2022.lin
HQ-LinSRV3	A,PTR: hq-linsrv3.sirius2022.lin CNAME: www.sirius2022.lin
HQ-CLI	A,PTR: hq-cli.sirius2022.lin

Топология L3



Топология VPN